Failures of Imagination:
Terrorist Incident Response in the Context of Crisis Management

Sara Eileen Bertin Thorne

The thesis is submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy of the University of Portsmouth

July 2010

Abstract

Since the terrorist attacks on the World Trade Center, New York in September 2001, the focus on terrorism and the ability of society and organisations to withstand such incidents has sharpened considerably. At the same time, business continuity and dealing with crises have moved to the forefront of organisations' awareness, not least due to improved regulatory requirements and guidelines.

However, this thesis contends that the current methodological framework for responding to terrorist incidents is flawed, resulting in the same issues becoming evident, over and over again. It is argued that an awareness and adoption of three key risk and crisis management methodologies: Fink's Crisis Management Methodology, Risk Communication and Isomorphic Learning, could improve the analysis of such incidents and hence better the response in future.

Three significant terrorist attacks were analysed within the context of contemporary literature and two factors were found to be the main cause of difficulties in managing the response to each of the incidents: communication and an inability to achieve organisational learning. It was argued that part of the reason for this was that organisations did not consider a link between crisis and terrorist incident response management and that learning from past experiences did not go beyond the most superficial level in most instances.

This thesis demonstrated how risk and crisis management methodologies could have addressed each of the issues that were identified in the case studies and clarified the contribution that they could make. Of primary importance was the recognition that events that may appear dissimilar are, on examination, frequently intrinsically similar and hence can provide valuable learning opportunities.

Table of Contents

12. List of Figures

List of Abbreviations

ACCOLC: Access Overload Control
ACPO: Association of Chief Police Officers
ACSNI: Advisory Committee on Safety of Nuclear Installations
AEAC: Atomic Energy Authority Constabulary
ALG: Association of London Government
ATCSA: Anti-Terrorism, Crime and Security Act 2001 (c.24)
BAA: British Airports Authority
BCM: Business Continuity Management
BTP: British Transport Police
CasWeb: Community Advice Service
CBRN: Chemical Biological Radiation Nuclear
CCA: Civil Contingencies Act 2004 (c.36)
CCTV: Closed Circuit Television
COBR: Cabinet Office Briefing Room
COLP: City of London Police
CPX: Command Post Exercise
CRIP: Commonly Recognised Information Picture
ECHR: European Convention on Human Rights
ELST: Emergency Life-Saving Technician
EMS: Emergency Medical Service
EPA: Northern Ireland (Emergency Provisions) Act 1966 (c.2)
ESU: Emergency Service Unit
ETA: Estimated Time of Arrival
EU: European Union
FAA: Federal Aviation Administration
FDNY: Fire Department of New York
FEMA: Federal Emergency Management Agency
GCG: Gold Co-ordinating Group

GCHQ: Government's Communication Headquarters

GLA: Greater London Authority

GLO: Government Liaison Officer

GLT: Government Liaison Team

Gold: the commander in overall charge of each organisation, responsible for formulating strategy for an incident

GSM: Global Systems for Mobile Communications

HO: Home Office

HPA: Health Protection Agency

HUMINT: Human Intelligence

ICAEW: Institute of Chartered Accountants in England and Wales

IMS: Incident Management System

IRA: Irish Republican Army

LAS: London Ambulance Service

Leaky feeder: special type of coaxial cable which can be used to provide radio coverage inside buildings and tunnels

LESLP: London Emergency Services Panel

LFB: London Fire Brigade

LFEPA: London Fire and Emergency Planning Authority

London Prepared: London Resilience website providing public advice about how to prepare for emergencies

LRF: Local Resilience Forum

LRRF: London Regional Resilience Forum

LRT: London Resilience Team

LU: London Underground

MDP: Ministry of Defence Police

MPS: Metropolitan Police Service

NBC: Nuclear Biological and Chemical

NCC: News Co-ordination Centre

NPA: National Police Agency

NYPD: New York Police Department

OECD: Organisation for Economic Co-operation and Development

OEM: Office of Emergency Management

PACE: Police and Criminal Evidence Act

PAPD: Port Authority Police Department

PATH: Port Authority Trans-Hudson

POAC: Proscribed Organisations Appeal Commission

PTA: Prevention of Terrorism Act 2005 (c.2)

SCC: Strategic Co-ordination Centre

SDF: Self Defence Force

SIAC: Special Investigation Appeals Commission

SIGINT: Signal Intelligence

SOC: Specialized Operations Command

SOD: Specialized Operations Division

SOP: Standard Operating Procedure

SRAD: Schematic Report Analysis Diagram

TACT: Terrorism Act 2000(c.11)

TETRA: Terrestrial Trunked Radio; a digital trunked mobile radio standard developed by the European Telecommunications Standards Institute

TfL: Transport for London

TRTA: Teito Rapid Transit Authority

UN: United Nations

WMD: Weapons of Mass Destruction

WTC: World Trade Center

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award.

Introduction

Purpose of this Research

This thesis will consider three key terrorist attacks that changed how countries viewed terrorism and impacted greatly on the public psyche. It is contended that existing responses to terrorist attacks no longer fitted the threat that was faced and as a result, agencies and emergency services tried to force the procedures that they had to fit this new world context. Examination of the three cases included within this thesis highlight the problems that occurred and underline the requirement for a new approach: following each attack, the responses were subject to the same difficulties and issues that had plagued previous incident responses, yet lessons either were not learned, or learned only in part. The aims of this thesis focus are on two areas:

1. Did common issues exist in the response to three key terrorist attacks that hindered aftermath management?

2. How can risk and crisis management methodologies help to address these and provide more robust arrangements, improving resilience?

In order to meet these aims, several key objectives should be achieved:

- To advance an understanding of responses to terrorist attacks, determining good and bad practice.
- To identify which risk and crisis management methodologies may be most appropriate to inform anti-terrorism methodologies and incident response.
- To question the belief that terrorism aftermath management is completely different from crisis management requirements and hence necessitates a different approach.

This thesis will argue that situational measures (anti-terrorism) can mitigate damage but a lack of foresight and a reactive approach will exacerbate the situation, as Ross (2009) in Freilich and Newman (2009:229) supports.

The Terrorist Attacks

The three case studies that have been chosen are: the 1995 Sarin attacks on the Tokyo subway as this was the first incident of a Weapon of Mass Destruction (WMD) attack by terrorists. It alerted responders to the reality of such an attack and the need to make provision for such. The second case study to be reviewed is the September 11th suicide aeroplane attacks on the World Trade Center as these attacks heralded a new style of terrorism and on a scale that was previously unimagined. The attack was the most lethal act of terrorism by any sub-state group in modern times (Guelke, 2009:viii). The lessons learned from this attack improved the response to the third case study, the 7th July 2005 London bomb attacks. This case study was chosen as it was the first incidence of a suicide bomb attack on the UK mainland and tested the response to the incident in such a way that had not been experienced previously. It is also pertinent that in contrast to the others, the London attack was largely expected hence the response organisations did have a chance to prepare in advance. It is this final case study on which this thesis will focus for several reasons: firstly, this is the first time in the United Kingdom (UK) that there had been a deliberate suicide attack and secondly, this is the most recent large scale terrorist attack that has happened in the UK. As such this provides a valuable learning opportunity as it is within the British context so is analogous with how we think, the systems that we have in place and can provide more than generic guidance regarding lessons learned.

This thesis will focus on the issues above in relation to crisis management practices for terrorist events so that recommendations can be made to improve the response to these. It is intended to identify common issues that affected the management of these incidents to enhance existing knowledge in this field. This should make realistic resilience easier to achieve. The apparent trend, as perceived by the researcher through the course of this

research, towards an increase in the probability of such incidents means that a new set of incident management needs must be met when faced with the nature of the perceived and actual terrorist threat.

Some of the issues that were identified in each of the case studies included in this thesis had been identified in previous incidents yet had not been addressed; the reasons for this are not clear. For example, the Inquiry into the response to the 7th July 2005 attacks found that the communications technology used by the emergency services was not working adequately below ground (Review Committee Report, 2006:120) despite the same problem being highlighted in the King's Cross disaster (Fennell, 1988). Therefore, this research will evaluate the responses to terrorist incidents that have had a distinguishing feature and have altered how responders manage their aftermath. The findings will then be used to try to identify good practice and areas for improvement that may be beneficial for future preparedness.

There are several reasons why this research should be beneficial for practitioners and theorists. Firstly, a considerable body of work exists on crisis management and terrorism as separate fields; since 2001 and the World Trade Center attacks, there has been a significant increase in terrorism research and a greater focus on emergency planning and crisis management. However, little of this work has been applied to bring these two fields together in a risk management context. Arguably had this occurred, responses to terrorist incidents could have been improved earlier. This is somewhat surprising in light of emergency planning requirements and the introduction of new legislation that firmly places the onus on organisations and the emergency services to have rigorous processes in place in the event of a terrorist attack (Appendix I: Terrorism Legislation). Thus this research will contribute to both the theoretical and practical knowledge about the management of terrorist incidents and crises.

Secondly, it is recognised that terrorist incidents are exceptionally difficult events to manage that can easily evolve into disaster. The emergency response agencies must work within the context of highly structured and disciplined organisational structures. In

contrast, those bringing about terrorist outrages are able to design incidents that frustrate these arrangements, bringing about a crisis. It is proposed that a clear identification of good practice and exploration of previous incidents will enable development of crisis management guidelines that will improve the effectiveness of the management of such incidents and help to prevent their escalation.

One of the overriding elements of each of the responses to the case studies is the rigid, prescribed processes that were triggered. While there must be an element of pre-determined actions in such situations that have been developed through rigorous testing and training, the necessity of flexibility in crisis management should not be overlooked. This thesis will argue that response agencies and organisations must develop scope for flexibility in response to such terrorist incidents if they are to manage them successfully in future.

Thirdly, as the legislative requirements become more stringent and the possibility exists for corporate manslaughter charges to be brought against individuals, it is increasingly important that the emergency services and other organisations can demonstrate that they actively managed the potential hazards and took all of the necessary precautions when responding to an incident. This thesis will aim to provide recommendations for actions that will provide a more coherent and effective response to terrorist incidents.

The threat that that has been faced globally since 2001 in particular therefore requires a different approach and training from that which was previously established; flexibility is now more than ever a key ingredient in response to such incidents, not least due to the rapid onset and frequent ill-structure that terrorist incidents display.

The thesis has been sub-divided into three sections and within this into eight chapters. Part One considers the theoretical literature on risk, crisis and terrorism. Part Two comprises three terrorism case studies which form the basis of the empirical work conducted in the course of this thesis. Part Three draws together the theoretical discussion

and analysis of the research findings and will identify good practice for the management of the response to future terrorist incidents following the empirical research.

The Challenges of Today

Today's current climate of political violence and the 'New Terrorism' (Laqueur, 1991:81) presents many new challenges and forms of terrorist attack for emergency decision makers to confront. The proliferation of new technology means that terrorist networks are far more loosely-structured than previously, hence detection and tracking is more difficult. The apparently limitless source of funds, training and the new determination displayed by the terrorists means that we now face a threat which is arguably greater than any seen in the last 20 years. Although not all terrorist attacks involve suicide bombers, the willingness of people to accept martyrdom in the recent suicide bomb attacks around the world, for example in Pakistan, Iraq, Afghanistan and the 7th July attacks in London in 2005, means that any deterrent must take account of this; something which old-style provisions perhaps did not.

If we add to this technology such as mobile telephones to act as detonators and the internet to not only enable communications but also to learn about new techniques, raise funds and promote the 'cause', it can be seen that we have a socio-technical problem where the social, human element, is probably the weakest and most unreliable link. The very nature of socio-technical systems means that they have a clear potential to evolve into potential disasters if not managed correctly (Borodzicz, 2005) and it is for this reason that the thesis will consider risk theory, including systems theory and terrorism literature to try to understand the terrorists, the attacks and their management more clearly.

Counter-terrorism policies in the West have been shaped by globalisation strategies. Whilst such strategies ensure access to labour and natural resources, so too has this enabled terrorists to reach these same resources with greater ease and greater potential targets as Newman in Freilich and Newman (2009:33) recognises.

Many terrorist incidents are ill-structured in response as the scale or nature of the attack may well have been unforeseen. The location of the incident may also have some bearing on this as it may further complicate events, for example, a bomb detonated on a subway system as in the 7th July 2005 attacks in London will be far harder to respond to than explosion above ground. The reason why an incident may be ill-structured and more prone to developing into a crisis or disaster can be conceptually presented in many different ways depending on the theoretical perspective that is adopted. In 1992, Ulrich Beck felt that there had been a clear paradigm shift from a class society to a risk society in how human relations are changing whilst for Turner (1978) it was felt that it was the mismatch in the relationship between social and technical systems that caused a situation to become ill-structured. The increasing reliance on technology and the increasing complexity of this technology Perrow (1984) argues is the driving force behind the propensity for an incident to have the potential for disaster; something which Dynes and Drabek (1994) develop and modernise through their link to the continuing process of industrialisation. It is these theorists, amongst others who will be considered in Chapter Two.

However, it is not only system and technological considerations that should be thought about here. In terms of the perceived increase in terrorism, one has to ask what is the driving force behind it? It is therefore important to look at more human elements too such as cultural sensitivities, media portrayal of nations and a genuine commitment to accept that today we live in a multi-cultural society and internationalisation is a natural extension of this. This is particularly important in order to remove many of the prejudices that may drive fear and resentment and encourage an environment where extremism can develop. This thesis will consider the role of the media and communication within the area of human elements as a driving force of terrorism. Just as the threat of both perceived and actual terrorist incidents has evolved and keeps evolving, so must our response and preparedness to deal with any incidents that may arise, whether real or imagined. It is not enough to say that we have plans in place; these must be rigorously tested, updated and tested again to ensure contemporary resilience to such attacks.

These considerations form part of Chapter One that examines the notion of terrorism, its definitions, evolution, tools and techniques and what this means for anti- and counter-terrorism strategy. It is useful now to move to this chapter to set this research in context.

1. The Terrorism Literature - A Conceptual Review

1.1 Introduction

In today's global environment, terrorism occurs in a variety of competing and often conflicting world views and ideologies. As Marsella (2004) in Moghaddam and Marsella (2004:11) comments, this is further complicated by omnipresent military, legal and political pressures. In recent years, a great deal of new legislation has been created to address the terrorist threat. The relevant Acts can be found at Appendix I. Much of the existing research addressing legislative reforms in this field has focussed on the threat to human rights not least as a result of the rapid enactment of many of the revisions and new Acts. An overwhelming focus on increasing power to the executive appears to characterise much of the present governmental response.

This chapter will review the contemporary literature on terrorism to understand its history, causes and the role of the media. This literature review is important for this thesis to identify how terrorism has changed in recent years from what existing responses and legislation were developed to address. This highlights how changes need to be made to respond to the evolved threat and it is these changes that this thesis will define and recommend. The ongoing development and the future of terrorism will also be considered to outline the threats that exist globally and the guise in which these are likely to exist in the future. Religious and International Terrorism will be considered however, for the purposes of this thesis, State and Dissident Terrorism will not be included other than a definition and brief discussion to exemplify their place in the discourse. It is useful to note at this point that there are several key points that run through the literature on terrorism: there is no single profile of a terrorist and there is much debate surrounding the definition of terrorism. These and other key points will now be considered.

1.2 The Genesis of Terrorism

In the French Revolution, the first use of the word "terrorism" in its modern context by Edmund Burke, the British statesman and philosopher is observed, coined when describing the regime de la terreur, or the Reign of Terror, in the late eighteenth century

in France. Martin suggests that that this is a good example of state terrorism carried out to further the goals of a revolutionary ideology; those who disagreed with the Jacobin dictatorship, or who were perceived to disagree with it, were put on trial at a Revolutionary Tribunal. Those found to be enemies of the state were executed (Martin, 2010:24).

Stohl (2005) in Bjorgo (2005:201) suggests that terrorism differs from ordinary political violence as the act or threat of violence is only the first step. It is designed to influence targets beyond the initial victimisation and seeks to influence the behaviour of others, not merely eliminate victims.

The current focus on terrorism may lead some to believe that it is a relatively new phenomenon, with its origins largely in the twentieth century. In fact, on examination of the literature, terrorism in one form or another has been in existence for thousands of years. (Martin 2010:24) cites Flavius Josephus in the History of Jewish War who noted that a faction of rebels existed ('Zealots') who were masters of guerrilla warfare and who used to destroy symbolic property belonging to both Romans and members of the Jewish establishment. Whittaker (2002:13) comments that Judaea was in fact plagued by the hit and run style of terrorism of the Zealots. Arguably this is one of the earliest descriptions of terrorism.

In order to begin to understand the origins of terrorist violence, it is useful to begin with a respected framework such as that developed by Friedland. This framework was developed to analyse the "antecedents of political terrorism" (1992:82). Friedland proposed that terrorism is a group activity and adopts a specific strategy or strategies, with its roots in inter-group conflict. In addition, it is helpful to consider the ideologies behind the actions. At first glance, Friedland's assertions seem a fair view, however, one of the key points he makes is arguably incorrect: surely not all terrorism has its roots in inter-group conflict? For example, the Oaklahoma bombings in 1995 carried out by Timothy McVeigh were not as a result of an inter-group conflict. As such, this is a good example of how definitions and debates need to evolve to reflect lessons learned and

newly acquired understanding about what constitutes terrorism. This is the reason why this thesis should propose the changes to the response and management of the aftermath of terrorist incidents and to measures for resilience.

By the mid 1990s, the appearance of new adversaries with new motivations and rationales began to challenge conventional wisdom, particularly regarding the use of weapons of mass destruction (WMD) (Hoffman, 2003 in Silke, 2004:xvii). The New Terrorism that now faces the world adds a new dimension; it does not aim at clearly defined political demands, instead it focussed on the destruction of society and the removal of large sections of the population (Laqueur, 1999:81). Contemporary terrorism may be typified by fewer attacks, however the number of casualties of such attacks is far higher as Whittaker (2004:76) identifies. It is hard to say whether the increase in casualties is due to the nature of the attacks, technological advancement of some of the weapons or due to increased urbanisation of areas where these attacks occur. Arguably the reason for the increased casualties is irrelevant: whether it is due to more effective weapons or more crowded locations does not matter. What responders must concern themselves with is how to minimise the effects of terrorist attacks through their own resilience capability and work towards better counter-terrorism strategies to reduce the propensity for such attacks to occur in the first place.

Terrorists also no longer operate in a vertical command structure but adopt a more horizontal organisational structure, with loosely formed cells acting fairly autonomously, making them far harder to track and their movements more difficult to anticipate (Martin, 2010). Similarly, links to the rest of the organisations with which they are affiliated are more difficult to ascertain due to this less tightly coupled organisation, although some suggest that the cells may now be becoming more organised (UK Now Number One Al-Qaeda Target, 2006: para.8). This looser coupling within terrorist organisations could be a response to reduce the propensity for ‘accidents or crises’ within the organisation as Perrow (1984) recognised; a theory that is discussed more fully at 2.3.4.3 of this thesis.

Terrorism is evolving into something far more sophisticated in at least two new directions as Whittaker (2004:115) suggests. More funds will be needed to provide hyper-modern devices which can be remotely operated. State of the art communications equipment will be commonplace, reiterating the difficulty in trying to track such movements (Whittaker, 2002, 2004). Technology is arguably the greatest source of threat as 'throughout history technology has changed the power balance between attacker and defender' (Schneir (2006:87). Such developments will require greater support and intelligence from the public to help to track such movements and provide vital information. Good relations with all sections of the community are therefore essential for the government and organisations to foster and this highlights the importance of risk communication theory discussed at 2.3.1 of this thesis to help achieve this.

Whatever the origins of terrorism are, it is important to distinguish between factors on an individual and on a group level. Simonsen and Spindlove (2000) distinguished between rational, psychological and cultural origins of terrorism. For them, rational terrorists make a cost-benefit analysis of their goals and objectives, whilst psychological motivations frequently stem from the individual's dissatisfaction with their life and accomplishments. Cultural motivations derive from the perception of outsiders and possible threats that they may pose to the terrorists' group survival. Conversely, at group level, terrorists may wish to focus government or society's attention on particular perceived inequities or respond to dramatic events that may have occurred. Peer group influences may also be a factor as Crenshaw (1992) supports.

As can be seen, the above points largely relate to the individual but it is also important to understand group motives and explanations in order to improve responses to terrorism. Overall, these can be broken down into three main areas which are: acts of political will, sociological explanations and psychological explanations. The former is employed to force changes that are desirable for the group. It is a rational choice and is described by some as the outcome of a learning process. Experience in opposition would have provided the groups with information on the potential ramifications of their actions (Crenshaw, 1998:11).

Sociological explanations, according to Martin (2010:66) generally hold that terrorism is a product of inter-group conflict resulting in collective violence. It is not a "senseless" act in the true sense as it is goal directed and is a rational choice as the perceived, solely viable option. It is argued that underlying this reasoning are two theoretical concepts; structural theory and relative deprivation theory. Understanding these two ideas may help to remove some of the mystery surrounding terrorist motives. Structural theory identifies social conditions that affect access to services and quality-of-life measures. In terms of terrorism, this theory often emphasises weaknesses in the state systems and policies that enrage cross sections of the population (Barkan and Snowden, 2001:53) citing Goldstone (1986:1-17).

Psychological explanations incorporate some of the motives for terrorism such as moral convictions and over-simplified definitions of good and evil and will be discussed below at 1.3.

1.3 Terrorist Motivations and Root Causes

Our degree of understanding of the motivations of terrorists can affect our ability to respond and hence directly impact on the extent of our vulnerability (Ditzler, 2004 in Moghaddam and Marsella, 2004:188). Ditzler's observation succinctly summarises the importance of the subject of terrorist motives, and why governments must attempt to understand them in order to improve their counter-terrorism processes.

When considering the levels of causes and motivations of terrorism, it is argued that it is useful to distinguish between preconditions and precipitants of terrorism; the former set the stage for terrorism in the long run and the latter are specific events or phenomena that immediately precede or trigger the outbreak of terrorism (Lia and Skjolberg, 2004; Crenshaw, 1990). It is possible to further break these down into structural causes such as globalisation, accelerator or facilitator causes such as the evolution of the 'new media', motivational causes that may be actual grievances people have experienced, and triggering causes that are provocative events (Bjorgo, 2005:4). Such a breakdown of

these factors may help in the design of counter terrorism measures through furthering understanding of what drives such acts of insurgency so that steps such as greater communications with relevant groups to try to clarify information and reassure communities may be achieved. This, as a step towards counter-terrorism, can be a vital tool as it operates both ways between government and local populations. The importance of such a risk communication approach for counter-terrorism is considered in detail at 2.3.4.3 of this thesis as referred to earlier.

Consistently throughout the literature there is the idea of root causes of terrorism whenever terrorist motivations are considered and it is these that it is argued that we need to understand if we are to effectively combat terrorism. Sinai in Bjorgo (2005:216) argues that in order to defeat ongoing or emerging terrorist insurgencies, understanding the underlying root causes must be the first line of analysis in combating terrorism but stops short of implying that resolving these will automatically halt the insurgency in a peaceful fashion.

However, this is not what this thesis wishes to advance. Instead it is the idea that the more the preconditions and drivers to terrorism can be identified, the more we can understand the nature of the terrorist threat and can therefore better tailor responses and policies to match these. How realistic is this though? The suggestion that single factors may be the determining factor that makes someone perform a terrorist act or makes them more likely to seems somewhat simplistic. As Clarke and Newman observe, trying to uncover the root causes of terrorism is to 'do the impossible' (2006:187). The idea of trigger causes however is a more realistic proposition. It is this view that Bjorgo (2005:3) suggests may be more useful. These are not enough in isolation but if combined with other more basic preconditions, may result in insurgent activity. This thesis suggests that Bjorgo's view is the more helpful in the fight against terrorism as it fosters a more proactive, iterative approach rather than Sinai's assertion that may encourage states to become complacent if they identify a perceived root cause. Sinai's view here may also be somewhat problematic if the terrorists' world view is completely unacceptable for the terrorised society. How can this be addressed if this is correct? This thesis proposes that

this may be the situation that is faced more frequently in years to come as extremist views become even more polarised. If this is so, it will no longer be possible to tackle the perceived root causes and instead efforts must be focused on factors and Bjorgo's trigger causes that combine in such ways to generate terrorist motivation, perhaps increasing the chance of success as it would generate more realistic, achievable goals.

Perhaps a more important point to consider is that the concept of root causes implies that terrorists are passive objects of social, economic and psychological forces, as some of Crenshaw's (1998:11) earlier points suggest. This does appear at odds with her first factor of 'political will', which emphasis rational choice amongst terrorists. In retrospect it may prove more productive to consider terrorists as rational, intentional actors who develop deliberate strategies to achieve political objectives. In light of this, it may be better to consider dynamic processes rather than static causes as Bjorgo (2005:3) concurs. It must be remembered that the identification of preconditions for terrorism may decrease the probability of attacks being executed however they do not make it a certainty (Moghaddam, 2004 in Moghaddam and Marsella, 2004:117). This further adds weight to the argument for a proactive, less legislature-based fight against terrorism which is the main focus of this thesis, rather than a purely military approach

Martin (2010) refers to motivations rather than root causes when considering terrorism. He posits that terrorist motivations can be broken down into four key areas:

- Moral convictions of terrorists
- Simplified definitions of good and evil
- Seeking utopia
- Codes of self-sacrifice.

The first point relates to the whole-hearted belief in the righteousness of the terrorists' cause; both their beliefs and actions are wholly justifiable. This belief occurs in many social settings but perhaps the two most frequent examples occur when firstly, a group deems that it has been morally wronged and that an immoral, powerful enemy is

operating against them using betrayal, exploitation and repression. In some instances, of course, this can be a legitimate concern if there has been a history of repression. The second setting transpires when a group construes a moral superiority over the enemy for whatever reason: if this was to be taken to its most extreme interpretation, it could potentially be suggested that this is how the West's actions in the Middle East and Afghanistan have been construed by some. However, arguably, anti-state groups could also use the same argument: are they not also trying to create stability for the suppressed groups whom they claim to represent? Furthermore, there are also cases where anti-state terrorism may try to disrupt the stability of society rather than attempt to create it, such as was seen in the attempted coup in Equatorial Guinea that allegedly occurred with the knowledge of the British government (Barnett and Bright, 2004).

The second point is often as a result of some form of political analysis and an unswerving belief in their cause and the injustice of the enemy's cause. This can be seen in Afghanistan where the Taliban could also argue that this is what is happening to their people as a result of Allied actions there.

The third point is somewhat subjective as it depends on the terrorist's belief system. In some cases this can only mean change in the current order. For others this can equate to a complete paradigm shift with changes in a society's ideological perspectives. This is a complex reasoning to try to counter as if individuals or groups believe that they will reach a utopia, how can any alternative be seen as attractive?

The fourth point relates to an important aspect in understanding terrorist motives. When terrorists adopt this belief system they feel that it justifies their behaviour and provides a moral superiority that otherwise may not exist. Participants may even feel cleansed as a result of the acceptance of self-sacrifice even to the point of willingness to die for their cause. Examples of this have been seen in the suicide bombers videos that have been aired on the internet and it is this that poses a particular challenge for the authorities to address. Again, risk communication theory is recommended as a useful starting point to help tackle possible feelings of isolation and to begin to break down barriers. What is

clear is that those who utilise terrorism and those who are affected by it are capable of holding a number of seemingly incongruous views about the nature of terrorism. Unfortunately, there does not appear to be a single homogenous factor for terrorism (Horgan, 2005 in Bjorgo, 2005:44).

Terrorism is therefore a nebulous concept. Such quandaries highlight the futility of attempting to identify root causes and add further weight to Bjorgo's suggestion that trigger causes should be the focus for countering terrorism in the medium to longer term. It is this assertion that this thesis will carry forward.

1.4 Extremism Vs Mainstreamism

Today there is a changed threat: the New Terrorism, spurred on by new technologies, characterised by asymmetrical methods, loose, cell-based networks, potential acquisition of weapons of mass destruction (WMD) as seen in the 1995 Sarin attacks on the Tokyo underground (reviewed in Chapter Four) and politically vague, religious or mystical motivations, again evident in all three attacks considered in the case studies later in this thesis. This is in stark contrast with the "old style" of conventional weapons, clearly identifiable organisations and movements, explicit grievances and relatively surgical target selection (Martin, 2010:28), for example as witnessed in the past attacks by the IRA both in Northern Ireland and mainland UK and by ETA in Spain.

When terrorism is discussed it may be helpful to also consider the notion of extremism as it could be argued that it is extremists who cross the line to commit acts of terrorism. Behind each act of terrorism there is a deeply held belief system (Martin, 2010:210). Wilcox asserts that extremism is more than just the content of one's beliefs, rather it is also the style in which those views are presented that signifies extremism (1996:54). This is perhaps a more pertinent definition that has more useful implications for terrorism analysis when governments and agencies seek to identify what it is that they are facing.

In order to try to develop strategies to deter terrorism, it is useful to consider some of the common characteristics of extremism to gain a better understanding to develop more appropriate counter-terrorism strategies. Martin (2009:39) identifies four distinct areas:

- Intolerance
- Moral absolutes
- Broad conclusions
- New language and conspiratorial beliefs.

Intolerance is demonstrated through the attachment of negative and divisive labels to those who disagree with the "cause". Characterisations of the so called enemy are often highly personalised and may result in them being dehumanised. This is an element of Moral Disengagement theory that will be discussed at 1.9. Moral absolutes are used often to create a clear distinction between good and evil and hold, what terrorists believe, is a morally correct vision of the world. This further seeks to create a moral superiority over other non-believers. Broad conclusions are often used to simplify the nature of the extremists' opponents and no exceptions are made to the generalisations. The evidence for these conclusions is based within individual's belief systems rather than objective data. New language and conspiratorial beliefs are created to demonise the enemy and set the terrorists apart from those do not share the same belief system; actions are seen as logical by terrorists but illogical to those outside the group. Once again, this is evident in the New Terrorism.

Martin (2010:53) raises an interesting point as to whether political violence always occurs at the edge of society or whether it is a rational choice of members of mainstream society. Those involved often claim that their actions are proportional to the acts of their oppressors whilst governments who take a more authoritarian stance claim that their actions are also justified as a proportional response to a current threat. It could perhaps be argued that the distinction between extremism and 'mainstreamism' in this instance may become somewhat blurred. This will of course have implications for terrorism responses. Today the 'threat from within' (Thachuk, Bowman and Richardson, 2008) suggests that it

is indeed society as a whole that should be the focus of counter-terrorism efforts, something that this thesis supports.

1.5 A Taxonomy of Terrorism

Much argument exists regarding a formal definition of terrorism and the approach to developing a definition is broadly in line with the evolution of judicial interpretation of the political offence exception (Guelke, 2009:167). Terrorism appears difficult to define even for government agencies: definitions are often reviewed and updated in light of changing events and even considering the etymology of the word is not particularly helpful. In 1988, Schmid and Jongman identified more than 100 definitions of the term 'terrorism' alone. Why is defining terrorism so problematic? Perhaps two clear reasons are that it is constantly evolving and that it covers many types of behaviour perpetrated for many different reasons, as Alvarez and Bachman acknowledge (2008:238).

It could be argued that this is just semantics but it is imperative that governments at least attempt to develop a formally accepted definition of terrorism as this is what will be used to determine whether a violent act was actually a terrorist incident and hence whether anti-terrorist responses should be activated, as Martin (2010:37) concurs. It is important to ensure that everyone is talking of the same thing when discussing terrorist acts and also when discussing different types of dangerous events otherwise how can they be managed? This will be discussed in Chapter Two at 2.4.1.

In addition, such definitions provide some help in trying to understand the nature of terrorism and help to construct a mental picture of what is and is not terrorism, even though this may not be complete or completely accurate (Alvarez and Bachman, 2008:245).

Of course, different people will have different perspectives on the definition of terrorism and this subjectivity also extends to the fact that definitions may depend on circumstances and attitudes which alter with time (Whittaker, 2002:11). It can therefore

be seen that this is a vital issue to address as the absence of agreed definitions acts as a hindrance to counter-terrorism. Whittaker (2002:181) suggests that if terrorism is so case-specific and varied, it is therefore almost impossible to get the firm legal grounding that will make most counter-action legitimate and publicly acceptable. The possible ramifications of such a statement do not need expansion but illustrate clearly the scale of the challenge faced by those charged with protecting society.

One area where there does appear to be agreement regards terrorist typologies; five key typologies have been identified, as Martin (2010:46) notes, which are state terrorism, dissident terrorism, religious terrorism, criminal terrorism and international terrorism. It is not necessary for the purposes of this study to detail each of these but a brief summary of the characteristics of each is useful to appreciate the differences. State terrorism is committed "from above" by governments against perceived enemies, either internationally or domestically. For example when the Israeli Secret Service allegedly murdered an individual in Dubai (n.a. 18th February, 2010). Dissident terrorism comes "from below" by non-state groups against perceived enemies. Criminal Terrorism is motivated largely by profit and the Mafia is sometimes cited as an example. Religious terrorism, perhaps the most relevant in the current climate, is motivated by an absolute belief that terrorist acts are necessary for the greater glory of the faith. Lastly, international terrorism occurs when targets are selected because of their symbolic representation of international interests, for example, the World Trade Center attacks.

It is clear however that these are not mutually exclusive categories, as can be seen in the September 11th and July 7th attacks and arguably the Sarin attacks; these were examples of religious and international terrorism. An appreciation of each of these elements should help to design more robust responses to future attacks. At this point it is pertinent to consider religious terrorism as this appears to be a common feature in the three case studies considered later in this thesis.

1.6 Religious Terrorism

Acts of religious terrorism are committed in the name of the faith frequently as a primary rather than secondary motive and those who participate believe that they will be forgiven or even rewarded in the afterlife (Martin, 2010:172). Hoffman (1998:92) suggests that it is not surprising that religion has become a more popular motivation as in the post-Cold War era, old ideologies have been discredited.

1.6.1 Primary and Secondary Motives

However, religion is not always the primary motive in religious terrorism but depends on the cultural and political environments of each terrorist movement. When it is a primary motive, it is at the heart of political and social agendas and can be seen, for example, amongst jihadi Islamic fundamentalists. It is important to note here however that religious terrorism is not equated with radical Islam; all religions have fanatical followers who have engaged in terrorism and to attempt to distort this picture is to make any arrangements to protect against and respond to terrorist acts futile. When religion forms the secondary motive, groups are often primarily motivated by nationalist or independence desires. Some religious affiliation is regarded as desirable as it is often an element of their national or ethnic identity but their secular identity is the impetus for their actions as Martin concurs (2010:174). An important caveat here is that religious terrorism can occur within groups and not only between them.

International Terrorism is also a major consideration in two of the three case studies in later chapters. It is sensible to therefore highlight the nature of targets for such terrorism at this juncture.

1.7 International Terrorism

Kegley observed ‘international terrorism represents one of the defining elements of politics on the world’s stage today’ (1990:3).

Symbols of international interest are generally the targets for international terrorism, not least due to their relatively low cost but significant benefits (Martin, 2010:271). Since terrorist acts are designed to create a threat to the image and power of the target group, symbolic targets are often chosen. Such symbolism is important to understand as it may be a key element in understanding the ultimate function of the act as Ditzler (2004 in Moghaddam and Marsella, 2004:193-194) suggests. The World Trade Center and Pentagon attacks in September 2001 are a good example of this.

It could be argued that in countries where internationally symbolic targets exist, measures should be taken to harden these against attack. However such hardening measures can result in risk transfer such as that seen in London following an Irish Republican Army (IRA) attack in the city. Defensive cordons were erected, with chicanes and search points on every access road as Freilich and Newman (2009:235) highlight. This concept is discussed in detail in the context risk transfer within the risk and crisis theory at 2.3.3 of this thesis. It is posited that target hardening should occur within reason but should not be the sole or main response in counter-terrorism strategies.

Whenever international terrorism is spoken of, the term asymmetrical warfare is frequently used. Asymmetrical warfare describes the more unconventional and unpredictable elements of political violence which makes it particularly hard to counter. The almost guaranteed media attention for international incidents also means that even smaller terrorist groups can gain worldwide exposure. Overall, it is argued that there are two defining characteristics of this type of terrorism: it is specifically selected by violent extremists as a methodology and it is an identifiable type of terrorism. As Martin (2010:272) asserts, it is a tactical-strategic instrument of terrorism and a category of terrorism. He goes on to suggest that there are in fact often frequent linkages between seemingly domestic dissident groups and international terrorism as they may select targets that only tangentially symbolise the course of perceived oppression and require them to travel abroad in order to mount an attack. The implications of an attack on the global stage means that their cause receives far greater publicity and hence acts as some

form of compensation for their perceived injustices. This 'spillover effect' where domestic struggles are played out internationally is increasingly seen on a global scale.

1.7.1 Reasons for International Terrorism

Ideological reasons can be suggested to be a main driver for terrorist acts; perceived occupation by foreign armies, foreign business interests or forms of administration could all be perceived by terrorist groups as legitimate reasons to perpetrate terrorist acts (Martin, 2010:279).

'Perceived efficiency', although simplified, has also been cited by some (Kegley, 1990:21) albeit a highly abhorrent argument, for employing international terrorism. This can take several guises which include the chance to maximise publicity, the potential to inflict maximum psychological anxiety and also creates the opportunity to increase the chance for having their demands met as the countries involved become the focus of global attention and in some cases concede to terrorist demands in part due to the increased scrutiny (Martin, 2010:282). The options in response to terrorist attacks will be considered in section 1.11 of this thesis. Martin goes on to suggest that there may also be tactical reasons why revolutionary theory translates to international operations for some groups. For him, it may be due in part to the increasing globalisation where members can live in multiple countries yet still remain in regular contact, as was seen by the Hamburg cells of al-Qaeda who were involved with the 9/11 attacks. This dispersal of cells means that it is far harder for the authorities to identify and track them, which is the main attraction, as discussed earlier.

1.7.2 International Terrorist Environments

Terrorist networks operate in specific environments and in order to develop a more coherent understanding of them, it is useful to employ a framework for interpretation. Martin (2010:287) has developed a constructive model that defines four environments although they are not mutually exclusive definitions. The four environments are described as:

- Monolithic

- Strong multi-polar
- Weak multi-polar
- Cell-based.

Monolithic terrorist environments emphasise state-centred behaviour, with a single threat deriving from a single source. Strong multi-polar environments also emphasise state-centred behaviour but several sources support the favoured groups. This environment also makes the important assumption that all movements are linked to state sponsors with no autonomy. Weak, multi-polar environments place more emphasis on the terrorist groups rather than solely on the state. Although state sponsorship is taken for granted, the group has more autonomy than in previously noted environments. It is far harder to counter this environment as movements are more adaptable. The cell-based environment emphasises the terrorist movement and assumes that terrorist movements are not constrained by government. The cell movement is very fluid and thus very hard to counter (Martin, 2010:288). By identifying relevant environments, it may help to produce more effective counter-measures.

In conclusion, it is necessary to also note the existence of another environment that is increasingly seen: that of the "stateless revolutionaries". These groups operate solely in the international arena and hold no domestic presence in a home country. Their motives are secular ideological revolution, or sectarian radicals defending a faith or representing stateless ethno-national groups; al Qaeda is an example of the second motivation (Martin, 2010:296).

1.8 Mala Prohibita or Mala In Se?

In any discussion surrounding terrorism, morality is invariably touched upon and there are two concepts within criminal justice that are pertinent to any study of terrorism; those of *mala prohibita* and *mala in se*. The former refers to acts that are made illegal by legislation, declared so by society but not because they are inherently wrong, for example gambling prohibition. This is more of a moral prohibition than prohibition because it is a

fundamental evil. Mala in se, in contrast, refers to crimes that are immoral or wrong in themselves; these are difficult to justify and will never be legalised, for example rape or murder.

It is here that discussions of terrorism can become more complicated: the morality of the acts will certainly be relative, dependent on whether you are a victim of these, a perpetrator or an independent party. To quote the famous saying, "One person's terrorist is another person's freedom fighter" (Unknown) may be uncomfortable but certainly true. Similarly, if freedom is the asset to be protected, is extremism as a defence a vice? These are all things that need to be considered when building resilience to terrorism, distasteful though it may be because any counter-terrorism processes must be able to convince potential terrorists that there is a better way forward that does not involve terrorist acts. To do this, the individual's viewpoints must be understood and considered in terms of tailoring and developing appropriate information and communication strategies.

