

Current notions of  
defence, foreign  
affairs, intelligence  
and development  
are **redundant** in  
the new security  
environment . . .



**National Security  
for the Twenty-first  
Century**

Charlie Edwards

## **About Demos**

### *Who we are*

Demos is the think tank for everyday democracy. We believe everyone should be able to make personal choices in their daily lives that contribute to the common good. Our aim is to put this democratic idea into practice through our research and dissemination.

### *What we work on*

We focus on six areas: public services; science and technology; cities and public space; identity; arts and culture; and global security. Many of our projects link more than one area, and we consistently seek to explore and strengthen our understanding of those connections.

### *Who we work with*

Our partners include policy-makers, companies, public service providers and social entrepreneurs. Demos is independent of any party – we work with politicians across political divides. Our international network, spanning six continents, provides a global perspective and enables us to work across borders.

### *How we work*

Demos knows the importance of learning from experience. We work collaboratively with communities and individuals, and we test and improve our ideas in practice by working with people who can make change happen.

### *How we communicate*

As an independent voice, we can create debates that lead to real change. We use the media, public events, workshops and publications to communicate our ideas. All our books can be downloaded free from the Demos website.

**[www.demos.co.uk](http://www.demos.co.uk)**

First published in 2007

© Demos

Some rights reserved – see copyright licence for details

ISBN 978 1 84180 190 2

Copy edited by Julie Pickard, London

Typeset by utimestwo, Collingtree, Northants

Printed by IPrint, Leicester

For further information and  
subscription details please contact:

Demos

Magdalen House

136 Tooley Street

London SE1 2TU

telephone: 0845 458 5949

email: [hello@demos.co.uk](mailto:hello@demos.co.uk)

web: [www.demos.co.uk](http://www.demos.co.uk)

# National Security for the Twenty-first Century

Charlie Edwards

DEMOS

# DEMOS

## **Open access. Some rights reserved.**

As the publisher of this work, Demos has an open access policy which enables anyone to access our content electronically without charge.

We want to encourage the circulation of our work as widely as possible without affecting the ownership of the copyright, which remains with the copyright holder.

Users are welcome to download, save, perform or distribute this work electronically or in any other format, including in foreign language translation, without written permission subject to the conditions set out in the Demos open access licence which you can read at the back of this publication.

Please read and consider the full licence. The following are some of the conditions imposed by the licence:

- Demos and the author(s) are credited
- The Demos website address ([www.demos.co.uk](http://www.demos.co.uk)) is published together with a copy of this policy statement in a prominent position
- The text is not altered and is used in full (the use of extracts under existing fair usage rights is not affected by this condition)
- The work is not resold
- A copy of the work or link to its use online is sent to the address below for our archive.

Copyright Department

Demos

Magdalen House

136 Tooley Street

London

SE1 2TU

United Kingdom

[copyright@demos.co.uk](mailto:copyright@demos.co.uk)

You are welcome to ask for permission to use this work for purposes other than those covered by the Demos open access licence.



Demos gratefully acknowledges the work of Lawrence Lessig and Creative Commons which inspired our approach to copyright. The Demos circulation licence is adapted from the 'attribution/no derivatives/non-commercial' version of the Creative Commons licence.

To find out more about Creative Commons licences go to [www.creativecommons.org](http://www.creativecommons.org)

# Contents

Acknowledgements	7
Methodology	9
Executive summary and recommendations	11
<b>Part 1. Britain and the world today</b>	
1. A new security paradigm	21
2. The public value of security	52
<b>Part 2. Adapting to the twenty-first century</b>	
3. Managing the system	63
4. From 'need to know' to 'need to share'	82
5. Great expectations	97
6. Carrots, sticks and sermons	109
Notes	111



# Acknowledgements

I am very grateful to the Cabinet Office, G4S Global Risks and Thales for supporting this work.

I have benefited enormously from the advice and guidance of many people in government, the private sector, non-governmental organisations and academia. In particular I would like to thank the steering group: Stuart Croft, Gareth Crossman, Richard Flynn, Stephen Hawker, Will Jessett, Bruce Mann, Iain Mathewson, Dennis Mills, Denis O'Connor, David Omand, John Tesh and Martyn Thomas.

I am grateful to all those people who spoke at the project's three seminars: Paul Cornish, Stevyn Gibson, Anton La Guardia, Nick Mabey, Jamie MacIntosh, Onora O'Neill, Alan Richards and Adam Strangfeld.

I would particularly like to thank a number of people who have made important contributions along the way: Geoffrey Edwards, Alex Evans, Derek Leatherdale, Elaine Ruffle, Dominic Wilson and Peter Wilson.

Finally, thank you to all my colleagues in Demos and the wider network who have been so supportive in the past 12 months: Tom Bentley, Peter Bradwell, Alessandra Buonfino, Jaime Dipple, Catherine Fieschi, Peter Harrington, William Higham, Duncan O'Leary and Julie Pickard, as well as the interns – especially Prachi

Bhatnagar, Ivonne Duarte, Tim Gore, Neil Padukone, Amin Samman  
and Sally Spurr.

All mistakes and omissions remain my own.

Charlie Edwards  
November 2007

# Methodology

This pamphlet is the result of a 12-month project supported by the Cabinet Office, G4S Global Risks and Thales.

The project draws on existing policy and academic work, quantitative and qualitative research and conversations with politicians, senior civil servants and representatives from the private sector, non-governmental organisations (NGOs), academia and the media.

During the course of the project 60 formal interviews were conducted including with politicians, senior civil servants, intelligence officials and police officers. These interviews were held off the record.

Research by Ipsos MORI was carried out in early 2007 on the public's perceptions of national security. This was further supported by data from government departments and independent organisations. In the final stages of the project focus groups were conducted by Spiral on behalf of Demos with the aim of interrogating the polling data and providing some contextual analysis.

During the project three seminars with experts were held at Demos. The first seminar focused on national security as a public service and asked whether the national security architecture could learn lessons from the transformation and reform of Britain's public services in the past decade. The second seminar focused on open government and the need to shift the culture from 'need to know' to one that focused on a 'need to share' where the responsibility is to

## **National Security for the Twenty-first Century**

---

provide information. The final seminar looked at current and future threats and hazards to the UK and asked if the national security architecture could adapt to the twenty-first century.

# Executive summary and recommendations

*There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things. Because the innovator has for enemies all those who have done well under the old conditions, and luke warm defenders in those who may do well under the new.*

Machiavelli, *The Prince*

The British government lacks a clear and coherent view of the nature and priority of risks<sup>1</sup> to the United Kingdom.

The national security architecture is flawed in its design. The government remains structured around functions and services with separate budgets for defence, foreign affairs, intelligence and development. Whitehall departments, intelligence agencies and the police forces that make up the security architecture have changed very little in the past two decades, despite the end of the Cold War and the attack on the World Trade Center in 2001.

This model of government may have suited the security environment of the Cold War when the UK faced a threat to its national survival but the complex and uncertain security environment demands a fundamental review of how government is organised. This is especially true if government is to respond to ‘wicked’ problems, issues that are unbounded in time, scope and

resources. The common, unifying, external threat of nuclear war has been replaced by a plethora of security challenges such as trafficking and organised crime, international terrorism, energy security, pandemics and illegal immigration. They are dangers that are present, but not clear.

The government remains faced with a set of problems it cannot solve on its own. In order to respond to the new security paradigm, the UK's security architecture must adapt, not just in terms of processes and structures but in the mindsets of ministers and civil servants. At the same time, it must develop close relationships with its 'strategic partners', the private sector and the wider public, which raises further challenges of transparency, information sharing and trust.

This pamphlet sets out a definition of and an approach to 'national security', a concept understood by some as an abstract notion relating to the 'condition of the state', and referred to in security and intelligence legislation. It argues that the concept of national security can serve a more vital role, as a principle for organising government. The pamphlet draws on reforms and innovations from governments elsewhere in Europe and the United States and suggests some radical and innovative ideas on which to shape the future of the national security architecture.

Its core argument is that while the UK government has been able to 'muddle through' by creating new units within departments, merge teams and allocate more resources for agencies to expand, the present and future security environment urgently demands a more integrated and strategic approach. Tinkering with the machinery will continue to pay short-term dividends but it will only ever achieve marginal improvements. Long-term success must be based on a more inclusive, open and holistic approach to national security.

### **Outline of the pamphlet**

Part 1 of the pamphlet describes the new security paradigm and the response by the UK government to the myriad of global challenges it has faced in the last two decades. Chapter 1 examines the new security

environment and explores the public's response to the security challenges facing the UK at the beginning of the twenty-first century. Chapter 2 assesses how well the UK government has responded to threats and hazards in recent years, outlining the significant successes and failures of its policies and decisions.

Part 2 of the pamphlet outlines how the government can transform itself in response to the challenges identified in the pamphlet. The changes revolve around three essential principles of adaptation in government:

- the need for a holistic approach to national security, based on systems thinking, which allows individuals, agencies and departments to take a much broader perspective than normal; this includes seeing overall structures, patterns and cycles in systems, rather than identifying only specific events or policy options
- the creation of an open and transparent national security architecture for ministers, civil servants and the government's strategic partners – the private sector and the wider public
- a transformation of the national security architecture based on the principles of public value, an intellectual framework for reform in government that, although still in its infancy, has huge potential for changing the way in which the government measures its performance and maintains the trust and confidence of society.

Chapter 3 examines the case for a holistic approach to managing national security. Initially this will require a robust and comprehensive strategy to ensure the government is able to identify priorities in the international system, articulate its approach to national security, and develop a collaborative framework for action involving the government's strategic partners.

The announcement that the government will publish a national security strategy before Christmas is a step forwards but questions

remain as to whether it will have any impact on the security architecture given the short period of time Whitehall has had to develop a strategy.

Furthermore, there is growing concern that the government is becoming too focused on international terrorism, to the detriment of other threats and hazards to the UK. Based on the government's national risk assessment (NRA) and intelligence assessments a national security strategy must seek to identify the government's key priorities and place them in context with each other. The chapter concludes with a number of ideas for reform including the creation of a national security secretariat subsuming the present Defence and Overseas Secretariat, the Civil Contingencies Secretariat and parts of the Security and Intelligence Secretariat (not the assessments staff).

Chapter 4 focuses on the importance of openness and transparency in national security, and how relationships within Whitehall, between the executive and Parliament, and the government and the public must be based on a set of firm principles for making national security transparent, accessible and accountable for all. The chapter ends with a number of ideas for change including the case for developing a technology platform for sharing information among Whitehall departments, agencies and police based on the success of Intellipedia in the United States.

Chapter 5 argues that departments and agencies within the national security architecture must learn the lessons from the past and current wave of public service reform, particularly how departmental performance is gauged and measured. Given the problems associated with the current performance model, which focuses too heavily on targets, departments within the security architecture need to adopt a more nuanced approach to 'targets' based on a mixture of *outcomes* and *observation*.

Instead of performance criteria based largely on statistics (such as the number of police in Afghanistan) the government should experiment with quantitative data supported by *contextual narrative*. This will mean increasing the amount of data and information on issues such as conflict prevention, and poverty reduction strategies

from a wider set of sources including NGOs and the private sector.

This will be essential if the government is to identify progress in relevant policy areas and for acknowledging success and failure in the system. Such an approach will also become increasingly important in order to maintain the trust and confidence of the public in the government's ability to respond to the threats and hazards of the future. The chapter concludes with some ideas for change.

The pamphlet ends with a summary of the new approach to national security.

## Recommendations

### National security strategy

1. A national security strategy has the potential to transform the way government approaches issues of national security but the development of **a strategy must be comprehensive and supported across the political spectrum, within Whitehall and by the public.**
2. While the publication of a national security strategy is welcome the government should go further and **create a national security secretariat, based in the Cabinet Office and subsuming the Overseas and Defence Secretariat, Civil Contingencies Secretariat and parts of the Security and Intelligence Secretariat.**
3. In collaboration with the **prime minister and cabinet the national security secretariat should identify three to five most serious and immediate priorities for UK national security.** These might be serious and organised crime, counter-proliferation, counter-terrorism and energy security.

### System reform

4. **The government should create networks across Whitehall on issues such as 'governance and rule of law', 'trade and diplomacy', 'climate change' and 'security**

**sector reform?** This will require changed departmental structures based more heavily on teams and projects, which are able to call on expertise from outside. These networks will be the responsibility of a senior civil servant, accountable to both a minister and Parliament.

5. **Clarification of ministerial roles on issues of national security is needed.** At present too many key policy areas or departmental units in government have little or no ministerial leadership. This is *not* a call for a new ministerial post in the Cabinet Office on security but rather a plea for better ministerial oversight on a range of policy areas such as security sector reform and conflict prevention and on units that fall between departments such as the new Stabilisation Unit.
6. **Public value** must become the intellectual framework for public services and national security.
7. **A national training centre** should be created for the intelligence agencies and law enforcement.
8. Based on the current IT programme SCOPE, **the government should go further and create a similar system of information-sharing software based on the successful Intellipedia in the US.**

### **Accountability and oversight**

9. **The post of ‘spokesperson on national security’** should be created and based in a new national security secretariat.
10. The government should make public **an annual threat assessment.**
11. **A quadripartite parliamentary select committee on national security** should be created – bringing together existing select committees that focus on UK national interests, security and defence policy. The government must allocate more resources to parliamentary select committees including a panel of national security experts

who can be called on to undertake investigations in specialist areas.

12. The Intelligence and Security Committee (ISC) should not become a parliamentary select committee. Instead **the ISC should be strengthened by recruiting a team of independent investigators while more resources should be provided for the ISC secretariat.**



# **Part 1**

## **Britain and the world today**

---



# 1. A new security paradigm

*There is a danger that we fail to stand back and reflect and . . . make the long-term cool-headed assessment we need to have about the likely repetition of such events and to decide what, for the long term, needs to be done to strengthen our security.*

Rt Hon Gordon Brown MP, Chancellor of the Exchequer,  
13 February 2006

The world is in a constant state of flux. Emerging economies, fledgling democracies, conflicts and natural disasters cover the globe like pieces from a kaleidoscope. Globalisation continues to drive change across the world at unprecedented speed. Innovations in technology, changing demographics, and revolutions in the global economy are transforming the structures and hierarchies of societies, business and government. The world, it is said, is becoming flat,<sup>2</sup> a term coined by Thomas Friedman to describe the convergence of political and economic, social and technological forces across the globe.

In the past most individuals in society were confined to limited roles, bypassed in the circulation of knowledge, power and capital.<sup>3</sup> Today, knowledge is no longer the preserve of a few states, elite institutions or a handful of individuals. The flow of goods, people and commerce has created an atlas of ideas.<sup>4</sup> As Charlie Leadbeater and James Wilsdon argue:

*Reverse migration . . . heralds a new phase of globalisation, one in which ideas and innovation will flow from many more sources. In the last 30 years, global supply chains have transformed how we make products. Our pensions, savings and bank accounts now depend on seamlessly connected global markets. Something similar is about to happen to the way we develop and apply ideas. Innovation will emerge from global networks that link research, testing, development and application.<sup>5</sup>*

The flow of capital has transformed the global economy. The surge of capital into emerging markets stood at US\$235 billion in 1996, five times the level in 1990. In 2005 technological innovations and faster communication networks saw capital flows topping \$6 trillion.

The dynamism and vibrancy of this interconnected world has the potential to create wealth, freedom and security. More trade in goods and services, and better movement of capital has aided investment and development, while global opinion, mobilised through new technologies, has focused our attention on human rights in countries such as Burma, and on environmental problems such as the melting of the polar ice cap.<sup>6</sup>

Such a connected world, however, is increasingly vulnerable to shocks, disruption and uncertainty anywhere in the system. At the time of writing, the global economy looked fragile. Oil recently reached a new high at a record US\$80.36, wheat hit a new record of \$9.11 a bushel after the US Department of Agriculture predicted global stockpiles would shrink to a 30-year low, and gold hit a 17-month high. All of which symbolises the nervousness and vulnerability felt in the market place.

In this global network, issues switch effortlessly from the domestic to the international arena, and increasingly diverse interests need to be coordinated and harnessed. To take one recent example from the business world, in August 2007 underlying fears relating to the collapse of the so-called sub-prime mortgage market in the United States wiped billions of dollars off the value of shares owned by individuals and institutions in London and around the world.<sup>7</sup>

As former Prime Minister Tony Blair suggested in 2006, globalisation has profoundly changed the nature of our society:

*It forces businesses and people to step up a gear simply to keep abreast with the pace of change: commercial transactions are completed without delay, communications happen instantly; goods can be moved rapidly without delay.*

*Government is not immune from these changes. For it to continue to maintain its legitimacy, it needs to change its outlook radically.<sup>8</sup>*

The UK government has found it hard to intervene effectively in political and economic problems with changes in the global system often reverberating unpredictably throughout British society: cartoons shown in Danish newspapers create civil unrest on the streets of London; drugs from the poppy fields of Afghanistan lead to violence on Glasgow estates; while hurricanes off the west coast of America raise the price of petrol in the UK.<sup>9</sup> Cause and effect are no longer close in time and space.

### **A new security paradigm**

The emerging new security paradigm has its roots in the early 1990s and the end of the Cold War but it was not until the attacks on the World Trade Center on 9/11 that the government began to comprehend the scale of the challenges that the international system faced. The collapse of the Soviet Union did not bring about a radical change in the international system. Since 9/11, however, the government has struggled to describe and respond to a radically changing security environment. This has not been a calm and detached intellectual exercise but one that has been accompanied and influenced by a series of diplomatic shifts and noisy events.<sup>10</sup> The focus of 9/11 was the threat of international terrorism, but the event raised our awareness of how fragile our international system was. In doing so it renewed the focus of governments on other emerging security challenges such as the threat from organised crime, and

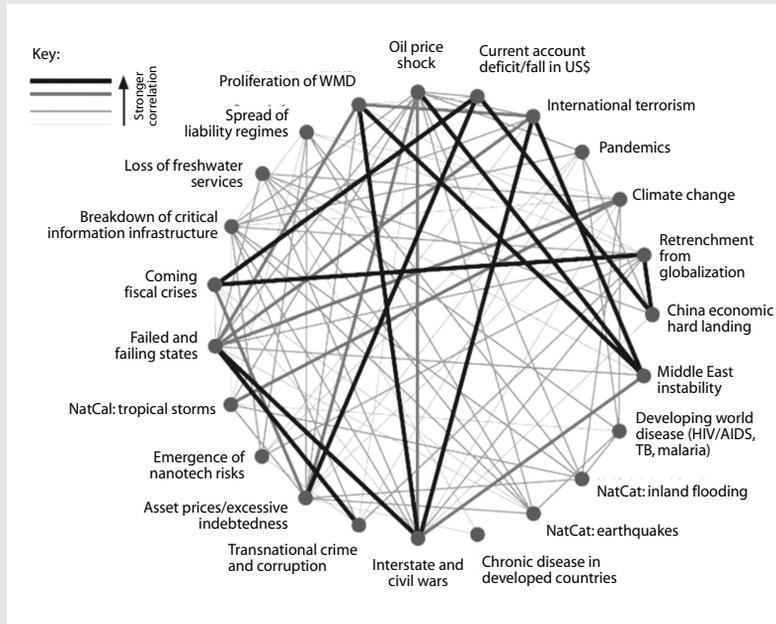
energy security. At the heart of this paradigm are five drivers of change, or *tectonic stresses* as Thomas Homer-Dixon labels them. These are:

- population stress arising from differences in the population growth rates between rich and poor societies, and from spiralling growth of megacities in poor countries
- energy stress – above all from the increasing scarcity of conventional oil
- environmental stress from worsening damage to our land, water, forests and fisheries
- climate change from changes in the makeup of our atmosphere
- economic stress resulting from instabilities in the global economic system and ever-widening income gaps between rich and poor people.<sup>11</sup>

As figure 1 illustrates, risks are increasingly interconnected and no longer clearly delineated in time and space. These tectonic stresses drive multiple risks – threats and hazards which are becoming ever more familiar to the UK: serious and organised crime, international terrorism, the proliferation of weapons of mass destruction (WMD), espionage, fragile states, natural disasters, pandemics, energy security and attacks on the critical national infrastructure.