1.9 Modus Operandi: The Terrorists' Protocol

When terrorist groups utilise methods that would invariably cause the deaths of their enemies, which may include innocent bystanders, they frequently cognitively restructure the moral value of killing through a process of moral disengagement, although from their own perspective, they are still morally engaged. It is this apparent lack of compassion that causes many onlookers to oppose their campaigns despite possibly sympathising with the goals and objectives of the extremists (Martin, 2010:337). If one takes a completely neutral view, this can also be seen when nation states injure civilians and statements are made to the media concerning 'collateral damage', for example as in Afghanistan (Zenko, 2009). As a result, governments and organisations must ensure that they consider the perception of others regarding their actions, not merely the end goal that they are trying to achieve.

Disengagement may include de-humanising victims, or blaming them for bringing suffering on themselves, as Bandura (2004) in Moghaddam and Marsella (2004:124)

observes. Bandura goes on to note that the most effective set of mechanisms for disengaging moral control is the cognitive restructuring of harmful conduct through moral justification and sanitised language (Bandura, 2004 in Moghaddam and Marsella, 2004:130). This disengagement comes about through training rather than existing from the outset. This is why extremist preachers and terrorist training camps are so frequently the target for counter-terrorism and should remain so as they are integral to the process of terrorism.

Terrorist acts seek to destroy the psychological security that defines victims' way of life (Ditzler, 2004 in Moghaddam and Marsella, 2004:205). This was evident particularly following the 9/11 attacks when the numbers of people travelling by air fell (Blalock, Kadiyali and Simon, 2005:1) as a result of the attacks and more recently the drop in visitors to London immediately after the July 7th 2005 attacks (Robertson, 6th July, 2006). Creating a climate of fear is one way that terrorist groups can project an image of strength that is not based on their actual capabilities (Alvarez and Bachman, 2008:248). Given this, consideration of terrorist objectives is therefore a necessary step in the creation of response plans and why discussion of these is included here. The goal of terrorism could then be argued to be the production of fear rather than the destruction of targets.

Given the developments and tactics of terrorism, is it still effective? Arguably, it is, even if only to raise awareness of the terrorists' cause. But what is the measure of effectiveness to these groups? Martin (2003:268) suggests five criteria by which terrorists may claim victory however this list is not exhaustive. He suggests that media and political attention are common indicators as any publicity for these groups is seen by them as positive as it highlights their cause. Events that have an impact on their audience, causing them to change their travel plans or their opinions is another measure of success that may be used as it is felt that the audience has been manipulated. Allied to this is the notion of the disruption of normal routines, particularly if a transport system is targeted and citizens feel that they have to change their arrangements through fear of further attacks; something which the Aum Shinrikyo cult hoped to achieve in the Tokyo Sarin attacks in

1995. This incident is considered in Chapter Four. Similar issues are also identified in Chapters Five and Six.

1.10 The Function of the Media

Earlier in the discourse on international terrorism, it was noted that some groups select internationally symbolic targets in part for the increased media coverage and publicity that such an action would generate. The role of the media is an important consideration now in any treatise on terrorism; the way that acts are portrayed, the way advice is presented to the public, the way reports may be biased means that understanding the media and engendering good media relations is a crucial part of the fight against terrorism today; something which crisis management already actively considers and will be considered in Chapter Two. Conversely, the use of the media by terrorists is also an important area to consider when a frequent collateral objective for terrorist groups is to maximise the role of the media and generate a level of exposure that would be hard to duplicate (Ditzler, 2004 in Moghaddam and Marsella, 2004:1964) even with the largest advertising budgets. The modern terrorist therefore engages in psychological warfare aided immensely by sophisticated media, without which they would be unable to spread their message and be isolated from the rest of the community (Whittaker, 2004:112).

1.10.1 Publicising the Cause

Media-oriented terrorism may occur where acts are deliberately executed to attract the attention of the media and are given high priority by news programmes and publications (Kelly, 1998:54). It could be argued that there may be a temptation to make attacks so presentable in media-conventional terms that objectivity may take second place to the visually gripping, as Whittaker (2004:95) agrees. Some may even go so far as to cultivate relationships with reporters and create more legitimate organisations that promote media relations as could be seen, for example, in the operation of Sinn Fein (Martin, 2010:384). However, even this may not be enough to effectively communicate the terrorists' message, which is why some employ mass communications technology to better spread their message efficiently and in a timely fashion, thus increasing its impact. This may be

by personally using technologies to send their message or through more skilled presentations to be sent through media outlets. If this is done skilfully enough, sympathisers may be able to increase public pressure on governments to respond or provide some form of concession (Martin, 2010:384). The Internet has proved a useful resource for terrorists and their sympathisers not only through quick and cheap communications between cells and group members but also the creation of websites that promote their message. Perhaps somewhat surprisingly, many of these sites are not violent and inflammatory but instead portray suppressed victims with rich cultures and heritage. Whatever the outcome, terrorists now manipulate the media to disseminate information about their cause and to facilitate delivery of their message around the world. Conversely governments manipulate the media to suppress terrorist propaganda and try to manipulate public opinion (Martin, 2010:392).

1.10.2 Mass communications and the 'New Media'

New media use existing technology and alternative broadcasting formats to analyse and disseminate information and frequently present opinionated political and social commentary (Martin, 2010:388). The distinguishing feature of this genre could be regarded as the extent to which discussion opportunities using it attract public officials, citizens and members of the mainstream press (Davis and Owen, 1998:7).

The perspective of governments and the media will now be considered, leading on to a consideration of terrorists' manipulation of the media. This will show how responses need to be developed to minimise the chance of success of such actions.

1.10.3 Governments' Standpoint

Any government policy must be popular and coherent and in order to achieve the former, some degree of control is often sought over the media's presentation of events. However, there is a fine line between censorship and genuine concern to try to avoid creating panic amongst the public. How this balance is found and managed is no easy feat. Fink (2002:96) suggests, as will be discussed at 2.10 of this thesis, that a useful starting point is for governments and organisations to develop a goodwill reservoir in peaceful times so

that in a crisis, it is easier to disseminate appropriate information as credible, open information that can be relied upon. This will form part of the recommendations from the thesis.

If such information could be disseminated in a controlled, trustworthy manner, panic is less likely to ensue. Consider the statement by Sir Ian Blair following the July 7th attacks in London and the confusion and consternation caused by his inaccurate statements: a point which is further discussed at 6.10.

The present culture of openness regarding statements to the public concerning the current terrorist threat is certainly a step in the right direction. However, this has to be consistently applied otherwise people may become suspicious and perceive a situation as more grave than it may be. The recent escalation in the threat level faced by the UK was largely explained however when the reasons for this were questioned by the public and the media, ministers became evasive citing National Security as the reason for their lack of explanation. It is such statements that do not help in these circumstances as the public either feel that ministers are hiding something or that they do not think that the public may be intelligent enough to cope with such information. The worst outcome could potentially be that the public think that ministers do not actually know enough about the situation that may be faced, undermining public confidence, increasing fear, something which Lord Carlile, as the government's reviewer of terrorism legislation, rightly noted (UK Terrorist Threat Level Raised to Severe, 23 January 2010). The lack of a clearer response and the allusion to something greater could potentially cause consternation, thus increasing the level of fear. Perhaps the best response in this situation that can certainly be made without jeopardising National Security, is that general intelligence information suggests that it is pertinent to raise awareness in the community, to be vigilant and act as another deterrent for terrorists, rather than hiding behind other such statements. If a policy regarding communication with the public is to work and is genuinely supported, it must be fully embraced.

It is possible for governments to also use the media in a positive manner for security, to allay fears and to reinforce a common sense approach to terrorism. However, care is needed to avoid management from developing into manipulation. For democratic societies, terrorism can cause serious problems for the ruling governments due to the impact on the psychology of citizens and the attention that it may command (Heymann, 1998:9) hence good media relations are an integral part of any preparation and execution of counter-terrorism plans. Shrivastava (2005:66) posits, further discussed at 2.10, that attack consequences can also include psychological trauma which reaches beyond the victims through the media. If this is not effectively managed, mass panic could ultimately ensue or at least a culture of fear; neither of which is desirable for the good of society.

If good relations do not exist, there may be considerable tension between governments and the media that may exacerbate a dangerous event. The tension arises from the necessity to keep the public informed and deliberate attempts to disseminate propaganda (Martin, 2003:280). The other judgement call to be made rests with the media and that is the decision as to where to draw the line in order to report the news without disseminating the terrorist message (Martin, 2003:281). The Arab television station Al-Jazeera has been a focus of such discussion in relation to its broadcasts relating to Al-Qaeda and other terrorist groups.

Given the influence that terrorism can have on government policy, it is perhaps not surprising that terrorist acts are given priority in the media. However, their treatment is inconsistent and some broadcasts can at times even appear to glorify the violence and not explore the underlying causes of it. This may be in part due to the competition between media organisations and the pressure to get the exclusive story rather than to ensure an objective representation of the event, hence the news triage is often driven by attracting the greatest number of viewers or readers and empathy with victims will always attract the public (Martin, 2003:285). How the story is reported also affects the public's perception of the act and the perpetrators. Labelling by the press frequently reflects social norms although there may be a move to use more positive terms than "terrorist" and may be more euphemistic (Bandura, 1998) in Reich (1998:178).

Information is power and this is no different for terrorists. Using the media as a weapon, focusing on symbolism means that terrorist groups can influence governments and societies more easily (Martin, 2010:396). The contagion effect is also something that needs to be considered, which refers to the theoretical influence of media exposure on the future actions of similar extremists (Weimann and Winn, 1994:157-160). If a terrorist campaign has been particularly "successful" then others may be motivated to employ similar tactics. Some argue that examples of the contagion effect include the taking of western hostages in Lebanon on the 1980s and hijackings in the twenty years from the 1960s-1980s (Martin, 2003:295). The theory has also demonstrated some validity and there does appear to be some correlation between media coverage and time between terrorist cycles (Weimann and Winn, 1994:219). From this consideration of the literature regarding the media and terrorism, the importance of appropriate communication and the need for this to be at the heart of counter-terrorism strategy is clear; countering terrorists' media-oriented strategies through more effective dissemination of information and public education must be key elements of a proactive programme (Post, 2005) in Bjorgo, (2005:67).

1.10.4 The Media's Perspective

Ideally, all news stories would be presented objectively. However "media spin" is often observed in order to sensationalise an event and obtain maximum coverage for the story. In every form of news media, a "news triage" occurs where stories are selected with some given higher priority than others (Martin, 2003:279). Given this, editor bias is invariably reflected in the choice and ordering of stories and an event as dramatic as a terrorist attack will be high priority for news agencies. Consequently this will affect audience perception of the environment, not least because many editors will concentrate on the event itself and may not include information about the terrorist cause or their symbolic message (Martin, 2003:280).

Freedom of the Press and the public's right to know are generally accepted in democratic societies. However, some form of regulation may at times be necessary, for example if national security is at stake. Self-regulation is the main focus in the West although this

can be quite inconsistent. Governments can also selectively release information during terrorist incidents to take the decision out of the hands of the media (Martin, 2003:297). This emphasises the need to foster good media relations between the government and the Press in order to try to prevent sensationalism of such events and to enable better management of crisis events. The link between the media and terrorism can be seen as an almost symbiotic relationship due to the high news value of terrorist acts (Laqueur, 1999).

The importance of the media in crisis management will be discussed in detail in the following chapter at 2.10.

1.11 Responding to Terror: The Options

The key element to consider in responding to terrorism is not to over-react, as the causes of terrorist groups are best served when society becomes polarised, as Gupta (2005) in Bjorgo (2005:28) suggests. The key then is to fight terrorism on ideological grounds and offer alternatives, as Whittaker (2004:61) also suggests, through the creation of alternative routes out of terrorism for those who wish to leave, through dissuasion and to facilitate breaking away, although exactly how this would be done in light of the close-knit nature of terrorist groups, remains questionable. Post (2005) in Bjorgo (2005:67) similarly highlights the importance of facilitating terrorists leaving through the creation of pathways out of terrorism. Amnesty programmes as used by the Italian government for former Mafia members may be one way to address this.

1.12 The Future?

It is impossible to accurately predict the future of terrorism, particularly in the longer term. Nonetheless, it is possible to suggest future scenarios based on a longitudinal framework of history and trends as Martin (2003:385) concurs.

In the short-term this thesis argues that it seems unlikely that the sources of terrorism will change and that the fascination with WMD, the use of more sophisticated technology and the increasing use of a cell-based structure will remain with us for the foreseeable future.

Many authoritarian states still exist and this is unlikely to change in the near future. States will continue to believe that terrorism serves their interests as Martin (2003:386) suggests. In countries where religious and ethno-national conflicts remain, dissident terrorism is also likely to continue. As discussed earlier, social reform may help to address such grievances as may ongoing international co-operation. Similarly, Extremism appears unlikely to cease soon, particularly in light of the ongoing military campaigns in the Middle East and Afghanistan; attacking internationally symbolic targets will remain a prominent tactic as long as such acts are guaranteed media coverage to publicise the cause. Further developments in new technologies and communications are likely to ensure that they remain at the heart of the New Terrorism and facilitate networking and communications between cells. The growth of cyber-terrorism appears inevitable as we continue to grow as an information society.

Martin (2010:524) asserts that terrorists are making resolute efforts to acquire WMD, although there is no definite evidence to support this and many, including Alvarez and Bachman (2008:271) think it unlikely. However, the threat alone of such a weapon can also achieve the desired effect so it may be that the future may hold more threats of their use rather than their actual use. Any new technologies would be costly to acquire both in monetary and time terms but for some larger organisations, such as al-Qaeda, this may not be problematic. It is here that caution should be exercised to avoid scaremongering and unnecessary panic amongst citizens; another strong reason for good media relations and adoption of risk communication methodologies.

1.13 In Conclusion

From this discussion it is evident that terrorism can never be eliminated but it is possible to minimise terrorist threats. Terrorism therefore is akin to risk as a concept, proving the

link between the application of risk and crisis theories and methodologies to the management of terrorist incidents, validating the purpose of this thesis.

It would appear that the best defence against terrorism is a government with broad, popular support through normal channels of law enforcement without resorting to counter-terror (Kirkham, Levy and Crotty, 1969:4 in Bernhardt, 1970:146). Although this observation was made nearly thirty years ago, it is suggested that it is still relevant today. To support this, the moderate voices within society must enable support for integrating the benefits of modernisation with humanist principles that uphold human rights, equality and dignity as Bandura (2004) in Moghaddam and Marsella (2004:150) posits. Without a moderating influence, the cycle of attacks and retaliation will merely continue and society will become further divided.

Ultimately, any government response must consider three key measures as Sinai (2005) in Bjorgo, (2005:218) addresses: governments must recognise and prioritise what they consider to be the most significant root causes. Next, they must also consider clear definitions in combating terrorism and consider the short, medium and long term, as well as devise a method to measure the effectiveness of policies. Lastly, all government levels should be involved in the process to avoid a piecemeal, disjointed approach.

Whatever counter- and anti-terrorism options are adopted, it is important to ensure that they are not knee-jerk reactions to events else governments risk exacerbating an already dangerous problem. What can be argued is that international terrorism is a reflection of events in global politics and is therefore not unforeseen.

This chapter was intended to help to understand the causes and triggers of terrorism and how those affected may begin to respond. Without such theoretical and background understanding, responses to terrorism and improving resilience will be futile as we may well be using outdated interpretations and methods to fight a constantly evolving threat.

When combined with the following chapters, it is intended that the reader will have a far greater understanding of the threat that we now face and also of how we may begin to build longer-term responses.

The next chapter will consider risk and crisis literature to highlight the key theoretical perspectives in this area. It is intended that the information presented here will be used to inform recommendations for practice, together with lessons learned from the included case studies in Chapters Four, Five and Six.

2. Risk and Crisis: Theoretical Underpinnings

2.1 Introduction

Organisations increasingly have to face many types of risks and crises that present varying degrees of threat to their operations. Theorists argue that there has been an increase in dangerous events that Ulrich Beck described as a change from a 'class society' to a 'risk society' (Borodzicz, 1999:1).

Burke (2005:639) recognised that terrorism and threats to individuals and organisations are affecting organisational behaviour and these effects exist at several levels in interconnected areas. It is for this reason that it is necessary to consider risk and crisis literature in the course of this research to inform analysis and recommendations.

Two areas will be considered during the course of this literature review: firstly, risk approaches will be discussed. This is important to provide the academic, theoretical underpinnings for this thesis. Secondly, crisis management literature will be reviewed in order to highlight the specialist nature of crisis management and how it differs from risk management. This is an important area to consider as it has ramifications for how first responders and governments may develop their emergency preparedness in light of recommendations.

2.2 Risk: The Story So Far

Although risk may be considered by some to be a contemporary topic it has in fact been an area of interest for scholars since the time of the Ancient Greeks and Egyptians (Borodzicz, 2005:2). However, it was not only Western scholars who considered the subject of risk: early Chinese philosophers developed the 'I Ching' or Book of Changes as an aid to decision making which is still used my many today, as Borodzicz (2005:2) identified.

Perhaps one of the most detailed outlines of the development of risk since the seventeenth century was provided by Mary Douglas (1990) and has been supported by many including Lupton (1999:5-6). Douglas suggests that the notion of risk originated in the field of gambling and the mathematics associated with this in probability theory. Risk referred to the probability of achieving a certain score combined with the magnitude of the potential gain or loss. In the eighteenth century with the growth in international trade and use of ships to transport goods, the concept of risk was used in marine insurance. This was presented as a neutral idea that took account of both gains and losses: insurers would calculate premiums based on a ship returning home either with a full cargo or sinking with all on board.

In the nineteenth century, the study of economics developed new ideas of risk where individuals were thought to be risk averse and entrepreneurs were risk takers, requiring incentives to accept the risks of their investment. This could be seen as justification for the increasingly prevalent capitalist philosophy. It was here that the concept of risk perception began to alter in light of the changed social context.

In the twentieth century, the concept of risk evolved to refer only to the negative outcomes in engineering and science. It is from this that the fairly widely accepted definition of risk developed: a future event with a chance or probability that it will occur and the response if adverse consequences affect it.

For social scientists, a very different notion of risk was taken. For them, risk was not a one-dimensional concept: they argued that risk means different things to different people in different contexts and that risk is a socially-constructed concept (Royal Society Group, 1992:7). This is something that has already been observed in Chapter One at 1.8 in the quotation ‘One man’s terrorist is another man’s freedom fighter’ (Unknown), proving the importance of multiple realities for this thesis.

In the latter part of the twentieth century, noticeably since the 1980s, the idea of accountability and blame came to the fore when discussing risk. A ‘blame culture’ now

exists where someone must be culpable for the risks that affect us. Douglas and Wildavsky (1982) argue that as the world has become a more individualist place, so risk has become a tool of the legal system. The pressure is not against taking risks but rather against exposing others to risk which can therefore be seen to drive the notion of blame.

In today's world, Beck (1998) in Franklin (1998:11) suggests that in a risk society, modern society becomes reflective and an issue and problem for itself. Ewald (1995) in Lupton (1999:6) furthers this by postulating that we are governed by events that do not yet exist but that strongly influence our present actions and affairs so risks are a kind of virtual, yet real, reality. However, Denney (2005:32) suggests that Beck is unduly pessimistic and rationalistic, over simplifying the position as he does not take account of subtle differences in risk perception amongst individuals. Nonetheless, Beck is still highly influential in this field. If we are to consider the current attitude to the terrorist threat, it could be argued that Beck is correct that we do live in a risk society but Denney's note of caution is also correct; consider the idea of the official threat level to the UK and how individuals interpret that. Some fear that terrorists are hiding in every city in the UK, while others take a more pragmatic view that, yes, a threat exists but it is not all encompassing. Ewald's comments can also be seen in the so-called 'climate of fear' (Alvarez and Bachman, 2008:248) surrounding terrorism.

Many questions surround the notion of risk and Turner (1994:149) suggested that this rests on whether risk is something that is taken or something that afflicts us, i.e. is it a choice or a circumstance? As this review of the literature proceeds, it will become clear that confusion still exists as to the nature of risk.

2.3 Theories of Risk

Borodzicz (2005:13) suggests that Risk theories can largely be divided into three areas although this is not the only method of categorisation:

- Sociological
- Psychological

- Cultural.

It is argued that this tri-fold classification is the most useful approach to the theories of risk as it is an intuitive breakdown of the approaches.

As this thesis is examining terrorist incidents and specifically the responses and resilience to these, it is the sociological approaches that will be focussed upon as these are directly applicable to this research. Psychological and cultural approaches, while interesting, do not contribute directly to the specific focus of this research. For this reason, consideration of some of these can found at Appendix II.

Most risk theory today is dominated by an ontology that is 'framed by the assumptions of earlier periods' (Healy, 2006:78). This observation echoes that made in the previous chapter at 1.2: here too it was recognised that the current response to terrorism is also framed by assumptions of earlier periods. This is why such responses are now outdated and need to evolve. Such evidence further supports this thesis in its assertion that responses to terrorist incidents need to be reconsidered and that they can usefully be informed by risk and crisis theory.

Sociological approaches will be used to inform analysis and recommendations of the case studies included in this thesis and will be carried forward to develop the generic recommendations that this thesis generates. These approaches comprise:

- Risk Communication
- Systems approaches (also known as socio-technical)
- Risk Homeostasis Theory.

2.3.1. Psychometric Approaches

Although sociological approaches are the focus of this thesis, it is necessary to consider briefly the area of psychometric approaches. This is because one of the most important risk management methodologies for this research, risk communication, grew from this school of thinking.

Psychometric approaches tried to contemplate the qualitative elements of hazards that people take account of but are not included in formal risk assessment. These are divided into two general factors that of 'dread' and 'unknown' risk as Slovic (1987) asserted (Maule, 2004:22). Appendix III provides a useful example of this. Perceptions are affected by experiences and individual world views. Borodzicz (2005:18) noted that early studies in this field measured the extent to which people expressed a preference towards particular risks and how this related to actual fatalities. The aim was to re-educate the public where necessary so that their risk perception did not conflict with expert opinion; the start of the risk communication school. One important distinction to note when considering risk in this context is that between voluntary and involuntary risks where the former were considered to be self-imposed (personal risks) and the latter were exerted by an outside influence over which individuals had no control and affected others (general risks). Research on risk perception has often not addressed these differences and has worked on an undifferentiated notion of risk (Sjoberg, 2003:19-20). Personal risks were often judged as smaller than general risks and it is therefore important to understand the rationality behind the reasoning.

More recently, researchers in this field have attempted to consider issues of social and cultural group membership in responses to risk which arguably would impact on how risks are perceived and would further the work already carried out (Lupton, 1999:23).

Previously in many studies it was assumed that the larger the risk, the more people want it to be mitigated, which is not the case (Sjoberg, 2003:21). It is more important for them to know that the risk had been mitigated if it had severe consequences, rather than it being dependent on the size of the risk in question. As Sjoberg (2003:21) posits, the psychometric paradigm has worked on the assumption that demand for risk mitigation is related to perceived risk but it is unclear if general or personal risk is the most important factor for this.

The Royal Society report (1992) highlighted the importance of Otway and von Winfeldt's 1982 research in this field, which proposed that any measurement of risk needed to be

sensitive to the system of understanding in which that risk was viewed and by definition, also suggested that even where irrational lay persons' views exist, these may actually be subject to a logical framework as they were constructed within their perceived reality. Their studies were replicable and the results could be measured: something that had not always been the case in such research.

2.3.2 Risk Communication

Risk communication can then be seen to have grown from the field of risk perception as it was noted that the language used by experts when communicating with lay people was often highly technical and difficult to understand (Powell and Leiss, 1997; Lupton, 1999:19). In addition, quantitative information that was unclear was frequently passed on to lay people: something that Borodzicz (2005) and Covello (1991) amongst others recognise.

Maule (2004:17) argues that effective communication is critical for translating risk management knowledge into effective practice which supports the assertion of this thesis that risk communication has a key role to play in the response to terrorist incidents.

Risk communication work can be characterised as focussing on the dialogue between experts and lay people. Hayenhjelm (2006:2) suggests that this is achieved in one of two ways: either as an attempt to bring the attitudes of the public closer to that of the experts or to engage the public in a dialogue valuing their contribution as important to decision making as Slovic (1987), Renn (2003) and Wester Herber (2004) for example, concur. Lay people tend to arrive at different assumptions from the experts (Maule, 2004:19).

The aim of this approach is to try to narrow the gap between expert and lay people through information and education, providing instruction for dangerous events. It was argued that this would improve risk management as the two sides would be talking about the same thing and hence it would create a more unified approach to the management of risk. Misunderstandings and therefore unnecessary panics would also be reduced, providing conflict resolution through mutual understanding. By increasing understanding it was thought that individuals would then become more tolerant of risk. The ultimate aim

was to achieve behavioural change amongst the general population and the establishment of realistic risk management goals. The value of such an outcome in the context of responses to terrorism is clear, again strengthening the use of such an approach as part of the counter-terrorism strategy.

Another distinction between risk communication approaches is that of one- and two-way communication which depends on whether the information has been disseminated to the public or communicated in dialogue, although this distinction is often used to distinguish between traditional approaches to risk communication (one-way) such as dissemination of information from experts to lay people and the newer approaches (two-way) that are more open such as shared decision making (Hayenhjelm, 2006:2). Hayenhjelm goes on to assert that the roles of participants are often asymmetrical as they play different roles depending on access to information and agenda setting (2006:4). These roles may be a communicative role where individuals have influence in defining the agenda or informational and epistemological roles where individuals have expertise about hazardous activities and mitigation or lastly, a risk role where they have influence over the activities and decisions concerning them (Hayenhjelm, 2006:5).

No discussion of risk communication would be complete without reference to the media as they reflect the nature of definitions of risk in our society. Denney (2005:83) suggests that there is competition within the field which centres on four processes:

- control: over timing and visibility of the risk message
- legitimacy: having the risk story treated as credible and authoritative
- trust: maintaining and enhancing public trust in the message
- precedence: establishing the dominant definition of the situation and structuring the agenda for debate (Petts et al, 2001).

This could be argued to suggest that it is this, rather than the true representation of risk that drives the media's portrayal. Denney (2005:84) further suggests that the social amplification of risk framework may also go some way to explaining the creation of risk

in media messages, as it tries to integrate individualistic and culturalist perspectives to explain why some things may be viewed as a risk and others are not (Kasperson and Stallen 1992). There are problems with the model though as attempts to test it have been inconclusive and attempts to establish a link between media messages and public understanding of risk have failed (Wahlberg and Sjoberg, 2000).

The theory continues to develop, especially in light of today's media coverage where lay perceptions of events may be particularly influenced by media reports, perhaps increasing the frequent divergence between lay and expert opinion. This assertion is supported by risk communication theorists including Irwin (1995) who note that lay perceptions are influenced by various social, cultural and psychological factors which are therefore less rational. Conversely, expert approaches take a more objective view which does not take account of subjective factors, or at least does so only marginally. This view was reinforced through risk research in the early years which was largely performed within a scientific context and reinforced this polarised view of risk management. The dilemma of risk communication is when individual behaviour is focussed upon: people are mostly worried about others and when they are worried for their own sake, it is impossible to tailor reassuring measures to take account of all individuals' contexts. Perception and action in response to risk can largely be determined by previous experiences (Maule, 2004:21).

More recently, there has been increasing concern within this field about the pluralistic nature of risk and as a result, there has been a greater focus on understanding the ways that risk may be perceived: as Wynne (1992) proposes, it is useful to consider how conceptions of risk are constructed and the deeper social assumptions within which they are embedded, supporting the points raised earlier in this section.

This approach is particularly important within the scope of this thesis when considering counter-terrorism processes and communication with the public. However, it is not just that lay people need to listen to experts; it is a two-way process. One of the most compelling arguments for this was the Braer Tanker disaster in Shetland. Locals had

always predicted such an event but the experts did not listen so that knowledge was not realised (Borodzicz, 2005:34). In recent times, risk communication theorists have returned somewhat to the risk perception hub through the focus on the pluralistic nature of risk and hence how it may be perceived. This is of course dependent on the frame of reference of the actor perceiving the risk, thus Wynne (1992) suggested that it is of more use to consider how perceptions of risk are created.

It is debateable whether any meaningful communication has actually occurred between experts and lay people. If it does, it is imperative that the individuals' frame of reference is also considered in order to determine why risks have been perceived in a certain way and how the world has been constructed within individuals' minds. This would certainly help to achieve a process of mutual understanding which is the ultimate aim of this approach. However caution is needed as information may be distorted in order to achieve a specific outcome as Irwin (1989:19) recognised. Independent assessment should therefore be incorporated into risk communication processes. Irwin went on to note that one of the main issues that needed to be addressed is the apparent dependence of official organisations on risk definitions that are presented in expert terms. Until this is addressed, it is arguable whether, even if meaningful dialogue did occur, it would overcome the difficulties in mutual understanding.

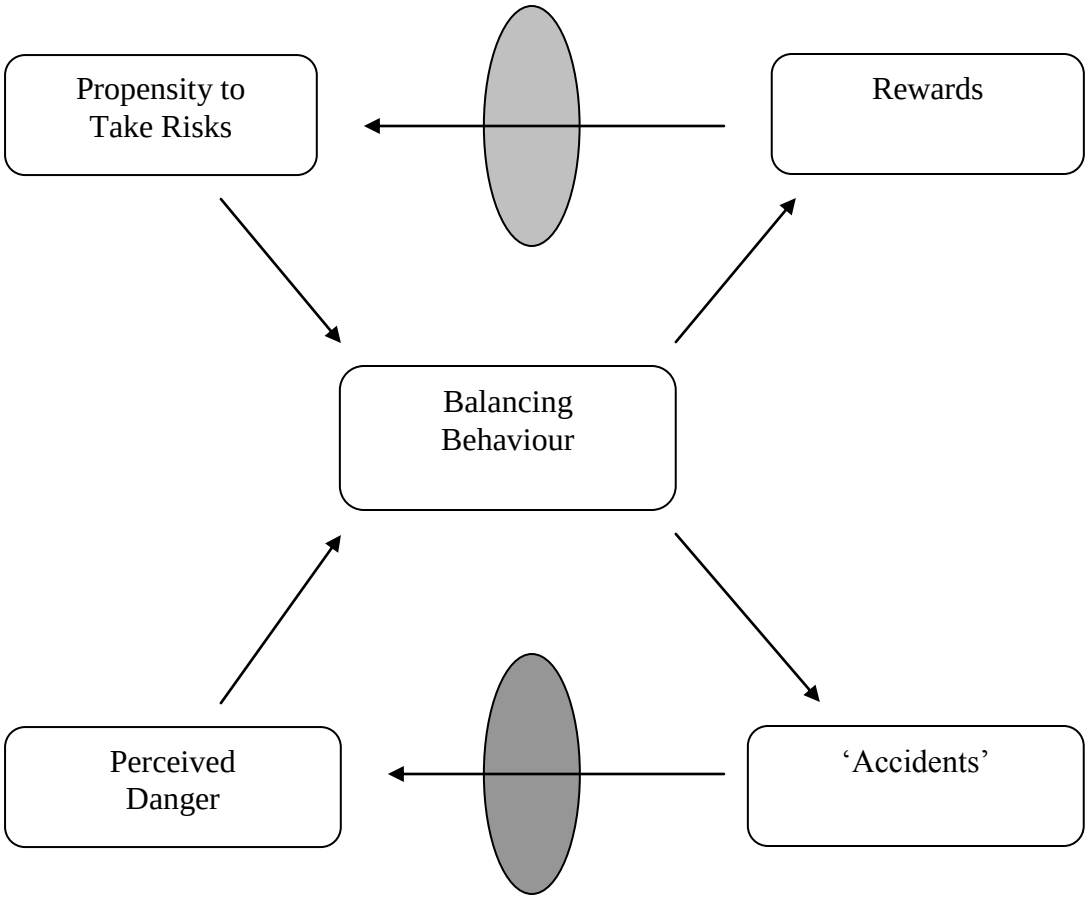
2.3.3 Risk Homeostasis and the Notion of Risk Transfer

The work of Gerald Wilde (1982) is important to consider here as he developed the notion of risk homeostasis which Adams went on to develop in 1988 and 1995 with his 'Seatbelt Theory'. It could be argued that this should be included within the psychological approaches to risk however due to the disagreement between the experts regarding the introduction of seatbelt legislation in the UK, it is suggested by this thesis that it is more appropriate to include it with the discussion of risk communication. Adams noted that although the number of serious injuries and deaths of car drivers and passengers fell following the introduction of seatbelt legislation, the number of pedestrians and cyclists who were killed or seriously injured in road traffic accidents increased. Drivers appeared to feel safer within their vehicles and so took more risks,

driving faster and in a more reckless manner, hence the increase in other road users' injuries. Adams (1995) therefore said that the probability of risk will always equal '1' as it can never be eliminated, only transferred elsewhere. The use of target hardening as an anti-terrorism measure, discussed at 1.7 is a strategy that decision makers should consider in light of Adam's theory as such a response may merely transfer the risk elsewhere.

Risk homeostasis is also a valuable theory as it highlights the dangers in assuming that risk can be removed and also allows for the influences of cultural factors and individual differences in the interpretation and perception of risks, i.e. the risk thermostat. The diagram below highlights this particularly clearly.

Figure 1: The Risk Thermostat with Cultural Filters: adapted from Adams (1995:43)



Risk homeostasis and risk transfer force us to look beyond the first-order effects and focus, importantly, on the second and third-order effects that may otherwise go unnoticed, causing severe difficulties at a later stage.

2.3.4 Systems Approaches

During the 1920s, biologist von Bertalanffy suggested that organic systems displayed common internal similarities despite external differences. His ideas have been translated to other areas, not least in risk and crisis management, where it was recognised that a major incident is a system failure which comprises human and technical elements. Failure in either of these can result in a crisis as Borodzicz (2005:23) identified.

Socio-technical approaches were first referred to by the Tavistock Institute which considered the problems resulting from organisational change in the British coal industry. As Borodzicz (2005:23) states, the term 'socio-technical system' was applied to individual production units in one of the Institute's mining studies (Trist and Bamforth, 1951). They argued that a number of benefits arose from considering organisations as 'open technical systems' which influence and respond to, the wider environment. It was from here that the benefits of considering organisations from systems approaches were really realised.

Turner was one of the main proponents of this approach. For him, it was the interaction between social organisations and technical processes that produced the "socio-technical" problem resulting in disaster (Turner, 1978:3). Furthermore, it has been suggested by Turner (1978), Horlick-Jones (1990) and Cox and Tait (1991) that social and technical systems are in fact inclusive systems of operation and are mutually reliant on each other for the success or failure of the system as a whole. Borodzicz (2005:23) suggested that we only have to look at the results of many public inquiries where it has been argued that the way in which disasters are perceived should be reconsidered (Toft and Reynolds, 1994:3), which Cox and Tait (1991:93) concur.

Turner developed his Incubating Disaster Aetiology to show how a minor event can, if unnoticed or mishandled, escalate eventually into a full-scale disaster. Accidents are ultimately latent failures of socio-technical systems which occur after a period of incubation has passed (Borodzicz, 2005:24). One of the most significant insights relating to 'incubation' is how so-called anti-tasks which are those practices that have unintended negative consequences, will have more significant consequences the higher in the hierarchy they occur (Healy, 2006:85). This is an important point that those managing terrorist incidents should clearly be aware of. Consideration of this model to the case studies under review should help to identify key learning points, utilising the notion of Isomorphic Learning (Toft and Reynolds, 1994) discussed below at 2.3.4.2 that should be addressed. Turner's Disaster Aetiology comprises six stages that illustrate how disasters may occur and escalate (the model is included at Appendix IV).

2.3.4.1 Turner's Disaster Aetiology

The first stage is the 'notionally normal starting point' and comprises the bringing together of culturally held beliefs and codes of practice in order to form a system of operation. This may be at the creation of the organisation or later in its life such as if there has been a change in its function. It is fairly typical at this stage to find that an independent risk assessment of technical and social systems has been performed in isolation with a total failure to consider the interaction between the two systems. This is argued by this thesis to be evident in the Government's emergency planning revisions, commented on at 2.9.

Such lack of consideration may result in system failure being programmed into the organisation's operation without management realising this (Borodzicz, 2005:24). Latent risks not identified here will be transferred to the second stage, 'incubation'.

During the second stage, the system will continue to function with minor problems. These however will not be treated seriously as they do not fit with the organisation's perception of a hazard. They are likely to be seen as normal operational difficulties rather

than system faults which may violate the integrity of the system and hence are not thoroughly addressed. Risks then progress to the third stage, the 'precipitating event'.

The third stage of the model raises the awareness of the decision makers involved in stage two. The response will be to act in the perspective of previously held beliefs about the system. As this is no longer appropriate, the system will not respond to these actions and will progress to stage four, the 'onset of disaster' (Borodzicz, 2005:24-25).

Stage four is conceptualised by an ill-structured crisis scenario which is at odds with that previously envisaged by decision makers and whose implications were therefore not realised. The errors or failures, such as ineffective plans or poor use of resources that preceded this stage come together to create the scenario.

Stage five comprises rescue and salvage and will frequently require flexibility and improvisation in response to what has occurred to re-establish the system. Pre-determined emergency plans will be ineffective. Standard responses may well exacerbate the situation here. The model then moves on to stage six, the 'learning phase'.

Stage six is the final stage and is characterised by learning. Those responsible for the system come to terms with what has happened, often through a formal inquiry process and recommendations may be made for the future. The focus at this point is to identify what went wrong and why, to ensure that this does not happen again. Plans and resources will be reconsidered and there will be a definite effort to try to gain something positive from the experience that may have nearly finished the organisation (Borodzicz, 2005:25). It is here that some of the crisis management theory may be useful to try to profit from what has occurred and turn the situation around. This will be considered later in this chapter so that it may be applied to the response to terrorist incidents.

Turner's ideas can best be seen in the emphasis now on organisational culture (Healy, 2006:86) in order to manage risks and incidents more effectively as well as better prepare for them. However, this is not without its critics as Gundel (2005:108) suggests that

although omissions and poor management may lead to incubation periods for major incidents, some information can only be understood after the event, thus the notion of a definable incubation period is not an 'appropriate illustration of reality'. Roux-Dufort (2007:108) echoes this somewhat by suggesting that it is more appropriate to examine crises as a *process* of organisational weakening that degenerates until 'the point of disruption they call the precipitating event'.

2.3.4.2 Isomorphic Learning

Organisational systems are becoming more complex particularly in light of the increasing trend of globalisation. This can be argued to increase the propensity for crises to occur and make the identification of potential problems much harder. It is here that isomorphic learning is particularly relevant as Toft and Reynolds propose that organisations can learn from each others' mistakes; a point that is frequently overlooked particularly in the current competitive climate when organisations do not want to show their fallibility in case rivals exploit it. Toft and Reynolds (1994:4) also suggest that even if an organisation does not suffer an adverse event, it is advisable to examine the industry as a whole, not just identical organisations, to fully benefit from isomorphic learning opportunities. Toft and Reynolds (1994) posit that as disasters happen infrequently, an organisation cannot predict such an event purely through reflecting on its own experiences. However, if disasters or major incidents are examined in the context of an industry as a whole, then similar incidents in different contexts are likely to be found and organisations can begin to learn from each other. It is for this reason that the three case studies considered in this research are included in this thesis.

The same disasters keep happening because little is learned from them. Fink (2002:43) also recognised that the best predictor of future events is past events so examining how frequently a crisis of that nature that has just occurred would be a sensible part of risk management. However, if organisations are to do this, they need to be able to recognise similarities between past experiences and the present situation. Furthermore, the lessons learned also need to be passed on effectively so that appropriate action is encouraged, as

Toft and Turner in Smith and Elliott (2006:203) concur. This is not always an easy task but the importance of achieving this must be realised.

As Borodzicz (2005:27) rightly notes, in this context, isomorphic learning is merely hindsight but how does it make the transition from hindsight to achieving learning regarding the event? Toft and Reynolds suggest that this is where there needs to be an explicit exchange of information between those who learn from the disaster and those who are responsible for managing the risk of disaster. This assertion is supported by his and Reynold's reference to several instances that confirm Turner's Disaster Aetiology and highlight how they might also be used to help prevent similar events from reoccurring (Borodzicz, 2005:27). It is here that one of Lagadec's most famous quotes is particularly relevant when he noted that the disaster "most often, is anticipated, and on multiple occasions" (Lagadec, 1982:495).

It would therefore seem that isomorphic learning can be of significant benefit for organisations in their risk management efforts but that much still remains to be done in identifying patterns of organisational reactions to failure (Toft and Turner in Smith and Elliott, 2006:203). Only then can ways to reduce these failures be created.

2.3.4.3 Normal Accidents

Perrow (1984) focused on the increasing complexity of organisational systems and the 'advanced technological society' in which we live; something perhaps we now call globalisation? He argued that major accidents were an inevitable consequence of our society and were most likely to occur when two or more processes broke down in an unforeseen way which he coined 'normal accidents' (Borodzicz, 2005:30). The looser coupling that is evident in terrorist networks now may be a conscious or sub-conscious response to address these potential issues, as noted at 1.2.

Boin and McConnell (2007:50) also recognised that modern societies are more inclined to breakdown through the increased dependence on their critical infrastructures which also encourages a feeling of vulnerability to new threats, such as terrorism. Furthermore,

they felt that conventional contingency planning and crisis management had serious limitations in face of critical infrastructure breakdowns: something which a terrorist incident could easily bring about, supporting the purpose of this thesis.

Normal accidents Perrow (1984) argued, were more likely to happen when system components were tightly coupled and/or 'interactive complexity' existed within the system. This may also affect the response to events as the level of flexibility in these is likely to be reduced within tightly coupled systems and they tend to be controlled quite rigidly from the centre of operations. It is suggested that complex systems therefore exhibit nonlinear behaviour (Wolf and Sampson, 2007:125). Time is a key factor for Perrow's theory: if misinformation is presented to operators during a critical time period, a series of system failures may occur that are not effectively controlled (Borodzicz, 2005:31). This has important ramifications for crisis management as flexibility is central to managing crises. Parallels can also be seen between this theory and Turner's where poor information can result in system failures, further emphasising the need for clear communications.

Initially, Perrow's theory seems acceptable and offers a good explanation as to why systems fail. However, Perrow cites interactive complexity and tight coupling as two separate issues; something which may not be so as they could be argued to be the same thing, as Borodzicz (2005:31) supports. Furthermore, how could they be differentiated between in order to apply these concepts to real issues? Perrow goes on to differentiate between tight and loosely-coupled systems, the latter having similar features to a tightly-coupled system but are not directly dependent on each other, hence are not as susceptible to normal accidents. Again, debate arises as to what exactly constitutes the loose system coupling.

Perhaps the greatest criticism of Perrow's theory is his apparent technological determinism whereby he suggests that normal accidents are an inevitable consequence of today's society and as such there is little that we can do to stop them occurring. Arguably

we should consider Perrow's theory as an interesting observation rather than an aid to managing risk.

It can be seen that running through all discussions on risk, regardless of the approach, are two common themes: that of debate surrounding the definitions and nomenclature of events and that regarding the importance of consensus on these issues. There also appears to be a growing acceptance that a generic capability regarding risk management may be the best way forward. A single definition of risk and agreement amongst theorists is still a long way off it would seem.

This chapter will now move from the macro-level consideration of risk to consider the micro-level of crises and their management.

2.4 Crisis: The Events and Their Management

The nature of threats today are far more trans-national in character than previously, rapidly affecting other countries through such things as electronic communications and air travel as Rosenthal et al (2001) note. The events of September 11th 2001 (9/11) have resulted in a paradigm shift in the thinking, planning and perception of 'man-made' disasters (Moore in Lakha and Moore, 2002:107).

Any type of management requires plans to be created and crisis management is no exception. However, these plans do not exist in isolation. Paton (1999:129) and Peterson and Perry (1999:243) argue that a necessary relationship exists between plans, training programmes, resource allocation and simulation exercises. However, as Borodzicz and van Haperen (2001:2) suggest, this is not always translated into practice. Elliott in Smith and Elliott (2006:399) highlights that it is necessary to invest in preparing for crises through allocating time and resources to the task and also to consider the role played in planning by core beliefs and assumptions that will impact on attempts to create a crisis resistant culture. The successful management of individuals and groups is the key to successful crisis management. McConnell and Drennan, (2006:59) identify four key

difficulties facing this process: most crises and disasters are low-probability events but are a large draw on resources, competing with the provision of an organisation's main product or service. Secondly, contingency planning requires ordering of possible threats, yet crisis reacts against such clear packaging. Thirdly, crisis planning requires integration across institutional networks whilst today's environment is characterised by fragmentation across public, private and voluntary sectors. Fourth, proper planning requires active preparation through costly training and exercises which may represent readiness but the reality may be somewhat different. Whilst these are useful observations by McConnell and Drennan, they do not suggest what can be done to address these issues.

Traditionally, crisis planning was viewed as something on the fringes of an organisation's operations. Threats were seen as likely to come from external perpetrators rather than internal failures and contingency planning followed the predominant Cold War mentality. The view was often taken that any plans could be adapted for any crisis (McConnell and Drennan, 2006:68). In the 1990s, global government effort focussed on imagining worst-case scenarios and planning for these, shifting to the opposite end of the spectrum. Arguably neither approach was helpful as they were not realistic representations of the situation.

Recently there are argued to have been four main types of crisis planning reforms which shift towards harder policy tools. The first is the creation of specific bodies to oversee civil contingencies and the second considers contingency arrangements. The third focuses on new legislation and the fourth considers good governance (McConnell and Drennan, 2006:68). All of these reforms have ensured that crisis planning and management are now centre stage in organisations and not at the periphery as was once the case.

In light of this, the crisis manager must therefore develop procedures and cultures that have the capacity to cope with whatever may occur, despite the fact that it is impossible to foresee every possible event.

2.4.1 Semantics or Substance?

There is a lack of consensus regarding what constitutes a dangerous event and whether there are differences between emergencies, crises and disasters.

It is important to know what constitutes any or all of these to improve the management of the event and to ensure that when communicating with others, we are talking of the same phenomena and not something different (Quarantelli, 1995:224): something that is just as important for managing the aftermath of terrorist events or the threat of these, as noted at 1.5. Gundel (2005:106) supports this assertion commenting that classifying dangerous events is the first step in controlling them as they can be named and analysed. Older typologies that distinguished between man-made, natural and social causation are somewhat outdated as it is now recognised that it is nearly impossible to separate multiple causations as they come as an ongoing process, rather than distinct events.

Wells (1995:5) observes that:
'dividing disasters into categories allows for more sophisticated analysis in terms of understanding risk perception, risk management, disaster prevention, civil protection and other related issues'.

This was supported by Borodzicz (1999:6) who offered three working definitions of emergencies, crises and disasters:

- **Emergencies** can be defined as situations requiring a rapid and highly structured response where the risks for critical decision makers can, to a reasonable degree, be defined.

- **Crises** also require a rapid response, which is why they are sometimes misconceived as emergencies. The risks for critical decision makers are however difficult to define due to their ill-structure and that the effects of responses are, or appear to be, unclear.

- **Disasters** are distinct from the above in that they represent the product of the former and leave an indelible effect on the affected system. Disasters are the irreversible and typically overwhelming result of a diachronic ill-handling of emergencies and crises and therefore are a failure to manage the emergency or crisis.

This thesis argues that these distinctions are invaluable for managing the response to terrorist incidents hence their inclusion here.

Roux-Dufort (2007:107) suggests that under-theorisation of the concept of crisis has led to problems with its definition and that there has been little interest in the description of intermediate states between normality and crisis. The researcher would suggest that the evidence in the proliferation of literature on the subject does not support this assertion, as can be seen within this chapter. It is suggested that in fact *over* theorisation of the concept may have made the situation overly complex and made agreement on definitions harder. Roux-Dufort (2007:106) does however concur with Turner (1978) in that a crisis begins with a process of incubation long before the triggering event.

Beatty in Hiles and Barnes (2001:180) describes an emergency as:
'any unplanned event that can cause deaths or significant injuries to employees, customers or the public, or that can shut down your business, disrupt operations, cause physical or environmental damage or threaten the facility's financial standing or public image'.

This definition contains elements of all three definitions offered by Borodzicz (1999:6).

Perry and Lindell (2006:29) suggest that emergencies are unforeseen but predictable narrow-scope events that occur regularly. Reponses can therefore be prepared and training given. There are no wider consequences and they can be rapidly brought to a close. This therefore follows the definition offered by Borodzicz (1999:6).

Setbon (1993) in Lagadec (1995:3) concurs that crises are ill-structured so the response to them is likely to be unclear. Conversely, 't Hart (1993:9) considers a crisis to threaten the core values of the affected system which must quickly be dealt with at times of deep uncertainty: this contains elements of the definition of disasters offered by Borodzicz (2005).

As discussed earlier in this chapter at 2.3.4.1, Turner's Disaster Aetiology suggests that emergencies, crises and disasters are distinct events, requiring different management techniques and if left unchecked, emergencies may escalate to become crises, which in turn may escalate to become disasters, so is congruent with Borodzicz's (1999:6) views and definitions of dangerous events.

Lagadec (1995:3) recognises the lack of structure in crises and how this contradicts the structure of an emergency where a clear trace exists that triggers warning procedures and mobilises resources, explicitly recognising a difference between the two types of events, again supporting Borodzicz's (1999:6) definition.

One of the most influential writers on crisis management, Uriel Rosenthal, felt that crises included emergencies and disasters and that it was the distinction between first and second-order response techniques that established the complexity and severity of the event, as Borodzicz (1999:8) noted. Rosenthal defined a crisis as:

'a serious threat to the basic structures or the fundamental values and norms of a social system…'.

This comprises elements of all three definitions offered by Borodzicz (1999:6) and it is possible to see the influence of this definition on Beatty's (2001) thinking of the definition of emergency in Hiles and Barnes (2001:180).

Heath in Hiles and Barnes (2001:47) defines a crisis as comprising four key elements:

- Missing/uncertain (unreliable) information
- Little time to act or respond
- Threat to people or resources valuable to people
- Resources required to resolve the situation exceed those available.

Heath's definition clearly supports that of Setbon (1993) in Lagadec (1995:3) and Borodzicz (2005). These clearly concur with some of these elements as they note that crises appear suddenly and there are four key elements that indicate a crisis: missing or unreliable information, little time to respond, a threat to people or resources and the resources required to resolve the crisis exceed those available. Furthermore, there is a focus on the short-term and there is a perceived or real loss of control.

Within the field of crisis theory, a clear school of thought emerged that instead of differentiating between different types of dangerous events, it focussed on the idea that a crisis moves through different stages in its lifetime. These bear some similarity to the different events but are not classified as such, being seen as life stages of the same event. The proponents of this view will now be considered.

Meyers and Holusha (1986:206) suggest that a crisis is not static, increasing and declining in importance as time elapses:

STAGE	**SEQUENCE**
PRE-CRISIS:	evidence → acknowledgement → resolve
CRISIS:	climax → assessment → direction
POST-CRISIS:	rebuilding → recovery → reform

They argue that specific tasks should be performed in each stage:

- PRE-CRISIS: intelligence gathering, threat assessment, scenario development and testing simulation training

- CRISIS: fact gathering, situation evaluation, options assessment, action selection, instruction issuance and progress monitoring
- POST-CRISIS: scenario reconstruction, early warning system design and strategy development

(Meyers and Holusha, 1986:226).

Gundel (2005:110) also does not differentiate between different types of events but instead differentiates between different types of crises. For him, there are four types: conventional, unexpected, intractable and fundamental. Conventional crises are predictable and have known influences on other factors, hence their probability and prevention actions are well known. Unexpected crises are rare therefore preparation for them may be limited and it is vital here that communication is good between responders, regulatory agencies and management. Intractable crises can be anticipated but the response may be in conflict with other interests and some damage may be irreversible. Here, organisations, Gundel suggests, should focus on exploring the affected system and on anticipating such an event. Fundamental crises are the most dangerous; they are unpredictable and preparedness does not exist: 9/11 may be an example of such a crisis. These categories are clearly comparable with the notions of emergency, crisis and disaster supported by Borodzicz (1999:6).

Smith (2006) in Smith and Elliott (2006:154) has also focussed on the concept of crises and for him, a crisis has three distinct phases. The first leads up to the crisis when an organisation fails to note the impending situation. This is roughly analogous with Turner's (1978) definition of an emergency which may go unnoticed and escalates to the next level. The second phase occurs when the organisation is in the throes of the crisis and here time is critical to prevent further escalation; again this matches Turner's definition. The third phase is post-crisis where the organisation attempts to restore external confidence in the organisation and its systems; again this follows Turner's aetiology. It is interesting to note however that Turner views these as distinct events, yet for Smith they are phases of the same event.

As has been noted, crises may begin in many ways. Perhaps one of the more useful considerations of this was made by Moore in Lakha and Moore (2002:92). He suggested that there were six main ways that a crisis may commence starting with a 'big bang', where the crisis is triggered by a sudden event. Alternatively, a 'tidal wave' may cause it, where an organisation is suddenly hit by an avalanche of problems and difficulties combine to make effective management virtually impossible. With this type of commencement there are likely to be inadequate resources and communications difficulties. The 'rising tide' beginning occurs where the problem gradually creeps up and there is no clear starting point: here, the crisis may only become apparent in hindsight. His next starting method is that of the 'cloud on the horizon' where a crisis may be in danger of spreading from one place to another: preparatory action is required to stop the threat evolving elsewhere.

'Headline news' occurs where media or public alarm to a perceived threat may cause a crisis even if fears prove to be unfounded. The issue itself may be minor in terms of the actual risk, hence it is vital to manage the information to reduce the threat. The issue of media management and its role in crises will be considered later at 2.10. 'Internal incidents' occur when a government of board of directors may be affected by their own crisis or an external crisis that affects the ability to function normally. From this it can be seen that most crises that may affect an organisation can be grouped under one of these headings which means that as the crisis has been recognised, its management may now begin.

For Fink (2002:15) a crisis is an unstable time in which a decisive change is impending, which may be positive or negative. It is interesting to acknowledge here that Fink explicitly recognises the positive aspects that a crisis may bring, as many authors only do this when talking about risk management. Crisis then is not necessarily bad but is merely characterised by risk and uncertainty. He goes on to propose that a crisis can comprise four phases: prodromal, acute, chronic and crisis resolution. The first stage is the warning stage, if one exists. If the crisis is recognised here, it is much easier to manage, as Augustine (1995:149) concurs, as can be seen later in this chapter at 2.5. The second

stage is the point of no return and even if the crisis cannot be controlled, it may be possible to exert some influence over it. The key characteristics of this stage are speed and intensity. The third stage is the clean-up stage, a period of recovery and self-analysis. Further crisis management planning often occurs at this time. The last stage is the chance to turn the event into an opportunity, hence can be seen that Fink's model closely resembles Augustine's, Meyer's and Holusha's and Turner's models. Moore in Lakha and Moore (2002:102) concurs, suggesting that within every crisis there are opportunities for success as well as roots for failure. McConnell and Drennan (2006:110) also recognise that crises bring forth changes and transformation. It is perhaps emphasis of such points that is recommended to improve acceptance of the benefits of such methodologies.

Moore (2002) in Lakha and Moore (2002:91) suggest that there are distinct events that comprise the crisis life cycle such as information acquisition and assessment, situation analysis, establishment of goals, development and implementation of options and feedback. This echoes Meyers and Holusha's (1986) typology, suggesting that this is a valid approach to crises.

Meyers and Holusha (1986:226) suggest that the following crisis classification factors are a useful tool for helping to manage crises:

- **Dimension** – the size of the stake at risk
- **Control** – the organisation's ability to influence the environment
- **Time** – how much time is available for manoeuvring
- **Options** – the number and quality of choices

(Meyers and Holusha, 1986:207).

It is the inter-relationships between these factors and the crisis that dictates which management tools should be applied.

Definitions of disasters appear more frequently than for emergencies. Hiles in Hiles and Barnes (2001:292) argues that in recent years, disasters have been downgraded to 'operational accidents', introducing a new term to the plethora already in existence.

Dombrowsky (1995:242) suggests that disasters do not cause effects but instead it is the effects that we call disasters, offering another viewpoint. Borodzicz (1999:10) argues that disaster is perhaps the most difficult phenomena to define due to its 'apparently amorphous nature' and that it may also be viewed as 'insufficient resources to deal with a situation or an overwhelming situation', citing Gilbert (1995) and Dombrowsky (1995) as proponents of the latter interpretation. Boin and McConnell (2007:51) concur with Borodzicz (2005) and Turner (1978) in that disasters are viewed as events where life, property and infrastructure do not remain intact. Seemingly under these definitions, the terrorist attacks included in the case studies here would fall under this category.

Alexander (2005:159) suggests that disasters are extreme events with natural, technological or social causes that have consequences in terms of casualties, destruction, damage and disruption. Emergency is a broader term that includes disasters, catastrophes and smaller disruptive events. It is an imminent or actual event that threatens systems and requires a co-ordinated and rapid response. They can, and should, be planned for. This again supports the broad themes identified by Dombrowsky (1995), Gilbert (1995), Borodzicz (2005) and Boin and McConnell (2007).

As there is disparity in the nomenclature for levels of dangerous events, so the overall management processes also suffer a lack of consensus. Within the crisis management literature, some argue that the terms 'crisis management' and 'disaster recovery' are interchangeable, others argue that crisis management is part of business continuity management (BCM) or vice versa. This thesis supports the view that crisis management is part of business continuity management for the purpose of this research, as it will be argued that management of the event is only part of improving resilience to such attacks and preparedness for them.

Sharp in Reeves (1998:6) acknowledges that many managers believe that BCM is just another name for disaster recovery. He argues that the two are at opposite ends of the spectrum as disaster recovery focuses on recovery following the event, whilst BCM is about anticipating what could go wrong and planning and rehearsing for it. In addition to these definitions and explanations, Borodzicz in Reeves (1998:11) suggests that business continuity, contingency management, corporate risk or security management have all been used interchangeably to describe preparing for the unknown.

This apparent confusion appears to support the assertion that some degree of consensus must be reached regarding definitions of events to enable better management and to pool expertise and knowledge to improve preparation and response.

2.4.2 The Dynamics of Crises

Crises come in many guises and can change rapidly (Augustine, 1995; Heath in Hiles and Barnes, 2001). Crises may arise from many things, although as Augustine (1995:148-149) noted: 'the spectrum is so wide that it is impossible to list each type'. The apparent infiniteness of crisis mutations could suggest that rather than trying to plan for each envisaged mutation, it may be more prudent to create instead a more generic capability that could be adapted to meet whatever occurred.

Moore in Lakha and Moore (2002:92) supports these assertions, noting that the severity of a crisis may stay the same throughout or may change with time in response to actions taken by the parties involved. It may also begin in any number of ways and although the crisis begins in one category, it may evolve into another. This is something that should be considered when creating crisis management plans and ensuring adequate flexibility within these.

2.5 Crisis Management Methodologies

On examination, the literature reveals an overwhelming tendency to view crisis management as an holistic process involving prevention, planning, acute response,

recovery and learning, although it is not possible to identify every conceivable worst case scenario that may affect an organisation (Boin and McConnell, 2007:52; Smith in Smith and Elliott, 2006:99) whereas traditionally crisis management involved merely reacting to the event. Crisis management is often regarded as a negative activity and has in the past perhaps been regarded as unproductive in terms of the value and time it may take up. Before the events of September 11th, many managers were reluctant to think about it (Moore in Lakha and Moore, 2002:83).

Boin and 't Hart (2003) identified some tendencies in crisis management and these have been applied by McConnell and Drennan (2006: 68) to their thoughts on crisis management. Crisis preparedness is divided into two areas: that of a conservative approach which adopts a 'can cope' attitude which reflects a low-level approach. Here organisations establish plans and rehearse events that may never occur. In contrast, high-level preparedness recognises the real threats that organisations face and demonstrates a willingness to prepare and plan for all sorts of crises that conservative organisations are likely to resist. It will become clear in the proceeding discussion that this is evident in many of the processes employed by organisations.

Many authors offer advice and assertions on what crisis management entails and how it should be performed. Heath in Hiles and Barnes (2001:49) suggests that effective crisis management means seeking to:

- mitigate or reduce the sources, size and impacts of a crisis situation;
- improve crisis onset management;
- improve crisis impact management;
- enhance recovery from a crisis through effective and rapid recovery management action.

They suggest a '4R' approach: reduction, readiness, response, recovery with three transition points from pre-crisis to crisis management, from crisis onset to crisis impact management and from this to recovery management. Again, it can be seen that this

reflects elements from all of the considered definitions. All appear to agree that it involves measures that aim to bring the crisis under control through co-ordinated information exchange, effective management structures and co-operation between participants. Crisis management must be integrated and any plans must be in response to the crisis, not because of it, whilst being duly flexible and tested in various scenarios (Moore in Lakha and Moore, 2002:95). The subject of training and testing plans will be considered later in this chapter at 2.8.

Perhaps one of the best known writers on crisis management, Norm Augustine, developed a crisis management model from his own experiences. Within this he distinguished six stages of crisis management (1995:149):

1. Avoiding the crisis
2. Preparing to manage the crisis
3. Recognising the crisis
4. Containing the crisis
5. Resolving the crisis
6. Profiting from the crisis.

Avoiding the Crisis

This is often missed altogether despite being the cheapest and easiest method for controlling a crisis. Augustine suggests this is because many managers view crises as unavoidable, everyday occurrences.

Preparing to Manage the Crisis

This involves preparation of a crisis management plan. Preparation for a crisis must look beyond immediate effects to second-order effects, which can be just as serious. Establishing a crisis team, a crisis centre, making contingency plans, providing ready and redundant communications, and testing those, are useful preparations (Augustine, 1995:151).

Recognising the Crisis

This stage can be the most challenging as a problem may be misclassified. It is at this stage that managing expectations and perceptions is crucial as it is often these that cause the crisis so that perception becomes reality. Fink (2002:98) also recognised the importance of this point and emphasised that media relations are crucial in times of crisis.

Containing the Crisis

Conflicting advice is a frequent feature of this stage and too much information may exist. It is advisable to establish a crisis management team to contain the crisis whilst remaining staff concentrate on keeping the business running (Augustine, 1995:155). The organisation's stakeholders should be kept informed: Meyers and Holusha (1986:225-226) concur.

Resolving the Crisis

Speed is of the essence in resolution. The longer that a crisis is left, the worse it can become and the harder it will be to resolve.

Profiting from the Crisis

Augustine describes this stage as the opportunity to recoup some of the losses and to try to repair the damage (Augustine, 1995:156). Showing commitment to stakeholders and being honest about what happened is an important part of this stage as well as in Stage 3.

In contrast to Augustine, Meyers and Holusha (1986:257) offer seven steps:

1. Take charge
2. Understand the circumstances
3. Define the problem
4. Rank the options
5. Move decisively
6. Eliminate the cause
7. Prevent reoccurrence.

For them, the first step begins once the crisis has broken. However, Steps 2 and 3 are broadly similar to Augustine's Stage 3, whilst Step 5 is the equivalent of Augustine's Stage 4 and Step 6 is congruent to Augustine's Stage 5.

Meyers and Holusha's Step 7 is included by Heath in Hiles and Barnes (2001:44) under the heading of BCM which for him comes under the umbrella of crisis management. Heath defines crisis management as involving 'all aspects of what may precipitate a crisis situation through to recovery' (Heath in Hiles and Barnes, 2001:48). This also supports Augustine's Stage 1 assertion that the first step in crisis management is to prevent its occurrence, adding weight to the argument for preparedness.

Heath in Hiles and Barnes (2001:52) suggests that crisis management has four sides:

1. Managing the processes involved in developing and preparing for crisis management
2. Dealing with the crisis situation
3. Looking after organisational stakeholders
4. Managing the communication processes involved, especially those with the outside world.

The third and fourth points correspond to Augustine's Stages 3and 4. Again, this mirrors Augustine's six stages from Stages 1 to 5 and only excludes the final "Profiting from the crisis" stage.

Moore in Lakha and Moore (2002:98) also proposes a crisis management typology comprising six broad activities:

1. situation monitoring
2. crisis detection support
3. containment
4. response

5. de-escalation
6. recovery.

1. Situation monitoring

At this stage, the organisation monitors the picture to determine if everything is as it should be. This is an ongoing process throughout the year for the organisation.

2.Crisis detection support

Here, methodologies are used to examine routine situational monitoring from activity one. The aim is to identify events and trends that suggest something is untoward and a positive focus must prevail as to whether a threat exists or not.

3. Containment

This activity will occur when a threat to high priority goals or values has been identified. The acquisition of information should be the focus to understand the causes of the threatened crisis. Alternative options must be identified and a plan should then be implemented.

4. Response

The identified strategy should be implemented in accordance with the plan developed in activity three. It is important to assess and evaluate the effect of the action taken and if necessary, revise the options.

5. De-escalation

Here, a timetable is established to return to normality. At every stage of the implementation, there must be a risk assessment, with plans in place should the crisis re-escalate.

6. Recovery

The situation now returns to a normal level which may be higher than prior to the events but is still acceptable. Conversely, it may be lower than previously.

It can be seen that Moore's model has elements of the definitions of Meyers and Holusha (1986), Augustine, (1995) and Heath, (2001).

Despite the confusion surrounding nomenclature, it appears that the recommended processes themselves are similar, agreeing on the basic principles involved. This could be argued to provide some degree of authority to the recommendations for crisis management.

The general agreement on what crisis management entails does then beg the question:
'Are generally agreed definitions for emergencies, crises and disasters really important if, despite lacking at present, the literature ends up agreeing on the final management principles anyway?'

It could be argued that they are necessary as they could help in training key decision makers so that the distinct skills necessary for each event could be identified and honed, and the identification of key individuals and organisational groups would reflect this (Borodzicz, 1999:2).

2.6 Barriers to Effective Crisis Management

No matter how good the intentions to be prepared may be, the reality is often somewhat different, not least due to certain tensions that may exist. McConnell and Drennan (2006:62) have recognised this and identified four clear tensions that exist between the ideal and reality of crisis management. The first refers to the difficulty between the high potential impact of crisis versus the low priority of crisis management, hence it is seen as a drain of resources for something that may never occur. This reflects the frequent short-term accounting view that often prevails in crisis management. Furthermore, there may be a focus on the last crisis rather than full preparedness planning. As referred to earlier, Moore in Lakha and Moore (2002:83) also recognised this but felt that less resistance existed following 9/11.

The second tension arises from the need for planning and order versus the uncertainty and disorder of a crisis. Planning in crisis management appears to take one of two routes: that of one generic plan addressing measures for different threats or separate plans for different threats but integrated management plans. Even with plans, aspects of crisis response must often be improvised (McConnell and Drennan 2006:64).

The third tension refers to the point that for crisis management to be successful, it must draw on the expertise of individuals and networks; in many organisations, departments are run almost as self-contained businesses so this can be a challenge in itself. The events of 9/11 highlight the problems that can occur with inter-agency and department working and were seen in the Commission Report on 9/11 which criticised the New York Fire Department and Police Department for considering themselves operationally autonomous which adversely affected preparedness for a major incident. This is discussed more fully in Chapter Five of this thesis. Similarly this was also evident in the Sarin attack considered in Chapter Four of this thesis. This strengthens the argument of the relevance of crisis management methodologies for managing the response to terrorist incidents.

The fourth tension identified by McConnell and Drennan is often overlooked and concerns crisis training. This may not be utilised or tested appropriately or equated with proper preparedness due to several factors: cost of training which increases with the higher the fidelity of the exercise, lessons learned are not always put into practice and lastly, crises do not respect organisational training and may not fit the scenarios that have been trained for (McConnell and Drennan, 2006:67). This will be further addressed in 2.8.

Smith in Smith and Elliott (2006:99) takes more of an overview of the barriers that may exist and instead suggests that there are three sets: the first is problems dealing with individuals and the psycho-social issues that may result relating to perception, assumptions and core beliefs that shape our behaviour. The second set is at the cultural and group level and reflects wider issues of how the organisation actually works. Culture plays a crucial role in crisis management as it can be an opportunity and a threat for crisis

management as it may precipitate a crisis by creating the environment within which a crisis can escalate or it may be central to the organisation's ability to cope with the situation (Smith in Smith and Elliott, 2006:152). The third set is at the systems level and concerns the structural and environmental pressures that impact on an organisation at various times, which may hide the existence of a crisis. It can be seen that implementing effective crisis management can be problematic. Through explicit recognition of some of the key barriers to crisis management it may help organisations to plan for these and address them to prevent them from being a hindrance.

2.7 Pessimism Reigns?

For many people and organisations, the idea of a crisis is something quite negative; it is something that should be avoided where possible and if this is not an option, a crisis is something that should dealt with rapidly and moved on from. However, there is a growing school of thought that crises can actually offer positive benefits and for those able to engage with these, success an profitability may beckon.

Meyers and Holusha (1986:28) suggest that most crises offer opportunities and that seven gains may accompany or result from a business crisis:

1. Heroes are born
2. Change is accelerated
3. Latent problems are faced
4. People can be changed
5. New strategies evolve
6. Early warning systems develop
7. New competitive edges appear.

Augustine (1995:148) holds a similar view suggesting that the essence of crisis management is finding, cultivating and harvesting that potential success.

2.8 Training and Testing Plans

Staff training and testing crisis and contingency plans is an area where views appear congruent; it is seen as a highly beneficial practice and an essential part of crisis management, and indeed if lacking, may be one of the causes of failure to successfully manage the crisis (Lagagdec, 1995:7-8). Levitt and March (1988:333) in Toft and Reynolds (1994) recognise that the speculation that learning can improve organisational performance is confirmed through numerous studies of learning by doing, case observations and theoretical analysis, adding weight to the argument for its use in crisis planning. Planning should be proactive.

Boin and McConnell (2007:53) argue that there is much to be gained from the prior specification of roles and responsibilities, resource allocation and systems testing; something that was clearly seen in the dramatically improved evacuation times for the World Trade Center on September 11th, discussed in Chapter Five of this thesis. Perhaps somewhat perversely, it is suggested that the best time to consider crisis plans is when a crisis occurs as this destabilises existing systems making it easier to adopt new practices. Nonetheless, it is still important to have valid plans prior to any crisis occurring. Crises and disasters do not guarantee change and learning but allow existing procedures and cultures to change course (Boin and McConnell, 2007:57).

There are some contradictions in crisis planning however: how does one plan for something that violates the regular patterns which planners rely on in order to try to prevent it? There are also in-built vulnerabilities such as the requirement for multi-agency co-operation as Boin and McConnell (2007:53) recognise (something that was an issue in the Sarin attack considered in Chapter Four of this thesis) and the issue of cost of something that may never actually be needed. Furthermore, so called 'symbolic readiness' may result where paper plans suggest a readiness that bear little resemblance to the actual challenges that may result from a crisis.

Meyers and Holusha (1986:226) actively recommend simulation training as part of pre-crisis activities. Borodzicz (1999:1) and Borodzicz and van Haperen (2001:18) also support the use of simulations for multiple purposes. Whatever simulations are used, it is

imperative to include a debriefing at the end to reflect on events and to support the learning experience.

Crisis management plans should be built on routine arrangements and it is important that those who will respond to a crisis are included in the planning process and training exercises (Moore in Lakha and Moore, 2002:97). There should arguably be one plan that should cover all likely hazards. Alexander (2005:162) suggests that it is worse to have two plans than none at all as the risk of conflicts and ambiguities would be greater. Modern emergency planning is generic, written in general terms with specific chapters covering the most likely threats, hence economies of scale can more easily be achieved and multiple impacts can be addressed through the one plan.

It is suggested that by simulating a crisis, managers can make real world decisions in a safe environment and test their theories. Ideally it should encourage managers to experiment with different options however, it is still problematic to recreate events that may unfold as participants in the exercise may get a false impression of the operational realities as Moore in Lakha and Moore (2002:103) recognises. The researcher has also experienced this during her observation of a multi-agency simulation. McConnell and Drennan (2006:69) acknowledge that paper exercises will always appear preferable to active exercises although the latter is what thorough crisis management really requires and what this thesis advocates.

Before any cultural and procedural changes occur following crises, it is important to think about societal resilience as a whole as this is a key part of the successful management of crises and effective responses rely, to a large extent, on the resilience of citizens (Boin and McConnell, 2007:54). It is to the concept of societal resilience that we should now turn.

2.9 Societal Resilience and Emergency Planning

In today's global climate it is argued that the public must take some responsibility for its own safety, something which Alexander (2005:171) supports. Recent decades have seen

significant increases in the number, scope and complexity of incidents and as a result, more attention has been given to emergency preparedness and management (Alexander, 2005:158). Despite this, the public is rarely involved in emergency planning. Following the attacks of September 11th 2001, the UK approach to emergency planning has clearly focussed on organisational resilience. However, such a focus on a top-down approach does not help to promote societal resilience (O'Brien and Read, 2005:353).

Government funding also appears to focus largely on institutional resilience, again doing little to promote societal resilience. The term 'resilience' is used more and more in disaster management, reflecting the move to a more holistic and proactive approach that has the community and its recovery ability at its focus. The term brings together all the components of the disaster cycle: response, recovery, mitigation and preparedness. On examination, it appears that the government's reform process may not have taken a holistic approach and has perhaps focussed on particular areas, undermining the concept of resilience (Alexander, 2005:354).

In order to enhance societal resilience, the populace must have a general awareness that a crisis may strike. First responders must also be identified and training provided and this should be incorporated into the crisis management plan. Working with communities is vital and ideally, contingency planning and business continuity plans should be conducted in full consultation with the local community (Boin and McConnell, 2007:54).

Shrivastava (2005:68) suggests that the current approach of using trained medical and civilian defence personnel could be severely challenged when considering the scope of what may occur in a major incident. He also supports the assertion that the public themselves should be trained in first-response strategies and that they can also play vital surveillance roles in times of heightened security.

True resilience therefore is dependent not only on organisational plans but also on the ability of society to look out for and respond to major incidents.

2.10 Crises, the Media and Communication

There is no doubt that the media plays a key role in terms of crisis. Initial reaction to this may be that they it is a purely negative role, spreading panic and serving no useful purpose, for example the discussion at 1.10.3 of this thesis highlights some of the adverse effects that the media may cause. However, this is not always the case and it is vital to effective crisis management that formal media management is employed as part of the crisis management plan and that the benefits that the media can offer in times of crisis are recognised.

During a crisis, any organisation should be striving to remain in control and manage the message that is going out to the public, as well as general communications and the crisis itself. Facts should be gathered as quickly as possible, as Fink (2002:98) concurs.

Perhaps the most pertinent point in media management is that crisis communications should begin when there is no crisis and when a 'reservoir of good will' may be created (Fink, 2002:96). The organisation should have current, good relations with the media and should have high credibility with them. This is vital if credible information is to be relayed to the media during a crisis. It should be noted that the same message is not suitable for all groups: employees, customers, government and others all require different information so require specific communications. Any messages that are conveyed must be done so with one voice and all spokespeople should be readily available to the media (Fink, 2002:100). Inconsistent or inadequate information can cause the situation to escalate and ensure that the media and those receiving the information are then dissatisfied with the response that they receive from the organisation.

As soon as the crisis becomes public knowledge, the media will demand attention and it is here that the crisis communication plan comes into its own. This should also help to engender pro-active attitudes towards the media, within the organisation (Moore in Lakha and Moore, 2002:103). Any communications must be bottom-up as well as top-down (Smith in Smith and Elliott, 2006:156).

2.11 Crisis in the Context of Terrorism

As we have seen, terrorism is rooted deep in historical, economic, cultural and ideological conflicts as Shrivastava (2005:64) supports. It is a source of crisis where the crisis is represented by large-scale damage, perceptions of loss of control and breakdown in social structures. By understanding terrorism as a source of risks and crises, risk and crisis management frameworks can then be applied.

Terrorism clearly has some distinct properties that are not evident in other types of crisis such as the existence of human agents who deliberately create the risk as Sjoberg (2005:44) supports. Shrivastava (2005:65) suggests that terrorism-spawned crises go through four distinct phases. The first is crisis preconditions which are fomented by a variety of ideological, social and economic conditions. Organisations do not experience direct damage here but instead are faced with uncertainty or risks of disruption. If preventative, corrective actions are taken, a fully-fledged crisis may be averted.

The second stage is 'crisis triggers' where attacks occur that create emergency conditions for an entire system or significant parts of it and can cause destructive structural transformations (Shrivastava, 2005:66). The third stage is crisis expansion where the effects of the crisis expand to cover more of the system and it becomes apparent that the institutional capacity and infrastructure needs restructuring.

The final stage is crisis resolution or normalisation where changes are made to the associated systems in order to prevent future crises. Crisis-impacted systems are reintegrated into the normal activities and processes of the organisation.

The key factor in any crisis situation is the existence of uncertainty and something that terrorists exploit through their choice of targets which maximises public perceptions of uncertainty and lack of control by the authorities. The consequences of attacks can be massive, not just in financial terms but also in psychological trauma that reaches beyond immediate victims through the media. Shrivastava (2005: 67) also points out that another consequence of terrorist crises is the added cost of doing business as security, business continuity and duplication of assets are all areas that need to be addressed following such an event, thus the consequences may emerge over time and last for extended periods.

Terrorism crises therefore warrant specific attention within the field of risk and crisis management as they have far-reaching implications for organisations and their stakeholders. It is suggested that in the current climate, terrorism crises should be seriously considered by organisations.

Despite the apparent lack of agreement surrounding the nomenclature, it is generally agreed that crises are ill-structured and a great deal of uncertainty surrounds the events making them hard to manage, although, training for crises may help to improve the response to them. In managing crises, speed is of the essence. The greatest danger with crisis response is that the event is misclassified resulting in an incorrect response, which may aggravate the situation, or at least not help it (Borodzicz, 1999:1).

The best preparedness is not achieved by merely having a plan as McConnell and Drennan (2006:60) support. Organisations should be continually involved in preparing for crises through isomorphic learning, simulations, training and crucially, ensuring that crisis management is embedded within core processes.

Whatever plans and processes are in place for crisis management, it is vital that the solutions are deep and enduring and not the short-term measures that were indicative of the past (Shrivastava, 2005:65). Any crisis management preparations must be fully embedded within normal organisational processes and take a long-term view in order to maximise their effectiveness. Organisations must also achieve isomorphic learning: as a result they are better able to draw lessons for the future and base any positive or critical analysis on profound professional knowledge (Moore in Lakha and Moore, 2002:103). If organisational shortcomings exist in risk management the consequences may be dire.

2.12 In Conclusion

Several key conclusions can be drawn from the review of risk and crisis literature. Firstly, there are several ways that risk can be perceived and managed and the way this is defined may also vary. Debate still exists regarding the importance of definitive nomenclature

however it appears that theorists are gradually moving towards the opinion that at least for discussion, concerns about terminology are important.

Secondly, familiarity with risks is an important factor for people: unknown risks were rated as more terrifying as were unfamiliar accidents, depicted at 2.This could be argued to add weight to the argument for a generic capability with which all would be familiar, to remove some of the 'unknown' factor, with add-ons for particular scenarios.

Thirdly, crisis management highlights the importance of preparedness: however, it is not enough merely to have a plan. Training in crisis scenarios must also occur and the crisis management processes must be firmly embedded within routine organisational processes. Organisational learning must also occur where organisations actively learn from others' experiences and use this in the development of their own plans. This would help to reduce the opportunity for a crisis to present a novel situation with the potential to destabilise the organisation.

But what of conclusions drawn from the literature within the context of this thesis? Firstly, it is clear that two conceptual approaches to risk are particularly relevant for the work here: Risk Communication and Systems Theory, both individually and, importantly, as a combined approach to managing risk. It is argued that by incorporating such theory into responses, a more rounded understanding of the situation and of the available options is ensured which in turn provides improved resilience and preparedness.

Similarly, adopting models of crisis management such as Augustine's or Fink's helps organisations to profit potentially from a crisis and maintain a proactive stance, strengthening their position.