Thus, in the past seven years, the government has directly and indirectly responded to and managed ongoing operations in the Balkans; the threat from the H5N1 virus; the terrorist attacks on the World Trade Center on 9/11; operations in Afghanistan and Iraq; the Boxing Day Tsunami; failed states such as Sierra Leone; the successful and failed terrorist bombings on the London transport network; Hurricane Katrina; the Pakistan earthquake; the explosion at the Buncefield fuel depot; the crisis in Lebanon; and severe flooding in parts of the UK.

**Figure 1. Visualising the interconnections between global risks**



Source: The World Economic Forum's Correlation Matrix, *Global Risks 2007 Report*

### Shocks, disruption and uncertainty

Three consequences arise from this interdependent world. The first is that shocks, disruption and uncertainty continue to have a greater immediate impact on British society than in the past. For example, in 2003 a 40-minute power cut brought chaos to London and the southeast affecting over 250,000 people and leaving trains stranded and 60 per cent of the tube network affected.

A second consequence, given the multitude of trends, is that events often take us by surprise. As Nassim Taleb suggests:

*Our track record in predicting black swans [random events] is dismal; yet by some mechanism called the hindsight bias we think that we understand them. We have a bad habit of finding 'laws' in history (by fitting stories to events and detecting false patterns); we are drivers looking through the rear view mirror while convinced we are looking ahead.<sup>12</sup>*

The Cuban missile crisis appeared virtually out the blue, as did the rise in oil prices in the early 1970s.<sup>13</sup> Western intelligence agencies were caught by surprise by Saddam Hussein's invasion of Kuwait in 1990,<sup>14</sup> with the testing of nuclear weapons in 1998 by India and Pakistan, and most recently by the attacks on 9/11.

Natural disasters are also no exception. In the aftermath of Hurricane Katrina, Homeland Security Secretary Michael Chertoff said that government officials had not expected both a powerful hurricane and a breach of levees to flood the city of New Orleans. But this was not exactly true. In July 2004 the Federal Emergency Management Agency (FEMA) had run a major disaster simulation exercise in which Hurricane Pam hit the New Orleans area. 'The virtual storm brought winds of 120 mph, 20 inches of rain in parts of southeast Louisiana, and storm surges that topped the levees and flooded the New Orleans area.'<sup>15</sup> As the committee chairman Tom Davis said:

*Hurricane Exercise Pam was so very prescient. And yet Katrina highlighted many, many weaknesses that either were not anticipated by Pam, or were lessons learned but not heeded. That's probably the most painful thing about Katrina, and the tragic loss of life: the foreseeability of it all.<sup>16</sup>*

Seven years before the Asian Tsunami, Samith Dhamasaroj, then director general of the Thai Meteorological Department, warned of the possibility of a devastating tsunami hitting the country's southern coast, and suggested placing early warning systems in three tourist destinations. Not only did senior officials ignore him, but some

provinces banned him from entering their territories as he was damaging their image with foreign tourists.<sup>17</sup>

Closer to home, in summer 2007 the British government came under fierce criticism from politicians, local authorities and the public for not doing more to prepare flood defences in Yorkshire, Lincolnshire and the Midlands. In response to the criticism the chief executive of the Environment Agency, Baroness Young, said that no matter how much preparation there had been, there would still have been some flooding. She argued, ‘the Met Office had warned of heavy rain, but they can’t be specific [because] it is difficult to anticipate where these events will happen’.<sup>18</sup>

A third and final consequence of this new paradigm is the emergence of risk in private and public sector management thinking to become an organising concept.<sup>19</sup> A primary objective of risk management is the ambition to measure everything by forging an intimate conceptual connection between impact and measurable probability. This ambition is the result of a wider cultural trust in numbers and although it is accepted that threats and hazards may be difficult to define and a probability analysis may be imperfect, a vast industry has grown up to support the government in attempting to manage such risks.

Managing risk is not only the focus of national governments but of international organisations. In January 2007 the World Economic Forum (WEF) recommended that country risk officers should be appointed in governments to provide a focal point for mitigating global risks across departments, learning from private-sector approaches and escaping a ‘silo-based’ approach.

### **A twenty-first-century paradox**

For all the frenetic activity of government, policy initiatives, large-scale set piece exercises and ministerial announcements, it is an intriguing paradox of the last two decades that while national security has become more frantic and urgent the real world has afforded the UK a relative lull from the most dangerous threats to the nation.<sup>20</sup>

This goes to the heart of our everyday lives too. The sociologist Lee

Clarke suggests that the great paradox [of today] is that despite the greater risk of 'worst cases' society has never been safer or healthier. To prove this Clarke compares two earthquakes in Turkey and the US suggesting that, 'even the poorest denizens of the rich, modern world are vastly better off than their counterparts in the third world . . . a 7.4 magnitude earthquake broke near Izmit, Turkey, on August 17, 1999, and killed seventeen thousand; a 6.8 magnitude quake hit the Seattle area on February 28, 2001, and one guy died from a heart attack, although seventeen thousand were left without electricity for a time'.<sup>21</sup>

This emerging paradox has been driven in part by the impact of globalisation on society and society's response to a more benign security environment. People certainly feel less safe and fear more because of the rising speed and global connectivity of our activities, technologies and societies, which have exposed them to potential risks more frequently. Furthermore the population tends to see security threats through the prism of local and current issues. In polling conducted by Ipsos MORI for Demos, 59 per cent of the UK population felt they were generally safe in the UK today but 62 per cent believed that Britain was now under greater threat of violent attack than at any time since the Second World War.<sup>22</sup>

The paradox is further exacerbated by the shrinking authority of government and the lack of trust in political parties, in terms of their ability to respond to the wide-ranging risks and their ability to articulate the complexities of national security in an open and accessible manner.

On the one hand this is a result of the limitations of government to effect change, but it is also a reflection of the government's determination to pursue a legislative approach rather than to review current approaches. In the past decade, for example, the government has passed some 53 acts of Parliament dealing with counter-terrorism, crime and criminal justice. Strikingly, this figure exceeds by ten the total number of such acts (43) passed in the 100 years leading up to 1997. In the process, the government has created somewhere between 1018 and 3023 new criminal offences and by 2006 the Blair

**Table 1. People's rating of the most worrying issues in Britain (1997–2007)**

	2007 (%)	2003* (%)	1997* (%)
Crime and violence	51	50	68
Immigration and control	45	44	15
Terrorism	33	42	21
Health care	30	40	N/A
Education	21	23	N/A
Poverty and social inequality	20	23	39
Threats against the environment	17	14	19
Taxes	17	18	12
Unemployment (and jobs)	12	12	45
Maintaining the welfare state	11	17	25
Corruption and financial or political scandals	10	11	15
Don't know	2	0	1

\*2003 base (972), 1997 base (1010), data recorded by telephone interviews

Source: Ipsos

government had spent more per head on law and order than any other country in the OECD.<sup>23</sup>

As the research by Demos and Ipsos MORI shows, however, legislative activity coupled with extra resources for police and the creation of a new agency to deal with organised crime has not achieved the significant reductions in people's perceptions of serious crime and violence (see table 1). Security commentators in academia and the media have suggested that this is partly down to the fact that the increase in legislation has made no impact on crime and security as there has been a shortage of effective administrators to run the services over which it provides the overall result. *The Economist* went one stage further by suggesting that the Home Office was 'not bad at churning out legislation, but pretty useless at implementing it'.<sup>24</sup>

This pressure to be seen to be active is explained by the government's former intelligence and security coordinator David Omand,

who suggests that: ‘what drives ministers and officials is genuine fear for public safety and, of course, concern that they will be found wanting by the public if they are not seen to be doing everything in their power. They are burned by media firestorms demanding public reassurance after each plot uncovered or adverse judgement in the courts.’<sup>25</sup>

The government’s approach to this paradox can partly be explained by the fact that public perceptions tend to be at odds with the real nature of risks. For example a day after the destruction of the World Trade Center, a commentator predicted in the *Los Angeles Times* that the next big thing would not be ‘some new technological innovation or medical breakthrough’ but ‘is likely to be fear’.<sup>26</sup> As the sociologist Frank Furedi argues:

*The past decade has seen a veritable explosion of new dangers. Life is portrayed as increasingly violent. Children are depicted as more and more out of control. Crime is on the increase. The food we eat, the water we drink, and the materials we use for everything from buildings to cellular phones, have come under scrutiny.*<sup>27</sup>

This description is not only applicable to individuals within society. It is apparent in the discourse and actions of governments around the world. As Wolfgang Sachs neatly put it in 1993:

*The North . . . no longer talks of the South as a cluster of young nations with a bright future, but views it with suspicion as a breeding ground for crises. At first, developed nations saw the South as a colonial area, then as developing nations. Now they are viewed as risk-prone zones suffering from epidemics, violence, desertification, over population and corruption. The North has unified its vision of these diverse nations by cramming them into a category called ‘risk’.*<sup>28</sup>

Yet there are few if any encouraging signs that this twenty-first-century paradox has been understood. Immediately after the London bombings, then Prime Minister Tony Blair stated ‘the rules had

changed'. Recently Home Office Minister Tony McNulty admitted that the government had made mistakes since the 7/7 terrorist attacks suggesting that two years later, 'the government was coming round to the view . . . the rules of the game haven't changed'.<sup>29</sup> More symbolically perhaps the Home Office recently changed its focus from working towards a 'safe, just and tolerant society' to 'protecting the public, securing our future'.<sup>30</sup>

### **The case for reform**

The national security architecture has yet to adapt to the twenty-first century. Existing habits of thought and institutions remain powerfully conditioned by the concept of the nation state that has dominated Western thinking since the seventeenth century. Today power is dispersing around and through the nation state. This is most apparent in the blurring of three traditionally important distinctions – between domestic and international spheres; between policy areas; and between public, private and non-profit sectors.<sup>31</sup>

This change is significant but rarely considered within contemporary discussions on domestic and foreign policy. The challenges faced by governments, such as terrorism, pandemics and immigration, for example, cannot be solved by one government but demands collective action by a global community.<sup>32</sup>

Immigration is a useful illustration of the mismatch between what drives international issues and how we address them. Aside from forced migration due to conflict, persecution, trafficking or environmental disasters, economics remains the driving force. Yet policy approaches to it derive from the older vision of international politics, one dominated by notions of border controls, citizenship and sovereignty.<sup>33</sup> As Michael Barber, the former head of the Prime Minister's Delivery Unit (PMDU), suggests:

*We have experienced the biggest wave of immigration since the 1950s and 1960s, indeed perhaps ever, and while the economic benefits are apparent, the wide ranging social implications for the long term have barely been touched on. Indeed, because*

*much of the immigration has been illegal, the government has sometimes preferred to narrow the scope of the debate. Yet 30 per cent of London's present workforce was born outside the UK.<sup>34</sup>*

Immigration symbolises the serious institutional mismatches that exist between the problems that need to be addressed and the institutional arrangements for doing so.<sup>35</sup> This should come as no surprise given that the current government structures and processes were designed for a world that was more stable and simple than at present.

And herein lies the problem. Ministers and civil servants *recognise* the inherent complexity of the present security environment but are not able to *respond* to it.

There are numerous reasons for this. The first is that the underlying assumption in government remains the explicit need to maintain the *status quo* and with it stability over the short term. As Geoff Mulgan argued in an article in *Prospect* magazine, 'governments overestimate their power to achieve change in the short term, and underestimate it in the long term'.<sup>36</sup> Homer-Dixon suggests one other reason for this:

*If we can get away with denying or ignoring the problem – like the international economy's chronic instability or building more houses on flood plains – we do so. We tell ourselves that the challenges aren't that serious and then simply continue with business as usual. Sometimes, lo and behold, benign neglect is the best strategy, and we muddle through successfully.<sup>37</sup>*

'Muddling through', however, is not sustainable in the twenty-first century, and improvisation can only ever be second best to a strategic approach in the long term. This is especially true in a world that is so interconnected. Moreover, muddling through has succeeded in the past only when a government has wished to maintain a policy or retain the initiative. In truth, few governments today can claim to set the agenda.

Second, governments invariably seek to reduce a problem to its constituent parts, even if, in some cases, that causes problems further along the way. This is partly explained by the need for simplifying narratives to explain complex areas of policy, but it also stems from a dangerous tendency to 'seek out and relay the information that confirms "our world view". And the further away one is from reality the worse the tendency is.'<sup>38</sup>

This is further exacerbated by the reality that national security issues remain a subject for a small group of individuals in government. Such has been the mystique surrounding national security, and the perception that individuals working in the area of national security have an expertise above and beyond other civil servants, that it has been rare for questions to be raised about the state of the national security architecture, whether it is fit for purpose and what reforms may be necessary.

Recent reviews into the capacity of the security architecture have largely (with one or two exceptions) resulted in extra resources for the police and intelligence agencies rather than necessary reform.<sup>39</sup> However, although few would question the necessity of extra resources, concerns remain that faults in the national security architecture lie less with constraints over resources than with the seeming inability of the architecture to reform in light of new threats and hazards.

Furthermore there is a real concern among some members of the security and intelligence community that departments and agencies (including the police) are becoming too focused on international terrorism to the detriment of other security challenges.

This is not just an issue for the UK government but a debate that is currently being had in the United States. Bill Bratton, chief of the Los Angeles Police Department (LAPD), recently argued that the US government was putting crime reduction gains during the past 15 years in jeopardy by switching too many resources from mainstream policing to counter-terrorism. In an interview in October 2007<sup>40</sup> he suggested that 'the federal government is a one-eyed Cyclops' only able to focus on one thing at a time. This is worrying given the obvious parallels with the end of the Cold War and the inability of

governments to meet the challenges of the 1990s, including the rise of international terrorism.

A final reason for the lack of reform of the UK's national security architecture is the reputation the government enjoys within the international community. Governments and administrations look on enviously as the UK government is seemingly able to harness the power of Whitehall for negotiations in the European Union, coordinate a response to an unfolding tragedy thousands of miles away, or bring its influence to bear on the US administration.

### **Fit for what purpose?**

The need for government to adapt to the twenty-first century has been argued for by Tony Blair and by the Cabinet Secretary, Sir Gus O'Donnell, in 2006. The capability reviews, led by the Cabinet Office, were aimed at driving improvement and a more joined-up approach in government which, Sir Gus suggested, would, 'pose some significant challenges to the machinery of government but above all to the leaders of the civil service'.<sup>41</sup> The challenge of creating a more joined-up government is described by Paddy Ashdown in his recent book *Swords and Ploughshares*:

*[T]here is no legislative framework to ensure coherence between departments; no mandate for the Cabinet Office to provide this coordination and leadership; no regular, joined up oversight of overseas and domestic policies, except at the highest level; no joined up, working-level staff structure to coordinate the full range of overseas commitments and ensure effective implementation of ministerial decisions . . . Departments are still focused on their own policies, their own budgets, their own cultures . . . The FCO division of the world nations in its departments bears no relation to the MoD's organisation, which, in turn, is different from the security agencies' approach . . . there are no fewer than six Whitehall units that deal with conflict issues and many of these have overlapping mandates.<sup>42</sup>*

Many of the examples that frustrated Ashdown can be found in the capability reviews of the Foreign and Commonwealth Office (FCO), Ministry of Defence (MoD), Department for International Development (DFID) and Cabinet Office. For example, the FCO capability review states that:

*the 2006 white paper provides a high-level statement on the FCO. However this statement has not consistently been turned into detailed working agreements with other departments . . . This means there is no single, widely understood and accepted mechanism in Whitehall for agreeing roles and responsibilities, and clarifying accountability.*<sup>43</sup>

The MoD capability review focuses primarily on its ‘insularity and reluctance to consult and work with others in the formulation of strategy and policy’. This can be changed, the review goes on to state, by taking ‘steps to make its work more accessible – even down to changing the language for different audiences or revising security classifications where possible’.<sup>44</sup>

For the DFID, the capability review takes issue with the lack of change in the department stating: ‘it is not yet evident that senior civil servants in the Department genuinely accept the need for change and take responsibility for making change happen’. Furthermore, ‘there is insufficient challenge within the culture of the Department, including at board level. Only 42 per cent of DFID’s senior civil servants feel that it is safe to speak up and challenge the way things are done in the Department.’<sup>45</sup>

The role of the Cabinet Office in national security has been seen as paramount. And yet the Cabinet Office needs to:

*define and clarify how the Cabinet Office is organised around its three core functions; supporting the Prime Minister, supporting the Cabinet, and strengthening the civil service, with a clearly stated rationale for each. In the absence of such clear definition, it is easy for confusion to arise amongst both staff and external*

*stakeholders as to which particular capacity – directing, enabling, enforcing, coordinating, or informing – a particular unit of the Cabinet Office is working in.*<sup>46</sup>

The truth is that very little of what the capability reviews about Whitehall departments had to say was new. In March 1967 for instance, the Secretary to the Cabinet, Burke Trend, wrote a personal note to Prime Minister Harold Wilson on the deficiencies of the Cabinet Office machinery relating to politico-military planning and the intelligence services. In his note Trend outlined his concerns over the lack of coordination and planning in government on security issues as well as the weakness of collation and distribution of intelligence throughout Whitehall.<sup>47</sup>

This lends further weight to criticisms made of the government's current response, which suggest that the present approach:

*demonstrates classic bureaucratic and organisational inertia, where policy is not determined by the nature of the challenge, but by the nature of the tools available, which have to be shown to be relevant and effective . . . critics argue, there has been a failure to understand the real meaning of 9/11, and a consequent unwillingness to devise new policy tools – or at least – to reconfigure existing procedures and mechanisms.*<sup>48</sup>

Furthermore these criticisms serve to highlight the growing disconnect between politicians and civil servants on reforms in government. In a speech to the Royal United Services Institute (RUSI), Gordon Brown stated that 'national and international action for security is inextricably linked and security issues dominate decisions in transport, energy, immigration and extend to social security and health'.<sup>49</sup>

Brown's argument was clear. National and international security are connected and no longer the preserve of one or two departments but the responsibility of all of them.

So it was interesting to note that the permanent secretaries of each of the MoD, FCO and DFID state in their introductions to the

capability reviews that ‘we have been meeting regularly as permanent secretaries of the “international departments” to discuss shared issues’.<sup>50</sup> Although this is positive in one respect, it does highlight the underlying assumptions of ministers and senior civil servants – that a divide between international and domestic departments remains intact regardless of political rhetoric.

## **Intelligence**

With the end of the Cold War the government sought to decrease the overall amount it spent on security and defence. Spending on the armed forces and relevant departments steadily decreased as did the number of civil servants. The budgets of the intelligence agencies had also steadily decreased and in the case of the Secret Intelligence Service (MI6) this amounted close to 25 per cent of its total budget, a significant reduction, and resulted in a situation where numerically the agencies combined were historically at their smallest.<sup>51</sup>

While it may have seemed logical to reduce the agencies’ resources in light of the Soviet Union’s demise, with hindsight this approach seems flawed and lacking in foresight. With the end of the Cold War came a plethora of risks the agencies had to respond to and this came with no major increase in funding. As such the agencies’ process of internal reform was slow and cautious.<sup>52</sup>

In the past six years the intelligence agencies have been forced to adapt to the changing security environment and with extra resources have been successful in intercepting terrorism but there remains a general question over the role of intelligence in the twenty-first century, what it does and for whom.