3. Research Methodology

3.1 Research Design

The purpose of undertaking most research projects is to generate a professional body of empirical knowledge (Corbin and Strauss, 2008: vii); this thesis is no different. In order to engender valid and reliable information, it is necessary for researchers to consider carefully the research design and methodology that they will use to collect, analyse and present this information. When performing any research study there is no overall consensus regarding how to conceptualise the doing of research (Robson, 2002:45). This can therefore pose some difficulties for those involved in research studies. Whatever the purpose of the study, research design is concerned with turning research questions into projects (Robson, 2002:79).

Before beginning to define the research design, the researcher must select the philosophical perspective that is most appropriate for the study. The development of a philosophical perspective requires the researcher to make several core assumptions concerning two dimensions: the nature of society and the nature of science (Holden and Lynch, 2004:397).

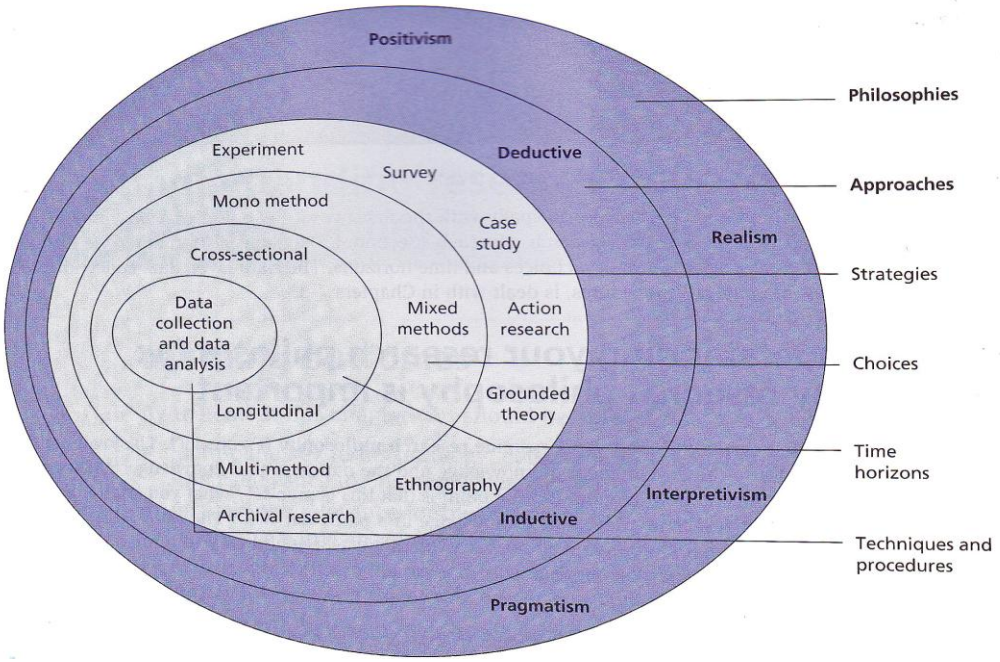


Figure 2: Designing the Research (Saunders, Lewis and Thornhill, 2009:108)

This thesis is not intended to generate and test hypotheses or to identify causal relationships between variables in order to predict events and try to prevent them. As a result of this, the researcher felt that a positivistic and quantitative perspective was inappropriate (Collis and Hussey, 2003:53; Corbin and Strauss, 2008:25). Positivists search for constant relationships between variables which, when translated into the social science world, are not always identifiable. This 'constant conjunction' between events in a strict sense is so rare as to be virtually non-existent, as Robson recognises (2002:21). Positivism is generally characterised by a deductive method of inquiry seeking theory confirmation in value-free, statistical generalisations (Riege, 2003:77). The positivistic tenet that only one reality exists makes it unsuitable for social science research, this thesis argues, as this research seeks to understand reality from multiple perspectives.

The phenomenological paradigm was adopted as the philosophical orientation for this study. This was confirmed as the most appropriate as the research is concerned with peoples' behaviour and activities and to some extent, understanding behaviour from participants' own frame of reference (Collis and Hussey, 2003:53). This last point is strengthened by Corbin and Strauss (2008:8) who note that the world is complex and events are a result of multiple factors interacting in often complex ways. In order to fully understand these, it is necessary to obtain multiple perspectives on events and locate experiences within those events; when considering the topic of this thesis, this comment is particularly significant and qualitative research was thus chosen, not least due to the richness of qualitative data. This type of research helps the researcher to extract and understand the inner experiences of participants and, arguably, copes better with the fluid and dynamic nature of most real-life events (Corbin and Strauss, 2008:13). If this is coupled with the tendency for qualitative research to begin with a broad research question, then this is further emphasised as an appropriate choice for this research.

From this it is evident that an inductive approach is the most suitable as the theory is developed from observations of empirical reality (Hussey and Hussey, 1997:13): that is particular instances are advanced from general inferences and themes are allowed to emerge which can provide greater insight to situations (Bryman and Bell, 2007:15). Such

emergence is invaluable in such a comparative study as this thesis when considering the three distinct terrorist events. It is argued that had the official inquiries adopted such an approach then better learning may have resulted and similar problems could have been more readily avoided. A clear example of this is where some of the issues identified following the 7th July attacks had already been identified eighteen years previously following the King's Cross fire but had not been acted upon. Again in the 7/7 inquiry, there is no acknowledgement that this was so.

Saunders, Lewis and Thornhill's (2009:490) observation that an inductive approach is still likely to contain deductive elements was seen in the course of this research. The researcher found evidence of this when developing her theoretical position in relation to the data: when the applicability of the adopted position was tested through further data analysis, a deductive approach was in progress.

Robson (2002:18) refers to qualitative research as a 'flexible' design strategy. This type of strategy often evolves during data collection and the data are usually non-numerical. Importantly, Robson stresses that a scientific approach can still be taken. For him, a 'scientific' approach means one where research is performed systematically, sceptically and ethically:

- *Systematically:* serious thought is given to what is being done and how by the researcher. In particular, the nature of observations, context and the researcher's role

- *Sceptically:* subjecting research ideas, observations and conclusions to scrutiny by yourself and others

- *Ethically:* research is performed according to a code of conduct so that those taking part in the research or those affected by it are safeguarded

(Robson, 2002:18).

3.2 The Research Aims

The nature of the research aims can often dictate the choice of methodology although researchers may have a natural tendency or preference for more qualitative or quantitative approaches. The aims are also important as they determine the boundaries for the study as it is impossible to cover every element of an issue in a single project as Corbin and Strauss stress (2008:25).

In a qualitative study, the aims should inform the reader what it is in this topic that is of particular interest to the researcher; this is often quite different from quantitative approaches. There may also be several key objectives on which the study is based, stemming from each other. Such is the case for this thesis. It is the central importance of the aims to this paradigm that requires careful consideration of their wording in order to achieve the hoped-for outcomes. Research aims and questions in a qualitative study can focus beyond individuals to entire organisations, families or industries, for example. As the research progresses, these are often refined as further questions arise which call for further data collection and analysis (Corbin and Strauss, 2008:27): something which the researcher experienced in the course of this study.

In developing the research aims for this thesis, the researcher followed Robson's recommendations:

1. *know the area:* be very familiar with the research area; write a paper, give a presentation or seminar, anything that forces the researcher into this position

2. *widen the base of your experience:* do not be limited by the research and questions that are current in the specific field. Learn from researchers in other fields and disciplines and talk to practitioners in the field

3. *consider using enhanced creativity techniques:* brainstorming, nominal group technique and the Delphi techniques can be beneficial to help to decide upon and refine the research question/s (Robson, 2002:57).

By considering the above recommendations, the researcher was better able to generate and refine the research aims for the study which were presented within the introduction to this thesis.

3.3 Research Methodology

This thesis comprises elements of exploratory and descriptive enquiry. Exploratory research seeks to determine what is happening, to seek new insights, ask questions and to generate ideas for future research whilst descriptive enquiry attempts to portray an accurate profile of events and requires the researcher to have extensive previous knowledge of the situation (Robson, 2002:59). As this research aimed to explore three terrorist incidents and the management of the aftermath in order to identify areas for improved future response and resilience, the exploratory element is clear. In order to do this, the incidents under consideration had to be presented in detail with a thorough understanding of the events themselves and their inter-relationships; here, the descriptive enquiry element of this thesis was evident.

Many sources of data exist such as interviews, documents, observations, and videos. The main sources for this thesis were official documents, articles, newspapers and textbooks. This multi-source approach enabled triangulation in data collection which contributed to ensuring validity and reliability of the presented information. These important concepts will be discussed in more detail at section 3.5.

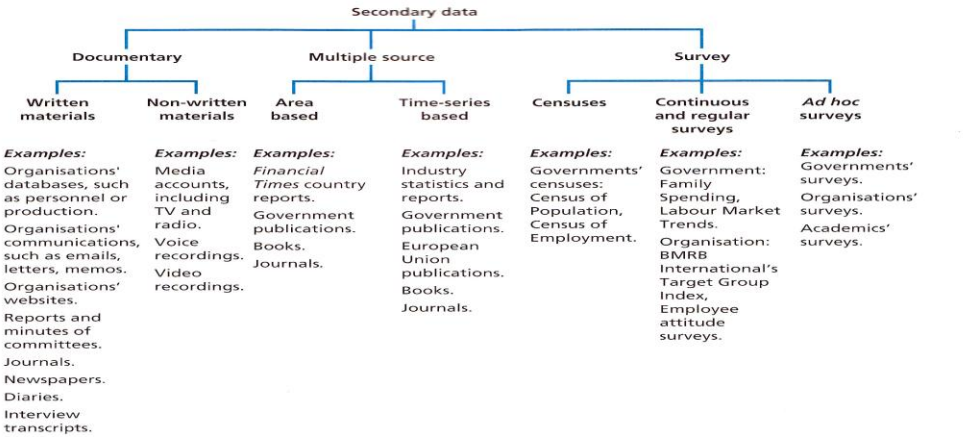


Figure 3: Sources of Data (Saunders, Lewis and Thornhill, 2009:259).

Reflexivity must be considered in qualitative research as the researcher will often, even unconsciously, convey their emotions or feelings to those involved in the study, despite trying to avoid bias. This arguably is evident within Chapters Four, Five and Six despite the researcher consciously attempting to distance herself from the analysis of these events and the frustration that was felt in reading the about the issues and errors that occurred. This may be picked up upon by those people who consciously or unconsciously alter their standpoint in response to this. This prompted Finlay (2002) to ask whether the researcher and the respondent actually co-constructed the research. It is the potential implications of this for any study that requires a researcher to develop their self-awareness in order to minimise adverse effects on the study. This can also have positive aspects as Finlay (2002) in Corbin and Strauss (2008:31) goes on to note not least through 'enabling public scrutiny of the integrity of the research through offering a methodological log of research decisions'. This will of course vary between researchers as some view it as more relevant than others, however, in light of the emptive topic of this thesis, the researcher has tried to ensure that she does not influence others' decisions and that she remains objective.

However, any objectivity displayed by the researcher must be tempered with sensitivity, meaning the ability to glean insights, being able to identify relevant details and being able to present respondents' views whilst taking the role of another (Corbin and Strauss, 2008:32). Familiarity with the information can also help to achieve this; the use of three key case studies by the researcher and awareness of a broad range of literature on each of these helped to achieve such familiarity. Sensitivity thus helped the researcher to arrive at concepts that are grounded in data (Corbin and Strauss, 2008:41).

3.3.1 Literature Review

During the course of this research it was imperative to include a thorough literature review considering both terrorism and risk and crisis management. Through exploration of the existing literature in these areas, it was then possible to identify where this thesis would fit into the current knowledge and, more importantly, what it would contribute to the current body of knowledge. Bryman and Bell (2007:95) suggest that reviewing the literature should help researchers to identify those concepts and theories relevant to this

area, identify any significant controversies, understand what research methods and strategies have been utilised by others researching this area and perhaps most importantly, if there are any inconsistencies in the findings related to this area.

In conducting the literature reviews for this thesis, the researcher would agree with these outcomes as she experienced these for either or both of the literature reviews earlier in Chapters One and Two. Throughout the reading, research parameters become clearer and the research aims become more refined: a process that can be likened to an upward spiral (Saunders, Lewis and Thornhill, 2009:60) as the illustration below clearly highlights:

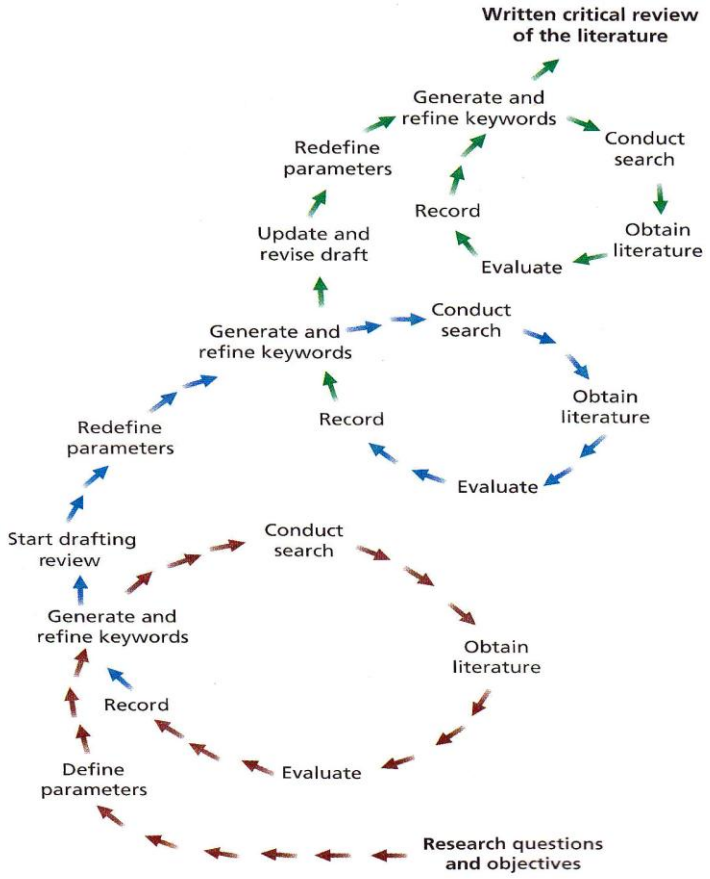


Figure 4: The Literature Review Cycle (Saunders, Lewis and Thornhill, 2009:60)

There are many sources of literature available to help a researcher gain an insight into a particular issue and previous research. Broadly, these can be divided into three categories: Primary, Secondary and Tertiary. This categorisation represents the flow of information from the original source. The further away from the source they are, the less detailed and accurate the information may be but the more easily accessed it is (Saunders, Lewis and Thornhill, 2009:69).

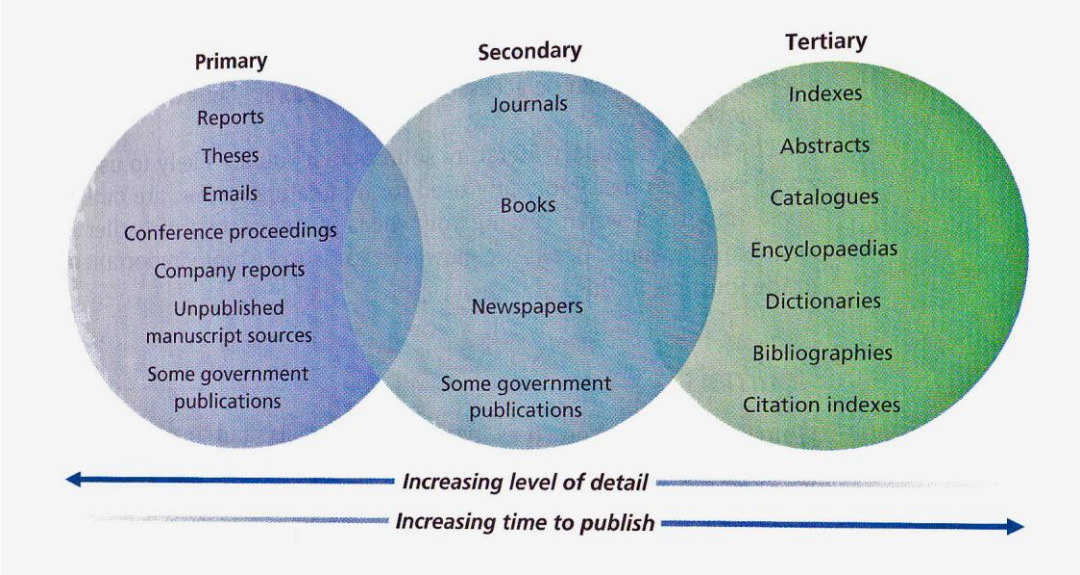


Figure 5: Primary, Secondary and Tertiary Data (Saunders, Lewis and Thornhill, 2009:69)

Understanding this enables the researcher to identify the most appropriate sources of literature for the study. The majority of research projects will make most use of secondary literature. There are several associated advantages of this:

1. unobtrusiveness – because data has already been collected, it is an unobtrusive measure. This is particularly important when dealing with topics such as terrorism which may be particularly emotive and sensitive.

2. unforeseen discoveries – reanalysing data can lead to unforeseen or unexpected new discoveries.

3. data permanence – secondary data will generally be permanent and in a form that can be checked relatively easily by others. Such qualities greatly enhance the reliability and validity of the data.

4. Longitudinal studies may be feasible: this was evident from the initial report in the 7/7 bombings and the later, follow-up reports

(Saunders, Lewis and Thornhill, 2009:69).

Although there are some clear advantages in using secondary data, there are of course disadvantages which may include:

1. data collected may not match the researcher's need therefore it may not be appropriate for the research question. Fortunately, this was not the case with any of the source documents here as the purpose for which they were collected is the same purpose as that of this thesis.

2. no real control over data quality as it has been collected by someone else. Within this thesis, it is hoped that the sources used are reliable as they are compiled by public bodies and respected authors.

3. The initial purpose may affect how data are presented. Again, as at point 1, the researcher and source author's aims are broadly matched so this issue should not affect the integrity of the thesis findings or recommendations.

(Saunders, Lewis and Thornhill, 2009:69).

In order to meet the aims and objectives of this thesis, the researcher felt that primary and secondary literature sources would be most appropriate due to their level of detail.

Inquiry reports and organisations' reports formed the majority of the primary sources whilst journal articles and some review reports formed the basis of the secondary sources. The increased level of detail included in such sources, combined with the closeness in terms of time from the event to publication, meant that the researcher could trust the information far more as valid, reliable sources; time had had less chance to blur or confuse the detail.

This was particularly relevant in light of the emotive nature of the topic and the events under consideration.

3.3.2 Case Study Methodology

The case studies included here are not intended to retrospectively advise those response agencies involved in the incidents but rather to provide an incremental analysis of terrorist event consequence management and build on the insights gained from these. Although the observation could be made that there is little difference between what this thesis is attempting methodologically to do here with the case studies, that is to reflect on accounts of the event and highlight areas for improvement, there is in fact a significant difference that arguably improves the quality of recommendations that will be made: none of the committee or inquiry reports thoroughly considered similar events to identify areas for improvement nor did they examine risk and crisis management methodologies to better inform their analysis and decisions. Arguably this ensures a more comprehensive understanding of events and possible recourse that will be more effective.

Lessons learned will be used to inform recommendations for future incident management and to gain additional insights. To further this, first and second-order effects will be considered. First-order effects are those effects that are directly related to the original incident, for example following 9/11 for a while, the number of airline passengers fell. Second-order effects are often viewed as the 'knock-on effects' of an incident so using the 9/11 example again, the value of airline shares fell following the attacks.

Case studies are empirical inquiries that:

- investigate a contemporary phenomenon in depth and within its real-life context, especially when
- the boundaries between phenomenon and context are not clearly evident

(Yin, 2009:18).

This methodology is about theory building and the need to understand a real-life phenomenon through the attainment of deeper understanding (Riege, 2003:80). From this, it can be seen that it is an all-encompassing methodology and is particularly appropriate for the nature of this research study, confirmed by Saunders, Lewis and Thornhill (2009:145).

As the researcher hopes to produce management guidelines, it is advisable to review some examples of terrorist incidents to provide context for the study, and to try to identify areas where good practice has occurred or problems were created. This will inform the content and structure of the researcher's suggestions. Therefore, the thesis had an element of formative evaluation (Robson, 2002:208) as it is intended to provide guidance for the development of a new framework for organisations and is also partly exploratory, determining what happened in some terrorist attacks and how they were managed. Yin (2009:4) supports the use of case studies for this type of study as he states that the case study methodology 'allows investigators to retain the holistic and meaningful characteristics of real-life events'. Case studies are a valuable technique for examining contemporary events not least as their strength is the ability to deal with a range of evidence such as interviews, documents, artefacts and observations, which other methods may not be able to cope with so effectively (Yin, 2009:11).

Due to the unique nature of terrorism case studies, it is argued that a multiple embedded case study methodology is the best way to analyse and evaluate practices, as each case will be different from the next. The researcher views the multiple case study approach as the same as a single case study approach within the same methodological framework, as Yin (2009:53) concurs. The embedded nature of the case studies refers here to the unit of

analysis, that is, there is more than one organisation and event under consideration here (Saunders, Lewis and Thornhill, 2006:140). The use of such a methodology adds to the reliability of the results as evidence may be considered more compelling and hence produce more robust results. Any multiple case study design should not follow a sampling logic but instead a replication (Yin, 2009:60). However such a method also has disadvantages such as the increased time and resources required of the researcher as opposed to that for a single study. As a result, the decision to use multiple case studies must be carefully considered.

Case studies are a phenomenological methodology and hence are appropriate for the chosen paradigm (Collis and Hussey, 2003:60, Robson, 2002:89). The case studies will cover pre-documented events in order to provide examples of how such incidents were managed and the lessons that could be drawn from these. These will also be partly experimental as the research will examine any problems in the implementation of new regulatory and procedural techniques and evaluate the benefits (Collis and Hussey, 2003:68).

3.3.2.1 Designing Case Studies

The case to be investigated can be anything from a person to an organisation to a particular setting. Multiple case studies may also be used as in this thesis. As Robson (2002:183) suggests, the first case study provides the initial evidence and guides the selection of subsequent case studies. The findings from these studies then form the basis of the generalisation that is made. Reliability and validity are also therefore improved.

Within the case study chapters a descriptive element exists in order to help the reader to fully appreciate the contexts within which each attack occurred, the nature of the response and the interactions that helped, and hindered, on the day. Qualitative research often incorporates an element of description as it is the basis for more abstract interpretations of data and theory development and hence is basic to theorising (Corbin and Strauss, 2008:54).

Developing theory is complex and for this thesis, the definition given by Corbin and Strauss was felt to be most appropriate:

'…theory denotes a set of well-developed categories (themes, concepts) that are systematically interrelated through statements of relationship to form a theoretical framework that explains some phenomenon' (2008:55).

Corbin and Strauss (2008:56) also suggest that because formal theories are usually derived from investigations of a concept under a variety of different related topics and conditions, they become much more abstract and give greater applicability than do substantive or middle-range theories.

A case study methodology has several advantages such as the generation of "rich" data and the opportunity to develop detailed knowledge of a case within its context. However, there are several disadvantages that should be accounted for during the research process. Firstly, negotiating access to suitable organisations may be problematic and time consuming. It can also be difficult to determine where to place the boundaries for the study; no organisation exists in isolation, they interact with society and the environment (Collis and Hussey, 2003:70). Lastly, the researcher will be considering a case at the present time; actors may not have knowledge of previous and following events and hence it may be difficult to fully understand the current situation.

Although some may suggest that a case study methodology is not as scientific as some other approaches, the researcher argues that this enables existing theory to be challenged and that it provides a source of new research questions, as Saunders, Lewis and Thornhill (2006:140) concur.

3.3.3 Data Collection

Case studies are inherently multi-method involving analysis of documents, records and sometimes interviews (Robson, 2002:165). Topics and issues identified within these case studies will be used to focus the recommendations for future event preparedness.

3.4 Research Analysis

Analysis should begin ideally after the first interview, observation or review; a sequential approach like this aids identification of relevant concepts and helps to identify new lines of enquiry (Corbin and Strauss, 2008:57).

3.4.1 Analysis Questions

Corbin and Strauss (2008:72) suggest that there are four key types of questions that may be used in research analysis, although questions may not be limited to these:

- Sensitising questions: These help the researcher to identify what might be occurring, for example what is happening, who is involved and how would the actors define it?

- Theoretical questions: Theoretical questions assist in recognising process and variations to connect concepts, for example, how do events change over time? What would happen if?

- Practical questions: These help to develop the structure of the theory, for example, is my theory logical? Where are the breaks in this?

- Guiding questions: Such questions guide interviews, document gathering and analyses. Questions often become more focussed as the research progresses and relationships and interactions become clearer (Corbin and Strauss, 2008:72).

The researcher employed this question set to focus the analysis and to ensure coherence. Once the analysis was complete, it was necessary to code themes and issues that had been identified in all of the three case studies that were deemed central to the management problems.

3.4.2 Comparative Analysis

In order to try to identify areas for improvement and good practice, the researcher felt that comparative analysis of three cases, within a case study methodology would be most appropriate. Such an approach requires comparison of incidents for similarities and differences. In this thesis, these will be used to inform recommendations for management of the aftermath of terrorist incidents and for improving resilience. Context is particularly important here because it reveals circumstances that impinged on those caught up in the attacks and may help the researcher to make more valid and realistic recommendations.

Context must be considered at both the micro and macro levels: the former, for this thesis, will comprise the immediate conditions faced by victims, relatives and rescuers in each attack. The macro level considers the pre-cursor conditions to the attacks, including infrastructure and plans that led to the actual conditions during the incidents (Corbin and Strauss, 2008:230).

Data for this thesis were obtained from Inquiry Reports, review documents, articles, media reports and informal off-the-record discussions. The range of data sources meant that the analysis was to be fairly time-consuming.

The first step in beginning the analysis of the data was to summarise it. At times this was quite challenging and it was imperative to keep the meaning of what had been said whilst re-phrasing it into a few words. Care had to be taken to ensure that meanings were not changed or lost and that researcher bias was not introduced. An example of this was where individual's responses had been included in Inquiry Reports and if there had been an avoidable oversight, potential existed for frustration on the part of the researcher to bias the re-phrasing. The researcher therefore asked peers to review what she had written to ensure that such bias did not occur.

Re-phrasing helped the researcher to familiarise herself with the emergent themes from the data and possible relationships between these. Once these themes had been identified, categories within these were then established. Communication and resources appeared to

be the main categories for analysis as the vast majority of issues could be filed under these headings.

These categories were then further broken down following unitising of the data. It was found that a distinction was clear between internal and external communications, actions, equipment and resources. In unitising the data (Saunders, Lewis and Thornhill, 2009:493) chunks of data were attached to relevant categories above and codes then assigned to denote these. The identification of emergent themes can be seein within the conceptual model in Chapter Seven of this thesis. The coding process will be discussed at 3.4.3.

Turner's (1978) SRAD methodology for analysing events was initially used as the researcher felt that this could be a useful tool for gaining greater understanding of events and actions during these. However, although the methodology was initially quite useful for identifying actions and possible connections and effects of these, it was of less use for analysing the softer, fuzzier elements of the events (and arguably, the more important factors as these influence turning points in the events). As the analysis progressed, it became more apparent that the issues of communication and decision making in each event were the most important factors and the SRAD methodology was felt to be of less use in further analysis.

The researcher therefore ceased using this and instead moved towards manual coding of the softer issues.

3.4.3 Coding

The initial coding comprised noting events and interactions but this generated far too many occurrences to be of use. It was therefore necessary to try to identify themes within which these could be grouped. This then became an iterative process to reduce the number to a manageable amount. It was evident at the end of this process that there were indeed six distinct themes that were prevalent in each case study. These were: internal communications, inter-agency communications, public communications, actions, equipment and resources, denoted by the labels:

- INTCOM
- XCOM
- PUBCOM
- ACT
- EQUIP
- RES.

The researcher, as part of this process, began to make judgements regarding the data significance depending on how many times it had been identified within the case studies. Such quantitative assessment of qualitative data based on data frequency is quite normal as Bryman and Bell (2007:593) assert.

Such coding is an example of open coding using *in vivo* codes, as these are based on the terminology found within the data sources for this thesis (Saunders, Lewis and Thornhill, 2009:509). The categories that then appeared were used within axial coding whereby relationships between these were recognised.

The final list of codes given above was a result of this process. These could then be verified against the actual data.

An element of template analysis was also used, although not explicitly chosen, following the listing of codes and categories. This enabled them to be presented hierarchically which aided understanding. The researcher did find that some of the codes changed places in their levels of importance within the hierarchy. Saunders, Lewis and Thornhill (2009:507) note that this is quite normal within this method of analysis.

In parallel to the template analysis, an element of analytic induction (Saunders, Lewis and Thornhill, 2009:508) presented itself, in line with Johnson's (2004:165) definition:

> 'the intensive examination of a strategically selected number of cases (in this case three) so as to empirically establish the causes of a specific phenomenon'.

Although it could be suggested that a specific phenomenon *per se* was not the subject of the investigation here, the researcher argues that in terms of this thesis, the 'phenomenon' was the mismanagement of major terrorist incident responses. The researcher would suggest that perhaps use of the word 'phenomenon' is not altogether helpful when discussing what is an invaluable analytic approach as it may be misleading to both readers and researchers, implying incorrect disregard in some circumstances.

The researcher felt that analytic induction was a valid method for analysing data within this thesis as it is both inductive and incremental, enabling well-grounded explanations to be developed, as Saunders, Lewis and Thornhill (2009:508) concur.

Johnson (2004) identifies a potential drawback with such an approach where a researcher may fall into the belief that where a phenomenon results when certain conditions exist, this would always automatically follow whenever such conditions were present. This of course may not always be so.

The researcher felt that this was a caution to be heeded but saw no evidence of this within this thesis; within each case study included here, the same conditions existed in each and did result in the same phenomenon. Johnson's advice, whilst pertinent, was not applicable in this situation.

3.5 Quality Assurance: Validity, Reliability, Generalisability and Triangulation

The design of any research project should be such that it explicitly recognises the need for quality to be achieved in the course of the investigation. The research design is therefore central to achieving this.

3.5.1 Validity

Maxwell (1992) in Robson (2002:171) generated a useful typology for identifying possible threats to validity within flexible designs. Maxwell suggests that research studies

can be broken down into three areas: description, interpretation and theory and threats can exist within these. It is pertinent to consider these in more detail:

- *Description:* inaccurate or incomplete data can threaten the validity of the data. Recording interviews can help to avoid this, supported with rigorous note-taking.

- *Interpretation:* researchers must ensure that interpretations from the data stem from the data itself and are not imposed or meanings assigned from the outside.

- *Theory:* researchers must consider alternative explanations and understanding for what is being analysed. This includes avoiding researcher and respondent biases.

(Robson, 2002:172).

Further to this, Yin (2009:40) and Riege (2003:80) suggest that there are four tests that should be carried out to ensure research quality. These are construct validity, internal validity, external validity and reliability. For each of these tests, there exist corresponding design tests which will also be considered here.

3.5.1.1. Construct Validity and Confirmability

Construct validity considers the appropriate measures for the concept being studied. Within case study research, the use of multiple sources of evidence, the establishment of chains of evidence and the use of key informants to review drafts, are all useful methods to help to achieve this validity in this context (Yin, 2009:41). Riege, (2003:80) highlights the need for researchers using case studies to specifically avoid subjective judgements during design and data collection phases to help to achieve construct validity.

The design test that corresponds to construct validity is confirmability, Riege (2003:81) argues. This aims to test whether the data interpretation is logical and unprejudiced. Miles and Huberman (1994:278-9) suggest that researchers should ask themselves whether the research methods are explained in detail, whether the complete picture is given to readers and whether the obtained data is available to others.

3.5.1.2. Internal Validity and Credibility

This can be achieved by pattern matching and explanation building as Yin (2009:41) suggests or 'cause and effect' relationships. Furthermore, addressing rival explanations can also help to achieve this. In terms of a case study methodology, this can be achieved by establishing phenomena in a credible way (Riege, 203:80).

Credibility is the parallel construct to internal validity. Within this design test, peers or interviewees approve, or otherwise, the research findings. Questions to be asked here include how rich are the descriptions? Are findings internally coherent? Are concepts systematically related? (Riege, 2003:81).

3.5.1.3 External Validity and Transferability

External validity considers whether a study's findings are generalisable beyond the immediate case study (Yin, 2009:43 and Riege, 2003:81). Yin highlights the argument that in case study research, it is possible to make generalisations as here, we are considering analytic not statistical generalisation. The ultimate aim is the development of understanding of constructs.

Transferability demonstrates external validity by proving that findings are detailed enough for readers to assess the transfer of findings to their own circumstances (Riege, 2003:81).

All of the design tests here could be assessed through peer review of the write-up. The researcher was able to test the validity of her findings by asking colleagues to read through these and comment on the above. Such feedback was invaluable during the course of this thesis.

3.5.2 Reliability and Dependability

The very nature of qualitative research means that formal reliability testing may not be possible, certainly not in the standard form that quantitative research allows. As a result,

researchers arguably have to be more thorough and careful, proving this to their readers (Robson, 2002:176). Audit trails can help to achieve this.

The objective for reliability is that should a later investigator follow the same procedures and conduct the same case study, they should arrive at the same findings and conclusions (Yin, 2009:45 and Riege, 2003:81). This is not easy to achieve in case study research as people and their behaviour are not static unlike quantitative research measurements.

The design test here is dependability through the demonstration of stability and consistency in the research (Reige, 2003:81-2). By ensuring that the research questions are clear and that the research design is congruent with these, dependability should be easier to attain. If researchers approach the study as though they are constantly being observed, it should help to achieve this.

3.5.3 Techniques to Perform the Design Tests

Numerous techniques have been developed with regard to the design tests described above. Riege (2003:83) suggests the following techniques in order to establish the tests:

3.5.3.1 Techniques for Confirmability

Examining the raw data, findings, interpretations and recommendations, essentially auditing these during the collection and analysis phases is a useful technique to achieve confirmability. By implication, the raw data must be retained for later inspection if required.

3.5.3.2 Techniques for Credibility

Triangulation in collection and analysis is a valuable technique to employ. Peer debriefing may also be beneficial to foster credibility.

The research design phase can also provide the opportunity for techniques to enhance credibility. Taking account of the researcher's worldview and assumptions and self-monitoring throughout this stage can also be a valid technique to ensure credibility.

3.5.3.3 Techniques for Transferability

The development of a case study database during data collection and the use of cross-case analysis is a useful technique for transferability. This can be seen to have some similarities with the techniques for confirmability.

3.5.3.4 Techniques for Dependability

Here, overlap can also be seen with techniques for achieving credibility as the researcher's theoretical position and biases are taken into account. In addition, a dependability audit, where the process of inquiry is examined and documented. The auditor can then examine these processes to ensure that bias is avoided and dependability is established (Riege, 2003:84).

3.5.4 Generalisability

It is useful to make the distinction between internal and external generalisability. The former refers to generalisability within the studied setting. The latter refers to that beyond the setting (Robson, 2002:176). Case studies can pose issues that need to be overcome in terms of generalisability. As each case study is usually unique, generalisability can be problematic however analytic or theoretical generalisation may be possible (Yin, 1994). This thesis attempts to develop theoretical generalisability through expansion of the theoretical insights obtained in the course of the research that can then be applied to other events.

3.5.5 Triangulation

This is a valuable method to enhance the rigour of research (Robson, 2002:174). Triangulation can refer to the data, methodology, observer or theory. In each instance, multiple sources or individuals are used to increase the validity and reliability of the research. Holden and Lynch (2004:406) cite Gill and Johnson (1997) as further supporting the use of multi-method approaches as it leads to the convergent validation of research results through internal cross-checking. However, care must be taken to ensure that the multiple perspectives or sources of information do not begin to contradict each

other. If discrepancies exist between different sources of data, it may also be problematic to make a direct comparison (Robson, 2002:175).

Denzin (1988) identified four types of triangulation:

- Data triangulation: more than one method of data collection is used
- Observer triangulation: more than one observer is used in the study
- Methodological triangulation: quantitative and qualitative methods are combined
- Theory triangulation: multiple theories or perspectives are used by the researcher

(Robson, 2002:174).

Robson (2002:93) also recognised that much debate surrounds qualitative data and the issues of validity, generalisability and reliability. In order to address these issues, the researcher employed data triangulation in the course of her research through document analysis, 'off the record' discussions and case studies. An element of theory triangulation was also used in the reference to crisis and risk management theories to help generate recommendations for future practices. It is intended that these steps will enhance the quality of the research although according to Collis and Hussey (2003:78) validity is already high under the phenomenological paradigm as its aim is to obtain full access to the knowledge and meaning of those involved in the research setting.

3.6 Ethical Considerations

Ethical problems exist from the inception of any research study: what will you study, where will you do this, who will you ask? Ethical considerations do not only apply to the collection of data; they also apply to reporting the findings. For example, comments should not be misrepresented and any sort of bias should be avoided in the write-up. These are just a few of the issues that a researcher must consider.

Within business and management research, Saunders, Lewis and Thornhill (2009:184) argue that there are two dominant philosophical standpoints: deontology and teleology.

The former proposes that the ends do not justify the means, that is, any practice that is unethical is not acceptable. Teleology conversely argues that the ends do justify the means and that the benefits realised from the research should be compared with the costs of unethical behaviour. In light of the sensitive and emotive subject of this thesis, and given the researcher's personal beliefs, a deontological view of the research was taken.

Robson (2002:67) suggests some questions to consider before performing research: Is confidentiality always appropriate? What responsibility do researchers have for the knowledge that they have acquired? The researcher suggests that this is a useful starting point for any study.

None of the victims of the 7th July 2005 attack was interviewed as it was felt that their inclusion in this piece of research was not appropriate for its aims and as a result would be unethical to include. It is suggested that in future research it would be beneficial to obtain the views of those directly affected by the incident in order to focus victim support practices and make them more appropriate in the future. However, this is beyond the scope of this thesis.

A research ethics form was also completed for the University as the examining body to ensure that its ethical procedures were not contravened.

Whatever research study is performed, the researcher should remember that they are in a position of power and this should not be abused or taken for granted: never more so than when addressing sensitive subjects.

The next chapter opens Part II, the empirical element of this thesis, and will begin with the Sarin Gas Attacks on the Tokyo subway system in 1995.

4. Aum Shinrikyo and the Tokyo Sarin Attacks

4.1 Introduction

The Tokyo subway nerve gas attacks on March 20th 1995 provide an expedient case study for those involved in emergency planning and resilience to terrorism to consider. As Pangi (2002:2) asserts, this case study is a useful learning tool for those seeking to form a coherent domestic preparedness strategy not least because reviewing the attack and earlier incidents reveals potential opportunities to pre-empt or mitigate future attacks. Such a learning strategy is propounded by Toft (1994) in 2.3.4.2 of this thesis where he develops the idea of Isomorphic Learning or learning from experience. The Tokyo Sarin attack provides five important lessons: firstly, the attack was easily planned and secondly, the attack was easily carried out. Thirdly, that the chemical agent was easily manufactured and fourthly, that the potential death toll from such an attack is massive and lastly, that emergency medical systems within major cities may be unable to effectively respond to this type of attack (Martin, 2010:345).

The attacks, carried out by the Aum Shinrikyo (Supreme Truth) religious cult on the Tokyo subway system, were a very different type of terrorist assault as they comprised a solitary attack with no real, recognised precursor or ongoing campaign unlike the events of September 11th 2001, the subsequent Al-Qaeda operations globally or even earlier Irish Republican Army (IRA) attacks on the British mainland. It also raised concerns around the world that terrorists were moving towards the use of chemical weapons and weapons of mass destruction (WMD) which spurred on government programmes internationally to improve their readiness for such contingencies (Jenkins and Gersten, 2001:49). Creating the capacity for prompt intervention in such an attack could mean that potentially catastrophic effects could be substantially reduced (Pangi, 2002:1), again adding weight to the argument for improving resilience, furthering the cause of this thesis.

4.2 The Subway Infrastructure

Two separate subway systems make up the subway system in Tokyo; the TRTA, also known as Eiden Lines or Teito, which is the larger system and the Toei system which is

run by the municipal government. It was the older, larger TRTA system which came under attack in March 1995 and within this, three lines, the Marunouchi, Hibiya and Chiyoda were targeted. A map of the subway can be seen at Appendix V. The Tokyo subway is considered by many to be the best in the world, attaining 100 per cent punctuality at peak times and it was this commitment to keep the trains running on time that was an important factor in the response to the Sarin attack (Jenkins and Gersten, 2001:50).

In addition to the pressures of this level of punctuality, the volume of passengers was a further complication. Millions of commuters use the subway every day and at peak times it is not uncommon to see station staff pushing commuters into already hugely crowded trains. On the day of the attack, this had a two-fold effect as perpetrators were easily concealed and those who were caught up in the attack could not escape to safety as more passengers were being pushed on to the trains. It was estimated that more than one thousand commuters had been exposed to the gas within minutes (Jenkins and Gersten, 2001:50).

4.3 The Japanese Ethos

Peace, known as *heiwa* and fundamental human rights or *jinken* are two cultural concepts that are central in national and international security policy in Japan (Miyasaka, 2000:3 in Pangi, 2002:5). This ethos has fostered three national ideas on terrorism which are that firstly, the root causes of terrorism are poverty or prejudice or are in response to an oppressive government; as this thesis has already discussed, those who engage in terrorism are often well educated, middle class individuals, not from impoverished backgrounds as was previously thought. What the Sarin case illustrates is that such outdated thinking was on a global scale not merely something that was confined to the West. Secondly, that Japan's anti-terrorism strategy is highly risk averse, hence sparing lives is the most important consideration in a terrorist incident and thirdly, terrorism is a taboo subject not to be openly discussed; the Sarin attacks are often viewed as unique cases rather than acts of terrorism (Pangi, 2002:5-6). This mindset directly impacted on

the nation's approach to resilience to terrorism and had resulted in many in Japan feeling that anti-terrorism was a greater risk to society in terms of heiwa and jinken than terrorist acts may have been. It is only relatively recently that this has started to change.

4.4 The Attack in Context

Aum Shinrikyo (Aum) was founded in 1987 by Shoko Ashara and was a religious cult based on the belief that Armageddon was approaching. Ashara urged followers to arm themselves in order to survive Armageddon, which included stockpiling chemical and biological weapons (Martin, 2010:199).

A small group of Aum Shinrikyo members carried out their first Sarin attack on June 27th 1994. A converted refrigerator truck was used to release Sarin into the air in the village of Matsumoto. The targets were three judges who were about to issue the verdict in a civil case that concerned land rights to which Aum was a party. Fortunately the attack was not a complete success although seven people died and around five hundred were hospitalised (Pangi, 2002:6). The police investigating the incident refused to believe that it was a chemical weapons attack and instead blamed it on a local man who they claimed had accidentally created poisonous gases mixing fertilizer in his garden. The media however highlighted the improbability of this and pursued their investigations, raising the possibility of a link between the cult and the attack. Later that year, the link was confirmed when soil samples from outside the cult's compound confirmed traces of Sarin. Despite this, no arrests were made until after the March 1995 subway attacks (Pangi, 2002:7). Had good media relations existed such as discussed at 2.10, the police may have altered their thinking and perhaps made the link earlier.

4.5 The Sarin Attacks and Initial Response

The subway attack itself was fairly crude and comprised eleven plastic bags containing around twenty ounces of Sarin solution which were then punctured by an umbrella, or similar, within the train carriage. Two or three bags were left on each train and once

punctured, the solution turned to vapour and spread as a lethal mist. In all, five attackers were used, beginning their assault at 8am. By 8:10am, the attack had been completed. The three train lines that were selected all converged at the Kasumigaseki Station, which was to be the ground zero of the attack as it was home to most of Tokyo's government offices and is thought of as the power centre of the city (Pangi, 2002:8). Sixteen stations were affected that day: twelve people died and more than three thousand people became ill as a result of the attack (Jenkins and Gersten, 2001:53).

The first emergency calls were received at around 8:20am but at this time it was unclear what had occurred; callers spoke of explosions and injuries from fumes. The emergency services responded quickly to the attack, however, not enough ambulances were available so police vans were used instead. Such confusion was also seen in the 9/11 attacks, discussed at 5.4.1 and 5.4.2 of this thesis and in the 7th July 2005 attacks in London (discussed at 6.2 and 6.7). Clearly the same issues keep arising and need to be addressed, vindicating the purpose of this thesis and the assertion made at 2.3.4.2 that such problems keep occurring because lessons are not learned or addressed. Communication in times of crisis is plainly an issue that requires further attention.

Rescuers who were first at the scene and who went down into the subway stations became ill as did those who were exposed to the clothing of victims who came into contact with the gas. Interestingly, Sarin was considered as a possible cause but was then rejected as it was thought that with that kind of agent, far more casualties would have resulted. Several hours passed before the agent used and the dispersal method was known (Pangi, 2002:13).

Somewhat fortunately, the police had thirty sets of protective masks and suits available to them in preparation for a planned search of Aum Shinrikyo's premises on March 22nd 1995 that were used to protect them from the fumes. By 13:30pm, police wearing the protective clothing had recovered the bags and begun decontamination of the stations.

There was apparently some disparity between the speed at which hospitals were able to conclude which toxin had been used and hence which treatment should be administered. This was despite televised interviews with victims that clearly demonstrated that a nerve gas, similar to that in the Matsumoto attack on June 27th 1994 had been used; this was the first Sarin attack executed by the Aum Shinrikyo scientists (Jenkins and Gersten, 2001:56). Jenkins and Gersten go on to raise an interesting question pertaining to the number of fatalities and casualties: was lethality a trade-off for quantity? The Sarin mixture that Aum Shinrikyo prepared contained many impurities, in fact it was only thirty percent pure (Pangi, 2002:8) but it is not clear whether this was a deliberate act to slow down the vapourisation to achieve greater effects and protect the attackers, or whether it had merely been a side effect of a hurriedly prepared batch of Sarin; had it been purer, victims would have died instantaneously and the numbers exposed to the gas may have been fewer. Commuters would not board a train filled with corpses (Jenkins and Gersten, 2001:56). The impurity did alert staff to the presence of the chemical however as it caused it to emit an odour that in its purest form did not occur (Pangi, 2002:8).

Once the situation had been determined, within five minutes, the National Police Agency (NPA) requested assistance from the Self Defence Force (SDF) who jointly established a police/army investigative unit. A second unit was co-ordinated by the police, fire, rescue and medical responders (Pangi, 2002:18). However, considerable difficulties still occurred which added to the delays in rescue and response.

In spite of these initial delays, by late afternoon the subway system was running again. In addition to the police officers involved in the immediate response to the attack ten thousand more officers from the Tokyo Metropolitan Police Department, which had controlled the rescue operation, were used to increase security at locations around Tokyo where crowds congregated. Warnings were also issued to report any suspicious parcels to the police and not to approach these.

By March 22nd, the offices and facilities belonging to the sect had been searched and were kept under surveillance. Arrests were made in early April and by mid-April, more than one hundred cult members were held in custody. However none was immediately charged with the Sarin attack (Jenkins and Gersten, 2001:57). Cult members who had not been arrested retaliated through further chemical attacks, assassination attempts against the Chief of the National Police Agency and the murder of the cult's own Chief Scientist. The campaign abated on July 4th 1995 when four final gas attacks were attempted but failed.

4.6 Dangerous Event Management in Japan

As has been discussed, a general reluctance existed amongst officials to prepare for, or discuss, terrorism. Accordingly, consequence management plans and capabilities were largely under-developed which directly mired the response effort in both of the Sarin attacks. This meant that all essential services that would either mitigate or ameliorate the effects of a disaster were not fully integrated within response procedures (Pangi, 2002:9). Such reticence to think the unthinkable (Unknown) is not unusual when preparing for crises. The potential implications of this must be highlighted to those involved in crisis planning to reinforce the importance of such readiness.

The system in Japan is set up so that local governments are responsible for disaster management but in 1995 prior to the attack, it was recognised that the disaster response plan that was in place meant that local resources could be overwhelmed. In light of this, provision was made to ensure that surrounding hospitals would supply staff to a scene of disaster to assist the Emergency Life-Saving Technicians (ELSTs) (Pangi, 2002:10). Other localities were also involved through mutual aid agreements. National Crisis Management Agencies do exist and the governor of an affected prefecture is in charge during an emergency. To secure any assistance from national agencies at such a time, local government must formally request this; this can be a large obstacle to overcome, particularly if it is the SDF, who are part of the Defence Agency who are needed. The SDF cannot act without the consent of the Prime Minister. They also cannot act without a

formal request from help from local government. Without receipt of a request and approval, the SDF cannot participate in any rescue operations which could prove disastrous if their knowledge of chemical warfare and ability to rapidly establish communications systems and triage units is desperately needed (Pangi, 2002:11). Had training simulations been undertaken prior to the incident, the problems that arose from existing procedures may well have been identified so that changes could be made; this is supported by the discussion regarding training and testing plans at 2.8 of this thesis. Such inflexibility can cause an emergency to escalate to the next level as Turner's model at 2.3.4.1 of this thesis highlights. Arguably, this is what occurred to some extent in Tokyo, stressing the relevance of the risk and crisis literature review within this thesis.

For larger scale disasters that require a national response, the government would create a Headquarters for Major Disaster Countermeasures. The National Police Agency would assume a support role but would still maintain the authority to co-ordinate and command local law enforcement as Pangi (2002:11) stresses.

4.7 Major Issues and Lessons Learned

Many issues were raised during and subsequent to the attacks, which related to both general and specific circumstances. It is constructive to consider these as they are important points that any organisation should consider in such a scenario in order to mitigate its consequences. Jenkins and Gersten (2001:64) highlight twenty-one points that they deem worthy of special consideration and these could be argued to be a useful checklist to be employed by others: these can be found at Appendix VI. However the broad themes that were identified were a lack of planning and preparedness combined with a lack of on-going threat analysis, physical security including CCTV issues, equipment availability problems and communications issues. These are also issues that are seen in the case studies at Chapters Five and Six of this thesis, highlighting the necessity for the research performed here.

It is suggested following consideration of this list that it is a useful starting point but perhaps that it overlooks or detracts from some of the major considerations; those overarching points that tie these individual issues together and directly impact upon these. For this, Pangi (2002) highlights several key areas for consideration within which some of Jenkins and Gersten's points sit. It is this analysis that perhaps offers the more useful generic resilience advice that is appropriate for a range of organisations and industries.

4.7.1 Issue Identification and Response

This is an overarching concern identified by both, although Jenkins and Gersten (2001:64-65) break this down into several points as was seen again at Appendix VI, without necessarily acknowledging that this is one of the core issues underlying all of these problems. Recognising the problem is not enough: the information must also be disseminated up and down the chain of command.

Much has been said regarding the confusion at first and the conflicting announcements that were made to passengers. Despite this, one train was delayed by only seven minutes following the attack before moving on to the next station and finally being halted (Kaplan and Marshall, 1996:248-249). Although the station staff were the first responders to the incident, their difficulty in assessing the situation is not unexpected; staff were not trained for this type of incident, nor was there a centralised system to monitor any events at different stations (Pangi, 2002:13).

Several root causes of the delays have been identified and there are lessons here that are relevant for other organisations. Firstly, an attack of this type and this magnitude had never been seen before; no response plan or training had been provided for this novel event and no-one outside the military had contingency plans to deal with a WMD attack.

Secondly, the multiple sites element was not initially realised until the police had received enough telephone calls to alert them to this possibility. This was also seen in the 7th July London bombings where for a long time it was thought that five separate

incidents had occurred rather than co-ordinated attacks, discussed at 6.2 of this thesis. The final cause relates to the structure of agencies and departments in Japan and bureaucratic barriers that existed. Many agencies work separately and at times actually compete with each other. Compartmentalised bureaucracy or *Tatewari* as it is known, hindered co-operation and directly hindered the response to the attacks. This had also been evident following the Kobe Hanshin earthquake in 1995 (Asukai, 2000 in Pangi 2002:14), yet no immediate steps had been taken to remedy this.

In the Tokyo instance, it was station attendants who were the first to notice that something was seriously wrong, yet drivers were unaware of what was happening. As is often the case, the first first responders were civilians as was also recognised in the 9/11 aftermath discussed at 5.8.1 of this thesis, hence any training plans must account for this and include them. Still the focus was on ensuring the punctuality of the train system as attendants cleared passengers, removed the packets and mopped the floors. The problem was not fully realised until hundreds of passengers had left the subways and moved above ground (Jenkins and Gersten, 2001:62). In light of this, gas masks and procedures should also have been available to these staff as Jenkins and Gersten (2001:63) again note. It is not clear what was reported or when, nor how the subway operating authority compiled and interpreted the reports. It was unlikely that had the station attendants accurately and rapidly reported the incident, much time would have been saved in the response; time would have still been necessary to determine that a major co-ordinated attack was underway and by then, it may still have been too late and casualties are unlikely to have been significantly reduced. However, delays of twenty minutes and more than one hour in one case must still be questioned (Jenkins and Gersten, 2001:62). Time is critical in responding to a dangerous event to prevent it from escalating further, as explored at 2.4.1.

The authorities acknowledged that response staff needed WMD-specific training and in addition it was agreed that the SDF would supply information to the police and the media regarding chemical agents. They also provided training for the emergency services on how to deal with such an attack. Volunteers were similarly trained to respond to such events.

In the longer term, emergency planning was addressed by the Tokyo Municipal Fire Department in conjunction with Tokyo University. Training simulations were also utilised to supplement the revised procedures. In September 2000, some five years after the incident, Tokyo witnessed its first large-scale, multi agency simulation (Pangi, 2002:16). However, although it was felt that working relationships were improved as a result, regular collaboration did not transpire as standard practice amongst agencies (Iwaki, 2000 in Pangi 2002:16). There may be several reasons for this: perhaps senior managers were not fully supportive of simulations or perhaps the cultural issues already identified here hindered practice and this was not recognised. Some of the techniques highlighted at 2.8 of this thesis are argued to help to overcome such concerns.

4.7.2 Dangerous Event Management and Improvements

Despite some good actions in response to the attacks, there were still substantial planning, logistical and operational difficulties that contributed to the overall delay (Pangi, 2002:16). Two issues were identified: the first was that an incident management system (IMS) was not properly established due to the delay in recognising the severity and magnitude of the problem. IMS are crucial in the management of a dangerous event and comprise the emergency management teams that co-ordinate response efforts (Pangi, 2002:16). The second barrier related again to the structure of inter-agency relationships. Most acted independently without effectively communicating with other agencies (Pangi, 2002:17). This can also be seen in the 9/11 response at 5.5.8.

It appears that it took a long time for the train to stop after the gas had been released. However, it should be remembered that it would have taken a few moments for the effect of the vapour to be felt and perhaps a few more minutes for the train to reach the next station and affected commuters to begin disembarking. The train would be on its way to the next station before this was noticed and it may take several more stops before it was realised that the train was the transporter of the chemical. It is this that Jenkins and Gersten (2001:61) regard as a key issue, as prevention is not feasible for the subways and response to such an event is the responsibility of the emergency services. The transportation companies therefore need to consider what their response should be in the

narrow timeframe between the occurrence of the event and the response of the authorities. It is this question that will be revisited later in the context of the thesis as a whole. In the context of transportation companies, it is likely to encompass the question whether all or part of the transportation system should be shut down or evacuated. The focus is often to keep the system going and minimise disruption but if it must be shut down, all efforts are made to restore service as quickly as possible. This highlights the need for dependable detection and identification technology but it appears that this may still be some way off.

The government in Japan has definitely changed the way that authorities think about terrorism. It is now viewed in a wider context and formal, overarching response plans have now been developed in case of any future attacks. At the national level, interagency co-operation was specifically targeted and steps were taken to ensure that the divides between agencies were addressed including, importantly, clarification of the information alliances and formation of a chain of communication up to the Prime Minister. The post of Deputy Chief Cabinet Secretary was created to make decisions on initial government response to emergencies and to co-ordinate the measures taken by the different agencies. The post was supported by the newly created Office for Crisis Management (Pangi, 2002:20). A Council against Nuclear, Biological and Chemical (NBC) Terrorism was also created and meetings of the council were intended to facilitate discussions amongst national agencies who responded to terrorism.

What may still encumber any changes is the cautionary nature of the political system in Japan and the highly bureaucratic nature of this. In a crisis, where speed is of the essence, this can be hugely challenging. The top down structure of the agencies in disaster response also raises concerns as first responders are invariably at a much lower level, often local government, which may cause complications and delays in disaster management (Pangi, 2002:21). Lastly, the response plans are designed for national agencies whilst at the local level, response plans are far more generalised, although there is a general shift towards encouraging local authorities to emulate national models (Pangi, 2002:21).

4.7.3 Incident Communication and Corrective Actions

Proactive communications can expedite response and recovery actions. This is not just in terms of inter-agency communications but also those with the general public and the media. Panic can be avoided through concise, clear information transmission which can also prevent the situation from escalating. Similarly, it can ensure that the public trust the information that they are hearing and act in accordance with it. Those selected to deliver such information should also be chosen carefully to avoid the problems that arose after the 7th July bombings following broadcasts by Sir Ian Blair and then by lower ranking individuals, as considered at 6.10 of this thesis.

In the Sarin attacks, communications were hindered through both technical and cultural barriers; system overloads resulted due to the volume of information and patients suffered as emergency medical technicians lost contact with the ambulance control centre. Such overloads also occurred during 9/11 and 7/7 (see 5.5.2, 6.8.2 and 6.8.3), and are arguably a worrying trend as these were between six and ten years later. Such recurrence further validates this research. Information sharing was inadequate between agencies as was seen in the delay in hospitals receiving confirmation from the police that Sarin was the source of the problem (Pangi, 2002:22). Again, this problem was also seen in the 9/11 attacks, highlighted at 5.5.2, and 5.5.5 of this thesis and in the 7/7 response as referred to as 6.8.2 and 6.8.3.This strengthens the argument of this thesis that reflecting on previous incidents is invaluable and lessons are still a long way off from being learned. International communications with other countries that had reasons to be concerned were almost non-existent, fuelling panic around the world. Jenkins and Gersten (2001) also highlight broad communication issues in the aftermath of the Sarin attack, reiterating Pangi's conclusions.

The end result of this lack of information sharing, both internally and externally, was heightened unease and an obsession with Aum Shinrikyo (Pangi, 2002:24). Immediate, near term and long term responses were all adversely affected by this. At the time of the attack, no special alert had been issued despite the previous attempts at Yokohama and Kasumigaseki. The Matsumoto attack was also ignored. Jenkins and Gersten (2001:61)

suggest that had an alert status existed, a more rapid response could have been facilitated. As suggested earlier, this improved communication regarding the situation may also have helped to reassure and placate the public too.

Since 1995, steps have been taken to address identified deficiencies in the communications structure. Video and satellite communications systems have been introduced as have new reporting systems. In terms of cultural and bureaucratic communications barriers, these are being addressed although a professional reluctance to share information still exists to some extent. Gradually however, officials are recognising that they must share information in a timely fashion when dealing with a major incident (Pangi, 2002:25).

4.7.4 Personal Protection and Decontamination

As Pangi (2002) stressed, the above are vital issues to consider. Following the attacks, secondary contamination was a problem for rescue workers who became ill following exposure to the victims. Once hospital staff realised that a nerve gas had been used, patients were made to change their clothes and shower, yet this took time. The SDF who had the capability to decontaminate areas and offer advice did not assist hospitals at all (Pangi, 2002:28).Such lack of co-ordination was also visible following the 9/11 attacks where a lack of communication and co-ordination between responding agencies frustrated any attempt to establish a unified command and also hindered rescue efforts: points that are discussed at 5.8.9 of this thesis. Again, Jenkins and Gersten (2001) also recognise some of these issues, reflected in points 15, 16, 17 and 19 of Appendix VI.

Following the attack, protective and decontamination equipment was purchased by the Japanese government and a United States Marine Corps was seconded to provide specialist training. Yet this was initially only for the benefit of police officers, not civilians. Some national agencies and several local police departments also had decontamination equipment but this may not have been effectively deployed due to bureaucratic barriers or lack of detail regarding agencies' responsibilities (Pangi, 2002:28). It is interesting to note here that lack of response by some agencies was as

problematic as over response in such events, as was seen in 9/11, at 5.5.2, where off-duty personnel responded to the attack and sadly complicated its management but with the best of intentions. Such extremes highlight the importance of a reasoned, rehearsed response to such incidents to endure the best response. Hospitals also had to purchase any additional personal protection units above those provided. As this would have had to come out of their budgets, this may have dissuaded them from acquiring these due to financial constraints. However, the Sarin attacks have increased appreciation of the importance of pre-hospital and hospital decontamination facilities as Jagninas and Erdman (2004) in Beaton et al (2005:107) stress.

4.7.5 Medical Surge Capacity and Psychological Support

This has been defined as the ability of the health care system to cope with an influx of patients that exceed the normal patient load (Pangi, 2002:29). This capacity also needs to consider those with mental health needs following a terrorist attack (Beaton et al, 2005:106). The notion of "flex" is also paramount, that is the creation of availability of beds and care within secure healthcare facilities. Following the Sarin attacks, the system flexed at the wrong time and in the wrong direction, as key personnel were unavailable as they had been sent to the incident scene (Pangi, 2002:29). It transpired that part of the reason for the hospitals becoming overwhelmed was a category of patients classified as the 'worried well'. This class of patient is one of the most challenging and seek treatment due to fear or concern. Difficulties arise as they consume scarce resources and may block access for badly injured victims (Evans, Crutcher, Shadel et al, 2002 in Beaton et al, 2005:108). These patients still require evaluation, guidance and a plan of action however, so should not be ignored.

In July 1995 the Tokyo National Disaster Centre was established and became the first disaster oriented hospital in Japan. In times of non-disaster, the hospital was to take on an educational role, so would never be an idle resource. In addition, existing hospitals made plans to enable better response to mass casualty scenarios.

Very little provision was made for early intervention by mental health specialists subsequent to the attack; this was somewhat unfortunate as earlier treatment or counselling may have enabled speedier and more complete recovery for the victims. Japan has since adopted a thorough training programme for emergency responders to recognise and treat the symptoms of Post Traumatic Stress Disorder to help avoid such delays in the future (Pangi, 2002:38).

Japan had already begun to revise its disaster management plans in response to several natural disasters that ranged from typhoons to earthquakes, prior to the 1995 attacks (Pangi, 2002:38). Japan's experience highlighted the need for relationships between different agencies to be built and maintained, the telecommunications infrastructure to be able to cope with the demands that may be placed on it in times of crisis, and that psychological care provision as well as general medical care provision must be adequate.

4.7.6 Security and Training Infrastructure Improvements

At the time of the attack CCTV was very limited on the subway system both on the trains and at the stations. This meant that it took much longer and was far harder to ascertain what was happening at the time of the attack and also to identify the perpetrators. Staff on the transport system had little training that was beneficial to them during the attack and hospital staff also lacked training to recognise the symptoms of a nerve gas attack. Jenkins and Gersten's (2001) points 5, 6, 7, 8, 9 and 14 at Appendix VI highlight some of their key observations in relation to these points, which are useful for organisations to consider.

CCTV was increased in the wake of the attacks and alarms were fitted in public restrooms to further a rapid response. Again, this needs to be part of a wider provision and must be fully integrated into response procedures. Reports from personnel should also be formally integrated. Jenkins and Gersten (2001:63) further suggest that operator responsibility encompasses planning for the possibility that a temporary shutdown may be the best option in some circumstances; this needs to be part of a plan that is not dependent on orders from public authorities. Surveillance cameras that covered the entire

network could also have been beneficial as they might have helped to determine what was occurring more quickly. Arguably there is still some doubt whether this would be of sizeable benefit as part of remote diagnosis due to the number of commuters using the subway system and the associated problems with visibility, discussed earlier.

The benefit of increased staff training has already been mentioned in connection with station attendants but hospital staff would also have benefited from training that would help them to recognise the symptoms of a nerve gas attack more rapidly; emergency crews were mystified by the symptoms for up to two hours (Jenkins and Gersten, 2001:63) and this could result in fatalities if the correct treatment is not applied within the appropriate time.

Questions were raised surrounding the provision of security measures. It is possible that an increased police presence may have acted as a deterrent but it is obvious that the cult members were more than determined so this may not have had much of an effect. Similarly, passenger screening was impossible given that six million commuters used the subway and the increased measures that were used following that day still did not prevent further attacks.

4.8 In Conclusion

In less than four months, Japan had suffered seven serious attacks and as a consequence, its citizens were very concerned about what they had been facing. Added to this, many hoax threats were also made at this time, further heightening the sense of panic amongst communities. However, for Tokyo's six million commuters alternatives to trains and subways were limited so a decline in train use was short-lived.

As time went on, fear gave way to impatience with the Japanese authorities, something that was almost unheard of in a country where individual rights were deeply respected and religious diversity was especially tolerated (Jenkins and Gersten, 2001:60). The authorities focussed on dismantling the cult, not pretending that the vast public

transportation system could realistically be protected. Many outside Japan agreed that the authorities were correct in this but that it was necessary to prove definitively that Aum Shinrikyo was responsible, which took time. In hindsight better communication with the public at this time might have helped to lessen such feelings of impatience.

The Aum Shinrikyo attack stands out as previous attacks on surface transportation had not sought to take lives as a primary objective. Some countries have learned from the attack and sought to replicate such events in training scenarios to improve their response. Others have viewed such events as that of extremists and therefore not readily replicable and it is suggested that this denial and short-term outlook may seriously jeopardise any future responses to such events. Of course, the structure of the authorities will also influence responses to events and this should be explicitly considered when creating any type of contingency plan. Regardless of preparations however, this type of terrorism can never be completely eliminated.

The Sarin attacks were aimed solely at Japan however they resounded around the world and in response, governments sought to increase resources to improve their resilience to such an attack. The Aum Shinrikyo attacks changed the global view of terrorism as countries realised that a technological threshold had been crossed and raised the spectre of more lethal attacks using chemical or biological weapons (Guelke, 2009:xii).

Any attack involving WMD however does require specialist focus as this does differentiate it from a natural or manmade disaster, therefore this does need to be taken into account, such as the effects of primary and secondary contamination. Medical surge capacity as previously discussed is also vital. In this type of attack, mass panic and psychological trauma may be more likely therefore preparedness for this will assume that an appropriate response is exercised.

The next chapter will analyse the response to the 9/11 attacks in New York, 2001 in order to build on the knowledge gained here, to inform the recommendations of this thesis.

5. 9/11: The World Trade Center Attack, New York, 2001

5.1 Introduction

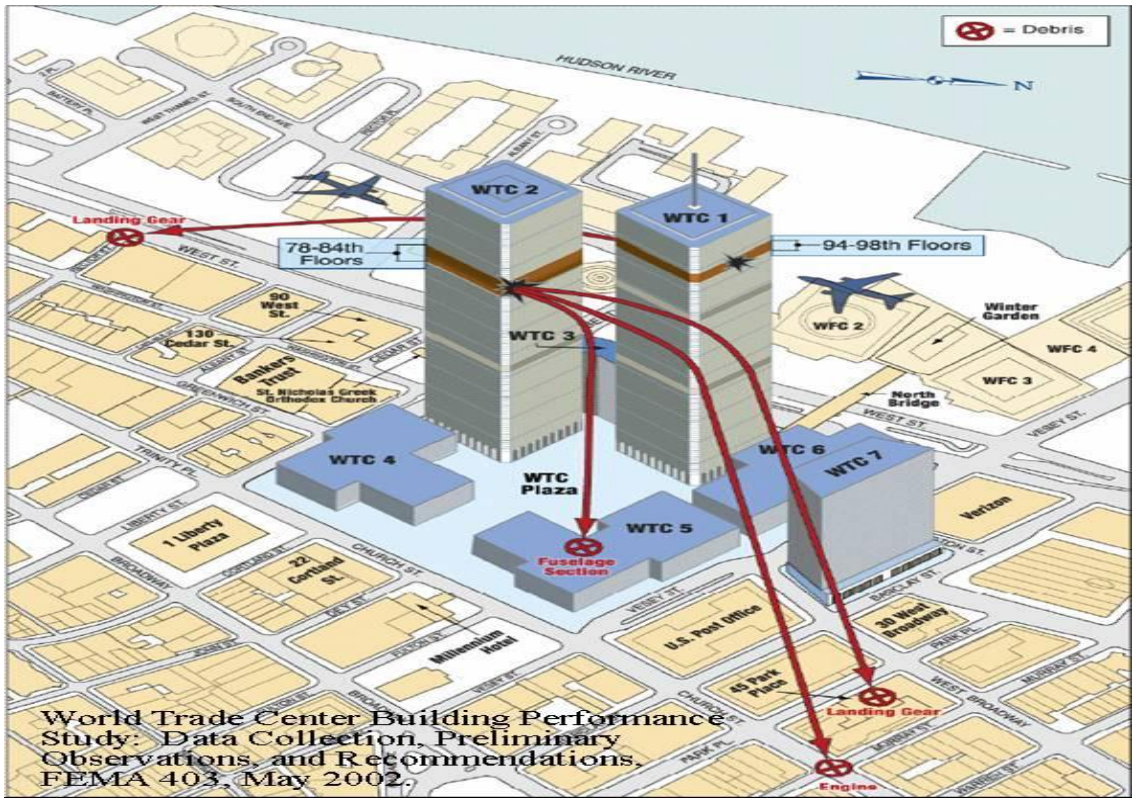
The World Trade Center and Pentagon attacks in the United States of America (USA) on September 11th 2001 and the foiled attempt in Pennsylvania, could reasonably be argued to have changed the global perspective on terrorism. The use of passenger aircraft as weapons was a new development in the terrorist arsenal that had not been foreseen and so began the 'War on Terror' in response to these events. 9/11, as it became known, heralded a paradigm shift in terrorism: in its methods and in response to terrorist attacks, and as such, the world changed forever; the international consequences were clear. In just one day, more than 3,000 people died and this, coupled with the audacity of the attack, provided the major impetus for the new focus on international terrorism.

The 9/11 attack stands out, as Guelke (2009:viii) concurs, as the most lethal act of terrorism in modern times. It is because of this that 9/11 is central to any discussion on terrorism and why it is important to include this case study within the thesis. This chapter will now consider the World Trade Center attack, its infrastructure and preparedness prior to the event and will then move on to explore the attack and the subsequent response. It is intended that the lessons learned here could be used by other organisations to help improve their preparedness and hence their emergency response, building on the lessons learned from the literature reviews and the Sarin attack response.

5.2 The World Trade Center Infrastructure and Preparedness

The World Trade Centre (WTC) was a sixteen acre site situated in downtown Manhattan, New York City. The Port Authority of New York and New Jersey owned and operated the Center and it was developed in order to operate as a headquarters for international trade within the combined port area. Seven buildings comprised the Center of which five were office buildings, one was a United States Custom House and the seventh was the twenty-two storey Marriott Hotel. In addition to these buildings, immediately below the five acre landscaped plaza around which all of the buildings were located, was a large

shopping mall which connected all seven building known as ‘the concourse’. Subway stations for each of the city’s three subway systems were also located below the tower in the mall.



At the time, the two towers, numbers One (North) and Two (South) WTC, were the fifth and sixth tallest buildings in the world, at 110 storeys each. Around fifty thousand people worked in the Center and nearly four times that number would visit the site on business or leisure every day. The numbers involved in the construction were equally large with 200,000 tonnes of steel, 600,000 square feet of glass and 425,000 cubic yards of concrete used to build the Center. Ninety-nine elevators were needed and five levels of parking were provided beneath the towers. The elevators however did not travel all the way to the top as so called ‘sky lobbies’ were built on floors 44 and 78 in each tower; essentially each tower was three buildings on top of each other (Global Security, 2001). Additional elevators carried passengers to the top of the buildings from these.

Each building contained three central stairwells. Stairwells A and C ran from the 110th floor to the raised mezzanine level of the lobby. Stairwell B ran from the 107th floor to level B6, six floors below ground and was accessible from the West Street lobby level which was one floor below the mezzanine. Each hallway contained smoke doors to prevent smoke from rising from lower to upper areas and these were closed but not locked, neither were doors from tenant space to the stairwells and it was generally possible to gain re-entry from the stairwells on at least every fourth floor (9/11 Commission Report, 2004:279). Doors leading to the roof were locked which tenants were not aware of and significantly, there was no rooftop evacuation plan, which the Port Authority admitted. Both North and South Tower roofs were sloped and obstructed with radiation hazards, making them impractical for helicopter landings or for civilians to gather. These are critical points that will be referred to again later in the chapter. The South Tower did have a helipad but it did not meet 1994 Federal Aviation Administration (FAA) guidelines (9/11 Commission Report, 2004:279). It is perhaps then not surprising that the number of casualties were so high and the extent of the damage so severe given the scale and nature of the complex.

Although this chapter focuses on the attack in 2001, this was not the first time that the WTC had been a terrorist target. In February 1993, a truck bomb was detonated, killing six people. Businesses were displaced for six months following the explosion which had been the work of six Islamic militants who were tried and sentenced to life imprisonment. It was alleged that the reason for the attack was to try to intimidate the USA into reducing its support for Israel in the Middle East and to stay out of the politics of the region. It is however important to include this as it had provided some experience for response crews and had also helped to refine and develop preparedness for any future events. Furthermore, it would appear that due to some of the actions taken in response to the 1993 attack, such as the highly dangerous helicopter rappel evacuation, some were under the impression that these were part of the WTC evacuation plan which was not the case (9/11 Commission Report, 2004:280). This may have had an impact on tenant behaviour following the 9/11 attack.

To address the problems highlighted by the 1993 attack, the Port Authority spent an initial $100 million to make improvements to the WTC, improve its fire safety plan and reorganise fire safety and security staff. The dedicated position of Fire Safety Director was created who would be responsible for the Deputy Fire Safety Directors, one of whom would be on duty at the fire command station in the lobby of each Tower at all times. The Deputy would have responsibility for communicating with tenants during an emergency and for conducting fire drills at least bi-annually. Fire safety teams were also created comprising a fire warden, deputy and searchers selected from employees on each floor. Following the 9/11 Commission investigation into the attack it would appear that some tenants felt that their evacuation on September 11th was greatly aided by changes implemented by the Port Authority (9/11 Commission Report, 2004:281). The benefit of reflecting on past experience and learning from the 1993 evacuation of the WTC was clearly beneficial. However, not all tenants received equal training and fire drills tended to involve tenants moving to the centre of their floors where they would use the emergency intercom phone to be told how to proceed. Neither full nor partial evacuation drills were held, rather participants were told generally never to evacuate upwards and that they would normally be instructed to evacuate to at least three floors below the fire. It was disappointing that the lessons were not applied equally to all tenants. Such piecemeal application of lessons learned vastly dilutes the benefits of the hard work and resources committed to learning and applying those changes. Although evacuation drills were practised, still some tenants knew less than others about the correct procedure, as did some of the telephone operators. Such disparities beg the question whether training was communicated well enough and whether full debriefing occurred. The Port Authority acknowledged that no protocol existed for rescuing people trapped above a fire; something which was of significance on 9/11.

Six weeks prior to the 2001 attack, Silverstein Properties took control of the WTC from the Port Authority following transfer by net lease. Some Port Authority staff remained on site to ease the transition but were no longer part of the official chain of command. Despite this, most Port Authority staff reported to the WTC to assist following the attack.

The WTC fire safety plan remained essentially the same following the transfer to Silverstein Properties.

5.3 Preparedness of First Responders

The following information is based on that within the 9/11 Commission Report. The principal responders on 9/11 were the Fire Department of New York (FDNY), the New York Police Department (NYPD), the Port Authority Police Department (PAPD) and the Mayor's Office of Emergency Management (OEM). Information from other sources is credited accordingly.

5.3.1 The Fire Department of New York (FDNY)

Unlike the Police Department, the Fire Commissioner did not have operational authority; the Chief of Department instead headed operations. In total FDNY had 205 engine companies and 133 ladder companies who were divided amongst battalions within nine geographic divisions. Each division comprised four to seven battalions which typically contained three or four engine companies and two to four ladder companies. The latter focussed on conducting rescues whilst the former's primary function was to extinguish fires (9/11 Commission Report, 2004:282). The Specialized Operations Command (SOC) had a key role in any major incident through specialised and highly risky rescue operations. Fire Dispatch Operations Division directed logistics and all emergency calls were routed through them.

On 9/11, FDNY personnel used analogue, point-to-point radios. Usually, companies would operate on the same channel which chiefs would monitor and in addition would have a separate command channel. The radios had very weak signal strength and so could only be heard by other FDNY personnel in the immediate vicinity. This problem was first noticed in the 1993 WTC attack so the Port Authority installed a repeater system in 1994 to enhance FDNY radio communications within the complex. However, the Port Authority asked that the system only be turned on when needed as it could cause interference for FDNY personnel in Lower Manhattan. Originally the system was

installed in 5 WTC to be activated by PAPD when FDNY units so requested. In 2000 this was changed so that an activation console was placed in the lobby fire safety desk of each tower, handing responsibility for its activation the sole responsibility of FDNY, at their request (9/11 Commission Report, 2004:283). Such response to lessons learned is to be commended as a good example of isomorphic learning, discussed at 2.3.4.2, supporting the premise of this thesis that the theory of risk and crisis management has much practical value. Such lessons were not learned following the Kings Cross underground fire in 1987 (Borodzicz, 1997:108) despite recommendations as was seen in the aftermath of 7/7 and the communications problems that ensued, discussed at chapter six of this thesis.

5.3.2 The New York Police Department (NYPD)

The Police Commissioner holds operational authority for the 40,000 officer department but his or her duties are not primarily operational. The Chief of Department largely ran the operational activities. Special Operations Division would be called upon in the event of a major incident as it included the Aviation Unit which provided helicopters for rescues and surveys and the Emergency Service Unit (ESU) which carried out specialist rescues. The NYPD did have specific and detailed standard operating procedures (SOPs) for incidents, depending on their scale (9/11 Commission Report, 2004:282).

NYPD radios were not subject to the same difficulties as the FDNY as each radio had at least 20 channels that could be used outside an officer's precinct. ESU teams also had these channels but during an incident would use a separate point-to-point channel that was not monitored by a dispatcher. In addition, the NYPD was responsible for supervising the city's 911 emergency call system through its 1,200 civilian operators. When a 911 call concerned a fire, it was transferred to FDNY dispatch.

5.3.3 The Port Authority Police Department (PAPD)

The PAPD was led by a Superintendent and there was a separate PAPD command for each of the Port's nine facilities, including the WTC. At the time of the attack the department comprised 1,331 officers trained in law enforcement and fire suppression.

The PAPD radio system comprised ultra high frequency radios that were capable of using multiple channels, however most officers used a single channel. The local channels only worked within the immediate vicinity of that command and the PAPD also had an agency wide channel but not all commands could access it (9/11 Commission Report, 2004:281). Such communication problems are not uncommon when other major incidents are considered. As will be seen at 6.8.3 and 6.8.4, such issues were also obvious during the aftermath of 7/7. Such occurrence of the same issues highlights the relevance of systems theory (reviewed at 2.3.3) and how despite external differences, there are many internal similarities validating the recommendations of this thesis regarding the value of risk and crisis management theory to the management of dangerous events.

At the time of the attack, the Port Authority lacked any SOPs to establish how officers from multiple commands would be staged and would respond to a major incident at the WTC. In particular, there were no SOPs governing how different commands should communicate via radio during a major incident, which could result in an emergency escalating due to confusion and lack of shared information as highlighted by Turner's model at 2.3.4.1. Such an oversight is surprising given the location of their responsibilities and the probably nature of any incidents that may occur. This is another factor that would be of significant importance following the attacks.

5.3.4 Office of Emergency Management and Interagency Preparedness (OEM)

Mayor Guiliani established the Mayor's Office of Emergency Management in 1996. The Office had three basic functions: to improve New York City's response to major incidents by planning and conducting training exercises with multiple agencies; to monitor the city's key communication channels and to play a central role in managing the overall response to a major incident (9/11 Commission Report, 2004:283).