At a time when the government receives ‘intelligence’ from myriad sources, such as *BBC Monitoring*, *Bloomberg News*, *Oxford Analytica* and The Economist Intelligence Unit, the intelligence community ‘remains mired in institutions, processes, and habits of mind that have been appropriate to the Cold War but manifestly are not now. Agencies need to be reshaped for an age of information. This is a time to re-examine first principles, which are now open to question in a way they haven’t been for half a century.’<sup>53</sup>

This is crucial given how overstretched the intelligence services are and the amount of information the agencies and the police must sift through. In the case of the July 2005 bombings in London, for example, 12,500 statements were taken; 5000 exhibits were examined forensically; and more than 6000 hours of CCTV footage had to be examined.<sup>54</sup>

### **Puzzles and mysteries**

To understand the challenge of intelligence in the twenty-first century it is helpful to make the distinction between puzzles and mysteries. A puzzle is when and where the next terrorist attack will be in the UK. The intelligence agencies, specifically the Security Service (MI5) and police, may have some information concerning potential terrorists and a likely target but they will not have the whole picture. The key to identifying the terrorists' whereabouts and the potential target will come from a mixture of human intelligence (HUMINT) and signals intelligence (SIGINT). The problem of what would happen in Iraq after the toppling of Saddam Hussein was, by contrast, a mystery. It wasn't a question that had a simple, factual answer. Mysteries require judgements and the assessment of uncertainty and the hard part is not that we have too little information but that we have too much.<sup>55</sup>

In this new security paradigm, therefore, analysts and policy-makers will continue to need access to traditional intelligence but it will become even more necessary to build partnerships with external communities – academics, think tanks, NGOs and the private sector – in order to create a clearer picture of the security environment.

### **Collaborating in government**

Since 9/11 and the July 2005 bombings the intelligence agencies have seen a rapid increase in their respective budgets. In 2001 the budget for security and intelligence was £1 billion. In 2007/08, it is estimated this will be £2.5 billion. With new resources MI5 has been able to mount a period of reorganisation, which includes regional centres across the UK as well as a major recruitment drive. At the same time the Metropolitan Police has merged its Special Operations units SO12

and SO13 to form the Counter-Terrorism Command (CTC), also known as SO15. Although more resources are clearly needed there is a danger that extra resources will mask the need for agencies and departments to collaborate, preferring instead to use resources to develop their own capabilities.

Collaborating across government and agencies often fails to challenge the traditional processes, and on occasions is ignored by ministers and civil servants who believe it will not demonstrate real change. Two examples highlight this approach: the recent decision to split the Home Office and the creation of the Post Conflict Reconstruction Unit to 'strengthen the UK's ability to help achieve a stable environment in countries emerging from conflict'.<sup>56</sup>

The decision to create a Department for Justice while leaving the Home Office to concentrate on terrorism, drugs, policing, security and immigration was questioned inside and outside government. Although there was little doubt that the government's strategy on counter-terrorism needed refreshing and the confusing lines of accountability in the Home Office and Cabinet Office made more simple, the announcement of the split to take place over only a few months caused a sensation immediately through Whitehall and beyond.

The split of the Home Office was a result of an internal review on the government's counter-terrorism strategy led by then home secretary John Reid. The review was seen by most senior civil servants and political commentators as being 'one part review to two parts political manoeuvring',<sup>57</sup> and caused widespread opposition with at least three previous home secretaries openly hostile to the proposed plans. Furthermore, it was a review that was seemingly led by a small team in the Home Secretary's office and which resulted in a regular diet of spin, including the notable headline from *The Times*, 'Reid to be MI6 security chief'.<sup>58</sup>

The *Guardian* meanwhile suggested that 'the secrecy of planning for change, a deadline that looks more political than practical and the pall of confusion still shrouding who does what, all suggest its first objective is evidence of action, even if it comes at the cost of delaying

the intended benefit of a sharper focus on fighting terrorism.<sup>59</sup> One senior civil servant in the FCO conceded:

*We've spent six months actually dealing with the machinery of government rather than dealing with the policy and the pursuit of the terrorists. There has been a lot of diversion of time in dealing with bureaucratic issues as it were . . . I'd like to think we're about at the stage where all the structures have settled down and we're about to get back on to refreshing policy and being effective at counter-terrorism.<sup>60</sup>*

One reason for deciding to divide the Home Office was the feeling that attempts to collaborate on different strands of counter-terrorism had not succeeded. Instead of pursuing a more collaborative approach to counter-terrorism and developing a set of more innovative ideas a swift and relatively uncomplicated division of responsibilities was seen as the more suitable approach.

In the short term the division may have created a greater sense of accountability and clarity within the Home Office by creating an Office for Security and Counter-Terrorism (OSCT)<sup>61</sup> led by a new director general. The Prime Minister also appointed Lord West, a former Chief of the Naval Staff, as Minister for Security and Counter-terrorism responsible for the OSCT. However, cracks have begun to appear, noticeably between the Home Office and the Ministry of Justice on prisoner numbers but more worryingly on the role of the OSCT itself, which to date has focused solely on counter-terrorism and not on wider security issues.

Second, joined-up approaches often fail to change the underlying culture of government departments. The creation of the Post Conflict Reconstruction Unit (PCRU) is a testament to this approach:

*Firstly, the PCRU . . . was conceived as an add-on for government, not as an integral coordinating and directing part of it. Creating little bureaucracies, each with a national flag on them, is the easy bit. The hard bit is to re-think our whole*

*approach to this, reshaping the inter-relationships of government, creating a national capability to match these and, perhaps most importantly, investing in an international structure to carry it out.<sup>62</sup>*

In this case the problem was further compounded by a lack of political leadership (there is no single minister to whom the PCRU is responsible to), which led to the PCRU being rejected by DFID, its parent department. This meant ‘its role had been reduced from an organisation whose primary purpose was strategy development and crisis planning, to one whose primary purpose is to be an occasional service provider facilitating those already engaged in the existing crises in Afghanistan, Iraq and elsewhere.’<sup>63</sup>

The government seems to have accepted some of the above criticism with the new Comprehensive Spending Review (CSR) stating that the PCRU will become a new Stabilisation Unit with a mission to:

*fill critical capability gaps in UK and international operations such as the rule of law, governance and policing advisers. The Stabilisation Unit will also facilitate cross-government assessment and planning to stabilise countries emerging from conflict, and will identify and integrate lessons from UK interventions into future stabilisation activities.<sup>64</sup>*

Although this new development is welcome (the new unit will manage a new conflict prevention pool) and suggests that there has been some genuine thinking on how to better focus the government’s energy and resources for post conflict operations, serious questions remain over whether it will have the necessary impact on the culture of Whitehall.

## **A failure of imagination**

One of the most serious criticisms levelled at the UK government is the lack of imagination within government on developing responses to threats and hazards. This criticism has been made privately with

reference to the lack of experimentation with the national security architecture and more publicly regarding the failures of intelligence post 9/11, such as the review of intelligence on weapons of mass destruction by Lord Butler.<sup>65</sup>

As Lord Butler noted in his review, ‘well developed imagination at all stages of the intelligence process is required to overcome preconceptions’. There is a case for encouraging it by providing for structured challenge, with established methods and procedures, often described as a ‘devil’s advocate’ or a ‘red teaming’ approach. Although the focus of Lord Butler’s criticisms was concerned with the intelligence process, his point that ‘there should be well developed imagination’ is valid across the security architecture.

This may also assist in countering another danger: when there are many variables, on any one of them the number of experts working on them may be dangerously small, and individual, possibly idiosyncratic, views may pass unchallenged. There are two reasons for this. First, so much of what goes down in history as ‘intelligence failures’ results from assumptions – ones that are often derived from mirror imaging – asking what we would do if we were in someone else’s shoes.

In *Blink* the author Malcolm Gladwell describes Paul Van Riper’s big victory. Van Riper was a Marine Corps veteran who was asked to take part in Millennium Challenge, a war gaming exercise created by the Pentagon. Divided into the blue team (Pentagon) and red team (Van Riper), the exercise aimed to test some new and radical ideas about how to go to battle. As Gladwell explains:

*On the opening day Blue team poured tens of thousands of troops into the Persian Gulf . . . They parked an aircraft carrier battle group just offshore of Red Team’s home country . . . They acted with utter confidence because their Operational Net Assessment matrixes told them where Red Team’s vulnerabilities were, and what Red Team’s next move was likely to be. But Paul Van Riper did not behave as the computers predicted . . . On the second day he put a fleet of small boats in the Persian Gulf . . .*

*then without warning, he bombarded them in an hour-long assault with a fusillade of cruise missiles. When Red Team's attack was over, sixteen American ships lay at the bottom of the Persian Gulf.*<sup>66</sup>

Organisations and people must change their way of perceiving risk, from thinking about *probabilities* to identifying *possibilities*. Take the example of 9/11. The American intelligence community has been roundly criticised for failing to pay adequate attention to the numerous signals prior to 9/11 that al Qaeda was planning a large attack. One reason is that probabilism blinkered their vision. Between 1998 and 2001 the FBI and CIA received information from several sources that terrorist organisations, including al Qaeda, were planning some sort of attack with hijacked aircraft. One plot was to fly an explosive-laden plane into New York's World Trade Center. Neither the FBI nor the Federal Aviation Administration acted on the information, however, because they 'found the plot highly unlikely'.<sup>67</sup>

Only a handful of imaginative approaches to national security have been discussed in government and in political debate more widely but they have often fallen short of expectations in both their scope and delivery. For example in late July 2007, the Conservative Party's National and International Security Policy Group published their report 'An unquiet world'.<sup>68</sup> The paper painted a picture of the security environment and called for a balanced approach to [the UK's] closest international relationships; a 'partnership for open societies' in the Middle East; and the appointment of a cabinet-level security minister dedicated to protecting Britain from terrorism.<sup>69</sup>

In launching the group's final report, Dame Pauline Neville-Jones argued that the 'need to look after the UK security should be our top priority, not as a matter of counter-terrorism and the armed forces, but as a much broader conception that we have'.<sup>70</sup> It was the first attempt by a political party to develop a national security approach, which a *Guardian* leader noted was, 'both welcome and beyond doubt'.<sup>71</sup>

The report, however, served to highlight a general lack of understanding about the complexity of ‘security policy’, and how the government should be organised to respond to threats and hazards of the twenty-first century, and in doing so it recommended the strengthening of the very institutions and Whitehall culture it sought to change. It was, in short, a traditional approach to reforming government, reflecting what Perri 6 suggested back 1997:

*[F]unctions have been put together and pulled apart many times during the twentieth century in the name of rationalisation. But the particular rationales have often had less to do with synergies of functions or the disappearance of old needs and the emergence of new ones than with the need to give or deny power to particular politicians of cabinet rank.<sup>72</sup>*

At the same time, a national security approach was beginning to be developed by Gordon Brown and his advisers, seemingly keen to distance the former Chancellor from the former Prime Minister. The result was a statement on constitutional reform in the summer of 2007:

*[F]rom now on the Government will regularly publish, for Parliamentary debate and public scrutiny, our national security strategy setting out for the British people the threats we face and the objectives we pursue. I have said for some time that the long term and continuing security obligation upon us requires us to coordinate military, policing, intelligence and diplomatic action – and also . . . I have decided to establish within Government a national security council.<sup>73</sup>*

The creation of a ‘national security council’ was considered a useful addition to government. Yet confusion over its role was confirmed when Brown announced in Parliament that he was *not* creating a national security council, as described by him the previous week but a cabinet committee on national security. The reason for this confusion, as described by one senior civil servant in the Cabinet

Office at the time, was that there were ‘too many references to “committees” in the green paper and we didn’t want to confuse people’. The cabinet committee on national security would instead be an amalgamation of three existing committees. Soon afterwards a list of new cabinet committees on national security were made public with one security analyst noting that all that had really occurred was a rebranding exercise.<sup>74</sup>

The division of a major department of state remains fairly unique in present day government. The process of reorganising a department remains by far the most traditional and relatively straightforward process in comparison with, for example, developing a collaborative approach to a policy area that will impact on culture, process and structures. At the more strategic end of government this becomes more common with the creation of small units and secretariats that endeavour to bring together disparate parts of the system and coordinate their activities. The creation of the Civil Contingencies Secretariat in 2001 is one such example.

Following 9/11, the crisis over fuel shortages, the foot and mouth epidemic and severe flooding, the Civil Contingencies Secretariat was created to bring together a range of responsibilities that had previously been dispersed across a number of different departments. Few disagreed that reform of emergency planning was very necessary and so from the outset the Civil Contingencies Secretariat was designed to identify and manage the risk of emergencies and coordinate the response of government departments. As well as providing a secretariat for the Civil Contingencies Committee (CCC) the secretariat has a number of objectives including:

- spotting trouble, assessing its nature and providing warning
- being ready to respond by tracking the preparedness of organisations at national, regional and local levels through formal preparedness assessments
- building greater resilience for the future by developing stronger resilience capabilities

- providing leadership and guidance to the resilience community through the development of a ‘national resilience strategy’
- providing effective management.<sup>75</sup>

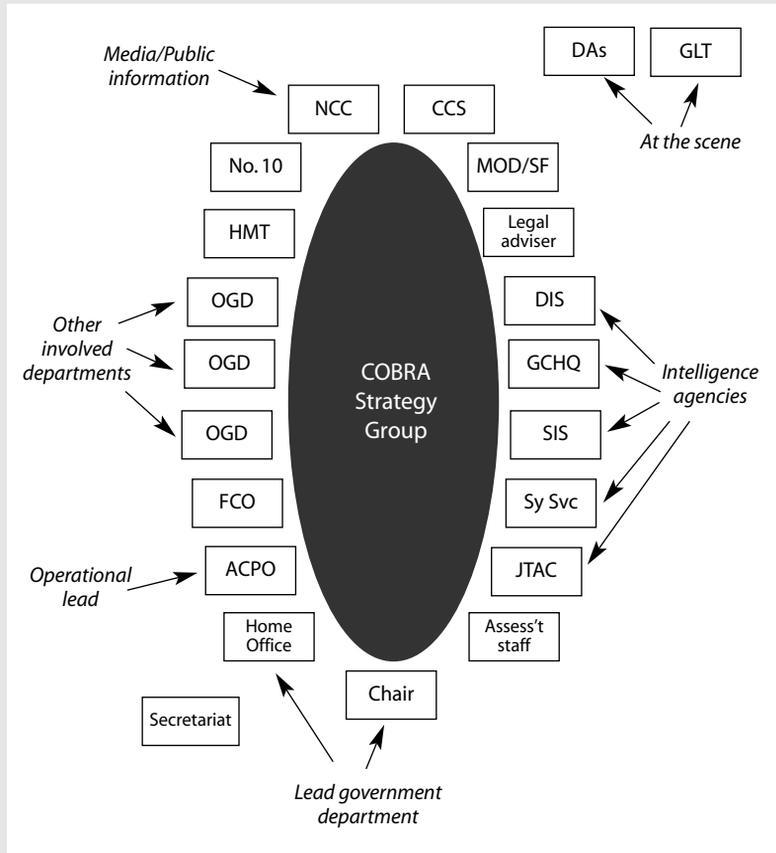
The reforms to Whitehall structures were complemented by the creation of ‘regional media emergency forums’ (comprising media organisations, local authorities, the emergency services, government agencies and the utilities) and the corresponding communications groups of ‘local resilience forums’.<sup>76</sup> The creation of a new secretariat was strengthened by the appointment of a security and intelligence coordinator in the Cabinet Office with the aim of ‘enhancing the capacity at the centre of government to coordinate security, intelligence and consequence management’.<sup>77</sup>

At the same time the existence of the Cabinet Office briefing rooms were made public. COBR(A) or ‘Cobra’, as it has become universally known as in the media, refers to one of the briefing rooms – room A. COBR(A) is a coordination facility based in the Cabinet Office, activated during a national emergency such as a terrorist incident. Key personnel from each department and agencies meet at the facility to develop and coordinate a response (see figure 2).

The publicity surrounding COBR(A) was driven in part by an understanding within government that the name was becoming a recognised brand and signalled the importance of the situation and that the government was getting a ‘grip of the situation’. Although COBR(A) nominally meets only when there is an emergency there have been a number of occasions when prime ministers have felt it would help manage change. For example, former Prime Minister Tony Blair and the then Home Secretary David Blunkett announced that they would be convening a meeting of COBR(A) to fight street crime in 2003.

Last, the Civil Contingencies Secretariat has introduced risk management as a methodology for coping with emergencies, which has led to the development of a NRA in government. The aim of this approach and of the government’s risk matrix (see figure 3) was to

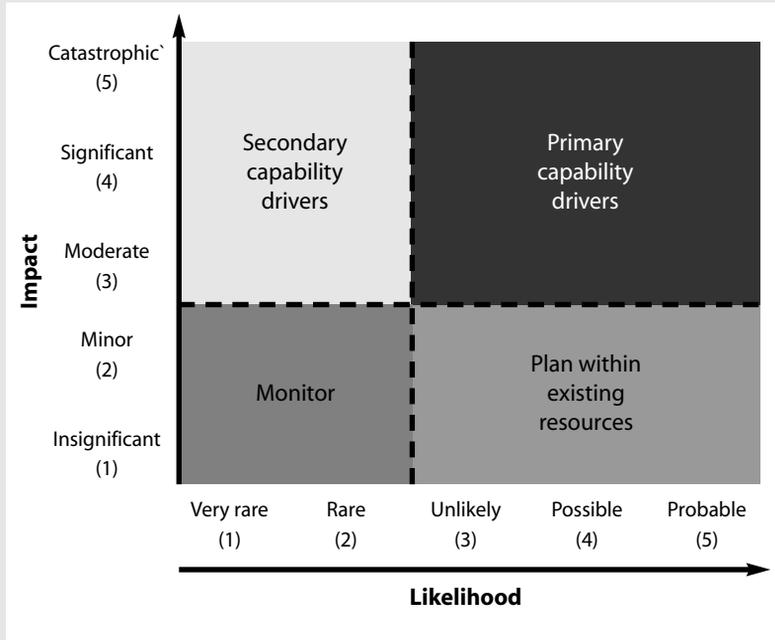
**Figure 2. 'Terrorist incident' Cabinet Office briefing room**



ACPO, Association of Chief Police Officers; CCS, Civil Contingencies Secretariat; DAs, Devolved Administrations (ie Scots, Welsh, Northern Irish); DIS, Defence Intelligence Staff; FCO, Foreign and Commonwealth Office; GCHQ, Government Communications Headquarters; GLT, Government Liaison Team; HMT, HM Treasury; JTAC, Joint Terrorism Analysis Centre; MOD/SF, Ministry of Defence/Special Forces; NCC, News Co-ordination Centre; OGD, other government department; SIS, Secret Intelligence Service (MI6); Sy Svc, Security Service (MI5)

Source: Cabinet Office

**Figure 3. The UK government’s risk matrix**



Source: Cabinet Office

develop a more robust approach to both threats and hazards facing the UK. For example, early in 2007 pandemic flu was considered ‘very high’ risk and was therefore deemed to be a primary driver of capabilities while some aspects of the threat from terrorism were deemed ‘high’ and therefore could be planned for within existing resources.

However, critics suggest that although the creation of a Civil Contingencies Secretariat was important it should have been provided with more executive initiative and authority. As Paul Cornish has argued, the issue at the heart of the current debate is whether the government’s preference for inter-departmental and

inter-agency coordination is really the best way to manage the response to present and future threats. Or that government is merely recycling some old ideas and methods, and relying too much on a strategy of muddling through.<sup>78</sup>

### **The strategic partners of government**

Today the government's strategic partners include international organisations, the private sector and the public. This is a result of the state's sovereignty '*leaking up* to multinational corporations, international organisations and international alliances' while at the same time '*leaking out* to business and non-profit organisations' and '*leaking down* to regional and local government'.<sup>79</sup> In the security environment this phenomenon has had a major impact on the UK government, with profound effects, the consequences of which have yet to be fully realised.

At the same time, there is a greater 'transnational' dimension to the UK's security. No longer is this largely a question of working with NATO allies but of working with the European Union too. The EU has taken on an increasing number of responsibilities in peacekeeping and civil-military missions in Africa and southeast Asia. Since 9/11 and the Madrid bombings in 2004 the EU has also begun to develop a more comprehensive role in policing and counter-terrorism in which UK personnel have been heavily involved.

This has led to a complex web of transnational, private and not-for-profit organisations involved in a broad range of missions. For example, a British unit was involved in the EU's military operation, Operation Artemis, in the Democratic Republic of Congo in 2003, a British general led EUFOR in Bosnia 2004–06, while European troops relied on a Ukrainian firm to ferry them to Afghanistan in former Soviet jets. In Iraq during the early period of the war, 60 firms were operating, employing more than 20,000 private personnel to carry out military functions, roughly the same number of troops as provided by all of the United States' coalition partners combined.<sup>80</sup>

In addition, the use of private security organisations goes well beyond the level of personal bodyguards and includes the local

protection of mines, oil fields, factories and other expatriate business. Private sector companies are hired to train police, clear mine fields, destroy ammunition stockpiles, and to remove small arms and light weapons. Outsourcing such work is not generally new in itself; it is the powers and capabilities of companies that are novel, and as a consequence radically changing the nature of the security environment.<sup>81</sup>

At home, the use of the private sector for national security has grown exponentially since privatisation began in the 1980s. The number of List X companies, those companies that have been approved to hold UK government protectively marked information above a certain classification, has grown steadily as both the volume and diversity of work in the national security arena has increased.

Although the UK government has classified the list of companies, it is possible to identify activities in the national security domain. They include the development and manufacture of electronic systems and industrial electronics for defence projects, general strategy and consultation on security policy, policing, governance and intelligence reform in fragile states, data warehousing and mining. Government and industry have also come together to form new alliances and develop strategies together.

In early 2007 suppliers, trade associations and research institutes (RUSI and Chatham House) launched the UK Security and Resilience Industry Suppliers Council (RISC) to provide a single industry voice and channel of communication for government on strategic issues affecting national security and resilience.<sup>82</sup> Later on in 2007 the Home Office's 'Security and Counter-Terrorism Science and Innovation Strategy' was published.<sup>83</sup> The strategy set out how the Home Office will work with 'partners in the private sector and academia, with international colleagues, and within government'.

The trend of outsourcing government work on security is unlikely to stop. Although the scale of outsourcing in the US is on a far greater level it is still instructive to note that according to the *Washington Post* the US Defence Intelligence Agency was preparing to pay private contractors up to \$1 billion to conduct core intelligence tasks of analysis and collection over the next five years.<sup>84</sup>

Finally, at the same time as security and defence work is being outsourced by government to the private sector, so the private sector is relying less on the government for its protection. The movement of security and intelligence officials from the public to the private sector has been steadily increasing and has led to a rapid growth in companies that offer a range of services from running prisons to devising risk management processes for major public events to pandemic services, travel security, and governance and development in fragile states.

## 2. The public value of security

The twenty-first century offers a radically different political landscape for debating national security. Many contemporary western societies are afflicted by a profound sense of malaise with political institutions facing a major problem of legitimacy. As Tom Bentley argues:

*the form of nation state democracy that dominated the second half of the twentieth century is holed below the waterline . . . our politics duck the big and difficult issues like climate change and pensions reform, but at the same time seems unable to put right even small things.*<sup>85</sup>

Underlying all of this is the lack of a clearly articulated account of what national security is and the value it creates for the individual and society in general. There is no shared framework for government and the public as well as politicians to deliberate over the long-term decisions and trade-offs that are required for national security. And although the government has argued that the responsibility for the nation's security rests with society as much as government institutions, its response has been to work behind closed doors, consult professionals and experts and decide future strategy in private committees. If it is 'Up to all of us', as the posters on the transport network tell us, then the government cannot simply communicate the risks. Instead it must engage with the public by creating opportunities for dialogue.

Public value takes as its starting point the idea that leaders in the public sector cannot take the underlying purpose, legitimacy or value their institution creates for society to be self-evident, simply because they are public institutions whose mandate has been supplied by democratically elected governments. Instead they need to be more proactive and flexible in three respects:

- in searching for valued purposes for their organisation (through activities that meet the changing needs of society)
- in providing opportunities for citizens and other stakeholders to authorise these purposes (through processes of accountability and deliberation)
- by doing more to identify and represent the value their work creates (through evaluating and communicating their performance more effectively).

And, as Mark Moore suggests, adopting a public value approach in government may mean:

*[r]ecasting the mission of the organisation and repositioning it in its political and task environment so that old capabilities can be used more responsively and effectively. On occasion it means reducing the claims that government organisations make on taxpayers and reclaiming the resources now committed to the organisations for alternative public or private uses. This is clearly the proper conceptual definition of managerial success: to increase the public value produced by public sector organisations in both the short and the long run.<sup>86</sup>*

Michael Barber, the former head of the PMDU, suggests that tied up in this definition of public value are a number of key elements:

- delivery of results
- organisational health of the institution and service
- efficiency

- public perception of the institution or service
- expenditure.<sup>87</sup>

Public value was developed as a way of remedying some of the defects associated with new public management (NPM), a management philosophy used by governments since the 1980s to modernise the public sector.

Public value improves on earlier theories of public administration (see table 2) by drawing attention to a wider range of ways in which the government can create value for the public in what they do, how

**Table 2 Theories of public administration**

	Traditional public management	'New public management'	Public value
Public interest	Defined by politicians/experts	Aggregation of individual preferences, demonstrated by consumer choice	Individual and public preferences (resulting from public deliberation)
Performance objective	Managing inputs	Managing inputs and outputs	Multiple objectives: <ul style="list-style-type: none"> <li>• service outputs</li> <li>• satisfaction</li> <li>• outcomes</li> <li>• maintaining trust/legitimacy</li> </ul>
Dominant model of accountability	Upwards through departments to politicians and through them to Parliament	Upwards through performance contracts; sometimes outwards to customers through market mechanisms	Multiple: <ul style="list-style-type: none"> <li>• citizens as overseers of government</li> <li>• customers as users</li> <li>• taxpayers as funders</li> </ul>

	Traditional public management	'New public management'	Public value
Preferred system for delivery	Hierarchical department or self-regulating profession	Private sector or tightly defined arms' length public agency	Menu of alternatives selected pragmatically (public sector agencies, private companies, joint venture companies, community interest companies, community groups as well as increasing role for user choice)
Approach to public service ethos	Public sector has monopoly on service ethos, and all public bodies have it	Sceptical of public sector ethos (leads to inefficiency and empire building) – favours customer service	No one sector has a monopoly on ethos, and no one ethos is always appropriate; as a valuable resource it needs to be carefully managed
Role for public participation	Limited to voting in elections and pressure on elected representatives	Limited – apart from use of customer satisfaction surveys	Crucial – multifaceted (customers, citizens, key stakeholders)
Goal of managers	Respond to political direction	Meet agreed performance targets	Respond to citizen/user preferences, renew mandate and trust through guaranteeing quality services

Source: G Kelly, G Mulgan and S Muers, *Creating Public Value* (London: Strategy Unit, 2002).

they do it, and the relationships they build with society in the process.<sup>88</sup> This gives rise to Mark Moore's concept of the 'strategic triangle' as a way of describing the full range of ways by which government departments and agencies can create value for citizens.<sup>89</sup>

Public value has the potential to transform the way the UK government manages national security. Public value is already being used as a framework for reform in some US intelligence agencies and closer to home is being operationalised in areas of public service.

One innovation introduced by the Labour government in the late 1990s was the introduction of a targets-based culture, which strove to measure the improvement in public services by developing a series of public service agreements (PSAs) between departments and the Treasury. PSAs set out the targets the department will seek to deliver in return for the public money it receives from the Treasury. PSAs span the whole of government including the national security architecture.

For example, box 1 shows a current PSA target for the FCO.

### ***Box 1. PSA 3 on conflict prevention, FCO***

By 2008, deliver improved effectiveness of UK and international support for conflict prevention by addressing long-term structural causes of conflict, managing regional and national tension and violence, and supporting post conflict reconstruction, where the UK can make a significant contribution, in particular Africa, Asia, Balkans and the Middle East. **Joint with the Ministry of Defence and the Department for International Development.**

Assessments are made on the basis of targets and sub-targets. For example the FCO's nine PSA targets for the 2004 spending review were underpinned by 71 indicators or sub-targets. Where applicable a PSA target will also state whether a target is to be shared with another department. In this case the target for conflict prevention is shared between the FCO, MoD and DFID. A summary of progress is taken, and the performance table sets out how the department is doing on its PSA targets (see table 3).

**Table 3 PSA 3 Conflict prevention**

			Progress		
A1	Afghanistan	<b>Amber</b>	<b>Amber</b>	Green	
A2	Balkans	<b>Amber</b>	<b>Amber</b>	<b>Amber</b>	
A3	DRC	<b>Amber</b>	<b>Amber</b>	<b>Amber</b>	
A4	Iraq	<b>Red</b>	<b>Amber</b>	<b>Amber</b>	
A5	MEPP	<b>Red</b>	<b>Red</b>	<b>Amber</b>	
A6	Nepal	<b>Amber</b>	<b>Red</b>	<b>Red</b>	
A7	Nigeria	<b>Amber</b>	<b>Amber</b>	<b>Amber</b>	
A8	Sierra Leone	Green	<b>Amber</b>	<b>Amber</b>	
A9	Sudan	<b>Amber</b>	<b>Red</b>	<b>Red</b>	
B1a	UN peacekeeping	<b>Amber</b>	<b>Amber</b>	<b>Amber</b>	
B1b	UN peacekeepers	Green	Green	Green	
B2	African peacekeeping	<b>Amber</b>	<b>Amber</b>	<b>Amber</b>	
Total indicators	12	Overall rating	<b>Amber</b>	<b>Amber</b>	<b>Amber</b>

Source: SR04 2005–2008 PSA target assessment progress, FCO, 2007

Each department monitors their agreed targets using a ‘traffic light assessment’. Confusingly the traffic light assessment is not uniform across departments and there are one or two subtle distinctions between the three as table 4 demonstrates.

Overall, the three departments believe that the government’s PSA on conflict prevention has seen *some progress* (DFID), and is *broadly on course with some slippage* (FCO/MoD).

Aside from the development of PSA targets, departments have also been required to respond to the Sir Peter Gershon’s review of public efficiency. While departments were given efficiency targets to meet (including lowering the headcount in departments) these were separated from the PSA targets and monitored by the Office of

**Table 4. Progress on conflict prevention**

Colour/Dept	Red	Amber	Green
MoD	<b>Not on course</b>	<b>(Broadly) on course</b>	Achieved or on course
FCO	<b>Slippage</b>	<b>(Broadly) on course</b>	Met early or on course
DFID	<b>Progress has been slower than expected</b>	<b>Either broadly in line with plans and expectations, or there has been some slippage</b>	As either exceeding or in line with plans and expectations

Government Commerce rather than the Treasury or the Delivery Unit.<sup>90</sup>

A target culture based solely on a drive for ‘value for money’ will not make government more efficient and effective in the long term. If a government department is going to change effectively it must understand the external and internal contexts in which it finds itself. The current ‘targets-based culture’ focuses on efficiency gains in the public sector not on meeting the goals and objectives of a particular policy. Debates on conflict prevention for example are complex and nuanced discussions, the subtleties and variations of which cannot be understood by such rigid processes.

Public value introduces new operational objectives for policy (eg increased legitimacy) alongside conventional goals, ensuring that the actions of government are more likely to reflect the full range of expectations that citizens have of governments. It recognises that departments and agencies need to be trusted, accountable and capable of *preventing* problems as well as efficient in addressing issues when they arise. And this inevitably introduces new forms of data and evidence into decision-making processes – not least the views of the

public itself. The old tools of governance and analysis therefore need to be part of a much wider repertoire in the future.

## Conclusion

Throughout the last century the basic structure of government has remained remarkably stable. The principles of organisation are simple and few, although they are not particularly consistently applied. Since the early 1990s the government has seen a period of dramatic and rapid change and has attempted to respond to the emerging complexities of the new security environment with traditional structures and processes of government. A handful of initiatives have been successful, the majority have not.

A central argument put forward in the first part of this pamphlet is that the government has failed to take into account Brown's warning in his speech to RUSI that 'there is a danger that we fail to stand back and reflect and . . . make the long-term cool-headed assessment we need to have about the likely repetition of such events and to decide what, for the long term, needs to be done to strengthen our security'.<sup>91</sup> The national security strategy is a case in point. Based on a political timetable allowing a preparation time of only a few months, the strategy cannot hope to influence change in the national security architecture. To give a sense of perspective the government's counter-terrorism pamphlet took approximately 12 months to develop while the national security strategy of the Netherlands took up to five years to conceive, develop and be made public.

And yet, the new security paradigm demands a different approach by the UK government. It requires new thinking on how government is designed and how it operates. Collaboration, for example, will be central to this approach. The test of whether this more integrated security concept is translated into practical effect will depend, in the UK at least, on whether government is reformed to meet the new challenges, in terms of adjusting departmental boundaries between the MoD, FCO, DFID and Home Office, questioning relevant budgetary arrangements, and creating a stronger central coordinating capacity in the Cabinet Office area.<sup>92</sup> With the exception perhaps of

emergency planning, the general feeling is that the government remains entrenched in departmental silos, and discussions of more collaborative initiatives are unlikely to lead anywhere.

The UK's national security architecture remains closed to experimentation and reform. Instead the government has, more often than not, mixed activity with achievement. This pamphlet argues that tinkering with the current system without applying a robust approach to adapting the national security architecture may have one terrible consequence.

Part 2 of the pamphlet outlines how the government can transform itself in response to the new security challenges of the twenty-first century. The changes revolve around three essential principles of adaptation in government:

- the need for a holistic approach to national security, based on systems thinking, which allows individuals, agencies and departments to take a much broader perspective than they do currently; this includes seeing overall structures, patterns and cycles in systems, rather than identifying only specific events or policy options
- the creation of an open and transparent national security architecture for ministers, civil servants and the government's strategic partners – the private sector and the wider public
- a transformation of the national security architecture based on the principles of public value, an intellectual framework for reform in government that, although still in its infancy, has huge potential for changing the way in which the government measures its performance and maintains the trust and confidence of society.

# **Part 2**

## **Adapting to the twenty-first century**

---



# 3. Managing the system

*One of the great mysteries of organisational life is how agencies survive year after year without a clue as to their mission.*

Paul Light

The government does not think in terms of national security as a comprehensive framework for organising relevant departments and agencies. The Security Service (MI5) ‘protects national security’ as does the newly slimmed down Home Office, the Secret Intelligence Service (MI6) functions ‘in the interests of national security’, while the FCO works for UK interests in a safe, just and prosperous world.

In the early phase of the project Demos brought together a group of experts on subjects including security, civil liberties, defence, emergency planning and business to help develop working definitions of ‘security’ and ‘national security strategy’ to get a better sense of the issues, stakeholders and operating space. ‘Security’ was considered to be:

*The confidence and capacity of the individual, community and state to anticipate and respond effectively to threats or hazards that may endanger their safety.<sup>93</sup>*

At the same time it was decided that the role of a national security strategy should be:

*to integrate preventative and contingency measures in order to anticipate and respond to significant threats or hazards to the nation.*

What is interesting to note is that both definitions emphasise an anticipatory approach to security and the role of ‘confidence’ at the individual, community (which can include a ‘group of organisations’) and state levels. Implicit in the first definition is the admission that the government ‘can never guarantee that we will get 100 per cent success but we do get 100 per cent effort from the security services’.<sup>94</sup>

The definition is also important because it makes explicit the fact that national security no longer remains solely in the hands of the state. For example, 85 per cent of the critical national infrastructure, those elements that are crucial to the continued delivery of essential services to the UK, is owned by the private sector.

### **A holistic approach**

In pursuing ‘national security’ as a concept for organising government, both the government and the Conservative Party have mooted the idea of a holistic approach to national security. But the challenge to national security in the twenty-first century demands a far more radical approach than has been suggested thus far. Such an approach has the potential to transform how government manages national security.

First, it has the potential to transform how the government develops and implements national security policy. There are useful parallels here with the approach to ‘UK Resilience’. For example, the government has seen the benefits of taking a holistic approach to ‘UK Resilience’ as prior to the Civil Contingencies Act there were ‘no structured processes for detecting and acting on emergency risks . . . and no ready mechanism for identifying and sharing knowledge of the way in which major emergencies could challenge societal interdependencies’.<sup>95</sup> A national security approach could bring together disparate parts of the system while placing global risks in context with one another giving an overview of the state of national

security. This will be particularly important given that international terrorism has become the focus of much of Whitehall's attention on 'national security' to the detriment of other threats and hazards.

Second, organising government around a revised concept of national security will force departments and agencies to adapt to new structures and cultures in government. Perhaps the most important and difficult change in this process will be moving away from the tired, and inappropriate, focus on the 'machinery of government' to thinking about the 'national security system'. This is not just an issue of semantics, as David Omand argued in a lecture at King's College London: 'The first idea is that organisations are more like people than machines. They have moods, they can sulk, they can have nervous breakdowns, and they can show all the symptoms of paranoia.'<sup>96</sup>

### **The machine is dead**

In his seminal pamphlet on why governments must learn to think differently, Jake Chapman argued that the dominant approach to policy-making was based on mechanistic and reductionist thinking (see table 5). This approach to policy, he argued, was deeply engrained in the culture of government, as he suggests:

*A conversation with a civil servant, politician, or senior public sector manager will yield a large number of phrases based upon the notion that government and organisations are machine like.<sup>97</sup>*

Mechanistic thinking assumes a rational approach to policy-making where problems are reduced into their component parts and are then tackled in a linear manner, pursued by different units across Whitehall. For example, the government's counter-terrorism strategy (CONTEST) – based on four strands: prevent, pursue, protect and prepare – was originally designed as a cross-government strategy but invariably individual departments and agencies took responsibility for separate aspects of the strategy and focused resources on their own work. While this was not an issue *per se* it meant departments

ignored holistic objectives and the possibility of taking a more collaborative approach. Remarking on the counter-terrorism strategy, one senior civil servant suggested:

*There are some fundamental flaws in the process . . . it started off with ‘what are you currently doing to contribute to that particular bit’ and we still haven’t worked out the balance between pursue and prevent . . . I would go to CONTEST meetings and there would be no discussion whatsoever on Iraq and Afghanistan – that was seen as a separate thing.*

**Table 5. Why governments need to think differently**

	Mechanistic thinking	Systemic thinking
<b>Management style</b>	Scientific management Command and control	Learning organisation Autonomy and innovation
Aim	Control the situation	Learn how to manage better
Presumptions	Organisations and agents are both controllable and predictable	Organisations and agents are adaptive and likely to respond non-linearly
Metaphor	Machine ‘levers’, ‘driving change’, ‘stepping up a gear’	Organism ‘adaptability’, ‘evolution through innovation’
Strategy	Centralise control with clear separation between design (policy) and operations	Delegate and grant autonomy so as to maximise local flexibility Ability to handle variation
<b>Thinking style</b>	Reductionist – break the problems down into smaller components	Holistic – retain the connections between components, discard detail

	Mechanistic thinking	Systemic thinking
Aim	Find a solution based on detailed analysis of how the parts work	Make an improvement based on identifying feedback and interactions between issues
Works best with	Complicated predictable problems for which there are agreed goals and recognisable solutions	Complex issues that involve multiple agencies and which have so far resisted all attempts at improvement
Epistemology	Presumes existence of objective facts to resolve decisions and disputes even in the social domain	Recognises the existence of different perspectives based on different values, goals and culture; problem-solving explicitly pluralist

Source: J Chapman, 'A systemic perspective on public services', Demos, London, 2005.