If the OEM's Emergency Operations Center was called upon, the Mayor, their senior staff and designated liaisons with relevant agencies would be activated. A field responder would ensure that these were co-ordinated. Despite this good planning, there were several oversights in the location of offices and the backup for these. OEM's headquarters were

based on the 23rd floor of 7 WTC which, in case of an issue with the elevators, would make access very difficult. In addition, there was no backup of this site; something which seems incredulous given the seemingly good planning for the management of other major incidents. As a result, the centre had to move further north after the chosen location became unsafe. The location of command centres is another issue that is problematic and makes management of the aftermath of an incident harder. Following 7/7, similar problems were observed when Gold Command chose to move from its original location to one at Hendon that had been used for emergency planning exercises. However, consideration of transport problems following the incident was lacking as travelling to all the control rooms for the emergency services was far harder as these were all located in central London (discussed at 6.8.1). Such decisions are clearly questionable.

In July 2001, Mayor Guiliani updated a directive to eliminate potential conflict among responding agencies where overlapping responsibilities and expertise existed. This sought to achieve its aims through designation of an appropriate Incident Commander for different incidents and OEM continued to act as an interagency co-ordinator. In spite of this, the FDNY and NYPD still viewed themselves as autonomous in terms of operations. It is suggested that on 9/11, they were not prepared to comprehensively co-ordinate their efforts in response to the incident. The OEM had clearly not overcome the problem (9/11 Commission Report, 2004:285).

Such inter-agency rivalry is not uncommon it would seem: such reluctance to co-operate was visible in the Sarin attack although this may have been due more to bureaucracy, as discussed at 4.5 and at other times following 9/11, as discussed throughout this chapter. Such frequency of occurrence suggests that this should be an area for further investigation as a matter of urgency.

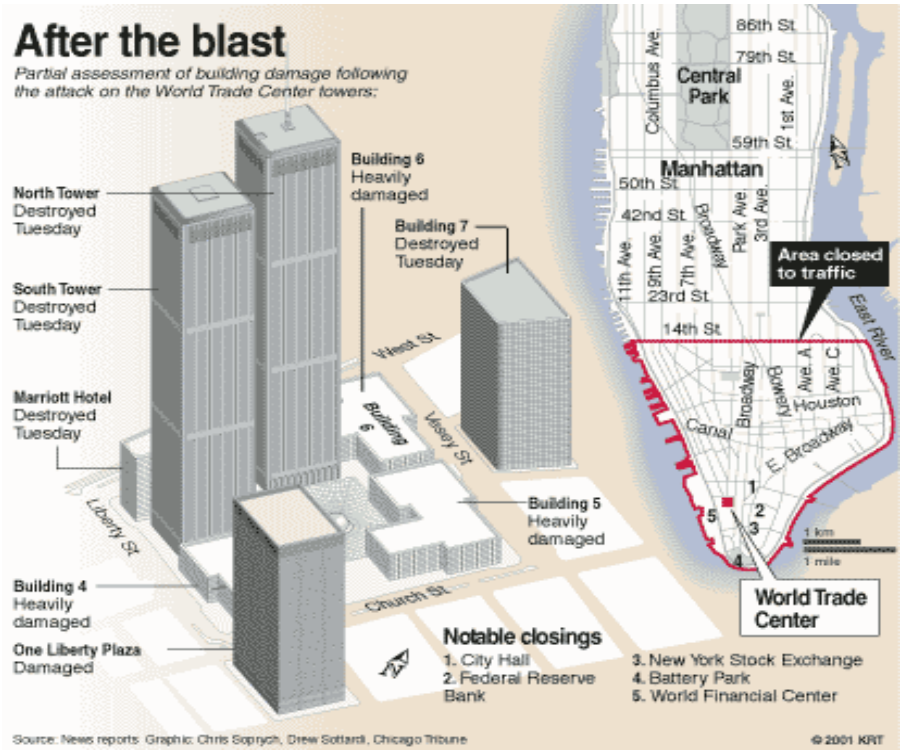
5.4 The Attack

Four aircraft were involved in the attacks on September 11th 2001. Two of those were used to attack the WTC. The sequence of events from that day transpired as follows:

- **07:59am** American Airlines Flight 11, carrying 92 people, leaves Boston's Logan International Airport for Los Angeles.
- **8:01am** United Airlines Flight 93, carrying 45 people, leaves Newark International Airport, New Jersey for San Francisco.
- **8:10am** American Airlines Flight 77, carrying 64 people, takes off from Washington's Dulles Airport for Los Angeles.
- **8:14am** United Airlines Flight 175, carrying 65 people, leaves Boston's Logan International Airport for Los Angles.
- **8:46am** American Airlines Flight 11 crashes into the North Tower of the WTC, cutting through floors 93 to 99.
- **9:03am** United Flight 175 crashes into the South Tower of the WTC.
- **9:43am** American Flight 77 crashes into the Pentagon. Trading on Wall Street is called off.
- **9:50am** Two WTC, the South Tower, collapses.
- **10:10am** United Flight 93 crashes 80 miles southeast of Pittsburgh, Pennsylvania.
- **10:29am** One WTC, the North Tower, collapses.

(Martin, 2010:11).

Although this brief chronology outlines all of the events that day, it is useful to look at the WTC attack in more detail for the purposes of this chapter. The diagram on the following page is a useful aid to comprehend the challenges and scale of that day.



5.4.1 The North Tower

When Flight 11 flew into the North Tower, it would appear that all three stairwells became impassable from the 92nd floor upwards. Hundreds died in the impact and hundreds more remained trapped but alive.

On impact, a jet fuel fireball erupted and shot down at least one bank of elevators. The fireball exploded onto numerous lower floors and created thick black smoke. The 911 system was flooded with phone calls and most correctly identified the target as the WTC.

The initial response to the attack evidently came from those in the building. Hundreds of tenants trapped on the 92nd floor or above this gathered in groups, primarily between the 103rd and 106th floors. A large group also massed on the 92nd floor and although they were technically below the level of the impact, they could not descend. People were also trapped in elevators and those on the floors in the 70s and 80s, as well as the 47th and 22nd floors were trapped or waiting for assistance (9/11 Commission Report, 2004:286).

Some confusion arose early on when the deputy fire safety director in the lobby, while immediately aware that a major incident had occurred, did not know for approximately ten minutes that an aeroplane had directly hit the building. Following accepted protocol, he initially gave announcements to those floors that had generated computerised alarms to descend to areas of safety and to wait for further instruction; this was accepted to be at least two floors below the smoke or fire. A full evacuation was ordered between one and ten minutes after the impact (9/11 Commission Report, 2004:286).

Some uncertainty about evacuation also arose due to damage to the public address system following the explosion. Many did not hear announcements as a result of this and were unable to use the emergency intercom phones. Arguably the possibility that the technology may fail should have been considered and a manual back up system should have been prepared, even if it was only some megaphones. This problem echoes the problems seen in the automated door locks in the following paragraph. Such problems are indicative of those suggested by Perrow (1984) at 2.3.4.3 and an over-reliance on technology resulting in tightly coupled systems. During such an event, communications are vital to prevent escalation as already argued at 5.3.2 and 5.3.3 of this thesis.

As a result of the emergency phone difficulties, many phoned 911 which added to the huge volume of calls already overloading the system. Transfers to the FDNY were in many cases delayed, lost or prematurely ended. Neither the FDNY dispatchers nor the 911 operators had information about the magnitude of the affected area and therefore could not even provide details as to whether callers were above or below the fire. Operators were also unaware of the impossibility of rooftop rescues so they could not knowledgeably answer when callers asked whether to go up or down. As a locum response, operators relied on SOPs for high-rise fires: stay low, remain where you are and await emergency teams' arrival (9/11 Commission Report, 2004:287). There appeared to be some reticence to advise tenants to do anything other than wait for the emergency teams and that may be due to the experience of the evacuation following the 1993 WTC attack; many of the injuries following that attack occurred during the evacuation.

However, training and plans should have instilled enough faith and knowledge that this should not be a consideration.

FDNY chiefs in the North Tower lobby quickly determined that all occupants should be evacuated immediately. By 8:57am they had instructed PAPD and building personnel to evacuate the South Tower as well due to the scale of the damage. These decisions, crucially, were not conveyed to 911 operators or FDNY dispatchers. In spite of this, several operators ignored protocol and advised callers to evacuate if they could. Those who called the Port Authority police desk at 5 WTC were also advised to evacuate if possible. Many who were not obstructed began evacuating without waiting for instruction. Again poor communications procedures hindered the management of the incident and it was common sense rather than procedures that saved some people. It was reported that some Port Authority civilian employees remained on upper floors to help those who were trapped and to assist in the evacuation. Further complications arose as some doors were jammed as a result of the impact however the evacuation was relatively orderly. Within ten minutes of the impact, huge quantities of smoke and heat were rising through the upper floors further debilitating tenants.

5.4.2 The South Tower

Many tenants in the South Tower were not immediately aware of what had occurred. Many decided to leave and others were advised to do so by Fire Wardens. Morgan Stanley, occupying more than twenty floors in the South Tower, evacuated its employees by the decision of company security officials.

Following protocol, at 8:49am, the deputy fire safety director in the South Tower told his North Tower counterpart that he would await instruction form the FDNY or others before ordering an evacuation. Crucially, at around this time, a public address announced that the building generally was safe, the incident had occurred in the North Tower and that tenants should return to their offices. This expanded advice, beyond the information that the incident had affected the North Tower, did not correspond to any known protocol or to any instruction given to the deputy fire safety director that day. As a result of this,

many tenants either remained in the building or reversed their evacuation. Security officials in the lobby who were not part of the fire safety staff also instructed tenants to return to their offices. Several tenants also called the PAPD desk in 5 WTC: some were instructed to await further instruction while others were strongly advised to leave.

At around 9:02am, a public address advised that tenants could begin an orderly evacuation if conditions warranted it. As before, this did not correspond to any established protocol. Such digression from established protocol can increase the risks associated with an incident as was witnessed here. It could be argued that had training simulations been practised more frequently and coherently, the effect of such actions could have been discovered in a safe environment and the lessons learned not to deviate from protocol that was tried and tested.

5.5 The Response

For the purposes of this case study, the response to the attack by the FDNY, NYPD, PAPD and OEM will be considered in two parts as first and second-order responses: their initial response which is crucial to the success of the rescue and management of the situation as a whole and then the subsequent response to the event following the immediate actions.

5.5.1 The FDNY Initial Response

Within five seconds of the incident the FDNY response began. At 9:00am, 235 fire-fighters were in attendance in addition to the nine Brooklyn units that were staged on the Brooklyn side of the Brooklyn-Battery Tunnel to await possible dispatch.

Senior FDNY leaders had begun responding from HQ in Brooklyn by this time. The Chief of Department and the Chief of Operations had a clear view of the WTC as they entered Manhattan. From this they determined that the mission would primarily be one of rescue and called for a fifth alarm which would bring additional engine and ladder

companies to the scene, as well as two more elite units. Twenty-two of the thirty-two senior chiefs and commissioners arrived at the WTC before 10:00am.

At approximately 8:52am a battalion chief, two engine companies and two ladder companies arrived at the North Tower. The battalion chief was initially the FDNY incident commander as the highest-ranking officer on scene. Soon afterwards the on-duty division chief for Lower Manhattan arrived and took over. The FDNY staff was advised that all 99 elevators in the North Tower were no longer operational and there were no assurances that the sprinklers or standpipes were working on the upper floors. Chiefs also spoke with PAPD and OEM representatives. One engine and one ladder company began climbing stairwell C to report back to the chiefs in the lobby. In line with FDNY protocol other units did not begin climbing immediately. Units began mobilising in the lobby awaiting the orders to go.

By 8:57am FDNY asked building personnel and PAPD to evacuate the South Tower as in their view, the impact in the North Tower had made the entire complex unsafe. At this stage the idea of a second plane hitting the complex was never considered. The FDNY chiefs were confronting critical choices with little or no information and were aware that it would be a rescue operation, not a fire-fighting operation (9/11 Commission Report, 2004:290). This is indicative of crisis and disaster scenarios, highlighted at 2.4.1 of this thesis. However, no-one anticipated a total building collapse although time is critical in such situations. The absence of any expert opinion being sought is quite concerning as it would reduce some of the unknown factors facing the EMS teams. EMS personnel were sent to one of four triage areas that had been established around the perimeter of the WTC and some entered the building to deal with specific casualties. Private hospital staff also began rushing to the WTC.

5.5.2 The FDNY Following Response

Following the impact of the second plane, the FDNY Chief of Department called a second fifth alarm. Importantly, by 9:15am far more personnel were en route or present at the scene than the commanding chiefs had requested. It is suggested that there were five

factors that account for this (9/11 Commission Report, 2004:297). Firstly, while the second fifth alarm called for 20 engine and 8 ladder companies, 23 engine and 13 ladder companies were dispatched. Secondly, several units self-dispatched. Thirdly, because the attacks came so close to the 9:00am shift change, many firefighters just going off duty were given permission to become part of the on-duty crews. Fourthly, many off-duty firefighters responded separately from on-duty units (in some cases when expressly told not to) or from home. This was particularly observed in the elite units. Fifth, numerous additional FDNY personnel who lacked a predetermined operating role also reported to the WTC, such as fire marshals.

Almost immediately following the South Tower impact, FDNY chiefs discussed strategy for the operations in both towers. Communications capability was a major area of concern following the problems highlighted after the 1993 attack. One chief recommended testing the repeater channel to see if it would work but earlier an FDNY chief had asked that the channel was activated. One button was pressed at 8:54am although it is not known by whom. This enabled communication between FDNY portable radios on this channel and furthermore, it enabled the master handset at the fire safety desk to hear communications by FDNY. However, transmission on the master handset was not possible unless a second button was pressed. This was never activated that day (9/11 Commission Report, 2004:297). As already highlighted at 5.3.1, the installation of a repeater channel was to be commended following the 1993 attack. However, human error, through not pressing the second button undid the benefits of this useful advance. This is a good example of the socio-technical accidents that Turner identified that was reviewed at 2.3.4.1 of this thesis.

As this was not activated, the chief on the master handset was unable to transmit and was seemingly unable to hear another chief who was attempting to communicate with him from a portable radio. Why this was so is unclear: it could be because the volume was turned down as was the normal setting when not in use, or, there was a technical problem. Either way, as a result, the chiefs in the North Tower lobby decided not to use the master handset as the repeater system appeared inoperable. The system was working, at least

partially, on portable FDNY radios and firefighters used repeater channel 7 in the South Tower. Again a lack of awareness regarding the actual situation was a major hindrance in trying to manage the aftermath. During the 7/7 incident, similar communications problems were seen with the British Transport Police and the problems that other emergency services were having. This is discussed further at 6.8.2 and 6.8.3.

Command and control decisions were affected by lack of knowledge as to what was occurring 30, 60, 90 and 100 floors above. One chief in the lobby admitted that the lack of information was a problem, including a lack of information from the NYPD helicopter as to what they could see. This hampered informed, critical decision making. It was even suggested by one chief that those watching events on television had more knowledge of what was happening above them than they did (9/11 Commission Report, 2004:298). This caused disagreement between chiefs as to whether those at or above the impact zone could be rescued or whether there should be limited firefighting to ease the path through fire zones. Some units were sent to assist specific groups whilst others were sent to ascend towards the impact zone and report back on their findings.

Attempts were made to monitor unit assignments on a magnetic board but the number of units and individual firefighters made this nearly impossible. As no instruction was made to the contrary, they proceeded to follow protocol and keep their radios on tactical channel 1, to be monitored by chiefs in the lobby. Those who ascended the building would work on a separate channel that would also be monitored by chiefs in the lobby. Firefighters found the stairways they entered intact, lit and clear of smoke in stairwell B. One battalion chief in the North Tower found a working elevator which he took to the 16th floor; the lobby command post was unaware of this. Yet again, a lack of communication was apparent. As they climbed, they met many tenants descending the stairwell, most of whom were calm and reassured by the firefighters' presence. At periodic intervals, firefighters would stop and check floors for tenants. Those who were left were told to evacuate immediately and give help to those who were struggling. Some firefighters became separated from their units as the climb went on due to fatigue from their heavy kit. At 9:32am a senior chief radioed all units to return to the lobby either due

to a false report of a third plane approaching or due to his judgement of the deterioration of the building. Once they realised that there was no third plane, chiefs continued operations and there is no evidence that any units returned to the lobby. At this time, a chief in the lobby was asked to consider the option of a rooftop rescue but could not reach FDNY either by dispatch or phone. The FDNY Chief of Department had however already dismissed this as impossible: yet another example of poor communications and a lack of joined-up management.

Communication became harder on tactical channel 1 because of the limited effectiveness of the radios and because so many units were trying to communicate at once; at times there was no response when trying to contact units. Exactly the same problems were seen during 7/7 when communications systems were overloaded and communications became hampered (6.8.2 and 6.8.3) and earlier at 5.3.3 with the PAPD communication problems. By 10:00am in the North Tower, one engine company had reached the 54th floor, at least two others had reached the 44th floor sky lobby and numerous units were between the 5th and 37th floors.

Following the repeater test, a senior chief and a battalion chief began operations in the South Tower and were joined quickly by an OEM field responder. Not many fire companies joined them initially as units that had been in or were en route to the North Tower were not reallocated to the South Tower. Similar confusion was evident during 7/7 when there were insufficient ambulances at Russell Square due to the confusion and proximity of the Tavistock Square incident. This is examined at 6.8.4 of this thesis. A battalion chief and a ladder company found a working ladder elevator to the 40th floor and then proceeded to climb stairwell B. Another ladder company soon arrived and began to rescue tenants trapped in an elevator between the first and second floors. The senior chief in the lobby was frustrated by the lack of units initially available to him (9/11 Commission Report, 2004:299). Contrary to the practice in the North Tower, the senior chief in the lobby and the ascending battalion chief kept their radios on repeater channel 7. For the first 15 minutes, communication worked well. It is thought that no FDNY chiefs outside the South Tower realised that the repeater channel was working and was

being used in the South Tower. The senior chief was initially unable to communicate requests for more units to the North Tower or to the outdoor command post. From around 9:21am the ascending battalion chief could not reach the South Tower lobby command post because the senior chief in the lobby had ceased to communicate on that channel. The majority of units that entered the South Tower did not use the repeater channel.

Even at 9:30am chiefs in the South Tower still needed additional companies; several reasons seemed to be responsible for this delay. Firstly, only two units initially sent to the North Tower immediately reported to the South Tower. Secondly, units were not sent until five minutes after the FDNY Chief of Department ordered the dispatch. Thirdly, those units sent to the Brooklyn-Battery Tunnel were not dispatched after the plane hit the South Tower. Fourth, units parked further north on West Street proceeded south on foot and stopped at the command post on West Street where some were told to wait. Fifth, some responded directly to the North Tower and in some cases it appears that some believed that the South Tower was 1 when it was actually 2 WTC. In addition, some could not find the staging area and lastly, due to debris and jumpers, some units attempted to gain entry via indirect ways (9/11 Commission Report, 2004:300).

More confusion was evident when a chief at the overall outdoor command post was under the impression that he was to assist with operations in the South Tower lobby however, due to his lack of familiarity with the complex, he instead ended up at the Marriott Hotel at 9:35am. On arrival, he found 14 units who had been trying to find safe access to the South Tower. He directed them to secure the elevators and conduct search and rescue operations on the upper floors. Four companies searched the spa on the hotel's top floor, the 22nd, and found no-one. Satisfied with operations there, the chief directed units to the South Tower but in fact pointed them to the North Tower. Three of the companies entered the North Tower via the Marriott and found a working elevator and took this to the 23rd floor (9/11 Commission Report, 2004:301). An additional second alarm was requested by a chief in response to the lack of units at the South Tower. Those units staged at the Brooklyn-Battery tunnel were dispatched to the South Tower; some had already responded but had gone to the Marriott. The seeming absence of maps and

general location confusion is quite hard to believe as it is so basic. However, it appears that this is not unusual during major incidents as this was also evident during 7/7 and the confusion between the Russell Square and Tavistock Square incidents discussed at 6.8.4 of this thesis.

The overall command post comprised senior chiefs, commissioners, the field communications van (Field Comm), numerous units and EMS chiefs and their personnel. Field Comm's two main functions were to relay information between the overall operations command post and FDNY dispatch and to track all units operating at the scene. Both of these functions were severely compromised by the scale of events. First of all, the means of transmitting information were unreliable and critical information was not conveyed. Secondly, their ability to keep track of which units were operating where was limited because many reported directly to the North Tower, South Tower or the Marriott. Thirdly, efforts to track units by listening to tactical 1 were severely hampered by the volume of traffic on that channel. The primary Field Comm van did have access to the NYPD's Special Operations channel, as used by NYPD Aviation, but this was in the garage for repairs and the back-up van did not have this facility. It appeared that none of the chiefs believed that a total collapse of either tower was possible. However, one senior chief was concerned that the upper floors would collapse and that firefighters should not ascend above floors in the 60s. However, this was not conveyed to chiefs in the North or South Towers (9/11 Commission Report, 2004:302). Such problems again beg the question why such things were not considered and whether simulation training was effective in its guise to that point, as it was clearly not preparing agencies for such events. The importance of appropriate back-up equipment is also highlighted here as this must be able to do the same job as the prime resource.

General authority for operations rested with the Chief of Department however tactical decisions stayed with lobby commanders. The highest ranking officer in the North Tower communicated with the Chief of Department and had two brief conversations which covered a status report confirming that this was a rescue not a firefighting operation and in the second, the Chief of Department suggested that given how the North Tower

appeared, it may be advisable to consider evacuating FDNY personnel (9/11 Commission Report, 2004:302). At 9:46am an additional fifth alarm was called and as a result 20 more than one third of all FDNY companies were now dispatched. At approximately 9:57am an EMS paramedic approached the Chief of Department to advise that an engineer in front of 7 WTC thought that the Towers were in imminent danger of total collapse (9/11 Commission Report, 2004:302). It is unclear why this expert opinion was not disseminated to others as it was clearly invaluable.

The FDNY overall command post and several other posts stopped functioning, as did the EMS staging areas following the South Tower collapse. This was due to their proximity to the building. Those in the North Tower had no way of knowing that the South Tower had collapsed unless they could see through windows facing the site. Some chiefs who took cover during the collapse were not in a position to influence FDNY operations for the next ten minutes or so. It is unclear whether the repeater channel continued to function after 9:59am.

It is thought that no-one on site received information about the South Tower collapse because every FDNY post had been abandoned, yet it was immediately communicated on the Manhattan dispatch channel by an FDNY boat on the Hudson River. Despite the lack of awareness of events, a chief in the North Tower lobby ordered an evacuation within one minute of the collapse. Another chief soon issued an additional evacuation order (9/11 Commission Report, 2004:306). However, evacuation orders did not follow protocol for when a building collapse was imminent and most evacuation orders did not mention the South Tower collapse. At least one chief gave the order on tactical channel 1 and at least 2 battalion chiefs heard this and relayed it to everyone that they met. This was another worrying display of a lack of regard for protocol as already witnessed in some of the communications.

There appeared to be four reasons why some firefighters did not receive evacuation transmissions. Firstly, some radios did not work due to problems with them and high-rise buildings. Secondly, the volume of traffic on tactical 1 may have drowned out the

transmissions. Thirdly, some firefighters in the North Tower were off-duty and did not have radios and lastly, some from the North Tower had been dispatched to the South Tower and it is likely that they were on a different tactical channel (9/11 Commission Report, 2004:307): again communications problems were at the heart of the difficulties faced by responders.

The FDNY response to evacuation orders also varied widely; some delayed or stopped their response to help those who were injured or to find missing colleagues, some units who had become separated tried to regroup and some did begin to evacuate but did not hurry. Several believed that had they known of the South Tower collapse, they would have used more urgency. When the South Tower collapsed, some firefighters searched the Port Authority Trans-Hudson (PATH) station below the concourse, unaware that the PAPD had cleared the area by 9:19am. Many chiefs, some of whom had been in the North Tower did not learn of the South Tower's collapse until 30 minutes or more after the event. Eyewitnesses claim that one senior FDNY chief who knew of the collapse strongly expressed the opinion that the South Tower would not collapse as it had not been hit on a corner (9/11 Commission Report, 2004:309). How much this affected proceedings is not known. This seems ridiculous when we know from above that the EMS paramedic had passed on intelligence from an engineer who thought that the towers would collapse.

5.5.3 The NYPD Initial Response

The initial plane strike was witnessed by numerous NYPD officers who immediately reported it to dispatchers. The NYPD Chief of Department raised the department's mobility level to 4 while en route to the scene. As a result, approximately 22 lieutenants, 100 sergeants and 800 officers from all over the city were sent to the WTC. Officers were to be stationed around the perimeter of the complex to direct the evacuations.

The Aviation Unit of the NYPD was dispatched at 8:50am to assess the feasibility of rooftop rescues and to report on conditions. En route to the WTC, the two helicopters conversed with air traffic controllers at the area's three major airports and informed them

of the situation. They had been unaware of the incident (9/11 Commission Report, 2004:291). At 8:56am an NYPD ESU asked to initiate rooftop rescues. Two minutes later they were informed that this was not possible due to flames and smoke on the roof. By 9:00am a third helicopter was responding to the WTC. Both FDNY and NYPD protocols called for FDNY personnel to be in NYPD helicopters in the event of an attempted rescue from a high-rise fire. No such personnel were placed in helicopters on the day of the attack.

Both 911 operators and FDNY were not advised that rooftop rescues were impossible and hence could not communicate this to callers. Numerous officers continued to enter the building to help with rescue efforts and around the city, the NYPD cleared major roads to ease EMS access. Both the NYPD and PAPD co-ordinated the closing of all bridges and tunnels into Manhattan to ease congestion and prevent the crisis from escalating further. By around 9:00am transit officers began shutting subway stations close to the WTC and evacuating commuters from those stations. If we are to focus on actions and knowledge here, it can be seen that the two responses are juxtaposed: NYPD and PAPD worked together well to help prevent event escalation by easing congestion whilst at the same time 911 operators and FDNY personnel were unaware of a key point that rooftop rescues were impossible. The disparity in communications is an area that must be focused on here.

5.5.4 The NYPD Following Response

Immediately after the second plane hit the WTC, the Chief of Department of the NYPD ordered a second Level 4 mobilisation, resulting in a total of nearly 2,000 NYPD officers responding to the incident. Operation Omega was mobilised, increasing protection of sensitive locations around the city and evacuating as necessary.

After the second tower was hit, the ESU officer running this command post decided to send one ESU team up each tower's stairwells whilst he continued to monitor the citywide SOD channel used by NYPD helicopters and the point-to-point tactical channel that the teams climbing the towers would use (9/11 Commission Report, 2004:302). The

first team entered the North Tower and tried to check in with FDNY chiefs but were rebuffed and OEM staff did not intervene. They began climbing and shortly afterwards a second ESU team entered the South Tower. The OEM field responder ensured that they check in with the FDNY chief, where it was agreed that they would ascend and support FDNY personnel. A third team entered the North Tower and did not check in with FDNY personnel. A fourth team entered the South Tower and a fifth team was next to 6 WTC preparing to enter the North Tower. By approximately 9:56am, the first ESU team had reached the 31st floor and noted that there appeared to be no more tenants descending. A final radio communication was received from another team in the South Tower that was ascending slowly due to the number of people trying to descend the stairwells (9/11 Commission Report, 2004:303).

In addition, three plainclothes NYPD officers without radios or protective equipment began searching for civilians, using office phones to call their superiors. One NYPD chief did instruct them to leave but they refused to do so. From 9:03am to 9:59am a group of NYPD and PAPD officers, as well as two secret service agents, continued to help civilians in the North Tower, instructing them to leave down an escalator to the concourse. Once there, another officer directed them further to avoid falling debris (9/11 Commission Report, 2004:303).

At 9:06am, the NYPD Chief of Department instructed that no units were to land on the roof of either tower. One of the helicopters confirmed that this was still the case at 9:30am. Another pilot thought that a portion of the North Tower roof may be possible to land on but did not hover directly over this area. Another pilot said that the heat was far too high to hover low enough for a rescue. At 9:51am an aviation unit warned of large pieces of debris hanging from the building. Before 9:59am no NYPD helicopter pilot predicted that either tower would collapse despite the fact that at 9:37am a caller from the 107th floor had told a 911 operator that a '90-something' floor was collapsing. This information was however inaccurately relayed to an NYPD dispatcher who was told that the 106th floor was crumbling 15 minutes after the call was placed. The NYPD dispatcher conveyed the information on the frequency used in the vicinity of the WTC and on the

Special Operations Division channel but not on the city-wide channel (9/11 Commission Report, 2004:303).

At 10:08am, a helicopter pilot from the NYPD Aviation Unit warned that he did not believe that the North Tower would last much longer as four minutes earlier it was seen to be glowing red. Immediately after the South Tower collapse, radio channels were overwhelmed in some cases but managed to remain operational enough that the two closest mobilisation units could be moved further from the WTC (9/11 Commission Report, 2004:309). The ESU teams in the North Tower also did not know that the South Tower had collapsed but by 10:00am, an ESU officer running one of the command posts ordered the evacuation of all units from the WTC as he had seen the South Tower collapse. This was reported to ESU units in the North Tower in his evacuation instruction, which was clearly heard by the two units already in the North Tower. The ESU team on the 31st floor passed this information on to the FDNY personnel also there to ensure that they knew of the evacuation order and continued to do this on the way down, although they were not always acknowledged (9/11 Commission Report, 2004:310). A firefighter did support this statement saying that he was not going to take an evacuation order 'from a cop' that morning. In contrast, another firefighter reported that ESU officers ran past without saying anything. Such rivalries are not uncommon however the fact that these were still evident during the event is disturbing as prejudices could not be put to one side at the most critical time. This was also evident earlier in this section where ESU personnel were rebuffed by FDNY staff in the North Tower. Ultimately lives were put at risk as a result of this.

Such inability to see the bigger picture of what is going on suggests that changes to training were urgently required and this should have been identified earlier.

The ESU team from the 11th floor, once near the mezzanine level, spread out in a chain formation to help civilians evacuate. Once out of the building, they remained in the area conducting additional searches but only two survived following the collapse. The ESU team that came from the South Tower remained at the North Tower until its collapse, but

all survived. The three plain-clothed NYPD officers were urged to leave by three FDNY personnel as they did not have protective equipment. They did so reluctantly, checking all floors on their way down. The FDNY refused to leave. At least one NYPD officer teamed up with a PAPD officer to act as a spotter for those civilians still exiting the building, to avoid falling debris and people (9/11 Commission Report, 2004:310).

5.5.5 The PAPD Initial Response

The on-duty PAPD sergeant at first instructed officers in the WTC command to meet at the police desk in 5 WTC. He instructed officers arriving from outside commands to meet him at the fire safety desk in the North Tower Lobby. Some were given WTC Command radios. One officer began climbing stairwell C and others began performing rescue and evacuations on the ground floors and in the Port Authority Trans-Hudson (PATH) station below the WTC complex. Within minutes of the attack PAPD officers began responding to the WTC. No SOPs existed for personnel responding from outside commands during a major incident (9/11 Commission Report, 2004:292). Officers also lacked interoperable radio frequencies hence there was no comprehensive co-ordination of the PAPD's overall response: a problem that was echoed during 7/7 as will be explored in the following chapter.

At 9:00am the PAPD commanding officer at the WTC ordered an evacuation of all civilians in the complex due to the magnitude of the damage at the North Tower. This order was given over a WTC police channel, which could not be heard by the deputy fire safety director in the South Tower. At the same time, the PAPD Superintendent and the Chief of Department arrived separately and made their way to the North Tower.

5.5.6 The PAPD Following Response

Initial responders from outside PAPD commands proceeded to the police desk in 5 WTC or to the fire safety desk in the North Tower lobby. Some were then assigned to assist in stairwell evacuations or to hurry evacuations along in the concourse, plaza or PATH station. Some were instructed to rescue those who were reported to be trapped above ground-level floors. Others began climbing to the impact zone. Others responded on their

own initiative. No predetermined command structure existed to deal with an incident of this magnitude so PAPD personnel began to formulate an on-site response plan at around 9:30am (9/11 Commission Report, 2004:305). This was further complicated by not knowing how many officers were responding and where they were operating. The value of appropriate simulation training is again highlighted here to avoid ad-hoc preparations that may not be the best way to manage the incident, as discussed at 2.8.

The South Tower collapse forced the PAPD command post on West and Vesey to move north but there is no evidence that those PAPD officers with WTC Command radios received an evacuation order over these. Some in the North Tower decided to evacuate themselves either alone or in consultation with other first responders. Some stopped in the descent to help those who were injured. When the North Tower did collapse, all those on the upper floors died but one PAPD officer, twelve firefighters and three civilians who were descending stairwell B managed to survive. The PAPD Superintendent, the FDNY Chief of Department and many senior staff were killed (9/11 Commission Report, 2004:311).

5.5.7 The OEM Initial Response

OEM officials began activating the Emergency Operations Center by calling the FDNY, NYPD, Department of Health and the Greater Hospital Association, instructing them to send designated representatives to the OEM, by 8:48am. Furthermore, the Federal Emergency Management Agency (FEMA) was asked to send at least five federal Urban Search and Rescue Teams. By around 8:50am, a senior OEM representative began to act as the OEM field responder and was soon joined by several other OEM officials including the director.

5.5.8 The OEM Following Response

Following the South Tower impact, the OEM senior leadership decided to remain in its bunker and continue operations from there despite the fact that all civilians had been evacuated from 7 WTC. At approximately 9:30am, a senior OEM official ordered the evacuation of the facility after a Secret Service agent in 7 WTC advised him that

additional commercial planes were not accounted for. Prior to this, no outside agency liaisons had reached OEM, despite the fact that OEM field responders were stationed in each towers' lobby, at the FDNY overall command post and at least for some period of time, at the NYPD command post at Church and Vessey (9/11 Commission Report, 2004:305). The location of senior leadership is vital during a dangerous event as they are central to providing continuity. The time wasted if a move is necessary can be crucial and the move itself can cause further problems as will be seen in the following chapter at 6.8.1.

Following the South Tower impact, communications, command and control became both increasingly difficult and increasingly critical. First responders assisted thousands of civilians even as incident commanders lacked knowledge of what others were doing and in some cases, what their own responders were doing. At 9:59am, the building collapsed in the space of 10 seconds, killing all those inside and many outside as it collapsed in on itself and caused a violent windstorm creating a huge cloud of debris (9/11 Commission Report, 2004:306). At 10:28am some civilians were still trapped in the North Tower and were becoming increasingly desperate.

5.6 Civilians, Fire Safety Staff and 911 Calls

Within the South Tower many had been waiting to evacuate when the plane hit, particularly on the 78th floor sky lobby. On impact there was much discrepancy in injuries: some were severely injured or killed while others were relatively unharmed. At least two small groups descended from that floor following the impact. Others stayed behind to help those who were injured. One civilian fire warden had been particularly helpful, not least because they had been provided with a torch so could negotiate a path through the dark and smoke far more easily. Something so simple can be and can make the difference between life and death; this importance was also observed following 7/7 and survivor's comments included in the Review Committee Report, discussed at 6.9 of this thesis.

Many tried to ascend the stairwells but in some cases reversed their ascent on information that some floors were in flames. In the confusion some began their descent again within which time thick, black smoke had filled the stairwells and caused many to pass out and a fire had ignited on the 82nd floor transfer hallway. At approximately 9:30am, a 'lock release' order was transmitted to the Security Command Center, on the 22nd floor of the North Tower, to unlock all areas controlled by the buildings, including doors to the roofs. Damage to the software that controlled the system, as a result of the impact, meant that this order could not be implemented. If tenants made it to the 70th floors, there was some relief due to well-lit stairwells and generally normal conditions. There is no mention of a manual override for something so important. If it was the case that this was not possible, it was a terrible oversight: one does not have to think too hard to envisage a time when software may not work correctly.

Within fifteen minutes of impact, debilitating smoke had reached the 100th floor and floors 90-100s were also severely affected within half an hour. Some of those on the 88th and 89th floors called 911 for help but the operators' lack of awareness did not help in their evacuation as callers were advised to remain where they were and await help. This information may have meant that tenants above the impact did not attempt to descend although stairwell A may have been passable. In addition, the volume of calls meant that the 911 system struggled and rigid SOPs according to which calls conveying crucial information had to wait to be transferred to either EMS or FDNY dispatch (9/11 Commission Report, 2004:295). The lack of understanding of the situation and the available information was again a key driver in some of the problems hindering evacuation.

Although evidence suggests, as mentioned earlier, that the public address system was not working, some reported hearing announcements to go downstairs and also the evacuation tones, both above and below the impact zone (9/11 Commission Report, 2004:295). By 9:35am the West Street lobby of the South Tower was overwhelmed with casualties. By 9:59am at least one person had descended from the 91st floor of the South Tower and had reported that stairwell A was virtually empty, whilst stairwell B only had a handful of

people descending. Immediately prior to the building collapsing, a team of NYPD ESU officers met a stream of people descending an unidentified stairwell in the 20th floor area. It is thought that they were descending from, at or above the impact zone.

In the North Tower, evacuations were ongoing. Although smoke, heat and fumes were an issue at some levels, from the upper 80s down, it appeared that the stairwell was relatively light and clear. Those who called 911 from below the impact were generally advised to remain in place. One group on the 83rd floor pleaded to know if the fire was above or below them or if operators had any news from outside. These callers were transferred back and forth several times and advised to stay put. Evidence suggests that these callers did not survive (9/11 Commission Report, 2004:296).

At 8:59am the PAPD desk at Newark Airport told a third party, not at the WTC, that a group of Port Authority civilian employees on the 64th floor should evacuate. At 9:10am, in response to an inquiry the employees, the PAPD desk in Jersey City confirmed that employees on the 64th floor should stay near the stairwells and await the police. When the third party enquired again at 9:31am, the police desk at Newark Airport advised that they 'absolutely' evacuate. The third party went on to inform the police desk that the employees had received previously contradictory advice from the FDNY which could only have come from 911 operators. These workers were not trapped but had chosen not to descend immediately after the plane had hit. They eventually began to descend but most of them died in the collapse of the North Tower. All those who reached the concourse were directed out of the complex to the North and East to avoid being struck by debris. By 9:59am, many tenants were still in stairwell C.

5.7 After 10:28am

Following the collapse of the North Tower, Mayor Guiliani, the Police and Fire Commissioners and the OEM Director moved to the Police Academy further north and set up an emergency command post there. It transpired that on that day, 2,973 fatalities occurred, the largest loss of life on American soil as the result of a hostile attack. The

FDNY lost 343 personnel, the PAPD, 37 and the NYPD, 23 (9/11 Commission Report, 2004:311).

5.8 In Review

The emergency response to the 9/11 attacks was necessarily improvised. The FDNY, NYPD, Port Authority and WTC occupants had to cope with an incident of an unimaginable magnitude that occurred and ended in around two hours. They were unprepared both in mindset and training for an event on this scale yet still the majority of those below the impact zone were able to evacuate (9/11 Commission Report, 2004:316).

5.8.1 Private Sector Challenges

The 'first' first responders, as in many incidents, were civilians. In the USA at the time of the attack, it was estimated that 85 percent of the nation's critical infrastructure was controlled by the private sector, therefore, they were likely to be the first responders in any future incidents. It is for that reason that the Commission Report assessed the readiness of the private sector to inform recommendations to address this need (9/11 Commission Report, 2004:317).

5.8.2 Lack of Protocol for Rooftop Rescues

Those caught at or above the impact zone in the North Tower had the smallest hope of survival as the stairwells were impassable through damage or conditions. The only hope would have been an air rescue but this was impossible for the following reasons: firstly, the doors to the roof were locked for security, secondly, following the impact, damage to the software in the security command station meant that a lock release order could not be effected. However, even if the doors were unlocked, structural and radiation hazards meant that it was not suitable to stage large numbers of people in that area. In addition, even if helicopter evacuations were possible in the conditions, which they were not, only a limited number of people could be taken at a time (9/11 Commission Report, 2004:317).

No evacuation plan existed at the WTC for those on upper floors, should the stairwells be impassable.

5.8.3 After the North Tower Impact

Of all the decisions made that day, the one that has attracted the most criticism is the decision of building personnel not to evacuate the South Tower immediately after the North Tower impact. The Report concluded that a firm and prompt evacuation order would likely have led many to safety and reduced the number of casualties.