The underlying problem, as illustrated above, is that mechanistic thinking makes an unreasonable number of assumptions about the intended objectives of each component of a policy area while failing to take into account the broader picture. This inevitably leaves ministers and policy-makers unable to manage unintended consequences that arise from their policy decisions further downstream.

Reducing policy to distinct issues and areas is not a problem in itself; it is only when civil servants and ministers fail to take into account the broader picture that problems invariably arise. This may be for several reasons including an inability to grasp the issue and understand the complexity of the problem. Instead, 'our learnt instinct is to troubleshoot and fix things – in essence to break down the ambiguity, resolve any paradox, achieve more certainty and agreement, and move into the simple system zone'.<sup>98</sup>

Mechanistic thinking also emphasises the importance of pursuing an evidence-based approach to policy development. Acting on evidence of what works can be highly effective but it also assumes a number of factors that are not universally true.

First, it presumes that the evidence collected in one context will apply in another. For example, in conversations regarding the shift in resources from Iraq to Afghanistan, one contractor working for a private security company explained that he had been chosen to present a paper on policing in Afghanistan on the basis that he could draw on ‘similar experience and evidence of what worked from his time in Iraq’.<sup>99</sup> In other words there is a danger of basing policy solely on available ‘evidence’ as it presumes that context is relatively unimportant or is sufficiently similar. Context is critical and varies significantly.<sup>100</sup>

An evidence-based approach also presumes a linear relationship between cause and effect. However, complex systems involve numerous feedback loops, which result in non-linear behaviour. Change in such systems is at least as much to do with internal structure as with external interventions. In the context of fragile states, for instance, the UK government recognised this problem. In 2004 the Prime Minister’s Strategy Unit (PMSU) developed a methodology to forge a common understanding of countries at risk of instability (CRI), stating:

*The right response in each situation should emerge from a sophisticated understanding of the country and regional dynamics, and the political and other resources that can be mobilised. In addition to country- or region-specific actions, global policy responses are also needed to enhance stability, eg to control conflict financing, reduce international organised crime, or increase peacekeeping capacity.*<sup>101</sup>

Central to the idea of the CRI assessments was that there would be a continuous process of learning that would be shared across government. A number of exercises were run in government using the

new methodology and, although there was some limited success, ultimately the methodology was dropped by the Strategy Unit as departments claimed they already carried out their own analysis. As one report has suggested, stove-piped analyses by single departments tend to miss the cross-sector linkages that contribute to the dynamics of instability and failure.<sup>102</sup> In reality the methodology was a victim of the politics of Whitehall, which obstructed much of the good work from occurring.

Finally, evidence on which policy is based will inevitably be quantitative and as such conceal as much as it reveals. Unintended consequences, which occur in all areas of public policy, are systematically ignored because the evaluation measures only intended outcomes.

The importance in identifying unintended consequences was recently illustrated in an Acbar (Afghanistan relief agency) report published in 2007 on aid distribution in the country. The report warned that donors' political objectives were distorting aid delivery by channelling most of the money to areas where agencies were unable to operate freely, neglecting other parts of the country. The report cited a disproportionate amount of aid that was being delivered to insecure or opium-producing areas, overlooking relatively stable areas and 'creating perverse incentives – for provinces to create insecurity to attract resources'.<sup>103</sup>

### **Networked security**

We recommend that the government adopt a systems approach if it is to remain cognisant of the complexities of the twenty-first-century security environment. This will be especially important as, for example, the process of reductionism will be further tested by the emergence of wicked problems. There is a growing literature on Whitehall's lack of strategic approach to 'wicked' problems. 'Wicked' problems, like national security, are 'problems which are unbounded in scope, time and resources, and enjoy no clear agreement about what a solution would even look like, let alone how it could be achieved'.<sup>104</sup> Wicked problems have ten characteristics:

1. Each attempt at creating a solution changes the understanding of the problem.
2. Since you cannot define the problem, it is difficult to tell when it is resolved.
3. There are no unambiguous criteria for deciding if the problem is resolved.
4. There is no immediate and no ultimate test of a solution to a wicked problem.
5. Every implemented solution to a wicked problem has consequences, some of which are unforeseeable or adverse.
6. Wicked problems do not have a well-described set of potential solutions (it's a matter of individual judgement).
7. Since every wicked problem is essentially unique, there are no 'classes' of solutions that can be applied.
8. Every wicked problem can be considered a symptom of another problem (there is no constant or 'root' problem underlying others in the set).
9. The causes of a wicked problem can be perceived in numerous, changing ways.
10. There is an unreasonable expectation that the team working on the problem will find a satisfactory solution, preferably the first time.<sup>105</sup>

Wicked problems are too complex and large to be directed by one department; they require a multitude of agencies, private sector and voluntary organisations to be managed in a collaborative network. Unsurprisingly 'wicked' problems have a major impact on how the government allocates resources, and which department is accountable for what. This is becoming increasingly true as wicked problems interact with each other, such as international terrorism and organised crime.

Finally, a networked approach also questions the traditional command and control approaches to national security. As illustrated

above the complexity of today's security environment means that no one individual or department will be in overall control and this will have an effect on the ability to 'command' multiple stakeholders.

For example, in Iraq coalition governments initially used their respective armed forces to train local police but as the conflict progressed governments took the decision to contract out the training to the private sector creating longer chains of command and distributing authority and responsibility to the relevant parties involved. This meant that at any one time a range of organisations were training the police, to a range of standards, and for different (but nevertheless legitimate) reasons. As such no one individual, organisation or government was ultimately responsible for the training of police in Iraq yet it was seen as a fundamental prerequisite for security in the country.

Democratically this is an obvious cause for concern as with the distribution of responsibility comes the difficult task of identifying which government department or individual is accountable for a decision. Furthermore it raises questions over leadership. For example, conflict prevention, as illustrated in part 1 of this pamphlet, is a policy area shared by three government departments, each one signing up to a common set of targets. But who is accountable for the work of the three departments on conflict prevention? Looking on the websites of the MoD, FCO and DFID, for instance, provides no answer and on closer inspection no minister in each of the three departments holds the brief for conflict prevention. The lack of leadership and accountability on shared policy areas greatly weakens the ability of government to respond to the challenges it faces. And while civil servants might shift into informal networks based on policy areas the lack of accountability for the government's policies and operations severely limits the ability of government to demonstrate success, learn lessons from mistakes and articulate progress to the wider public.

A command and control approach in government is becoming redundant in a complex world and will continue to be the case, as the academic Elaine Scarry suggests, with the empowerment of local,

private and informal actors in the provision of security and resilience. In an innovative analysis of Flight 93 and the plane that crashed into the Pentagon she notes:

*When the plane that hit the Pentagon and the plane that crashed in Pennsylvania are looked at side by side, they reveal two different conceptions of national defence: one model is authoritarian, centralised, top down; the other, operating in a civil frame, is distributed and egalitarian. Should anything be inferred from the fact that the first form of defence failed and the second succeeded? This outcome obligates us to review our military structures, and to consider the possibility that we need a democratic, not a top-down, form of defence.<sup>106</sup>*

In terms of resilience this latter point is especially important and demonstrates the benefits of an adaptable and distributed networked approach. For example, an estimated 2.2 million commuters were in New York City on 9/11. Soon after the second tower collapsed hundreds of thousands of residents and tourists were blocked from escaping as streets were clogged with debris and public transportation came to a standstill. Thousands of people soon began to converge on the waterfront and within seven hours between 300,000 and 500,000 people were evacuated. There was no plan in place, no previous exercises had been done for this type of evacuation and the only direction given to the boats and vessels was a short radio call 'All available boats'.<sup>107</sup>

### **Towards the collaborative state**

The UK government will increasingly have to take a networked and collaborative approach to the changing security environment. In some cases the government has attempted to do this but there has been little impact on the structures and processes of the security architecture especially when compared with the reorganisation and culture change that has occurred in the area of public services reform. This is primarily because the notion of joined-up government has

never really addressed the underlying logic of Whitehall, challenging departmental structures or incentivising policy-makers to work more effectively with practitioners and external stakeholders.

The systematic and deep structural change that has occurred in Whitehall on education, for example, has never occurred within the security architecture. Instead those within national security have sought to protect their own turf while pooling limited resources. The creation of the Post Conflict Reconstruction Unit (now the Stabilisation Unit) is a perfect example. The unit was created prior to broad agreement about its objectives, mandates, capabilities and authorities.<sup>108</sup>

And while limited reforms to departments might improve the system of collaboration the main reform would be adapting the role of the Cabinet Office. This would mean shifting some of the strategic responsibility of departments to the centre, an approach that would be fiercely contested by ministers and senior civil servants. The weakness of the current system is illustrated by one senior civil servant in the Cabinet Office:

*In the system that we operate in, departmental ministers and permanent secretaries have executive responsibility. So the Cabinet Office can't instruct them to do anything. We do coordinate but I would say that's the sort of least value-added . . . In the sense that coordination tends to produce solutions that are not controversial or which are lowest common denominator . . . because we don't have directive power, it's the power of analysis and argument that finds a way forward or doesn't, because that's actually all we have to bring to bear.*

And senior civil servants across Whitehall see the benefits of taking a different approach to the 'hole at the centre'. Take the following examples:

*We need a stronger joint planning staff in the Cabinet Office . . . looking at the way the machinery is working . . . it is pretty clear*

*to me that better combined planning capability could make a big difference to this already.*

Senior civil servant, MoD

*For me quite a lot of paths lead back to the need for a stronger central capacity.*

Senior civil servant, Home Office

But as Simon Parker suggests this would require a tremendous effort from Whitehall as organisations:

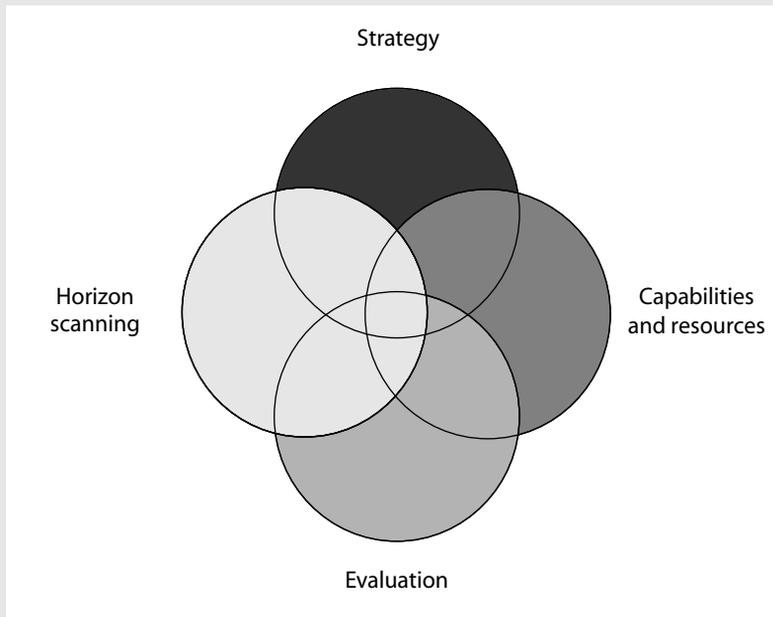
*all too easily become mildly competitive fiefdoms that sometimes resist connecting with the outside world. This is compounded by the closed relationship between civil servants and ministers, which has had the effect of screening the centre of government off from robust external challenge . . . short tenures mean that few cabinet members have the time or energy to reform their delivery machine except through big bang restructurings. The situation is not good for civil servants either – in the past they have often risked looking upward to the minister and not outward to the world they seek to change.<sup>109</sup>*

### **A new approach to national security**

The development of a UK national security strategy has the potential to transform the government's approach to national security.

To ensure a strategic approach to national security is made a reality, however, the strategy must be complemented by the creation of a national security secretariat based in the Cabinet Office. Creating this unit means a number of relatively *small* but nevertheless radical changes must occur in terms of how the Cabinet Office manages Whitehall.

First and foremost a national security secretariat must assume some authority and resources to develop, direct and evaluate national security policies from the centre. This would be a major step forward for government and would be seen as a threat to the power and

**Figure 4. Roles of a national security secretariat**

Source: Demos

authority of individual departments. But the reasons for change are clear. The government can no longer ‘muddle through’ on issues as important as defence and foreign affairs, organised crime and counter-terrorism. A coherent approach to national security is crucial. The secretariat would have four main roles (see figure 4).

### **A national security strategy**

A national security strategy<sup>110</sup> must be under the direction of the prime minister and cabinet, together with key departments and agencies (intelligence and police). The strategy should be validated by both internal and external stakeholders before being put before Parliament.

Gordon Brown has already taken a proactive approach to national security by announcing that the government will publish a strategy in the autumn and by convening the National Security Committee, the Ministerial Committee on National Security, International Relations and Development (NSID). However, the design and support of a national security strategy relies on a Cabinet Office structure that has also adapted to meet changing circumstances. One idea would be to subsume the defence and overseas and intelligence secretariats into a large national security secretariat that the Civil Contingencies Secretariat would also plug into.

This would have the added benefit of drawing together a number of loose strands in the Cabinet Office structure and strengthen the secretariat's new mandate in Whitehall. In doing so the new secretariat would continue to perform its four traditional roles of *influencing*, *negotiating*, *coordinating* and *directing* but would also take on the additional roles of *evaluating* and *leading*. Thus the co-ordination of national security would be overseen by a more robust, influential and powerful organisation.

### **Capabilities and resources**

A national security secretariat would have the following roles:

- Identify what capabilities and resources are needed for the national security architecture in collaboration with departments and agencies.
- Support the coordination of capabilities and resources in the national security architecture.
- Supervise the Joint Intelligence Committee (JIC) including the management and independence of the whole intelligence community.
- Maintain the readiness of the central crisis management facility and support effective crisis management arrangements across central government.
- Support the development and publication of a national threat assessment by the JIC for public consumption.

A secondary feature of the secretariat would be a new role in supporting and coordinating the allocation of a national security budget together with departments and HM Treasury. Based on independent evaluations by the secretariat in conjunction with the PMDU, national security policies and initiatives would be measured against a public value framework.

### **Horizon scanning**

A third role for the secretariat would be to develop and maintain a horizon scanning capability. The role of the secretariat would be twofold. First, it would work with departments, for example the Directorate of Policy Planning team at the MoD (which looks forwards up to 30 years) the FCO policy planning team and DFID as well as the Civil Contingencies Secretariat's Domestic Horizon Scanning Committee (which looks 12 months ahead). The aim would be to develop a common picture among government and strategic partners on global risks from across a time spectrum of 12 months to 30 years and foster a common understanding of the likely nature and extent of their impact on the UK.

For example, the secretariat might bring together a major scenario planning exercise with departments, NGOs and consultancy bodies on Europe and energy security looking forwards to 2050, or develop some medium-term scenarios with the MoD, DFID and FCO on conflict prevention in 2020. The results of the scenario planning work would then provide the basis for a deliberative strategy in Whitehall and influence policy recommendations.

Finally, the secretariat would develop close links with industry and academia, such as the scenarios team at Shell or the James Martin Institute at Oxford University. These collaborative partnerships would aim to complement, interrogate and support existing work by departments and the secretariat on scenario planning work.

### **Evaluation**

The third and perhaps most valuable role of a newly created national security secretariat would be its role in measuring and evaluating the

performance of the national security architecture, existing policies and initiatives. For example, on behalf of the prime minister and cabinet and with support from relevant departments it could be tasked with evaluating the government's approach to counter-narcotics operations in Afghanistan. The work would be carried out with the PMDU and would result in a presentation on the strengths and weaknesses of current strategy, potential opportunities for policy decisions going forwards and likely threats to its success.

As part of this new role in evaluating national security, the secretariat would also need to disseminate lessons learned from policies, pilots and operations across departments in Whitehall. Although the responsibility for implementing the lessons would be with the department the secretariat would aim to support them in this role and identify where synergies could be found across Whitehall.

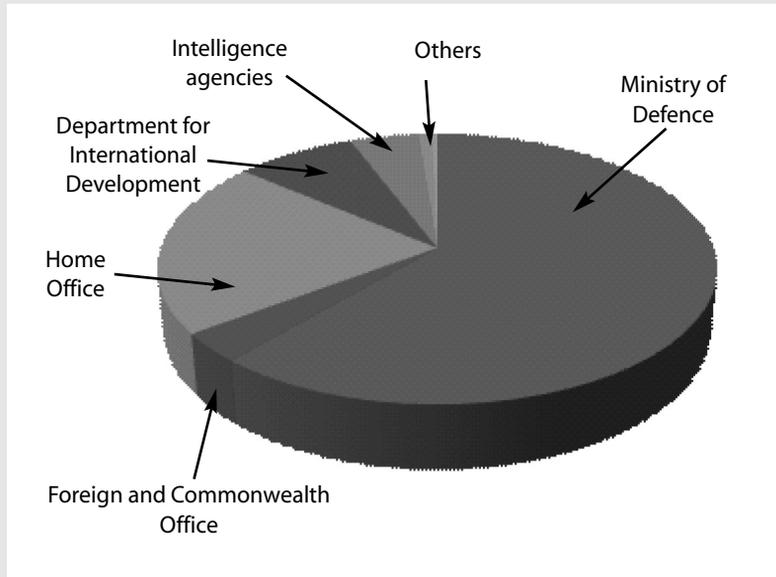
### **A national security budget**

Alongside a national security strategy, cabinet committee and secretariat, the government should consider initially developing an 'indicative' national security budget, bringing together the existing spending plans of the MoD, FCO, Home Office, intelligence agencies and other relevant budgets of the national security budget (such as the budget of Transec in the Department of Transport).

The aim of a national security budget would be to take a holistic approach to spending on national security and in doing so seek to rebalance the budgets of existing departments. A key issue behind the existing mismatch between resources and the role of government is the fact that currently departments prepare their own budgets according to their own analysis and assessment of threats and hazards to the UK. In the future all analysis and assessment should be brought together by the new national security secretariat in collaboration with government departments so that an indicative national security budget can be prepared.

Taking the relevant departments and agencies (including the Metropolitan Police) the national security budget of the UK equals approximately £48 billion. Based on the departmental budgets for

**Figure 5. A theoretical national security budget for the UK (based on government spending for 2006/07)**



Source: Demos

2006/07 the budget shows the stark reality of the present allocation of funding for the UK's security (see figure 5).

### **National security priorities**

To ensure a robust, comprehensive approach to the threats and hazards facing the UK, the Prime Minister and the national security secretariat should identify three to five key priorities for UK national security. David Miliband, the Foreign Secretary, and a small team are currently 'refreshing the FCO's strategy', which is questioning the relevance of the FCO's ten priorities. No department is able to manage so many priorities, particularly when some of them will be 'wicked' problems like international terrorism and climate change.

These key priorities will be threats or hazards that are of serious and immediate concern and have the potential to cause widespread destruction. They might include counter-terrorism, serious and organised crime, and counter-proliferation. As a reflection of the importance of these threats and hazards of immediate concern, the government should create three to five new senior civil servant posts, based within the national security secretariat, to assist the government and its key stakeholders on the development of policy and keep a watching brief on progress.

These posts should be filled not by 'policy tsars' nor Churchillian 'overlords', but by senior civil servants whose role will be to ensure a holistic approach is being taken by government. Each post will have access to limited resources to allow for initiatives or policy support. They will work hand in glove with relevant agencies and units in Whitehall. Each senior civil servant will be accountable to the head of the national security secretariat and the Prime Minister.

This will be further complemented by the development of specific networks in government on important areas of national security. While departments will continue to manage the everyday business of defence, foreign affairs and development, among others, new networks will be developed within government in areas such as 'climate change', 'conflict prevention' and the 'governance and the rule of law'.

These networks, which in some cases already exist, will need to be made accountable to ministers and Parliament. For example, a senior civil servant could be the network manager for conflict prevention. He or she would be accountable to a minister (perhaps from the MoD, FCO or DFID) and for bringing together the work of the whole of Whitehall and agencies on the subject. Should a select committee wish to create an inquiry into the government's work on conflict prevention they would be able to call on both the minister and network manager, who in turn could request information and progress reports from the system.

A systems approach to national security is crucial if government is to take a holistic approach to the risks facing the UK. Designing such

a system, however, will succeed only if it is based on the principles of openness and transparency, by collapsing walls between departments and agencies, developing new ways of sharing information across government and with its strategic partners, and, last, by becoming more accountable to Parliament and society.

## 4. From 'need to know' to 'need to share'

*The traditional culture of secrecy will only be broken down by giving people in the United Kingdom the legal right to know. This fundamental and vital change in the relationship between government and governed is at the heart of this white paper.*

Tony Blair

*Your Right to Know: The government's proposals for a Freedom of Information Act*

*With confidence and competence so much lower than they should be, it is not surprising that Whitehall fiercely defends its tradition of secrecy. The Official Secrets Act and the Thirty Year Rule, by hiding peacetime fiascos as if they were military disasters, protects ministers and officials from embarrassment. They also ensure there is no learning curve.*

Sir John Hoskyns, former head of Mrs Thatcher's Downing Street Policy Unit<sup>11</sup>

*We recommend a greater transparency of the threat level and alert state systems as a whole, and in particular that more thought is given to what is put in the public domain about the level of threat and required level of alert. After the July attacks there is an even greater need for members of the public to be better informed.*

Report into the London terrorist attacks on 7 July 2005,  
Intelligence and Security Committee

*Wikis and blogs allow us to stand on the shoulders of others and have brilliant ideas we would not have had otherwise in the service of protecting our country.*

Calvin Andrus, Chief Technology Officer,  
Center for Mission Innovation, Central Intelligence Agency

## **A culture of secrecy**

Government departments and agencies still retain a culture of secrecy that is more suited to the nineteenth century than the present. Open government may be a reality in some parts of Whitehall such as science and innovation but it is far from evenly spread. Today the public can look up the performance of their police force, view the minutes of departmental committee meetings, learn how a government committee processes intelligence, and read the latest counter-terrorism threat assessment on the Security Service's website.

The consequence is that there are few fields of government activity that have not, at least somewhere, been through a revolution in knowledge. But although that may be true in terms of *process*, significantly, the *mindsets* of many civil servants remain closed to change, preferring instead the anonymity that government often brings. During a revolution in information and communication technology this carries the risk that government will make bad decisions not because it has too little information, but rather because it has too much information about the wrong things.

The problem in the government lies in part with the classification system. The fault does not lie solely with the system itself but rather with the culture of secrecy it has created within government. In the current system, the burden is placed on the originator, the individual in government who creates the document. And as the former diplomat Carne Ross explains, the incentives tend to promote secrecy over openness:

*When you learn how to handle documents, for instance, you are taught that the originator of the document must classify it . . . You are taught that only those documents that would not*

*perturb you if they were handed out to passers-by on the street can be designated 'unclassified'. Unsurprisingly therefore, almost every document produced in the Foreign Office is classified 'restricted' or above.*<sup>112</sup>

While in this case the Foreign Office has succeeded in encouraging officials to downgrade the classification of many documents for financial reasons, the vast bulk of such internal communications remains classified in some form or other. And with the increase in electronic information the problem of storing such volumes of information will continue to be a significant area of concern.

### **Leaking secrets**

Much has been written on the balance that governments must maintain between secrecy and openness. In a democracy a government needs outside criticism and scrutiny but also requires space to be able to think and argue in confidence, especially on aspects of national security, 'without a running commentary of doubt and criticism'.<sup>113</sup> Secrecy, therefore, permits policy-makers and practitioners to explore and debate different options, consider alternatives, and weigh the consequences of their decisions before opening up the process to public consultation and scrutiny.

But secrecy also has the potential to undermine well-informed judgement by limiting the opportunity for input, review and learning lessons, thus allowing individuals and departments to avoid the type of scrutiny that might challenge long-accepted beliefs and ways of thinking. As Carne Ross argues:

*Policy-making does not benefit from secrecy or privacy . . . information is not reliable unless it is constantly re-examined, checked and tested against reality. Others, particularly those most affected by policy, must be allowed to participate, or at least to be heard.*<sup>114</sup>

One consequence of too much secrecy is that it can lead to leaking of

information. As the ethicist Sissela Bok argues:

*Leaking has a symbiotic relationship with secrecy. Without secrecy there would be no need to leak information. As government secrecy grows and comes to involve more people, the opportunities to leak from within expand; and with increased leaking, governments attempt to shore up secrecy.*<sup>115</sup>

This is particularly important because as classifying secrets becomes more layered and complex, so the potential for leaks grows as well. Secrets become vulnerable to betrayal, often from high in the chain of command, which in turn promotes greater disrespect for the system itself.<sup>116</sup> One example of this occurred in early 2007 when a major row erupted after Peter Clarke, the head of Scotland Yard's counter-terrorism command, suggested that details about a major anti-terrorism operation had been leaked to the media. The operation concerned the potential kidnapping and beheading of a serving British soldier. Much of the criticism centred on the government's culture of spin, with the Liberal Democrat spokesman Nick Clegg MP suggesting that 'there was now real evidence that the government's culture of spin was undermining rather than strengthening [the UK's] collective response to the terror threat'.<sup>117</sup>

Although the example above illustrates the dangers of a system that is too secretive, and one that can be easily betrayed, the majority of 'secrets' are leaked for other reasons, such as power struggles between ministers or departments, to avoid an official announcement or to attempt to influence a change in policy. Ultimately leaking appears to reward those within governments whose motivations may be the most dubious – not those interested in a more sustained and consistent approach to promoting greater openness.<sup>118</sup>

## **Opening government**

Following the reforms of the Conservative government in the early 1990s the pursuit of a more open and accountable government was taken up by the Labour Party on coming to power in 1997. Soon after

the election they published a white paper setting out proposals for a Freedom of Information Act. In its opening statement the proposal noted:

*Unnecessary secrecy in government leads to arrogance in governance and defective decision-making. The perception of excessive secrecy has become a corrosive influence in the decline of public confidence in government. Moreover, the climate of public opinion has changed: people expect much greater openness and accountability from government than they used to.*<sup>119</sup>

The statement neatly summed up the case for openness. Secrecy had led to arrogance in government and influenced the decline of public confidence of government, while the public expected government to be more open than they had been previously.

To these factors it is possible to add three other reasons for openness in government relevant to the national security architecture. First, there is a recognition in Whitehall that the government needs to communicate with the public to increase *their* resilience to events and incidents; second, that open government also supports the recruitment of a more diverse group of individuals from society to security and intelligence agencies; and last, that open government remains a method for raising issues in public that seek to either increase awareness of them or lower public expectations about the government's ability to respond to complex matters.

For example, in a speech in early 2007 the new chair of the Serious and Organised Crime Agency (SOCA), Sir Stephen Lander, attempted to lower the expectations of what SOCA could do by suggesting that, while the agency had a budget of £400 million and 4000 agents, 'it had been hamstrung by a mass of old, useless intelligence; and 380 different IT systems that are incompatible, and insufficient funds'.<sup>120</sup>

*I think we're more open than we were five or ten years ago . . . what holds people back in many cases is not institutionalised*

*secrecy, it's probably a lack of trust in how engagement externally is going to be played out.*

Senior civil servant, MoD

*I think it's become much too open, I think quite seriously the ability to do operationally secret work has been compromised by the recent degree of openness and the extent to which things have been put in the public domain . . . the Iraq dossier was a case in point.*

Senior civil servant, FCO

*Need to know . . . has become a default position for hundreds of people across Whitehall: it reinforces the cop-out tendency of managers.*

Senior civil servant, Cabinet Office

Accountability is a fundamental principle of open government. The parliamentary system contains many checks to ensure that a government remains accountable and does not abuse its powers. But the ability of Parliament to scrutinise, enquire and investigate matters on national security is severely hampered by both a lack of resources and political will to strengthen the committee structures.

Furthermore national security is not the focus of one select committee but is spread thinly across a number of them, as well as the Intelligence Security Committee (ISC),<sup>121</sup> which was established by the Intelligence and Security Act in 1994 to examine the policy, administration and expenditure of MI5, MI6 and the Government Communications Headquarters (GCHQ).<sup>122</sup> The weakness of the current system was illustrated recently to me by a retired security official, who explained:

*The Parliament's structure of select committees is for the world of 1960. The Foreign Affairs Committee does something called foreign affairs, the Defence Committee does defence, the Home Affairs Committee does criminal justice and immigration – but*

*it doesn't do terrorism [it does focus on terrorism legislation]. We've got the Science and Technology Committee occasionally venturing into CBRN [chemical, biological, radiological and nuclear] stuff . . . but it's the way it's run at the moment and the specialist advisers who support these select committees, none of whom are really natural security people – that's where you've got the deficiency.*

Furthermore, the lack of scrutiny was described to me by one senior official in government who believed that the system's weakness was a hindrance not a help to government:

*The most obvious example you will find is that they [the committees] are not scrutinising the counter-terrorism strategy or our resilience work and neither is any other committee with the single exception of the odd random intervention of the Intelligence and Security Committee. So there is a fundamental absence of parliamentary scrutiny and it's parliamentary scrutiny that drives Whitehall in the first place into doing things – that's a fundamental weakness.*

Much of the current focus on the accountability of the national security architecture is a product of the intelligence failures over Iraq and the subsequent 'dodgy dossier'. But there is also a renewed interest in the accountability of departments and agencies working on 'national security' since the major expansion of some parts of the architecture, particularly the growth of the intelligence agencies (MI5 in particular). Issues of accountability and scrutiny remain a matter of deep concern and there are signs that the government recognises this.

In an announcement in July 2007 Gordon Brown suggested that the government would first consult the ISC on how parliamentarians should be appointed and how the committee could become a more 'public' committee in the future by allowing more access to its meetings by members of the public and holding open meetings in Parliament. Second, Brown suggested the committee

would be strengthened by a 'beefed-up secretariat' and an investigator. This was welcomed but it soon became apparent that the recruitment of an investigator had been a recommendation of Lord Butler's 2004 inquiry into intelligence and weapons of mass destruction.

Accountability, though, is not solely confined to Parliament but is also a prerequisite for building a relationship between the government and local communities. This is one area where much work has gone on since the London bombings in 2005. On the first anniversary of the attacks, Sir Ian Blair, the Metropolitan's police commissioner, said it was not the police or the intelligence services that will defeat the terrorists, but communities. 'They must be our eyes and ears on the streets and tell us about their concerns.' But this means departments and agencies have got to shift from *communicating to* the public to *engaging with* them about risks, by creating opportunities and spaces for dialogue.

Finally, open government is important in managing the expectations of the public who, as our research found, remain confused, sceptical and often mistrustful of secret information. In the case of the London bombings it was the perception that something, somewhere had gone very badly wrong, a perception given more credence by the admission later on that MI5 had reduced the threat level a month before the attack and that the director general of MI5 had given her assurance of the security situation at a private meeting of Labour whips the day before.<sup>123</sup>

*The idea of a government is that there should be communication between them and the people. It isn't really happening at the moment. The more the better.*

Male, C1C2, London

*I'm not sure what they could tell me but if they have the information I would feel safer knowing it. I don't like the idea of secrecy.*

Male, AB, Birmingham

### **Burden sharing**

If we accept that the private sector and the public are now strategic partners of government then a new relationship must be developed between the three, based on openness, sharing information and feedback. The seeds for developing such relationships have already been sown with a realisation among policy-makers and practitioners that the government needs a network of public and private sector organisations to share the burden in responding to the challenges of threats and hazards. Although much work has been done by departments and agencies the impetus for change has been through legislation.

The Civil Contingencies Act, for example, requires category 1 and 2 responders to share information with each other as part of an integrated emergency planning framework. In doing so the government had to establish a governance framework which ‘gave observable permission to the involvement not only of government practitioners but also of non-practitioners in associations and communities, down to the level of individual citizens.’<sup>124</sup>

Building on this framework the government has also begun to develop a communication strategy on the basis that preparing the public to receive and act on messages from the government and practitioners would enable them to secure their own safety in an emergency.

This is welcome as it recognises the importance in government of starting from a presumption of openness rather than secrecy. The strategy has four key elements.

The first element is to ‘inform and desensitise’ and aims to strip away unnecessary secrecy, while debunking conspiracy theories. One civil servant explained this meant ‘working hard to create a narrative as the government understands there is often an information “vacuum” and something needs to fill it’. Second, the strategy has to ‘demonstrate competence and coherence’, arguably a weakness of government and one that has been recently exposed by the foot and mouth crisis of September 2007 with the revelation that a broken

pipe was the source of the outbreak of the disease. Third, the government strategy aims to 'reassure the public and build confidence and trust in their actions.' Finally, the communications strategy was designed to help build public resilience by instilling life-conditioning behaviour, before and after a crisis.<sup>125</sup>

However, doubts remain as to whether this strategy has led to change in government and local authorities. This is compounded by authorities being exposed to a vast amount of information. According to one study by De Montfort University, for example, information for local emergency planning is offered from a range of central resources. The challenge for those receiving information, therefore, is to process and prioritise potentially conflicting advice in a local context and, in doing so, risk missing important information among a potentially vast amount of communication.<sup>126</sup>

### **A responsibility to provide**

Pressure on opening up the security architecture has also been driven from real and perceived failings within government. For example, the intelligence agencies in the UK and US have been criticised for missing vital signs that might have prevented 9/11 and the July 2005 bombings in London. Critics frequently point out that both MI5 and MI6 are unable to 'connect the dots' as agencies remain stove-piped and coordination limited. There is an element of truth in the claim.

Obstacles to sharing information between departments and agencies are extensive. This may reflect the fact of the choice of an organisation not to share information outside its own walls or simply a lack of awareness that knowledge of an issue or a situation would be of use elsewhere in the system.

The recent capability reviews of government departments highlight this: 'There is not yet a general culture of knowledge sharing across Cabinet Office units'; the DFID should 'establish fora for regular engagement with, and exchange of best practice and knowledge among NGOs'. Regarding the work of the MoD, 'a variety of external stakeholders perceive insularity and reluctance to consult and work with others in the formation of strategy and policy' while

the emphasis at the FCO on keeping its information secure ‘inhibits the sharing and dissemination of knowledge systematically across the network’.<sup>127</sup> On issues relating to terrorism, for example, coordination among the intelligence agencies has been much improved by the creation of Joint Terrorism Analysis Centre (JTAC), based in MI5.

### **An open source revolution**

An open source revolution is happening in government with respect to what information is being collected and what types of information are being incorporated into assessments and briefs. The challenge for departments and the intelligence agencies, as illustrated in the story above, is one of sorting fact from fiction or signals from noise. Agencies and departments have a choice though. They can either accept that the volume of information is likely to increase and adapt existing structures in their organisation or they can adopt new practices in existing structures. Either way they must ensure that they change their mindsets first. One problem area is that there remains a tendency in government to see intelligence material as being the pinnacle of the hierarchy of information, hence the reason why open source material is still rarely considered by organisations like JTAC.

Such is the dramatic change in how information is produced, disseminated and collected that the intelligence agencies will have to reach out in many directions through a variety of means by engaging willing colleagues outside government – in universities, think tanks and NGOs.<sup>128</sup>

This is especially true when dealing with ‘open source’ material. Ultimately agencies are now in the information, not the secrets, business and therefore compete with a variety of private and public sector organisations. As such, policy-makers will become more not less reliant on intelligence because if collection is easier the result will be a selection process that is much more difficult.

The open source revolution also means that expertise will often lie outside government. Research undertaken by external organisations

may well provide a crucial piece of the puzzle but as one official suggests:

*We are too convinced that only our information is really worth having and that outsiders don't know the score. We don't bring travelling academics, journalists and businessmen into our areas of discussion – and not just for the occasional seminar but for confidential talks, showing them our so-called secret-stuff and asking them: 'What do you think?'*<sup>129</sup>

### **Ideas for change**

To achieve the open government many people aspire to will require a huge change in culture and mindset. This section identifies some further changes to support the government in its endeavour.

Foreign Secretary David Miliband has recently resurrected his blog and has been joined by a number of diplomats who will be posting comments regularly on issues relating to foreign affairs. This marks a radical departure for the FCO as much of its work remains closed to the outside world. As former diplomat Carne Ross explains, this lifestyle:

*is constantly reinforced throughout one's career. Telegrams are transmitted only when highly encrypted. All computers are hardened against electronic eavesdropping . . . So many and so ubiquitous are these limitations, that it is soon clear that the only people with whom one can discuss candidly what 'we' are doing are one's colleagues – other members of the club of 'we'. One should only talk to people with a 'need to know'. This excludes almost everyone, including those in whose name 'we' are acting.*<sup>130</sup>

### **Wikis and national security**

Blogging and wikis could be part of the greatest paradigm shift the security and intelligence community has ever seen. While blogs are vibrant and provide up-to-date commentary on daily issues, wikis

can be shaped to become part of an organisation's corporate knowledge. Enabling individuals across departments and agencies to share information and analysis on a broad spectrum of issues offers government a real opportunity to take a collaborative approach on national security. Although blogging does occur in some departments in Whitehall – the Permanent Secretary at the Home Office has his own blog for example – the time is ripe to go much further. The UK intelligence agencies should develop a variant on the US intelligence agency's highly successful Intellipedia.

Intellipedia was the brainchild of the Office of the Director for National Intelligence (ODNI) in the US. The wiki allows information to be assembled and reviewed by a wide variety of sources and agencies. In 2006, Intellipedia was the main collaboration tool in constructing a National Intelligence Estimate on Nigeria. Richard Russell, deputy assistant director of National Intelligence, said it was created so 'analysts in different agencies that work in X or Y can go in and see what other people are doing on subject X or Y and actually add in their two cents worth . . . or documents that they have'. Sixteen months after its creation, officials say, the top secret version of Intellipedia (hosted on the Joint Worldwide Intelligence Communication System, JWICS) has 29,255 articles, with an average of 114 new articles and more than 4800 edits to articles added each workday.