The advice to stay in place was understandable in its context as no-one thought that another plane would hit the WTC and evacuating thousands of people was seen as inherently dangerous. Added to this were the hazardous conditions outside following the initial impact. However, tenants could have been held in the lobby or alternatively directed through the underground concourse. Despite the initial advice over the public address system, the FDNY and PAPD ordered evacuation within twelve minutes of the North Tower impact and it is assumed this would have proceeded had the second impact not occurred.

5.8.4 Fire Safety Plan and Fire Drills Effect on Evacuation

It appeared that after the South Tower was hit, those on the upper floors wasted time ascending instead of searching for a clear path downwards; stairwell A was initially passable. They were not informed, even in fire drills, that rooftop evacuation plans did not exist and that those doors were locked. Those who did reach the stairs to descend were confused by stairway deviations and smoke doors, slowing their descent (9/11 Commission Report, 2004:318).

5.8.5 Impact of 911 Calls on Evacuation

The order by FDNY to fully evacuate at 8:57am was not conveyed to the operators and dispatchers who, in consequence, advised tenants not to self-evacuate whether they were above or below the impact zone. They also did not know that rooftop evacuations had

been ruled out so did not convey this information to callers; this could have put tenants in danger as they were not advised that they must therefore descend, not ascend.

5.8.6 Preparedness of Individual Civilians and First Responders

The location of all stairwells should be known and they should have access at all times to torches; these were invaluable in the evacuation. Specific challenges came to light following the events of 9/11 that faced the first responders. Incident command, command and control, communications and co-ordination were all areas where particular challenges were highlighted. In order to try to learn from events and to better prepare for future incidents, it was decided that these specific issues were examined.

5.8.7 The Challenge of Incident Command

As mentioned earlier in this chapter, in July 2001, Mayor Guiliani updated the directive 'Direction and Control of Emergencies in the City of New York'. It designated appropriate agencies for different emergencies to be responsible for the City's response to the incident. In such instances where no single agency immediately stands out, the OEM would assign the role of Incident Commander to an agency as the situation demands (9/11 Commission Report, 2004:319).

On 9/11, this was followed to some degree. The lead agency was the FDNY and others acted in supporting roles. A tacit understanding existed that FDNY personnel would have primary responsibility for evacuating tenants above ground floors, while NYPD and PAPD personnel would take over once they reached the ground floor. The NYPD also helped by clearing emergency lanes to the WTC.

Co-ordination was evident at high levels of command: the Mayor and Police Commissioner consulted with the FDNY Chief of Department at 9:20am. At the operational level, information was shared on an ad-hoc basis (9/11 Commission Report, 2004:319). This has already been seen in the Sarin case study in Chapter Four.

5.8.8 Command and Control within First Responder Agencies

It is clear that for a unified incident management system to succeed, each participant must have command and control of its own units and adequate internal communications. This was not always so on 9/11, or on 7/7 as will be evident in the following chapter.

It should be remembered however that an incident of this scale had never been seen before hence experience was lacking. The FDNY, the Commission felt, were not capable as an institution, to co-ordinate the numbers of units dispatched within the 16 acre complex. This resulted in numerous units massing in the Marriott Hotel and at the overall command post whilst at the South Tower, where units were desperately needed, few were present. If better understanding of the resources available existed, more units may have been dispatched to the South Tower at 9:37am. This lack of awareness was not helped by the internal communications breakdown as a result of radio problems within the complex (9/11 Commission Report, 2004:320). In addition, when the South Tower collapsed, the overall FDNY command post stopped operating which compromised the ability to understand the situation.

Although most people were not contemplating a total collapse of the towers, many were contemplating the chance of further attacks. If this had occurred, the FDNY response would have been severely compromised due to the concentration of so many off-duty personnel, especially from elite units, at the WTC. The department has worked very hard to address these shortcomings.

The PAPD's response was also adversely affected by the lack of SOPs and radio problems. The latter was exemplified by the fact that many officers from the tunnel and airport commands could not hear instructions on the WTC command frequency. Furthermore, senior PAPD officials became directly involved with frontline rescue operations which further complicated the incident. It is not clear if the PAPD has adopted new training exercises or major incident protocols to address these issues.

The NYPD suffered comparatively less internal command and control and communication issues, not least due to their past experience of mobilising thousands of officers for public event crowd control. The lessons and experience from this could be applied and adapted to fit 9/11. Most officers were outside the towers although ESU teams were inside. The division did have strict command and control over these teams and as there were so few of them, at least in comparison with the number of FDNY units, they were all able to report to the same ESU command post. It is not clear if non-ESU NYPD officers within the towers were so well co-ordinated (9/11 Commission Report, 2004:320).

5.8.9 Lack of Co-ordination amongst First Responder Agencies

Any attempt to establish a unified command on 9/11 would have been further frustrated by the lack of communication and co-ordination among responding agencies. The FDNY was not responsible for the overall City's response as the Mayor's directive would have required had it been in place at the time of the attack. The command posts were in multiple locations and the OEM headquarters did not play an integrating role in ensuring that information was shared between the agencies, even prior to evacuation. This was also true of information that was critical to informed decision making. A prime example of this was the information that was coming from the NYPD Aviation Unit helicopter about the condition of the towers. Had the FDNY had access to this information, they would have greatly benefited (9/11 Commission Report, 2004:321). This lack of real-time information was severely detrimental to the rescue efforts.

Contrary to a widely-held misconception, no NYPD helicopter predicted the fall of either tower before the South Tower collapsed and no NYPD personnel began to evacuate the WTC complex prior to that time. In addition, the FDNY, as an agency, knew that the South Tower had collapsed as early as the NYPD as it had immediately been reported by an FDNY boat on a dispatch channel. Due to internal breakdowns within the department, this information was not conveyed to FDNY personnel on the scene.

The NYPD, FDNY and PAPD did not co-ordinate their units within the complex and as a result, many redundant searches were made for civilians. It is unclear whether fewer first responders would have been in the WTC if there had been an integrated response (9/11 Commission Report, 2004:321).

It was felt by the Commission that it was not possible to responsibly quantify the consequences of the lack of co-ordination. It was recognised however that the Incident Command System did not function to integrate awareness among agencies or to facilitate interagency response. It is imperative that this happens if a robust response is to be provided in such instances.

5.8.10 Radio Communication Challenges

The location of the NYPD ESU command post was imperative in making an urgent evacuation order possible explaining the collapse of the South Tower, as referred to previously. The FDNY would certainly have benefited from the information. The conveyance of evacuation instructions to personnel in the North Tower had varied success and it appeared that a combination of the strength of the radios, the relatively small number of personnel using them and the lack of use of the correct channel by all, affected the success of the instruction to others. The same factors also affected successful communication amongst the FDNY personnel. It is not possible to know what difference it made that units were not using the repeater channel after 10:00am. The channel was at least partially operational before the South Tower collapsed but it is not known whether it continued to be operational after 9:59am (9/11 Commission Report, 2004:322).

Even without the repeater channel, at least 24 of the 32 companies who were dispatched to and in the North Tower received the evacuation instruction, either via radio or other first responders. Despite this, many still died. As a result, it was concluded that the technical failure of the FDNY radios was a contributory factor rather than the primary cause of many of the FDNY fatalities in the North Tower. In order to address the radio difficulties, FDNY has internally developed a ‘post radio’ that can be carried to upper floors to repeat and enhance signal strength. In terms of the PAPD, they have worked

hard to integrate the radio systems of their different commands. The reason for their lack of receipt of radio communications appeared to be due to a lack of access to the radio channel on which the PAPD evacuation order was given (9/11 Commission Report, 2004:323).

5.9 In Conclusion

In May 2004, New York City adopted an emergency response plan that expressly contemplated two or more agencies jointly acting as lead agency when responding to a terrorist attack. It did not however mandate a comprehensive and unified incident command that can deploy and monitor all first responder resources from one overall command post, which could be seen to fall short of an optimal response plan. Drawing on experience from the military, it is suggested that integrated into such a co-ordinated response should be a unified field intelligence unit, which should receive and combine information from all first responders, including 911 operators (9/11 Commission Report, 2004:322).

The attack dramatically changed the way of life in the USA. The country shifted to a security mode rather than the previous law enforcement mode and many questions were asked in the immediate aftermath of the attack about the morality and constitutionality of some of the methods employed by the USA in their bid to detain those who were responsible for planning the attacks. However, although there was a massive loss of life that day, many thousands more were saved and this should not go unnoticed.

The symbolism of the attack did not go unnoticed around the world; the WTC was a symbol of global trade and prosperity and the fact that a relatively small group of terrorists had so successfully damaged a homeland target, sent shockwaves across the globe. Furthermore, the gravity of the 9/11 attack highlighted the need to prepare for the new terrorist threat and the speed with which a response may need to be invoked.

The scale and nature of the attacks should not encourage planners to think that the planning behind them was complex and required huge resources and many requirements: all that was necessary was box cutters, some flying experience and the ability to read timetables and book tickets as Borodzicz (2005:162) highlights. This stresses the importance of screening all individuals who have access to aeroplanes as this is the only real way to try to prevent such an occurrence. As Martin rightly noted (2010:454) the terrorists entered the USA solely for the purpose of committing the attacks; they were never pre-positioned as sleepers to be activated for the attack.

Looking at the events of that day, it is clear that 9/11 marked a turning point in the history of terrorism, which is why it is so vital to learn all of the lessons that we can from that day.

The following chapter will review the July 2005 bombings in London to complete the learning from arguably three of the most pivotal terrorist attacks in recent times.

6. Case Study 3 – 7/7: The London Underground and Bus Attacks, 7th July 2005

6.1 Introduction

This chapter is based upon the Review Committee Report published in 2006. The Committee was established to identify lessons to be learned from the events and aftermath of the July 7th bombings. The Committee comprised five core members who were members of the London Assembly (Review Committee Report, 2006:1). The list of members can be seen at Appendix VII.

Although the observation could be made that there is little difference between what this thesis is attempting methodologically to do, that is to reflect on accounts of the events and highlight areas for improvement, there is in fact a significant difference that arguably improves the quality of the recommendations that will be made: none of the committee or inquiry reports thoroughly considered similar events to identify areas for improvement nor did they examine risk and crisis management methodologies to better inform their analysis and decisions. Arguably this ensures a more comprehensive understanding of events and possible recourse that will be more effective. More detailed discussion of this methodology was included in Chapter Three.

The attacks in London on July 7th 2005 were the largest co-ordinated terrorist attacks to be conducted in the United Kingdom (UK). This was the first time that London's emergency plans had been comprehensively put to the test following their review after the 9/11 attacks in the USA and the first time that suicide attacks had occurred on British soil. In light of this and due to the specific demands that were placed on first responders and organisations that day, it is important to include this case study within the thesis. This case study will be treated as a secondary analysis case study, as 9/11 and the Sarin attacks were. The lessons learned from these three events will be consolidated to develop recommendations for future preparedness that will be presented in Chapter Eight.

6.2 The Attacks

The first explosion occurred at 8:50am on an eastbound Circle Line train travelling from Liverpool Street to Aldgate Station. Within one minute, a second explosion occurred on another Circle Line train travelling westbound from Edgware Road to Paddington. Approximately two minutes later a third bomb was detonated on a southbound Piccadilly Line train. At 9:47am a fourth bomb was detonated, this time on a Number 30 bus in Tavistock Square. Fifty-two people died in the attacks and seven hundred were physically injured. Many more were traumatised by the incidents (Review Committee Report, 2006:12).

Immediately after the explosions on the underground trains the lights went out and communications between drivers and passengers and drivers and their line control centres were lost. This meant that they were unable to help transport and emergency services to establish what had happened. Between 8:50am and 9:15am there was chaos as conflicting reports were given about what had happened and exactly where. By 9:15am it was clear that there had been an explosion though the cause, severity and precise location were still unknown. For a long time it was thought that there had been five separate incidents and the emergency services were deployed accordingly. In fact, at the 11:15am press conference, Sir Ian Blair, Commissioner of the Metropolitan Police Service (MPS) was still reporting that there had been 6 explosions. At this stage, it appears that the Commissioner did not know for certain that this was a terrorist attack. However, it would seem that the emergency services on the ground realised this or strongly suspected that this was a terrorist attack. As occurred in 9/11, vital information was not being communicated across all levels of the emergency services. Why this was not conveyed is not clear and is cetainly of some concern: at 09:10am the City of London police recognised that there had been a bomb explosion. The confusion was in part due to the lack of 999 calls; usually this is what first alerts the emergency services to a major incident. However, as many of the explosions happened underground, the public were generally unaware of what had occurred (Review Committee Report, 2006:13).

It transpired that the drivers were unable to communicate with their line control managers due to the 'leaky feeder' antenna being damaged in the explosion. This was exacerbated by the antiquated radio systems that did sometimes fail anyway due to tunnel blind spots and interruptions to service (Review Committee Report, 2006:15). At Russell Square, the leaky feeder cable that enabled the British Transport Police's (BTP) radios to function was also damaged by the blast and they were therefore unable to communicate with colleagues at ground-level without making the 15 minute journey down the tunnel to the platform. A temporary cable was installed two hours later, to try to overcome this. The BTP was the only emergency service with radios that could function underground. The other emergency services either had to borrow these, or rely on individuals running back and forth from the platform to ground level (Review Committee Report, 2006:16). This was of particular concern following the King's Cross fire in 1987 when the same communication problem had been highlighted as an issue that required immediate attention (Fennell, 1988).

The fact that this appears to have been unanticipated is somewhat surprising given the anti-terrorism exercise 'Atlantic Blue' that was carried out in April 2005. The exercise was the biggest counter-terrorism exercise since 9/11 and envisaged bombs and explosives left on a London bus and the Underground. This was a transatlantic exercise involving 2,500 personnel in the UK and several thousands in the USA and Canada: communications were one of the main foci of this event (Townsend and Hinsliff, 2005). It is argued that if this had been a command post exercise (CPX) then problems such as those that occurred would have been foreseen. However this appears not to be the case as it was downgraded from a CPX to a desktop exercise instead: a press release from the Home Office stated that 'there would be no visible on the ground activity…allowing players to focus at the strategic level on communication issues across international boundaries' (Home Office Press Release, 17 March 2005). A Metropolitan Police Service publication, 'The Job', would appear to support this suggestion (Atlantic Blue Tests International Readiness, 15 April 2005). The reasons for such downgrading could have been related to the timing of the event: it coincided with the week of the General Election announcement and was just before the Prince of Wales's wedding and the Pope's funeral.

If this was to blame then the UK's part in the exercise should have been rescheduled as the utility of it was plainly reduced, roundly emphasised by the problems encountered three months later.

It is suggested that the five key elements in order to establish what had happened were:

1. the first 999 calls received by the emergency services;

2. the arrival of each emergency service on scene;

3. identification of the site of the incident and recognition that there had been an explosion;

4. communication between the emergency services about the nature and location of the incident;

5. the declaration of a major incident

(Review Committee Report, 2006:19).

Once a major incident has been declared, special arrangements within and between each service are triggered. The speed with which it was determined what had happened did appear to vary between sites but this was in part due to the location of the explosions and whether trains had entered the tunnels or not.

Having considered the overview of the events that day, the individual sites will now be considered.

6.3 Aldgate Station

The BTP received the first 999 call from a member of London Underground (LU) staff at 8:51am, reporting a loud bang and dust in the air. At the same time, the London Ambulance Service (LAS) received a call to attend Liverpool Street station. The London Fire Brigade (LFB) was called to a fire and explosion at Aldgate at 8:56am. Four units, including a Fire Rescue Unit, were deployed one minute later. The first fire engine arrived on scene at 9:00am. At this time, further units were mobilised to a reported explosion at Aldgate. At 9:02am further units were mobilised in response to reports of smoke in the tunnel. Two fire engines and a senior officer were sent to Aldgate and an additional fire engine was sent to Liverpool Street. The LFB declared a major incident at 9:05am.

The first BTP officer arrived on scene at 8:55am. He reported no structural damage but noted 'building shock' and smoke from the tunnel. Three minutes later they identified the incident site as between Aldgate and Liverpool Street but had not discovered any injured passengers at that point. Power to the track was cut off and at 9:01, BTP requested LAS to tend to 3-4 walking wounded. Six minutes later there were 25 walking wounded, some of whom were seriously injured. At 9:08am BTP at the scene reported that there had been a train accident and declared a major incident. At 9:10am the City of London Police recognised that there had been a bomb explosion and also declared a major incident. At 9:19am the BTP formally requested assistance from the MPS which is the lead police service in the event of a major incident, regardless of within which London service's jurisdiction the incident occurs (Review Committee Report, 2006:25). The MPS were already aware of the incident and the first officer arrived at 9:20am.

At 9:03am, the first ambulance arrived at Liverpool Street station followed at 9:06am by an Emergency Planning Manager. At 9:07am the LAS Emergency Planning Manager advised Central Ambulance Control to place hospitals on major incident standby, to identify safe rendezvous points in case of a chemical, biological, radiation or nuclear (CBRN) risk and mobilise equipment vehicles. The timing at this juncture is an area of concern when it is remembered that the explosion had occurred seventeen minutes earlier

and had this been a CBRN attack then everyone would already have been infected. At 9:14am (fourteen minutes after the LFB had first reported the explosion) an ambulance crew reported that there had been an explosion and that there were five fatalities. The first ambulance to arrive at Aldgate station arrived at 9:14am, 9 minutes after the LFB had reported a major incident and 13 minutes after the first request from the BTP. It appears that LAS were not aware of the Fire Brigade's assessment of the scene for 11 minutes and the BTP were still reporting a train accident at 9:08am, 8 minutes after the identification of an explosion by LFB. The Ambulance Service arrived on scene at Aldgate station 14 minutes after LFB and 23 minutes after the first 999 call was received.

6.4 Edgware Road

As at the other sites, London Underground workers were among the first responders. At 8:59am the LU Network Control Centre phoned the emergency services to request assistance at Edgware Road, Aldgate and King's Cross. It appears that the first 999 call was made by a member of the public in Praed Street who reported a fire and an explosion. At 9:00am, the LFB mobilised five units including a Fire Rescue Unit and a Fire Investigation Unit to Praed Street. The first units arrived there at 9:04am although this transpired not to be the site of the incident (Review Committee Report, 2006:29).

At 9:12am the first ambulance arrived at Edgware Road and by 9:14am the crew had reported back to the control room that there had been an explosion with up to 1,000 casualties. At 9:16am they confirmed that this is what happened and requested as many ambulances as could be mustered. At 9:32am the MPS declared a major incident.

At 9:07am Fire Control received a call alerting them to the location of the incident on the Hammersmith and City line at Edgware Road station. At 9:13am four vehicles were mobilised to Edgware Road; only one of these was redeployed from Praed Street. A member of the public established a reception area for survivors in a nearby shop. He noticed that at 9:15am two appliances were still at Praed Street whilst he could see no emergency vehicle in attendance at Edgware Road. The Fire Rescue Unit was eventually

redeployed to Edgware Road at 9:37am (Review Committee Report, 2006:30). Such location confusion has already been seen in the 9/11 response when NYFD personnel arrived at the Marriott hotel rather than the WTC tower and the confusion between the North and South Tower (5.5.2). The simple issue of familiarity with locations and correct information being conveyed to crews is plainly crucial and not something that should be assumed.

27 minutes after the explosion and 19 minutes after the Network Control Centre's first emergency call, the first fire engine arrived at Edgware Road. At 9:34am the LFB declared a major incident at the station. This was 20 minutes after the LAS had already reported to their control room that there had been an explosion with up to 1,000 casualties: it is unclear where the estimate of casualty numbers came from. It is important to focus on the time disparity between the LFB and LAS declaration of a major incident here: communications between agencies was plainly an issue, as it was in the Sarin and 9/11 incidents. However, unlike in those incidents, inter-agency communication was only a problem at the senior management level: on the ground the emergency services worked well together.

6.5 King's Cross/ Russell Square

The train between King's Cross and Russell Square was left completely isolated by the explosion. There were few 999 calls reporting the explosion as mobile phones did not work underground. Radio communication with the train had been disabled. It was impossible to communicate with anyone outside the train without leaving the carriages and walking down the tunnel to a station platform (Review Committee Report, 2006:33). The MPS was first alerted to the incident at King's Cross at 8:56am from CCTV footage of the station. The LFB received its first 999 call which reported smoke coming from a tunnel at King's Cross. At 9:04am a 'split attendance' was mobilised with three fire engines sent to Euston Square and one to King's Cross. Fire engines arrived at Euston Square at 9:07am and 9:11am however this turned out not to be one of the sites where passengers were emerging from the tunnels; again, similar confusion was evident during

9/11, discussed at 5.5.2. The first fire engine arrived at King's Cross at 9:13am. Six minutes and 23 minutes later, further fire engines were requested to King's Cross. There was no information to show that these further appliances arrived.

The first 999 LAS call reporting an incident at King's Cross was received at 9:04am. A LAS Fast Response Unit arrived there at 9:14am followed by an ambulance five minutes later. The MPS declared a major incident there at 9:15am. The LAS followed suit six minutes later (Review Committee Report, 2006:33). It is unclear when LFB became aware of the explosion at King's Cross however their ability to determine what had happened there was hampered by radio problems as these did not work effectively between the platform and a control position at the top of the escalator and outside the station. To overcome this, they used runners (running up and down escalators) to communicate from below ground to the surface. Importantly no Fire Response Unit was deployed to King's Cross in the initial stages of the response. The explosion occurred in the first carriage of the Piccadilly Line train at the Russell Square end of the train. It was via the Russell Square station that the seriously injured were brought to ground level.

At 9:18am the first 999 ambulance call was received reporting an incident at Russell Square, 25 minutes after the explosion. Passengers began appearing at the platform led by one of the two drivers. LAS despatched a Fast Response Unit at 9:24am which arrived at the station at 9:30am. LAS declared a major incident at 9:38am, 45 minutes after the explosion. At that point the Ambulance Service Professional Standards Officer at the scene was reporting 6-15 fatalities and 50+ casualties. This was 20 minutes after the BTP received reports of loss of life and limbs. The MPS treated King's Cross and Russell Square as the same incident and due to this it is not clear when they were aware of the incident at Russell Square (Review Committee Report, 2006:34). It would appear that no fire engines were sent to Russell Square at any point during the first hour following the explosions. There was no automatic deployment of the emergency services to Russell Square on discovery of the train at the King's Cross end of the tunnel; had this happened, they might have arrived at the scene earlier. The LFB did order a 'split attendance' but to Euston Square which turned out not to have been affected.

The London Underground Emergency Response Unit and the two drivers evacuated passengers from the first carriage and removed the seriously injured up to the station concourse at ground level in the absence of the LFB at Russell Square. This unit is a small, little known unit that is responsible for dealing with emergencies on and around trains; on 7th July they attended each scene (Review Committee Report, 2006:34). In the course of the review of events that day, it was discovered that these units do not have blue lights, do not have an automatic right to drive in a bus lane and also have to pay the Congestion Charge, although they are later reimbursed for this. They are now allowed to drive in bus lanes but only in emergency circumstances and they must produce a detailed audit trail to demonstrate the circumstances. As with the other emergency services, the Emergency Response Unit had no means of radio communication underground. At the time of the Review Committee Report, there were no plans to provide underground communications for them despite the fact that they work mostly on the tube network.

6.6 Tavistock Square

As this explosion occurred above ground on a bus, it was immediately apparent what had happened. It was 9:46am and the first 999 calls were made at 9:47am. 12 further 999 calls were made before 9:56am. Many medics were on the scene before this as the bus was outside the headquarters of the British Medical Association and many came out of the building to care for the injured.

It happened that the MPS had an officer already at the scene. The first ambulance arrived at 9:57am having come across the bus in passing. The first fire engines were despatched at 9:50am but it is unclear when the LFB arrived. From available records it is not clear when a major incident was declared by any of the emergency services (Review Committee Report, 2006:37).

6.7 Establishing What Had Occurred at Each Scene

It took some time to establish what had occurred at each scene below ground. At the same time, the London Underground Network Control Centre was putting together the information from the emergency services and its own monitoring equipment. On this basis, the Network Control Centre put in an emergency services call to three sites at 8:59am: Aldgate, King's Cross and Edgware Road. From the records it appears that emergency services were not immediately despatched to the scene although it is unclear why not. For some reason it would seem that the message did not get through to the right people. Yet again communications were exacerbating an already difficult situation.

Had the message got through earlier, it is doubtful whether much would have been different: the explosion had already occurred and fatalities already caused. However, there is always the question whether any casualty who was critically injured may instead have been saved. For that reason, it is important to ensure that such delays are investigated and not ignored.

In the event of a major incident, communication between the control rooms of the emergency services occurs through a 'first alert' system, through a first alert call. This is essentially a conference call between the emergency and transport services. This system was activated at 9:12am and the first conference call took place at 9:25am. At 9:15am the decision was made to declare a network emergency and evacuate the entire underground network (Review Committee Report, 2006:38).

6.8 The First Hour: Rescue and Treatment of the Injured

At any major incident, the rapid rescue and treatment of the seriously injured is the top priority for the emergency services. When there are several major incidents within a short space of time, it is vital that communications between each scene and their strategic or 'gold' commanders ensure effective deployment of appropriate and sufficient vehicles, officer and equipment to each scene and the removal of casualties to hospitals (Review Committee Report, 2006:42).

6.8.1 Strategic Co-ordination of the Response

The Gold Co-ordinating Group is responsible for the strategic co-ordination of the response. The MPS chair the group and it includes senior representatives from the other emergency services and authorities involved in the response. The Group was initially housed at New Scotland Yard but at its first meeting at 10:30am, it was decided to relocate to a suite at Hendon, which had been used for emergency preparedness exercises in the past and had good facilities. However, this caused some problems as the control rooms for all of the emergency services were in Central London, which meant that Gold commanders could not easily travel between there and their control centres. This was compounded by the suspension of the underground services and the resulting congestion on the roads (Review Committee Report, 2006:42). Although it was felt that Hendon was the correct location to use on 7th July, possible future locations were considered following the event that were more centrally located. It is unlikely that Hendon would be used if a similar event occurred.

Other Gold Command centres exist at Lambeth and Bow and it is suggested that these may be better options due to their proximity to the heart of London rather than Hendon. Bow however only became operational in late 2007 so would not have been available during 7/7 (Gumm, 2007). It is likely that Hendon was used as it was the base for the Exercise Atlantic Blue earlier in 2005 from which a similar event was simulated.

It should be recognised that the police Gold Command was already in place for the G8 summit in Gleneagles (Report of the Official Account of the Bombings, 2006:7) and this may have had an effect on how well or badly the incident was managed. It may also have had an effect on the speed of response as it was already in place. The Cabinet Office Briefing Rooms (COBR), the government's national crisis management facility that is activated in response to major incidents, was also already in place to co-ordinate any response to events in Gleneagles should they arise. COBR functioned around the clock until the 15th July (Report of the Official Account of the Bombings, 2006:7).

6.8.2 Reliance on Mobile Telephones

The difficulties caused by the incidents were compounded by significant communications problems. Managers within the LAS, City of London Police, the MPS and LFB relied to differing extents on mobile phones to communicate between sites and their Gold commanders. Following the attacks, the telephone networks experienced unprecedented volumes of traffic, even compared with that seen on a New Year's Eve.

In November 2005 emergency and transport services were asked what impact mobile telephone network congestion had on their ability to communicate. It was regarded as an inconvenience rather than a problem (Review Committee Report, 2006:43). Further questioning revealed that this did result in some serious communications problems within some of the emergency services. LFB admitted that managers relied on mobile telephones to communicate with their control room. Their debriefing report presented to the London Resilience Forum in September 2005 states that Incident Commanders were unable to contact Gold Support as mobile telephones were not working. However, the LFB's Command Planning System was used to send messages which apparently worked well. 3G telephones also worked well as did the TETRA police radio system as a back-up. The TETRA system was used by the BTP but no other emergency service on the day of the attacks. The City of London Police has since adopted a TETRA-based digital radio service (Review Committee Report, 2006:43).

The LAS also relied on mobile telephones as their primary means of communication between managers at the scene and the control room. Radios were available in their cars but these did not work on the day. The LAS Director of Operations told the Review Committee that the service had become too reliant on mobile telephones however they stated that they were then issuing pagers to managers as a back-up although they had been withdrawn two years ago as this system was virtually obsolete (Review Committee Report, 2006:44). The value of this back-up system could be argued to be questionable in light of this.

A system, Access Overload Control (ACCOLC), does exist that restricts the mobile telephone network access to the emergency services within a specific area but it is a last resort as it is expensive to invoke and can cause public distress and panic. It is initiated only by the Gold Co-ordinating Group. LAS asked the Group to activate ACCOLC as it was experiencing communication problems around Aldgate station. This was initially refused due to the risk of public panic and the fact that it was unclear whether the right personnel would be carrying ACCOLC-enabled telephones. In fact, had ACCOLC been activated key personnel who were not carrying this technology would have experienced worse problems as some calls were getting through and without telephones that were ACCOLC-enabled they would have been unable to make or receive any calls (Review Committee Report, 2006:44). This highlighted a major flaw as it could be argued what is the point in having such technology, at great cost, if the services cannot ensure that the appropriate people possess that technology?

It is unclear whether this was tested in Exercise Atlantic Blue or any other simulations in the lead up to 7/7. However, as communications were a key focus of the simulation and following the 1988 Fennel Inquiry into the Kings Cross disaster, this should certainly have been considered.

The City of London Police activated ACCOLC on the O2 network in a 1km area around Aldgate station as they were experiencing serious communication problems that hampered their response. Despite the Gold Co-ordinating Group decision, the City of London Police went ahead with the request at 12pm and remained closed until 4:45pm. O2 did carry out the necessary verification procedures established by the Cabinet Office but somewhat surprisingly these did not include verification with the Gold Co-ordinating Group (Review Committee Report, 2006:44). The Commissioner of the City of London Police defended the decision saying that it did not go against the Group's decision as he was not aware of their decision. This decision did not consider the other emergency services and the effect that this may have had on them which highlights why such decisions should be taken at strategic level with members of all the emergency services (Review Committee Report, 2006:46). Some disagreement existed between the

Commissioner of the MPS and that of the City of London Police as to whether the decision was appropriate and whether it was regretted. The Commissioner of the City of London Police stood by the decision and even suggested that the procedure for activating ACCOLC should be reviewed.

6.8.3 Communications within LAS

The London Emergency Services Liaison Panel's Emergency Procedure Manual states that the LAS is the lead organisation responsible for the emergency medical response at any major incident and with the LFB and police services, is responsible for the rescue and removal of those seriously injured. As mentioned earlier, the London Underground Emergency Response Unit also plays an important role in rescuing the injured on the underground network (Review Committee Report, 2006:48).

In addition to the mobile telephone problems, LAS also experienced problems with their radio systems and these appear to be as a result of failings in place for monitoring and managing radio traffic rather than solely technical issues (Review Committee Report, 2006:49). The LAS used both UHF radios for managers to communicate locally on scene and VHF radios for ambulances and key managers. The UHF system failed, in part, as there were not enough handsets available. The VHF radios were used to try to communicate between the scenes and the control room but these worked sporadically. Three key factors appeared to be responsible for this: firstly, two channels were used but were both initially routed through one channel which raised capacity issues. Secondly, managers at the scene did not know which channel to use as they would normally use mobile telephones. Thirdly, the volume of traffic stemming from the five separate sites meant that it was impossible to get through most of the time (Review Committee Report, 2006:50). This meant that managers and other LAS personnel were unable to communicate with the control room and their requests for further supplies did not get through. Similarly, they did not know what was happening at other incidents and could not obtain information as to which hospitals were still receiving patients.

The situation was relieved somewhat as the entire management of the London Helicopter Emergency Medical Service was at a meeting at St. Bart's and The London Hospital and several of the explosions occurred close to major hospitals from which medical staff came to help. Many senior managers were also at a conference in Millwall and were despatched for face-to-face communication. Without this, the difficulties facing LAS would have been far more prominent (Review Committee Report, 2006:50).

6.8.4 Deployment of LAS, Equipment and Supplies to the Scenes

The deployment of personnel and equipment was affected by the communications breakdown. It appears that even at 9:35am there were no ambulances at Russell Square. At all sites, LAS was experiencing a lack of essential supplies and dispersal of patients to hospitals was uneven, both due to the problems with communications. Luckily it appears that this had a minimal impact on the care of patients but had there been a far greater number of casualties then it could have had a far greater impact (Review Committee Report, 2006:51).

Aldgate was the site that was cleared the fastest, within around 1 hour and 20 minutes. At 10:09am the Emergency Planner advised the control centre to consider redeploying resources to another location as the site would soon be clear. It also had the most decisive response as it was rapid and additional units were soon requested as well as an equipment vehicle and a Medical Incident Officer. At Edgware Road, there was a less decisive response and it was not cleared until 3 hours after the explosion (Review Committee Report, 2006:51). It was not possible to examine the response over the course of the morning because accurate records were not kept. The LFB also reported a failure to accurately record information. Some survivors claimed that they saw the emergency services outside the stations soon after the explosions however they appeared to have been instructed not to enter the tunnel. Due to the lack of records, it is unclear at what time they arrived on scene in all cases.

The first ambulances arrived at King's Cross at 9:19am, 30 minutes after the explosion. Twenty minutes later the ambulance crew reported that there was still no officer at the

scene but that there were around 400 casualties and 15 ambulances were needed. The first manager arrived almost an hour after the explosion. The next communication was recorded at 10:13am when the duty officer reported that there were still 50 casualties and that more ambulances and an equipment vehicle were needed. 9 minutes later bus drivers took the initiative and took four busloads of casualties to the Royal London Hospital. They were directed here despite a call to the control centre seven minutes previously, requesting that the walking wounded be sent to St. Bart's instead. At 10:27am the 50 casualties were still trapped. The scene was eventually cleared 2 hours and 26 minutes after the explosion (Review Committee Report, 2006:52).

Russell Square was cleared almost three hours after the explosion and the response relied heavily on the voluntary assistance from the nurses and doctors from nearby hospitals. Up until approximately 11:00am there was still a shortage of ambulances and delays in deploying equipment. It appears that there were repeated requests for equipment that received no response; why this happened is unclear. The BTP reported at least 200 casualties at 9:18am and a Fast Response Unit arrived 12 minutes later. At 9:38am there was still only one ambulance and the Fast Response Unit in attendance (Review Committee Report, 2006:53).

At 10:22am an equipment vehicle was requested and 5 minutes later an estimated time of arrival (ETA) was requested for the ambulances that had been requested at 10:02am. No reply came. At 10:42am another ETA was requested. At 11:10am there were still only three ambulances on scene and a further 10 were required. At 12:12pm the scene was finally cleared (Review Committee Report, 2006:53).

This slow response was in part due to the communication problems and in part due to the close proximity of the Tavistock Square incident to Russell Square; for some time after the bus explosion, ambulances for both sites were directed to the same muster point on a nearby road. This was not realised until after 11:00am. Eventually a system of runners was established between the two scenes and ambulances were redirected to Russell Square. Since 7th July, the LAS has established new procedures which includes the

despatch of a predetermined number of ambulances to the scene even in the event of a communications failure and before they are specifically requested (Review Committee Report, 2006:53). Despite these problems, individuals working to rescue the injured managed to save many lives.

At Tavistock Square there was little information available on the response in the following hour as records were not kept. At 10:27am a shortage of fluids was reported despite the fact that eight casualties with serious amputations had been reported 22 minutes earlier. Finally at 11:31am the tactical or 'silver' officer reported that they had enough vehicles; this was the result of ambulances destined for Russell Square being directed to the same muster point as mentioned above. At 12:00pm, the LAS manager reported that the remainder of the casualties were still waiting to be taken to hospital (Review Committee Report, 2006:54).

6.8.5 Notification of Hospitals in the Vicinities

Emergency plans provide for an even distribution of casualties among accident and emergency departments at London's acute hospitals. In the event of a major incident, these hospitals are put on alert and will ready themselves to receive casualties. The NHS in London managed to clear 1,200 beds in three hours in order to receive casualties. It appears that not all hospitals in the vicinity of the incidents were notified as they were not all acute hospitals; this was despite the fact that they were in close proximity to some of the incidents, as Great Ormond Street was for example. Medical students acted as runners between this hospital and Russell Square (Review Committee Report, 2006:57). This is certainly a point that needs to be considered for future preparedness.

The presence of so many trained medics on site certainly benefited those caught in the explosions although how different the outcome would have been had they not been there is impossible to say.

6.9 The Uninjured and Walking Wounded

Survivors of the explosions spoke of the crucial importance of communication with someone in authority within the first 15 minutes after the explosion; those who did receive this spoke of the relief and reassurance that this gave. Those who did not receive this felt that they were left to speculate what may have happened and what they should do, increasing the fear and panic that they felt (Review Committee Report, 2006:60): this could then make the situation far harder to manage for the emergency services. Communication during a crisis is vital, stressing the importance of the points reaised at 2.10 and further validating the recommendations of this thesis that will be presented in Chapter Eight. For those outside the first carriage of the King's Cross/Russell Square train, help did not arrive for 25-30 minutes after the train was plunged into darkness. Those who tried to escape the train by breaking the windows discovered that they were only 10cm away from the tunnel wall so there was no way to get out. There was disbelief that loudhailers were not used to communicated from the platforms; this is certainly something that should be considered.

It appears that the internal lights went out and that the emergency lighting systems were disabled by the explosions, which is why passengers were in total darkness. As well as increasing fear, it also made the administration of first aid immediately after the blast very difficult. The lighting was only affected like this in the carriages where the bombs had detonated; Transport for London have said that in the other carriages, the emergency lighting system worked well. They are now looking into alternative forms of lighting. Survivors suggested that drivers should carry torches in their cabs (Review Committee Report, 2006:63). Such a recommendation seems quite incredible but is important to highlight as rescue workers may forget or not have such equipment in times of crisis, highlighted also in the Fennell Inquiry (Fennell, 1988:79).

The suggestion that torches should be in drivers' cabs may seem overly simple however oversights for such simple things are argued to be all too common: during 9/11 at 5.6 of this thesis, it was seen that a civilian had a torch and was able to rescue people as such equipment was not available to them within the building. Such simple things are vital in a

crisis but it is their simplicity that is their downfall: it is assumed that this has been accounted for meanwhile everyone assumes that someone else has done this and so no-one does anything. This is an important issue that will be discussed again in Chapter Eight of this thesis.

There was a lack of first aid kits on the trains and some drivers told passengers they did not have a key for the first aid box and that even if they did, they would be empty. Again this is something that is worryingly familiar as such disregard for safety was also evident 17 years previous again in the Kings Cross fire (Fennell, 1988). First aid kits are provided at every Underground station in the supervisor's office: space considerations meant that it was difficult to carry first aid provision on all trains and that if there was a problem, the train normally continued on to the next station where help would be administered (Review Committee Report, 2006:64). London Underground (LU) is carrying out an emergency equipment review covering all stations and trains to determine what changes are necessary. Mobile facilities may be considered. Evacuation instructions may also be useful, printed within carriages as they are in over-ground trains.

Passengers could not disembark even where they were clear of tunnel walls as they could not open carriage doors. Selected doors can be opened via internal and external door locks in an emergency and can be used by LU staff to facilitate a controlled train evacuation which is normally performed at the train ends and up onto the platform, onto an assisting train or along the track. If passengers tried to self evacuate from side doors they could put themselves at more risk through electrocution or the risk of being hit by an oncoming train. It is for this reason that LU has no plans to enable doors to be opened by passengers (Review Committee Report, 2006:66).

The first passengers to come from the tunnels were uninjured or suffering from only minor injuries. Some were led by police officers, transport staff or led themselves. Some merely left the scene in a state of shock. These people should have been corralled into a reception area so that their details could be collected and they could be triaged by LAS. This is included in The Manual: the London Emergency Service Procedure Manual

(Review Committee Report, 2006:68). The reception areas should be established by the emergency services and taken over by the local authority once they have established venues. Some local authorities had established casualty reception centres but these were not used in a systematic way: it appears that the emergency services were unaware of their existence (Review Committee Report, 2006:69). It appears that those passengers who did ask the police if they should leave their details were told to go home and watch the news to see what they should do. Other passengers who tried to stop commuters entering the underground stations told of how there were no ambulances or doctors at the Russell Square station (Review Committee Report, 2006:70).