### **Public assessments**

Sharing information does not apply just to the intelligence agencies. As this chapter has demonstrated a new relationship between the government, private sector and the public requires new forms of information sharing. Kevin Tebbit, the former Permanent Secretary of the MoD, was recently asked to review the Danish external intelligence agencies. In a speech to the Mile End Institute he explained that their intelligence agencies published:

*an unclassified assessment of their judgement of the threats facing Denmark. It's done at the same time each year to avoid it appearing to be affected or influenced by the political process*

*and it is offered to the Danish Parliament, the Danish Government, the Danish people at the same time . . . to help inform debate about why it is important for intelligence agencies to go about their business and, broadly speaking, what it is they find.*<sup>131</sup>

The UK government should learn from examples like the Danish one and consider publishing an annual threat assessment. This process already occurs in some areas of government, such as SOCA's annual assessment of organised crime.

### **Public dialogue**

In promoting an open relationship between the government and its strategic partners the government must commit itself to pursuing a strategy that goes beyond communicating issues to the private sector and wider public and instead engages with them. This will mean creating opportunities and space for dialogue to occur. To support this approach and rebuild trust between government and the public in particular, a spokesperson for national security should be created within the national security secretariat.

### **Managing knowledge in government**

Knowledge management is crucial in today's world but it remains the government's Achilles heel. In order to keep up with the volume of information and data, departments have to ensure their information and communication technology strategies deliver the necessary tools to support the exchange of knowledge, data and information across the government space. This is one of the most serious issues facing government, especially in the national security architecture. Innovative ideas have to be sought to both support the exchange of knowledge and capture institutional memory.

This latter point is crucial if government is going to learn the right lessons from past successes and failures. To that end the government should consider trialling an information platform for departments that is equivalent to the highly successful Facebook – which would

include information on civil servants, their past and present postings, employment, skills and specialisms, which is currently not available on current departmental intranet sites.

### **Parliamentary accountability**

Democratic government relies on the scrutiny of its actions by Parliament. The current system of select committees is under-resourced, under-skilled and the scrutiny of national security woeful. Relevant select committees for national security should be brought together to form a similar committee to that of the quadripartite committee on strategic export controls, which already exists. Furthermore, extra resources should be given to recruit specialists on security affairs.

### **Scrutinising government**

Finally, a democratic government must insist on the scrutiny of all government departments and agencies. While there is an ongoing debate concerning whether the ISC is made into a select committee it is very noticeable that there has been no formal account of SOCA since its creation. Given the importance of tackling serious and organised crime the lack of accountability on the agency's progress is palpable. This is worrying given the problems the chair of SOCA has made public. The Home Affairs select committee should instigate a review into SOCA's progress in tackling serious and organised crime. This should be held in public and serve to highlight the current successes and failures of SOCA's work to date.

## 5. Great expectations

*You've got to be very careful if you don't know where you're going, because you might not get there.*

Yogi Berra

*I don't think we have at the moment a particularly systematic way of assessing the different components and how to resource the different components.*

Senior civil servant, Home Office

*Control seems more necessary and less feasible than ever before.*

*People Flow, Demos 2003*

In June 2006 the shadow Foreign Secretary William Hague MP asked the UK government how many Afghan national police and Afghan border police officers had been trained since 2003. The parliamentary question was, by any standard, fairly innocuous and reflected the normal procedures of parliamentary accountability by which opposition parties are able to solicit facts and figures from the government. The Foreign Secretary's response was short and factual. On 24 April 2006, she replied, the figure stood at 30,263: 23,000 uniformed police (Afghan national police – ANP); 1700 highway police; 5200 border police; and 300 counter-narcotics police.

Fourteen months later the Liberal Democrats' foreign affairs spokesman Michael Moore MP asked the UK government a similar question. What assessment, he asked, had the government made of the capability and membership of the Afghan police force. The new Foreign Secretary David Miliband made reference to the US Combined Strategic Transition Command Afghanistan (CSTC-A) figure of around 76,000 members of the ANP, drawn from all regions of Afghanistan.

On the surface, progress on police reform in Afghanistan was very positive; not only had the ANP grown to around 76,000, it had exceeded the number originally agreed in the Afghanistan Compact benchmark for the police, which the government of Afghanistan and major international donors had agreed on at the London Conference in 2006. This was evidence of important and tangible progress towards a stable and secure Afghanistan.

Except the numbers offered were at best no more than guesses. In truth no one knows what the capability of the ANP is today – what is known instead, is how many Afghan men and women have been trained to become police officers. So while David Miliband had quoted a legitimate source, in truth the exact number of police remains a mystery and this has serious implications for the security of Afghanistan insofar as it becomes increasingly more difficult to gauge the effectiveness of the police and their contribution to the security of the country.

Furthermore the answer given by the Foreign Secretary failed to take into account the broader question of 'capability' Moore had made reference to. In focusing on the number of ANPs, Miliband's answer did not take into account the complexities of the police reform process in Afghanistan, which included:

- the need to reconcile the 'German vision' of the police as a civilian law and order force, and the 'US vision' of the police as a security force with a major counter-insurgency role
- the coordination of 25 countries and several international organisations involved in police reform

- combating the high rates of illiteracy and semi-literacy among ANP patrolmen and recruits, which made it difficult to provide effective training and severely limited the policing tasks that could be performed
- managing the weak or non-existent recruiting and vetting systems for police recruitment
- managing the lack of internal controls and accountability systems in a notoriously corrupt institutional environment
- developing a plan to manage the 95 per cent of donated equipment to the police that was non-standard, while the rest was sub-standard.<sup>132</sup>

When the FCO was asked about the capability of the Afghan police it had turned to what it knew – the number of police. But using such figures without providing any context and detail is wholly disingenuous. The truth is that crude, scientific management processes designed to measure inputs and outputs fail to provide a real and genuine picture of the situation. Such an approach has serious ramifications on how the government measures progress internally and how it explains success and failure to its key audiences. Most importantly this approach has an impact on how the government builds and maintains the confidence and trust of the public and international community in its ability to manage complex security issues.

### **Measuring success?**

An important innovation introduced by the Labour government in the late 1990s was a targets-based culture that strove to measure the improvement in public services by developing a series of PSAs between departments and the Treasury. Early on, the UK government set out its five aspirations for targets in a joint memorandum from the Treasury and the Delivery Unit of the Cabinet Office:

1. *Targets provide a clear statement of what the government is trying to achieve. They set out the government's aims and*

- priorities for improving public services and the specific results government is aiming to deliver.
2. *Targets provide a clear sense of direction and ambition.* The aim, objectives and targets in each PSA provide a clear statement around which departments can mobilise their resources.
  3. *Targets provide a focus on delivering results.* By starting from the outcome government is trying to achieve, the targets encourage departments to think creatively about how their activities and policies contribute to delivering those results. They also encourage departments to look across boundaries to build partnerships with those they need to work with to be successful.
  4. *Targets provide a basis for monitoring what is and isn't working.* Being clear about what you are aiming to achieve, and tracking progress, allows you to see if what you are doing is working. If it is, you can reward that success; if it isn't, you can do something about it.
  5. *Targets provide better public accountability.* Government is committed to regular public reporting of progress against targets. Targets are meant to be stretching. So not all targets can be hit. But everyone can see what progress is being made.<sup>133</sup>

Objectives and performance targets span Whitehall and include everything from enhancing access to culture and sport for children to achieving success in the military tasks the MoD undertakes at home and abroad. PSAs were designed to incorporate longer budget cycles and link funding to outcomes by shifting the focus on outputs while forcing departments to modernise. PSAs were also a mechanism to demonstrate improvement in a complex policy area and enabled ministers to show tangible progress, something that remains especially difficult when measuring different aspects of 'national security', as the technical note for the MoD's PSA on conflict prevention illustrates:

*Conflict prevention is a complex area in which to measure outcomes. A peace settlement can take many years to be consolidated, progress is unlikely to be linear and even when it is clear that a settlement has been achieved, it is hard to attribute the specific contribution made by UK funded programmes and/or associated diplomatic, development or defence activity.<sup>134</sup>*

The five aspirations outlined above serve a useful purpose in analysing the government's current performance regime in the national security domain.

Targets can provide a statement of what the government is trying to achieve, though this will rarely give the full picture. However, this is important in two respects. First, outlining aims and priorities in a specific policy area can lead to improved decision-making in government and, second, can demonstrate a commitment by the government to respond to security challenges facing the UK. For example, the overall mission of the Home Office and the department's seven objectives in meeting it can be seen on the Home Office website. In protecting the public, the department focuses on seven key objectives:

1. Help people feel safer in their homes and local communities.
2. Support visible, responsive and accountable policing.
3. Protect the public from terrorist attack.
4. Cut crime, especially violent, drug and alcohol-related crime.
5. Strengthen our borders, fast-track asylum decisions, ensure and enforce compliance with our immigration laws, and boost Britain's economy.
6. Safeguard people's identity and the privileges of citizenship.
7. Work with our partners to build an efficient, effective and proportionate criminal justice system.

Second, targets can provide a clear sense of direction and ambition. While this can mobilise necessary resources by developing business planning and communicating a clear message to staff, it also has an important external dimension. At a time when the security environment is complex and uncertain, providing a clear sense of direction and ambition is crucial in building and maintaining the confidence of the government's key audiences, such as the public, in the ability of the government.

Third, targets provide a focus on delivering results. As the memorandum states, 'by starting from the outcome government is trying to achieve, the targets encourage departments to think creatively about how their activities and policies contribute to delivering those results.' In theory a target will also encourage departments to take a collaborative approach. For example, there has been an increasing recognition by Whitehall of the importance of departments and agencies joining forces with NGOs and the private sector on operations in Iraq and Afghanistan. Although such efforts are important they are rarely coordinated or focused on a set of common objectives.

Fourth, targets provide a basis for monitoring what is and isn't working and support Whitehall and external stakeholders in tracking progress. The government's counter-terrorism strategy, for instance, states that it will 'measure our success by whether we reduce the impact of terrorist attacks on British citizens and our way of life'.

Last, targets provide better accountability to the public. A good deal has been published already on targets relating to national security and can be found on numerous departmental websites. Accountability can be further provided through speeches and off-the-record briefings. For example, although no formal targets on counter-terrorism have been published (indicative targets on certain aspects of the government work on counter-terrorism are being experimented with) the public can still get an impression of the extent of progress. In the most recent report of the ISC we are able to learn that:

*International Counter-Terrorism (ICT) continues to increase as a proportion of the service's overall allocation of effort. ICT rose*

*from about a third of total effort in 2002/03 to 42 per cent in 2003/04. In 2004/05, at 52 per cent, it comprised over half of the service's activity. This excluded Irish counter-terrorism, which accounted for 20 per cent of operational resource in 2004/05. Protective security and counter-intelligence work accounted for 13 per cent and 7 per cent respectively.<sup>135</sup>*

However, despite the general support for the government's use of targets many policy-makers and practitioners continue to have serious reservations about their operation in practice. If the government is to continue with measuring the performance of government based on targets then they will have to take the following into account.

First, targets can encourage individuals to face the wrong way insofar as the focus of the civil servant or public manager is on meeting the aims and objectives set internally rather than influencing change externally. Creating a target for the number of Afghan police trained was an entirely legitimate objective but it was limited to a single and relatively simple process. And while the process aims to meet the requirements of the government department it fails to take into account the wider needs and requirements of police reform. It can also be hijacked by political initiatives. As Andrew Wilder from the Afghanistan Research and Evaluation Unit has noted:

*[I]mmediate issues, such as the presidential elections and the growing Taliban insurgency, result in 'quick fix' solutions that prioritise the quantity of police over the quality. Such measures to quickly increase police numbers are undermining the longer-term objective of creating an effective police force. While too few police may indeed be a serious problem in some areas, a more serious problem is that the local police that are present are often corrupt and ineffective, and as far as the public are concerned do more harm than good.<sup>136</sup>*

The second potential distortion introduced by the use of targets is

that the target may usurp the purpose or goal of the system. For example, the Police Federation recently highlighted the arrest of a child for throwing a cucumber slice, a decision made in order to meet targets. A spokesman for the Federation said such cases were a result of officers chasing targets rather than doing their job. But current performance indicators for the police skew results, especially when more trivial crimes are counted alongside the more serious ones – unsurprisingly given the pressures of policing there is often a temptation to concentrate on easy targets.

The third distortion is more subtle because it involves manipulating the data on which the target is based. The most recent example of this phenomenon is the testimony by General David Petraeus, the US commander in Iraq, and Ryan Crocker, the US ambassador to the country, to the Senate Foreign Relations Committee on the US military's surge strategy. Using a variety of slides and graphs General Petraeus was able to demonstrate that the military objectives of the surge were in large measures being met. Questions remain, however, on whether the evidence he gave was comprehensive. Some US academics in particular have suggested that aggression in Iraq is highly seasonal, meaning there are fewer deaths in the summer because it's too hot to fight.

*The seasonality is pretty easy to see: violence peaks in spring, then declines during summer, peaks again in fall, and drops during winter . . . Taken as a whole the evidence pretty strongly suggests that the surge hasn't had any effect at all on overall violence levels. It's just moving in its usual seasonal pattern. Bottom line: you should be sceptical of any claims about reductions in violence unless they take seasonality into account.<sup>137</sup>*

The fourth distortion is one that the so-called frontline staff have vociferously complained about – the loss of productive time that is involved in collecting all the data required to demonstrate compliance or not with the target. Take for example the story of Richard Elliott.

Richard ran Bristol City's drugs action team but resigned because he could no longer bear the waste and bureaucracy:

*. . . the 44 different funding streams, each one with its own detailed guidance and micro targets from the centre, each one with its own demand for a detailed business plan and quarterly reports back to the centre; the endless service agreements he had to sign with every local provider with their own micro targets and a demand for quarterly reports back to him so that he could collate them and pass them back to the centre; the new annual drugs availability report to the centre; the annual treatment plan to the centre over 68 pages and nine planning grids with 82 objectives. He reckoned he and his staff spent only 40% of their time organising services for drug users – the rest of their time was consumed by producing paper plans and paper reports for Whitehall.<sup>138</sup>*

The fifth and final distortion is that targets frequently fail to distinguish variation or difference in context. For example, in conversations regarding the shift in resources from Iraq to Afghanistan it has been noted that NATO armed forces are being sent to Afghanistan on the basis that they can draw on similar experience and operations in Iraq. There are no easy answers for reforming the current processes for measuring and evaluating the performance of government. Imagination, however, remains crucial.

The negotiations between departments on the new set of PSA targets published in the latest CSR seemed to have got off to a good start with the Treasury in particular taking a more imaginative approach to the issues of security and conflict. However, it soon transpired there were disagreements about the scope and detail of the targets and all too quickly departments retrenched into their old ways. While negotiating within government is not easy there was a general sense of disappointment that the departments could not take a more progressive approach to measuring performance – much of which came down to the allocation of resources. The CSR did,

however, produce a new PSA target on ‘reducing the risk to the UK and its interests overseas from international terrorism.’ Given the level of resources for counter-terrorism the new PSA is welcome but it will be interesting to see both its influence on government policy and strategy and how it will make the various performance measures public.

Although value for money will remain a significant pillar of the target culture it will have to be complemented by a more creative and sustainable set of measurements that take into account the complexities of national security. This is especially true for the intelligence agencies, which have seen a major investment and which have, quite rightly, had to demonstrate to stakeholders how they are using the money.

This will be hard when there are significant difficulties in demonstrating the agency’s success. That problem is further exacerbated when ‘particular failures are accorded disproportionate significance if they are considered in isolation rather than in terms of the general ratio of failures to successes; the record of success is less striking because observers tend not to notice disasters that do not happen’.<sup>139</sup> And although it may be tempting to conclude that it is virtually impossible to measure publicly the success or failure of intelligence, Gill and Phythian suggest the following principles, the majority of which closely mirror a public value approach.<sup>140</sup> Agencies could measure their successes and failures based on:

- predictive success – analysis leading to timely warning, facilitating prevention or capitalisation
- absence of predictive failure
- maintenance of customer trust
- maintenance of public trust
- maintenance of effective partnerships with allied intelligence agencies
- maintenance or enhancement of the customer’s relative advantage.

## Ideas for change

One solution to the current problems associated with the target culture is not to think in terms of *doing* something differently but in terms of *thinking* about the situation differently. Success relies on four complementary approaches to reform. First, as illustrated in part 1 of this pamphlet the government recognises complexity and uncertainty but it needs to accept it as an everyday reality of government.

Second, argued in chapter 3, command and control approaches, non-linearity, and imposing stability on complex systems through rules will not work. Focusing on outputs and not outcomes will lead to unintended consequences. The emerging paradox of the early twenty-first century is that stability will be possible only through embracing ‘perpetual adaptation of the system’ as a whole and this will require two complementary approaches to be taken. The first and most fundamental is a more trusting relationship between the government, private sector and the public. In a complex system there will always be multiple goals and objectives so government should learn to acknowledge differences, and instead of imposing change, shape it. Second, this will require the government to experiment both with the system and through multiple interventions and evaluations. In doing so command and control approaches to policy implementation will become increasingly redundant in favour of more distributed models that place leadership and responsibility on local or ‘immediate actors’. This will be especially true for building resilience in local communities where the responsibility is on local authorities and where central government will play a less influential role.

Third, the UK government will have to prioritise public value as a new intellectual framework for national security. But public value does not just appear; it must be fostered and sustained by all relevant parties focusing on the core elements of public value: trust, legitimacy and fairness. Much work has already been done on aspects of public value in the Strategy Unit and elsewhere and departments should seriously consider the application of public value to their work.

Finally, a new style of leadership and management will have to

emerge to respond to the complexity of the security environment. No matter how much coherence there is at the centre of government this has to be supported by networks across the system that allow new approaches and methods to take root. In accepting this approach governments will have to distribute responsibility downwards, ceding some control and authority to local actors in return for greater collaborative partnerships.

## 6. Carrots, sticks and sermons

*The British people are reluctant global citizens. We must make them confident ones.*

Prime Minister Rt Hon Tony Blair, Labour Party Conference,  
September 2006

*In a century of global trade, global migration and global terrorism . . . there is no 'domestic' and 'foreign' any more.*

Rt Hon David Cameron, Leader of the Conservative Party,  
July 2007

The UK's national security architecture remains handicapped by an archaic and compartmentalised system that dates from the Cold War. Change is needed. If the government is to respond successfully to the threats and hazards of the twenty-first century then it must organise around the concept of national security.

Traditional notions of 'defence', 'foreign affairs', 'intelligence' and 'border control' are becoming increasingly redundant in the contemporary security environment. At best these notions tend to confuse roles and responsibilities rather than clarify accountability – at worst they act as barriers to collaborative ventures across government, strengthening the existing silo mentality and ensuring the government cannot create the effect it requires.

Central to a holistic approach to national security are the

principles of openness and transparency. In particular the government should focus on making the security architecture more accountable to Parliament and the wider public. This will require the government to move beyond communicating with the private sector and public to engaging with them concerning risks to the UK.

These principles are also central to a new culture in government that addresses the accountability deficit, collapses walls between departments and fosters collaboration among civil servants. Furthermore this culture must support information sharing across government through changes in process and the use of innovative technologies. Whitehall and agencies must move beyond the traditional mindset of 'need to know' to embrace the concept of 'need to share', where the focus of individuals in the system is on the 'responsibility to provide'.

Underpinning this approach to national security must be a new intellectual framework – public value. Public value provides a way of measuring the performance of departments, through the allocation of resources and selecting appropriate ways of implementing policies focusing on outcomes, trust and legitimacy. Public value will help to rethink the way government implements policy by allowing flexible and innovative thinking to emerge at the level of individual decision-makers. This will be a difficult process of change to embed in the culture of government without the support and imagination of ministers and civil servants.

Successive British governments have rarely taken a strategic approach to national security, preferring instead to focus on reorganising individual departments or creating new agencies and units to meet the demands of the security environment. Adapting the machinery of government may pay short-term dividends but it can only ever achieve marginal improvements. Long-term success must be based on a more inclusive, open and holistic approach to the national security architecture. Present and future challenges demand it.

# Notes

- 1 'Risks' are categorised as threats (malicious events such as terrorist attacks) or hazards (non-malicious events such as flooding). See UK Resilience website at [www.ukresilience.info](http://www.ukresilience.info) (accessed 25 Oct 2007).
- 2 TL Friedman, *The World is Flat: The globalised world in the twenty-first century* (London: Penguin, 2006).
- 3 D Tapscott and AD Williams, *Wikinomics: How mass collaboration changed everything* (London: Penguin, 2006).
- 4 See C Leadbeater and J Wilsdon, *The Atlas of Ideas: How Asian innovation can benefit us all* (London: Demos, 2007).
- 5 Ibid.
- 6 T Homer-Dixon, *The Upside of Down: Catastrophe, creativity and the renewal of civilisation* (London: Souvenir Press Ltd, 2007).
- 7 B Stein, 'A market crisis disconnected from reality', [www.iht.com/articles/2007/08/12/business/perspective.php](http://www.iht.com/articles/2007/08/12/business/perspective.php) (accessed 29 Oct 2007).
- 8 T Blair, foreword by the Prime Minister, in *Capability Review: The findings of the first four reviews*, Prime Minister's Delivery Unit, 2006.
- 9 C Edwards, 'The case for a national security strategy' (London: Demos, 2007), available at [www.demos.co.uk/publications/nationalsecuritystrategy](http://www.demos.co.uk/publications/nationalsecuritystrategy) (accessed 31 Oct 2007).
- 10 P Cornish, *Civil Defence and Public Resilience: The homeland security of the United Kingdom* (London: Centre for Defence Studies, 2003).
- 11 Homer-Dixon, *The Upside of Down*.
- 12 N Taleb, *The Black Swan: The impact of the highly improbable* (London: Allen Lane, 2007).
- 13 Using a scenarios methodology Shell was able to identify the drivers of changes and uncertainties of the oil industry and as a result, during the 1970s, was better positioned to handle the oil embargo, the dramatic rise in oil prices and the power of the OPEC cartel than many of its competitors.
- 14 At the time Robert Gates, then head of the CIA, was hosting a party; on being

- informed of the situation in Kuwait he was alleged to have replied, ‘what invasion?’.
- 15 Select Committee Hearing, *A Failure of Initiative*, the final report of the Select Bipartisan Committee to investigate the preparation for and response to Hurricane Katrina, US House of Representatives, 109th Congress, 14 Dec 2005, see [www.gpoaccess.gov/katrinareport/mainreport.pdf](http://www.gpoaccess.gov/katrinareport/mainreport.pdf) (accessed 31 Oct 2007).
- 16 T Davis, see *ibid.*
- 17 P Symonds, ‘The Asian tsunami: why there were no warnings’, [www.wsws.org/articles/2005/jan2005/warn-j03.shtml](http://www.wsws.org/articles/2005/jan2005/warn-j03.shtml) (accessed 29 Oct 2007).
- 18 J Booth, ‘Thousands cut off in Britain’s worst floods’, [www.timesonline.co.uk/tol/news/uk/article2123487.ece](http://www.timesonline.co.uk/tol/news/uk/article2123487.ece) (accessed 29 Oct 2007).
- 19 M Power, *The Risk Management of Everything* (London: Demos, 2004).
- 20 GF Treverton, *Reshaping National Intelligence for an Age of Information* (Cambridge, UK, and New York: Cambridge University Press, 2003).
- 21 L Clarke, *Worst Cases: Terror and catastrophe in the popular imagination* (Chicago: University of Chicago Press, 2006).
- 22 Demos and Ipsos MORI data.
- 23 HM Treasury, *Public Expenditure Statistical Analysis* (London: HM Treasury, 2006).
- 24 ‘Playing tough’, *The Economist*, 16 Nov 2006.
- 25 D Omand, ‘Security dilemmas: secret intelligence and an adversarial court system do not leave easily together’, *Prospect*, Dec 2006.
- 26 D Rieff, ‘Fear and fragility sound a wake-up call’, *Los Angeles Times*, 12 Sep 2001.
- 27 F Furedi, *Culture of Fear: Risk taking and the morality of low expectation* (London: Continuum, 2002).
- 28 Quoted in S Litherland, ‘North–south: global security elbows out development’, *Inter Press International News*, London, 2 Dec 1993.
- 29 ‘“Mistakes” made over 7/7 reaction’, *BBC News Online*, see [http://news.bbc.co.uk/2/hi/uk\\_news/politics/7015154.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/7015154.stm) (accessed 29 Oct 2007).
- 30 Home Office, see [www.homeoffice.gov.uk/](http://www.homeoffice.gov.uk/) (accessed 16 Jul 2007).
- 31 JM Bryson, *Strategic Planning for Public and Nonprofit Organisations*, 3rd edn (San Francisco: Jossey Bass, 2004).
- 32 C Ross, *Independent Diplomat: Dispatches from an unaccountable elite* (London: C Hurst & Co Publishers Ltd, 2007).
- 33 See Treverton, *Reshaping National Intelligence for an Age of Information*.
- 34 M Barber, *Instruction to Deliver: Tony Blair, public services and the challenge of achieving targets* (London: Politico’s Publishing, 2007).
- 35 Bryson, *Strategic Planning for Public and Nonprofit Organisations*.
- 36 G Mulgan, ‘Lessons of power’, *Prospect*, May 2005.
- 37 Homer-Dixon, *The Upside of Down*.
- 38 Ross, *Independent Diplomat*.
- 39 For examples of some of the ideas for reform see: House of Commons Select Committee on Defence, *Defence and Security in the UK*, sixth report (Norwich: TSO, Jul 2002); Lord Butler, *Review of Intelligence on Weapons of Mass*

- Destruction* (Norwich: TSO, July 2004); D O'Connor CBE QPM, *Closing the Gap: A review of 'fitness for purpose' of the current structure of policing in England & Wales* (London: HM Inspector of Constabulary, Sep 2005).
- 40 E Luce and M Garrahan, 'US switches resources to fight terror', *Financial Times*, 10 Oct 2007.
- 41 G O'Donnell, 'Introduction to the summary of the third tranche of capability reviews', see [www.civilservice.gov.uk/reform/capability\\_reviews/publications/pdf/Tranch\\_3\\_summary.pdf](http://www.civilservice.gov.uk/reform/capability_reviews/publications/pdf/Tranch_3_summary.pdf) (accessed 28 Jul 2007).
- 42 P Ashdown, *Swords and Ploughshares: Bringing peace to the 21st century* (London: Weidenfeld & Nicolson, 2007).
- 43 Cabinet Office, *Capability Review of the Foreign and Commonwealth Office* (London: Cabinet Office, March 2007).
- 44 Cabinet Office, *Capability Review of the Ministry of Defence* (London: Cabinet Office, March 2007).
- 45 Cabinet Office, *Capability Review of the Department for International Development* (London: Cabinet Office, March 2007).
- 46 Cabinet Office, *Capability Review of the Cabinet Office* (London: Cabinet Office, March 2007).
- 47 JW Young, 'The Wilson government's reform of intelligence coordination, 1967-68', *Intelligence and National Security* 16, no 2 (2001).
- 48 Cornish, *Civil Defence and Public Resilience*.
- 49 G Brown, 'Securing our future', speech to the Royal United Services Institute (RUSI), London, 13 Feb 2006.
- 50 Cabinet Office, *Capability Review of the Department for International Development* (London: Cabinet Office, March 2007).
- 51 Private information.
- 52 Private information.
- 53 Treverton, *Reshaping National Intelligence for an Age of Information*.
- 54 Home Office, *Report of the Official Account of the Bombings in London on 7 July 2005*, HC 1087 (London: TSO, 2006).
- 55 M Gladwell, 'Enron, intelligence, and the perils of too much information', *New Yorker*, 8 Jan 2007.
- 56 See PCRU website [www.postconflict.gov.uk/about.html](http://www.postconflict.gov.uk/about.html) (accessed 12 Oct 2007).
- 57 Ibid.
- 58 P Webster and R Ford, 'Reid to be MI6 security chief', *The Times*, 27 Feb 2007, see [www.timesonline.co.uk/tol/news/politics/article1444179.ece](http://www.timesonline.co.uk/tol/news/politics/article1444179.ece) (accessed 1 Nov 2007).
- 59 A Travis, 'Struggling Home Office split up to combat terrorism', <http://politics.guardian.co.uk/homeaffairs/story/0,,2046343,00.html> (accessed 28 Oct 2007).
- 60 Private information.
- 61 It is interesting to note that according to the Home Office website, 'The Office for Security and Counter-Terrorism (OSCT) has led the work on counter-terrorism in the UK for over 30 years working closely with the Police and Security Services', even though the office was only created in the spring of 2007,

- see <http://security.homeoffice.gov.uk/about-us/about-the-directorate/> (accessed 28 Oct 2007).
- 62 Ashdown, *Swords and Ploughshares*.
- 63 Ibid.
- 64 HM Treasury, *Meeting the Aspirations of the British People: Pre-budget report and Comprehensive Spending Review* (London: HM Treasury, 2007).
- 65 *Review of Intelligence on Weapons of Mass Destruction* (known as the Butler Inquiry), Report of a Committee of Privy Counsellors, Chairman Rt Hon The Lord Butler of Brockwell (London: TSO, 14 Jul 2004).
- 66 M Gladwell, *Blink: The power of thinking without thinking* (London: Allen Lane, 2005).
- 67 J Risen, 'US failed to act on warnings in '98 of a plane attack', *New York Times*, 19 Sep 2002.
- 68 P Neville-Jones, 'An unquiet world', submission to the Shadow Cabinet, National and International Security Policy Group, Jul 2007.
- 69 P Neville-Jones, 'Security issues', interim position paper, National and International Security Policy Group, Nov 2006.
- 70 P Neville-Jones, speech at the launch of the Conservative Party's National and International Security Policy Group Report at Chatham House, 26 Jul 2007.
- 71 'National security: governing by numbers', *Guardian*, 19 Dec 2006.
- 72 Perri 6, *Holistic Government* (London: Demos, 1997).
- 73 G Brown, 'Constitutional reform statement', House of Commons, 3 Jul 2007.
- 74 Private information.
- 75 Civil Contingencies Secretariat, see [www.ukresilience.info/ccs/aims.aspx](http://www.ukresilience.info/ccs/aims.aspx) (accessed 28 Oct 2007).
- 76 R Mottram, 'Protecting the citizen in the twenty-first century: issues and challenges' in Hennessy, *The New Protective State* (London: Continuum, 2007).
- 77 HCDC, *Defence and Security in the UK*.
- 78 Cornish, *Civil Defence and Public Resilience*.
- 79 Bryson, *Strategic Planning for Public and Nonprofit Organisations*.
- 80 P Singer, *Corporate Warriors: The rise of the privatized military industry* (Ithaca: Cornell University Press, 2003).
- 81 P Rogers, *Losing Control: Global security in the 21st century*, 2nd edn (London: Pluto Press, 2002).
- 82 RISC, [www.sbac.co.uk/pages/68601912.asp#aGroup\\_4](http://www.sbac.co.uk/pages/68601912.asp#aGroup_4) (accessed 31 Oct 2007).
- 83 Home Office, Security and Counter-Terrorism Science and Innovation Strategy, 12 Jun 2007.
- 84 W Pincus, 'Defense agency proposes outsourcing more spying', 19 Aug 2007, [www.washingtonpost.com/wp-dyn/content/article/2007/08/18/AR2007081800992.html?referrer=emailarticle](http://www.washingtonpost.com/wp-dyn/content/article/2007/08/18/AR2007081800992.html?referrer=emailarticle) (accessed 28 Oct 2007).
- 85 T Bentley, *Everyday Democracy: Why we get the politicians we deserve* (London: Demos, 2005).
- 86 MH Moore, *Creating Public Value: Strategic management in government* (Cambridge, MA: Harvard University Press, 1997).

- 
- 87 Barber, *Instruction to Deliver*.
  - 88 C Edwards and P Skidmore, *A Force for Change: Policing 2020* (London: Demos, 2006).
  - 89 Moore, *Creating Public Value*.
  - 90 Barber, *Instruction to Deliver*.
  - 91 Brown, speech to RUSI.
  - 92 K Tebbit, 'Countering international terrorism: joining up the dots' in Hennessy, *New Protective State*.
  - 93 This definition of security is now being used by the Olympic Security Directorate at the Metropolitan Police as the basis of their concept of operations.
  - 94 M Moore, 'Christmas terror attacks "highly likely"', *Sunday Telegraph*, 11 Dec 2006, see [www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/12/10/ureid110.xml](http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/12/10/ureid110.xml) (accessed 28 Oct 2007).
  - 95 B Mann, 'The UK civil contingencies framework – building common endeavour' in P Cornish (ed), *Britain and Security* (London: The Smith Institute, 2007).
  - 96 D Omand, a lecture on the central organisation for national security, King's College London, 2006.
  - 97 J Chapman, *System Failure: Why governments must learn to think differently*, 2nd edn (London: Demos, 2004).
  - 98 Ibid.
  - 99 Private information.
  - 100 Chapman, *System Failure*.
  - 101 Cabinet Office, *Investing in Prevention: An international strategy to manage risks of instability and improve crisis response* (London: Cabinet Office, Feb 2005).
  - 102 S Patrick and K Brown, *Greater than the Sum of its Parts? Assessing whole of government approaches to fragile states* (New York: International Peace Academy, 2007).
  - 103 R Morarjee, 'Expanding Afghan no-go zones take a toll on health', *Financial Times*, 26 Jul 2007.
  - 104 Chapman, *System Failure*.
  - 105 See H Rittel and M Webber, 'Dilemmas in a general theory of planning', *Policy Sciences* 4 (1973).
  - 106 E Scarry, 'Citizenship in emergency: can democracy protect us from terrorism?', *Boston Review* 27, no 5 (Oct/Nov 2002).
  - 107 J Kendra et al, 'The evacuation of Lower Manhattan by water transport on September 11: an unplanned success', *Joint Commission on Quality and Safety* 29, no 6 (Jun 2003).
  - 108 Patrick and Brown, *Greater than the Sum of its Parts?*
  - 109 N Gallagher and S Parker, *The Collaborative State: How working together can transform public services* (London: Demos, 2007).
  - 110 See Edwards, 'The case for a national security strategy?'
  - 111 P Hennessy, *Whitehall* (London: Secker & Warburg, 1988).
  - 112 Ross, *Independent Diplomat*.

- 113 G Mulgan, *Good and Bad Power* (London: Penguin, 2006).
- 114 Ross, *Independent Diplomat*.
- 115 S Bok, *Secrets: On the ethics of concealment and revelation* (New York: Vintage, 1989).
- 116 Report of the Commission on Protecting and Reducing Government Secrecy (also known as the Moynihan Secrecy Commission), 103rd Congress, 3 Mar 1997, see [www.gpo.gov/congress/commissions/secrecy/index.html](http://www.gpo.gov/congress/commissions/secrecy/index.html) (accessed 1 Nov 2007).
- 117 Ibid.
- 118 Ibid.
- 119 *Your Right to Know: The government's proposals for a Freedom of Information Act*, white paper, Cm 3818 (Norwich: TSO, 1997).
- 120 S Tendler, 'Only one in 20 underworld bosses is at risk of being sent to prison', *The Times*, 17 Feb 2007.
- 121 The ISC is different from a traditional select committee as it is the Prime Minister, in consultation with the leaders of the two main opposition parties, who appoints the ISC members. The Committee reports directly to the Prime Minister, and through him to Parliament, by the publication of the Committee's reports.
- 122 For the role of the ISC, see [www.cabinetoffice.gov.uk/intelligence](http://www.cabinetoffice.gov.uk/intelligence) (accessed 28 Oct 2007).
- 123 See, for example, 'MI5 told MPs day before 7/7 "no terrorism threat"', *Daily Mail*, 9 Jan 2007.
- 124 Mottram, 'Protecting the citizen in the twenty-first century'.
- 125 Ibid.
- 126 L Pratchett and A Dale, 'The domestic management of terrorist attacks: the local dimension', Local Governance Research Unit, De Montfort University, Leicester, Oct 2004.
- 127 See the various Cabinet Office capability reviews.
- 128 Treverton, *Reshaping National Intelligence for an Age of Information*.
- 129 J Dickie, *Inside the Foreign Office* (London: Chapman Publishers, 1992).
- 130 Ross, *Independent Diplomat*.
- 131 Tebbit, 'Countering international terrorism'.
- 132 A Wilder, *Cops or Robbers? The struggle to reform the Afghan National Police* (Kabul, Afghanistan: Afghanistan Research and Evaluation Unit, July 2007).
- 133 Joint memorandum to the Public Accounts Committee from the Treasury and the Delivery Unit of the Cabinet Office, 2003.
- 134 Technical note, MoD PSA 2005–08, MoD.
- 135 Intelligence and Security Committee, *Intelligence and Security Committee Annual Report 2005/06*, Cm 6864 (Norwich, TSO, 2006).
- 136 Wilder, *Cops or Robbers?*
- 137 See K Drum, 'Violence in Iraq', *Washington Monthly*, 1 Sep 2007, available at [www.washingtonmonthly.com/archives/individual/2007\\_09/011979.php](http://www.washingtonmonthly.com/archives/individual/2007_09/011979.php) (accessed 28 Oct 2007).
- 138 J Chapman, 'A systemic perspective on public services', Demos, London, 2005.

- 139 RK Betts, 'Analysis, war and decision, why intelligence failures are inevitable', *World Politics* 31, no 1 (1978).
- 140 P Gill and M Pythian, *Intelligence in an Insecure World* (Cambridge: Polity Press, 2006).

### DEMOS – Licence to Publish

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS LICENCE (“LICENCE”). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENCE IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENCE. DEMOS GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

#### 1. Definitions

- a **“Collective Work”** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.
- b **“Derivative Work”** means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.
- c **“Licensor”** means the individual or entity that offers the Work under the terms of this Licence.
- d **“Original Author”** means the individual or entity who created the Work.
- e **“Work”** means the copyrightable work of authorship offered under the terms of this Licence.
- f **“You”** means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work, or who has received express permission from DEMOS to exercise rights under this Licence despite a previous violation.

#### 2. Fair Use Rights.

Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

#### 3. Licence Grant.

Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:

- a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;
  - b to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works;
- The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

#### 4. Restrictions.

The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:

- a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients’ exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this Licence and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.
- b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary

- compensation. The exchange of the Work for other copyrighted works by means of digital file-sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.
- c If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.
- 5. Representations, Warranties and Disclaimer**
- a By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:
    - i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;
    - ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.
  - b EXCEPT AS EXPRESSLY STATED IN THIS LICENCE OR OTHERWISE AGREED IN WRITING OR REQUIRED BY APPLICABLE LAW, THE WORK IS LICENCED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES REGARDING THE CONTENTS OR ACCURACY OF THE WORK.
- 6. Limitation on Liability.** EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, AND EXCEPT FOR DAMAGES ARISING FROM LIABILITY TO A THIRD PARTY RESULTING FROM BREACH OF THE WARRANTIES IN SECTION 5, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENCE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- 7. Termination**
- a This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.
  - b Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.
- 8. Miscellaneous**
- a Each time You distribute or publicly digitally perform the Work or a Collective Work, DEMOS offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.
  - b If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
  - c No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
  - d This Licence constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This Licence may not be modified without the mutual written agreement of DEMOS and You.