The priority for the emergency services is understandably to focus on those most seriously injured which is why it is so important to have someone on scene to deal with the less seriously injured and collect their details. The Manual does not identify who will be responsible for this task which is why there may have been some confusion. This may have been exacerbated by the lack of reception areas within LU. Shops and hotels close to the affected areas had never been approached about the possibility of using their premises in this way.

There are several reasons why it is important to collect the details of survivors:

- in the months following the incident, survivors will have ongoing needs in terms of advice, information and support and the emergency services will need to inform them of the services that are available to them;

- they are potential witnesses to the police investigation;

- friends and relatives will need to be able to locate survivors and the police need to be able to return belongings

(Review Committee Report, 2006:73).

It was estimated that around 4,000 people were directly caught up in the attacks yet only 946 statements were taken by the police. This represents less than one quarter of potential witness statements and details. In addition, there were some difficulties in tracking patients once they were taken to hospital which added to the distress of patients and those relatives trying to trace them. This led to several relatives being given inaccurate information (Review Committee Report, 2006:74).

6.10 The Media

In the first hour after a major incident, the public need basic information about what has occurred and what they should do. In order to obtain the information, they will usually turn to the radio, television or internet which the government recognised in its emergency preparedness advice: 'go in, stay in, tune in'. In light of this, the media therefore has a crucial role to play following major incidents and should be involved in emergency planning as stipulated at 2.10. In addition, they should be provided with up-to-date information to broadcast to the public as soon as possible (Review Committee Report, 2006:78). On 7th July, the media were used quite effectively, not least due to the establishment of a Media Centre which was the result of consultation with the Media Emergency Forum. The media must be treated as an integral part of the response to major incidents despite some reluctance evident through comments made by Ken Livingstone, Mayor of London and Sir Ian Blair. This could have a two-fold detrimental effect as the Emergency Services may not then engage effectively with the media so the media may be critical of responses at key times. Secondly, if the media has not been involved in planning for the response, they cannot know how to effectively fulfil their public service role (Review Committee Report, 2006:79). It was noted that in the emergency scenario 'Atlantic Blue' (Metropolitan Police, 38, 951, April 15th 2005) no media representatives were allowed to participate; it is not enough to only pay lip service to the importance of the role of the media, they must be fully integrated in emergency planning.

It is worth noting that Sir Ian Blair's news conference at 11:15am did not fall within the guidelines set out in the Civil Contingencies Act 2004. The Act clearly states that the

advice that was communicated should have been given within an hour of the incident. Sir Ian felt that it was unreasonable to expect the police to issue advice within two hours of an incident. The 7th July Review Committee disagreed with this view (Review Committee Report, 2006:80). It may not have been possible to provide specific information but the general advice could certainly have been provided earlier. Arguably this supports the recommendations of this thesis regarding risk and crisis communication and its utility for the management of dangerous events.

The fact that the Commissioner of the MPS chose to give the initial news conference did have a detrimental effect on subsequent broadcasts. It was noted that when less senior officers broadcast updates later in the day, their advice was not seen to supersede Sir Ian's broadcast. Thus, when less senior officers broadcast that it was safe for people in London to travel home, their advice was not so easily conveyed (Review Committee Report, 2006:81). It also appears that the credibility of the information that was broadcast in the first two hours following the attacks was questioned by both news editors and the public, undermining the message.

The media was aware of the explosions within minutes of them taking place yet the official line was that there had been power surges on the underground network. It was not until the explosion on the bus at Tavistock square that official accounts actually reflected what had happened.

This is an important point to consider as there are two possible reasons for the delay in congruence: (1) there was a reluctance to declare the nature of the event until due to media coverage the nature of this was obvious and so was a political response or, (2) situation assessment was poor which meant that it genuinely took that long to confirm what had occurred.

If the first scenario is true, it could be argued that the possibility of mass panic was a driving force delaying the release of information. This is not a justification however as communicating a true and reasoned picture of such situations is one of the central tenets

of this thesis and is argued to reduce rather than increase panic. However, if the second proposition is true, it is arguably more concerning. The ability to recognise and declare a crisis event is one of the most important requirements in its management. Communications would therefore need to be investigated together with reporting procedures to identify which of these was correct. In light of the information already considered in this chapter, particularly Ian Blair's media address, it is suggested that a combination of the two was most likely. Communications are therefore again central to the problems here. Sadly such problems were evident in the past and had not been acted upon as again in the Kings Cross disaster (Fennell, 1988:83).

For local businesses and communities, some local authorities have established pager or e-mail alert systems in collaboration with the relevant police service to communicate information during a major incident. Prior to 7th July this was only available in some local authority areas. Following the attacks, some elements of the initiative are being replicated and developed elsewhere (Review Committee Report, 2006:82).

6.11 The Problems for Victims' Friends and Relatives

Those who had friends or relatives caught up in the day's events needed to have access to a telephone line in order to register the person as potentially involved or to find out if they had been found. The MPS Casualty Bureau did this as the first step in the criminal investigation and formal identification process. The decision to establish the Bureau was taken at 9:30am. The service level agreement for this with Cable and Wireless stipulated that it should be operational within four hours of the incident. Unfortunately it was not so until 4pm due to an incorrect connection at the switchboard at New Scotland Yard. It was deemed unacceptable that the number to call was not free and was charged at 10p per minute. This has now been changed and all of the profits that were made from the number were donated to charity. The volume of calls was too much and not everyone could get straight through however, the new 'Casweb' technology that is being introduced should be capable of handling a far greater volume of calls and will also

enable calls to be diverted to other forces in the UK. Information will also be able to be stored on a shared database (Review Committee Report, 2006:84).

It was noted (Review Committee Report, 2006:85) that many called the Casualty Bureau line for information on what to do rather than to locate loved ones. Increasing the capacity of the Bureau to receive calls would help this but it is also important to educate the public so that they are aware of what the Bureau does. Consideration should also be given to creating a resource to provide this information, whether it is via a website or an alternative telephone line. Several reasons have been suggested for the number of calls asking for guidance, not least due to the contradictory information that was broadcast that day. Throughout the day the 'go in, stay in, tune in' message was played constantly, even after the bus service was reinstated at 3pm. The lack of clarity about the purpose of the Bureau may also have added to confusion. Finally, no alternative telephone line existed for general enquiries despite the Civil Contingencies Act 2004 recommending it.
Conflicting reports as to why the 'go in, stay in, tune in' message was played long after it was necessary exist. The Mayor felt that it the responsibility of the media to time limit advisory messages. News editors in contrast said that they had not received any information as to the time-limited nature of the message. This caused unnecessary confusion and distress for the public that should have been avoided.

6.12 Advice to the Public Regarding Mobile Telephones

On 7th July, all mobile telephone networks suffered network congestion due to the volume of calls. Various technical fixes were implemented to try to address the problem but these were only partially successful. Only so much can be done to plan and manage such a dramatic increase in call volume.

One of the key lessons learned for the network companies was the need for processes for managing sudden increases in call traffic. Prior to 7th July their joint emergency planning had focused on how they would maintain business continuity in the event of damage to 'critical infrastructure'. As a result, on this day, their joint working procedures were not

immediately activated, due to the lack of damage to their infrastructure and the assumption that there would not be any problems because of this. More formalised procedures are now in place regardless of whether an event directly affects telephone network infrastructure (Review Committee Report, 2006:90).

6.13 Media Facilities

A media centre was established at the QEII Conference Centre. This decision was made at the first Gold Co-ordinating Group meeting at 10:30am. The centre opened three hours later. It was felt to be a success by all parties but there were still some lessons to be learned; for example, it was felt that it may have been useful to have had a permanent police public affairs presence at the centre. Similarly, some would have preferred that the centre had been up and running earlier in the day and others felt that the technical facilities could have been much better (Review Committee Report, 2006: 92).

Such problems could have been foreseen and addressed had the media had a role to play in the Atlantic Blue simulation earlier that year. The fact that it was reduced to a desktop exercise (Home Office, 17th March 2005) reduced the benefit of the training and meant that important issues like this were not identified.

Some of the mobile telephone networks tried to ask customers to reduce their telephone usage by placing messages on their websites and through the media. Unfortunately, in the case of the latter, this did not get through due to the volume of information already being made available to the public. It was felt that it would be inappropriate to send text messages to all network customers as this would use up valuable space on the network that could otherwise have been used for telephone calls (Review Committee Report, 2006:91). Even if the message had been successfully relayed to customers, it is questionable whether it would have been followed.

In terms of communications with businesses, it is acknowledged that there was a need for a more co-ordinated and consistent mechanism for communicating with them. The

London Resilience Forum is developing a solution and local authorities will decide whether or not to invest in this (Review Committee Report, 2006:94).

6.14 Other Communications with the Public

On the day of the attacks, official websites, especially Transport for London and the MPS experienced a huge upsurge in the numbers of people logging on to their sites, demonstrating the huge public reliance on the internet as an information source. It is important to acknowledge the importance of this medium and ensure that it is appropriately utilised in a major incident to disseminate information to the public.

6.15 In Conclusion

The Review Committee felt that one of the key lessons to be learned from the review of 7th July was that emergency plans should focus on the individuals rather than focussing solely on the impersonal incidents. Another key area that needed to be improved was communication. Communication was an issue both within individual services, between them and between emergency services and their control rooms. Coupled with this is the importance in becoming less reliant on mobile telephones as a means of communication due to the associated network problems such as when underground. The communication issue was highlighted following the King's Cross disaster yet it appears that this still has not been fully addressed. It is not acceptable that only the BTP had the ability to communicate via radios (Review Committee Report, 2006:120).

The Review Committee established some recommendations following their investigation into the response on 7th July 2005. One of the main recommendations was that the underground system should more rapidly roll out new facilities for passengers and train drivers to be able to communicate in an emergency and in the meantime, should investigate interim solutions to increase the resilience of radio communications between train drivers and line controllers (Review Committee Report, 2006:125). Again, such

recommendations had been made seventeen years earlier in the Fennell Inquiry into the King's Cross disaster (Fennell, 1988)

Communication with the public via the media was another main focus. It was recommended that in future resilience exercises, senior media representatives should be included as participants, not just observers. The MPS should work in consultation with the London Media Emergency Forum to revise its plans for providing basic advice to the public rather than detailed information, within the first hour following a major incident, if possible. The MPS should also appoint someone to act as a police spokesperson throughout the day (Review Committee Report, 2006:134).

It is interesting and concerning to note that again in the 1988 Fennell Inquiry into Kings Cross that communication issues both with the equipment and between levels and services was an area that was highlighted for improvement (Fennell, 1988:137). Again, recommendations had only partially been addressed so such ad-hoc response to such important recommendations further supports the conclusions of this thesis: just because something has been highlighted for action does not guarantee that it will be addressed and a reluctance to consider the detail, rather than just the bigger picture, may be detrimental to an organisation's risk management and safety.

On 21st July, Ministers began to consider the emerging lessons learned at a Cabinet level meeting which the Home Secretary chaired. Six main categories were identified:

- clarifying the 'Central Government's Arrangements for Responding to an Emergency';

- Closure and re-opening of the transport system along with reducing the vulnerability to it;

- A review of the capacity of the Casualty Bureau and its ability to handle the huge volume of calls;

- Support to victims and families of the deceased;

- The resilience of the telecommunications network and in particular, the capacity of the mobile telephone network;

- Enhancing the role and effectiveness of media co-ordination in Government

(Report of the Official Account of the Bombings, 2006:11).

If these recommendations are adopted, many of the issues identified on 7th July should be avoided in any future major incidents. It should be noted however that in spite of the identified problems and issues, the emergency services managed to clear all of the sites within four hours and saved many lives that day.

However, 'if' is not enough. As was evident following the Fennell Inquiry, it is apparent that many recommendations are not implemented. The fact that issues have been identified seems to have a cathartic effect on organisations and appears to invoke a pacifying effect and a resulting blindness to the risks that may materialise.

The next chapter will present the conceptual groundings underpinning this thesis. Chapter Eight will address those common factors evident in each of the case studies considered here and begin to suggest what should be done in order to help to prevent history from being repeated.

7. Conceptual Groundings

This chapter brings together the preceding chapters and intends to ground the conceptual thinking underlying this thesis. It will link the literature, methodologies and data before presenting the main findings and analysis in the following chapters.

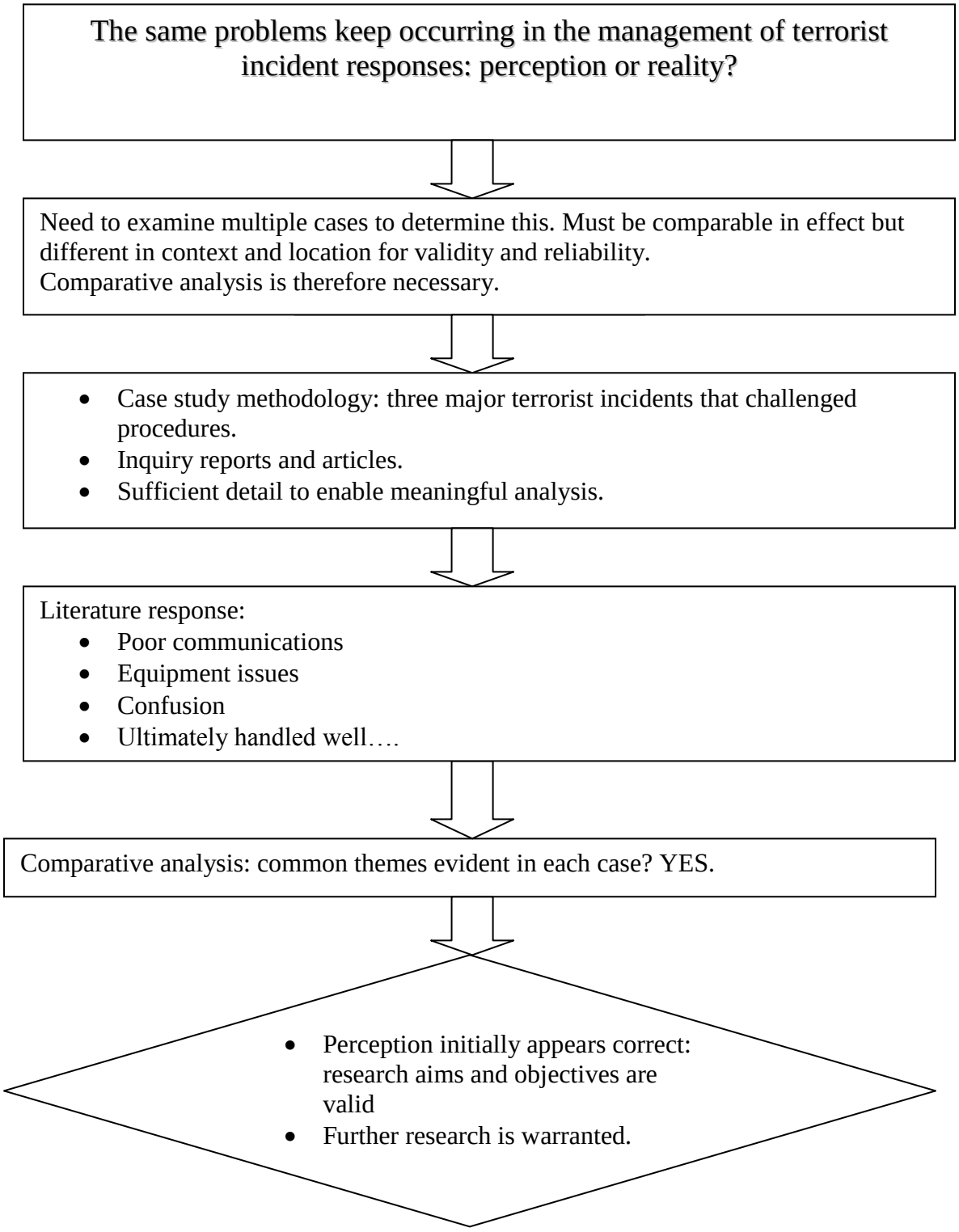
Two models will be presented here. The first conceptual model illustrates the underlying thinking regarding how to approach the research aims and objectives. The second theoretical model considers the literature and thesis findings and how these guided the recommendations that will be presented in the next chapter. Additional considerations within these models are also presented.

The conceptual model helped the researcher to clarify what it was that was to be investigated and the key questions that had to be answered. This would determine whether this was a valid area to research. Key concerns were also identified that the researcher would need to be cognisant of when carrying out the exploration as part of this PhD. The model helped to ensure that the thesis did not stray from the main focus despite the many lines of enquiry that could potentially have been followed. Each of these was interesting but ultimately would have moved away from what the researcher regarded as the most important and valid area to be investigated.

The theoretical model moved on from the more general, far-reaching considerations at the start of this research to the specific detail. The main components of this model were the literature findings and how these guided and related to the findings within this thesis. These elements would then shape the research findings and influence the recommendations that would be made.

It was evident that some overlap existed between the literature and the research findings however, there were also some differences that will be explored in the model at 7.2 of this chapter. The models will now be presented for further discussion.

7.1 The Conceptual Model



This is the initial conceptual model to demonstrate the thinking underlying this research. This model attempts to illustrate the conceptual thinking underpinning this research and the justification for the research aims of this thesis.

Once the researcher had established that there was a valid issue to research, a theoretical model was developed that identified the literature findings, thesis findings and the overarching issues to try to improve terrorist incident responses.

From the conceptual model above, the first item to be established was whether the question to be considered was valid. From the researcher's reading, it appeared that there was much similarity between the problems faced following major terrorist incidents. Was this the reality however, or merely a perception?

In order to try to answer this question, the researcher felt that it was necessary to examine several major incidents, ideally each in a different geographical location and carried out within different contexts. It was intended that this would aid the validity and reliability of the thesis through triangulation. Comparative analysis was therefore an integral part of this study.

As each incident was to be studied separately, a case study approach was clearly advantageous. The benefits of such an approach have already been discussed in Chapter Three of this thesis. It was imperative that sufficient detail was included in order to create as thorough understanding as possible of events and responses within each attack. The purpose was not to lay blame but to identify good practice and areas for improvement; Inquiry Reports had already been published but it was the researcher's belief that these did not go far enough and that they approached the review in a very specific, and arguably, blinkered manner that precluded identification and application of certain lessons learned. This was the crux of this thesis.

On examination of the literature it became apparent that four themes existed in the response to each terrorist incident that was considered here. These were: communications issues, equipment issues, confusion/decision making issues and the view that ultimately, each was handled well. Comparative analysis had identified these common themes in each case.

As a result of these findings, the researcher was reassured that this was a valid area to research and that there were clearly issues that had been overlooked in each case, resulting in the same problems over and over again. The theoretical model was now the main focus to consider, guiding the research progression.

7.2 The Theoretical Model

Literature Findings

- Poor communications
- Communication equipment problems
- Confusion regarding incident location
- Incident response ultimately handled well

Overarching Literature Issues

- Fear of failure
- Do not want to be seen as wrong

Common identified issues

- Poor Communications within and between organisations and agencies
- Communications equipment problems
- Confusion/poor decision making issues
- Reasonably well handled.

Thesis Findings

- Poor communications
- Communication equipment issues
- Lessons identified Vs. lessons learned
- Ring-fenced set of principles and actions
- Flawed decision making (hindered by communications issues)
- Problems identified in earlier incidents, yet not acted upon
- Evidence of practitioner-based methodologies (implicitly)
- Reasonable incident response: could/should have been handled better.

Overaching Thesis Issues

- 'Territorial' behaviour
- Lack of information sharing

It was therefore evident that although some of the same findings were evident in the literature and within this thesis, the thesis identified different overarching issues and some additional findings.

It must be remembered that the Inquiry Reports considered each event in isolation whereas this research was able to consider all of the events discussed here and hence identify potential lessons to be learned more readily. However, it is argued that this is what the Inquiries and formal reports should also have sought to do, if anything valuable was to come from the review of incidents. It is therefore not only recommendations for the preparedness and response to terrorist incidents that this thesis considered but also the way in which the information was gathered for this purpose. The researcher had not expected to find this at the start of this study.

The similarities evident in the literature findings and in the thesis findings concern communications problems, communication equipment issues and confusion or decision making issues. These of course had second-order effects that impacted upon decision making generally, however, the literature does not appear to consider any faults or concerns regarding decision making, unlike this thesis. It is contended that this oversight highlights the 'tick-box' approach that this research kept witnessing and lack of consideration of wider issues. It is this that must be addressed.

Whilst it is good that the serious communications issues have been identified and recommendations for improvements made, it is the view of the researcher that these do not go far enough and have wasted an opportunity to address the sadly, very familiar problems that keep occurring.

From the theoretical model, it is evident that the official Inquiries and the literature broadly, do identify flaws in response and begin to suggest improvements for the future. Despite this, it is contended that there is a reluctance to admit a degree of failure and clear evidence of a lack of information sharing and other territorial behaviour. There is also clear evidence of a so-called tick box approach to learning from experience, evidenced through the ad-hoc use of simulation and review of incidents and the lack of full buy-in to the training exercises (witnessed in the downgrading of the Atlantic Blue exercise, discussed earlier) and the failure to implement recommended changes following

previous incidents (such as the communications equipment changes that were recommended following the 1987 King's Cross disaster).

The reasons for these issues are not clear. An absence of risk cultures in the organisations concerned is suggested to be partly to blame but there is also, arguably, the reluctance to acknowledge that such incidents are likely to happen again. The idea of a ring-fenced view of the response to terrorism is also prevalent, blinding agencies and organisations to the idea that they may well be better prepared than they think they are due to the equivalence with crisis management and resilience procedures. Recognition of this would also begin to address the financial constraints, perceived or otherwise, that often hinder planning and preparation for dangerous events, as discussed in Chapter Two of this thesis. This is because many of the existing procedures could also be applied in the terrorism context, no longer requiring re-writing for this type of event, as posited earlier and below.

The use of the models presented here helped to clarify the issues underlying this research and also helped to identify the main areas for further consideration.

7.3 Crisis and Risk Management Methodologies: Where do we stand?

From the preceding chapters, it is evident that current thinking effectively 'ring-fences' the principles and actions associated with terrorist incident response away from crisis management practices.

Whilst in the past, many thought that any plans could be adopted for a crisis (McConnell and Drennan, 2006:68) there appears to be little evidence of anyone thinking in this way about terrorist incident response. Although the idea that a crisis is the same as an emergency or disaster is incorrect, the idea that a terrorist attack is distinct from other types of dangerous event is, this thesis argues, also incorrect. Why is this posited? Consider the definitions of crises presented in Chapter Two: they were said to require a rapid response and were frequently ill-structured. Rigid, highly-structured responses were

inappropriate, reducing flexibility and hindering the management of the event. Effects of decisions could be unclear. If the terrorist incidents in Chapters Four, Five and Six of this thesis are considered, the defining characteristics of crises above are plainly evident. It therefore follows that crisis management methodologies are an invaluable resource in the preparation for managing the response to terrorist attacks.

Furthermore, if it is considered that some of these methodologies, in whole or in part, are already utilised, the extension of their application to terrorist incident response seems to be a natural progression that should meet less resistance than new, unknown approaches. If these are coupled with Risk Communication theory to counter some of the communications issues and also Isomorphic Learning theory, both presented in Chapter Two, it is argued that a more robust, cohesive approach to resilience and response to attacks can be developed. The value of full buy-in to simulation training is also evident, moving from a lessons identified culture to a lessons learned culture. Arguably this is the underpinning of a robust risk culture.

The two main crisis management methodologies that were considered in Chapter Two were developed by Augustine and Fink. Although both methodologies are indeed valid, the researcher feels that Fink's methodology is the most appropriate for the purpose of this thesis.

Whilst Augustine's methodology is based on his experience, it is suggested that the model is a little too simplistic for such complex events as terrorist incidents and crisis management. The breakdown of events into the six stages is arguably more detailed than is helpful. In reality, events are likely to overlap several stages and the researcher suggests that identifying six stages may overly complicate event management. In contrast, Fink's methodology takes more of a practitioner-based approach. For the purposes of this thesis it is argued that much of what Fink suggests may be done, at least in part, is done implicitly by many of the parties involved in each of the terrorist incident responses. As a result, acceptance of a formalised approach may well be easier to achieve, not least due to the familiarity with many of the steps as they are certainly

intuitive. Such a practitioner-based approach is argued to be of far greater benefit for those charged with managing dangerous events.

Elements of Fink's methodology being carried out can be seen in each of the event responses discussed in Chapters Four, Five and Six. Although this is not done explicitly or knowingly as Fink's methodology, it does demonstrate the validity and utility of such an approach, supporting the recommendations of this thesis. For example, in the Sarin attack response in Chapter Four, the prodromal stage was overlooked when the first attack in June 1994 was not taken seriously. However, when the acute stage of the crisis occurred, when the situation had been determined, the organisations involved moved to control as much as they could and contain what was occurring.

The chronic stage of the crisis in the Sarin attiack was evident when it was recognised that existing procedures were not enough and changes were necessary. Arguably the resolution stage also shows some signs of existence when there was a move towards greater co-operation between agencies. However, this did not go far enough as there did not appear to be consideration of how practices more generally could benefit from the changes or a consideration of whether the 'real' crisis had actually been tackled.

Similarly in the 9/11 case study, it is evident that the prodromal, warning stage was missed, when it appeared that there were rumours that a major attack was being planned. The acute stage of the crisis can be identified, although it was not done so by the organisations here, when there was a chance for the second World Trade Center tower to be evacuated before the second plane had hit it. Had people realised at this stage what was happening, it is suggested that the potential existed to have saved more people. The chronic stage can be seen during and following the Inquiry into 9/11. Real reflection appeared to occur, whilst changes to equipment and procedures were brought about. Again, it was not that those involved were aware of specific crisis management methodologies, they were merely acting on lessons learned and common sense. The resolution stage, perhaps somewhat controversially, is suggested not to have been fully realised as the researcher would ask whether the real crisis has been tackled? Yes,

terrorism is at the forefront of America's attention but the underlying triggers could be suggested not to have been fully evaluated.

In 7/7, it could be posited that the prodromal stage was when the Atlantic Blue Exercise was downgraded. Had this been carried out as intended, arguably some of the issues that occurred on the day would have been foreseen and addressed. The acute stage during 7/7 can be seen in the recognition of what had occurred and when the first emergency services arrived on scene. However, this was also when more problems arose when ambulances were sent to the wrong locations and confusion existed as to what had actually occurred, witnessed in Ian Blair's press statements.

The chronic stage of 7/7 was, as in the case of 9/11, in the lead up to and during the Inquiry. Some issues were recognised and changes were recommended. However, also as in the case of 9/11, the researcher proposes the idea that the crisis resolution stage had not been fully realised in this case either. This is because there appears to be a reluctance to go far enough in identifying the problems that occurred on the day or in moving beyond paying lip-service to the idea of simulation training and information sharing. If this is not genuinely embraced then it is almost impossible to reap the benefits of any hindsight that may have occurred.

From this it is evident that elements of Fink's methodology can be seen in each of the terrorist incident responses examined within this thesis. However, the organisations involved have not utilised the methodology or been aware of it and as a result have not benefited from its explicit application. As it is possible to apply the methodology to each incident, as has been seen, the researcher is confident that this would be a useful tool both during a crisis and in preparation and debriefing, to improve event management. This would help to provide some clarity and potentially reduce some of the uncertainty that exists at such times and would build on some of the good practice that already exists in each case. Organisations and agencies would realise that they were already practicing some of what is proposed here which should help to gain acceptance. Supporting this

with other relevant risk and crisis management methods would greatly increase the resilience and ability of organisations to cope in such circumstances.

The adoption of Risk Communication principles would augment Fink's methodology and would help to translate risk management knowledge into effective practice, as Maule (2004:17) recognised. The benefits of such an approach also apply to interactions with the public, not only amongst those organisations responding to incidents. Again it is evident that this may help to avoid some of the confusion that was evident in each incident considered in earlier chapters, particularly in the 7/7 media reports and briefings.

The two-way Risk Communication approach advocated by Hayenhjelm (2006:2) is proposed to be of particular value here as this approach is far more open to shared decision making; something that was a serious problem in managing each of the three incidents.

If this is coupled with Isomorphic Learning theory, formalising the idea that it is possible to learn from previous events, not merely identify those similarities but to actually amend processes in order not to make the same mistakes again, or to ensure that good practice is harnessed and disseminated, it is possible that the same issues evident in each of the incidents examined here are less likely to be repeated. It is then that organisations move from lessons identified to lessons learned.

Many organisations do already consider case studies of incidents and look at what has gone before to help them to prepare for the future. However, this is frequently done on an ad-hoc basis or too informally, hence although simulations and preparations may take place, the value of these is largely negligible as they are not being used in the way that they are intended to be, in order to achieve the best results. It is the assertion of this thesis that if this was formalised and actively included the above theories and methodologies, a more robust process could be achieved.

Many of the other risk and crisis management theories considered here are interesting but are ultimately flawed, not least due their impracticality or unrealistic world view. It is for these reasons that the researcher has not recommended that the remaining methodologies would be of use for the purposes of this thesis.

The next chapter will discuss the findings of this research and how this meets the aims and objectives presented at the start of this thesis.

8. Main Findings and Analysis

This section of the thesis is divided into two parts: the first section will present the main theoretical conclusions addressing the aims and objectives of this research that were presented in the introduction. These conclusions will then be contrasted with current theory considering risk, crisis management and terrorism that was reviewed in Chapters One and Two. This is in order to be able to progress to the second section of this chapter. The second section will offer recommendations and critical observations on the management of the incidents considered in Chapters Four, Five and Six to improve resilience and preparedness for such events in the future and also to enhance current provision and responses to dangerous events.

8.1 Findings

The findings that were uncovered by this research relate clearly to the objectives stated at the beginning of this thesis and ultimately help to address the overall aims that this work is intending to achieve. That is:

> Did common issues exist in the response to three key terrorist attacks that hindered aftermath management?
>
> How can risk and crisis management methodologies help to address these and provide more robust arrangements, improving resilience?

The objectives that should be met in order to achieve these aims are:

- To advance an understanding of responses to terrorist attacks, determining good and bad practice.

- To identify which risk and crisis management methodologies may be most appropriate to inform anti-terrorism methodologies and incident response.

- To challenge the belief that terrorism aftermath management is completely different from crisis management requirements and hence necessitates a different approach.

- To question the belief that terrorist aftermath management is different from other dangerous event management requirements.

As is evident from the analysis of the case studies in Chapters Four, Five and Six, some strengths and weaknesses in the response to each of these events are evident. This thesis will now consider the identified weaknesses to suggest improvements to build on the strengths that were recognised in each case.

8.2 The Issues

Arguably the greatest issue or weakness in each of the case studies was that of communication. However, this was not merely one type of communication; problems arose regarding inter-communication between agencies and between agencies and the public and also intra-communication within single agencies. Communications equipment and the utility of this was also something that severely hampered the rescue efforts in each case; particularly concerning when the events considered here occurred over a period of ten years and worse, that such issues had been identified in some cases seventeen years before the incidents considered here. Such findings validate the purpose of this research and demonstrate that existing ways of learning from dangerous events are not being translated into practice. If key points within each of the case studies are considered, this becomes increasingly clear. These points will now be presented.

8.2.1 Communication Issues

Despite each terrorist incident occurring in a different continent and being carried out completely differently, when one ignores the external differences, internal similarities in terms of the issues faced immediately become apparent. Such recognition supports the

validity and utility of the Systems Approaches to risk that were introduced in Chapter Two as useful aids to analysis.

The response to the Sarin attack in Tokyo revealed two key areas of communication issues that related to cultural and technical barriers:

- System overloads due to the volume of information
- Inadequate information sharing between agencies, hindering response efforts and resulting in decisions that had to be made with little or no information.

However, if 9/11 is considered, it is evident that similar issues could also be identified:

- System and technical issues hindered radio communications either through overload on individual radio channels or due to weak signal strength or incompatible transmission channels

- Lack of SOPs regarding multiple commands

- Inter-agency communications issues characterised by lack of information sharing. This appeared sometimes to be an oversight and, more worryingly, to be deliberate at other times, due to inter-agency rivalry.

If 7/7 is reviewed, the major communications problems that are evident comprise:

- System overloads due to volume of calls and transmissions

- Signals being compromised below ground

- Inter- and intra-agency communications hampered through poor information sharing or guidance being ignored.

From this, it is clear that there are indeed similar issues that keep occurring, regardless of location, time or nature of an event. As well as proving the value of Systems Approaches to risk and crisis management, this specifically validates the Isomorphic Learning Theory (Toft and Reynolds, 1994) and arguably Risk Communication Theory. For this reason, this thesis contends that these two risk management methodologies can provide valuable insight into analysing and preparing for crises that at present is not provided by the methods that agencies and organisations are employing.

Where good practice regarding communications was evident, such as in the 7/7 incident where BTP officers possessed radios that could work within the Underground system, or in 9/11 where evacuation procedures had been improved following the first WTC attack in 1993, these regretfully, were not enough to make a significant and positive impact on events in the face of such serious shortcomings. This is particularly frustrating in the 7/7 context when underground communications issues were raised seventeen years earlier in the Fennell Inquiry into the King's Cross disaster (Fennell, 1988), referred to earlier in this research.

Associated with such communications issues is the resulting impact on decision making. It was noted following 7/7 that the extent of senior representation at the Strategic Co-ordination Centre was not always appropriate and could be argued to have hindered some decision making. Furthermore, throughout 9/11 it was evident that the lack of information sharing, inter-agency rivalry and misinformation all impacted negatively on decision making that day. Such issues were also identifiable in the Sarin attacks: inadequate information sharing was seen to hinder decision making.

It is not enough however to merely note that these issues exist. To be of use, suggestions to move forward must be proposed and it is these that this thesis will now present.

8.2.1.1 Recommendations in Response to Communication Issues

Firstly, the use of simulation training, or more rigorous use of simulation training is strongly recommended. This cannot be an exercise in lip service as the Exercise Atlantic

Blue simulation appeared to be in the UK. The downgrade from a CPX to a desktop exercise where there was 'no visible on the ground activity' (Home Office Press Release 2005) could be argued to have limited the lessons learned from this training and, more importantly, to have meant that critical oversights were not picked up on. For example, the absence of the media from the exercise meant that some of the communication issues that arose during 7/7 had not been foreseen. Ian Blair's broadcast and the subsequent messages could also have been trialled and the ensuing confusion avoided when the event occurred for real.

Secondly, where recommendations for improvements are made, such as in the Fennell Inquiry or following the 1993 WTC attack, these must be comprehensively addressed, not partially adopted. The apparent risk blindness that ensued should not have occurred. For once it was a case in each of these attacks that too much attention was paid to the big picture at the expense of the detail rather than the arguably more common alternative of too much attention to detail at the expense of the bigger picture. A seeming assumption that others had taken action or would do what was required was also a major failing in many of these cases. Again, simulation training would help to ascertain this before a real event occurred.

Thirdly, the adoption of Risk Communication principles, discussed at 2.3.2 of this thesis is advocated in order to improve communication in preparation for and during an incident between the experts and lay people. Such improvements would greatly help to ensure that messages were not misunderstood and that there was less chance for panic to be created as greater understanding of the situation would exist. Uncertainty is one of the most frightening things that people can face and when frightened, logic and reason are often abandoned. If uncertainty can be reduced through education and communication, agencies should be able to minimise an element of the complexity of situations that they may face, allowing them to focus on the most important factors.

The necessity of changes to communications arrangements was recognised following each of the attacks and some recommendations made to improve provisions. As this

thesis is being conducted within a UK context, it is the 7/7 attacks that will form the main consideration of this section. 9/11 and the Sarin attacks will be referred to where appropriate in order to highlight the similarities and differences.

The Multi-Agency Debrief for 7/7 was published in September 2006 by London Resilience and included a programme of work to address some of the issues that had been identified. Perhaps somewhat concerning is an overriding comment on the success of co-operation and co-ordination between responders (London Regional Resilience Report, 2005: para 2.3); from the analysis of the case study, it is clear that there were in fact serious problems with co-ordination on the day of the attack. Such blinkered views and understanding in reviews of responses to dangerous events is not uncommon. It is argued that such misconceptions are potentially dangerous and recognition of the reality is imperative.

The Debrief did however acknowledge that communications whilst underground were problematic. The suggested action in response to this was to reduce dependency on mobile telephones and educate the public on mobile telephone usage during a crisis. In addition, TETRA based systems discussed in Chapter Seven, were strongly endorsed (London Regional Resilience, 2005: para 3.13). It was noted within the report at paragraph 4.12 that some concern did exist regarding the lack of implementation of the Fennell Inquiry recommendations in 1988. In spite of this, the decision was taken that existing systems at local commander level were already compatible. It is this that is arguably the most disturbing comment following 7/7, demonstrating that little had been learned from events that day and that the short-term view of risk management had again been adopted. It is here that the need for a new methodological framework is possibly most evident.

By adopting a methodology that incorporates simulation training that is of high fidelity and utilises the Isomorphic Learning theory that explicitly recognises that the same disasters keep happening because little is learned from them, a more realistic and robust policy would be developed. An overwhelming impression of an idealistic recollection of

the success of the response is provided in the reports that followed the incident, which is of no help in improving resilience and response. Furthermore, when combined with Turner's Incubating Disaster Aetiology as a timeline to events during an attack, the propensity for escalation, the triggers and points of escalation would be more readily identifiable and hence avoidable. It is argued that use of such methodological frameworks as a standard inclusion when creating response plans would greatly improve their quality.

Communications with the public were also considered in the official Debrief and focused on the content of media messages and ensuring that the public are aware of any time limits for the information contained within these. Again however, there are factors that suggest that those in authority are reluctant to think more creatively or are not aware of crisis management methodologies. Within the Regional Resilience Report (2005: para 3.18) there was a recommendation that those in authority should monitor the media more effectively to identify incorrect reporting. Such antiquated thinking is in opposition to what we have learned and identified as good practice within the crisis management literature, reviewed in Chapter Two. It is evident that the media can provide many benefits in times of crisis and can be used in a proactive way, conveying important messages at appropriate times; an invaluable resource. Official views however seem to see the media as something that should be avoided in times of crisis and as a source of concern rather than help; somewhat ironic when one considers that the only problems with the media during 7/7 were Ian Blair's incorrect message, which was his error and the lack of direction to the media as to the time limited nature of the advice that they were conveying. Additional confusion following Metropolitan Police broadcasts were also not the fault of the media as it was the police force that chose to broadcast the first message via their most senior officer so that any later broadcasts made by lower-ranking officers may not have been seen to supersede those screened earlier that day.

This again stresses the importance of simulation training and the inclusion of all relevant parties in addition to fully engaging with the training; had Exercise Atlantic Blue not been downgraded from a CPX then it is argued that such confusion could have been foreseen and prevented. The statement that it was suggested that the media should be

invited to participate in some future exercises (London Regional Resilience Report, 2005: para 3.18) is argued to be too little, too late and is indicative of the outdated thinking that has hindered responses to date.

The value of Risk Communication theory (reviewed at 2.3.2) is also evident in this instance as the methodology aims to narrow the gap between experts and lay people, in order to improve the management of risk through improving understanding. If such change was brought about, better understanding and use of the media would be likely to ensue and arguably, less panic would be created as the public would have a more reasoned understanding of the situation that was faced. The specific methodologies that are argued to be invaluable here will be discussed in more detail a little later in this chapter.

Equipment recommendations were made within the above report to address some of the technical concerns highlighted during 7/7. Mobile telephones were recognised as unreliable during such events and the necessity for alternative communications methods acknowledged. The LAS purchased pagers to avoid reliance on mobile telephones. Again, this is argued by this research to be an inappropriate response to the problems that were identified: the technology for pagers is outdated and they are now a barely used communication medium. If a longer-term view was taken, surely questions would be asked regarding how long such a system would remain operational for and whether the system would still be supported in two to five years. Such a response was again indicative of the short-term view and lack of foresight. Once more, the value of learning from risk and crisis management methodologies is evident, not least to change the way of thinking.

The importance of exercise programmes, or simulation, was recognised within the London Regional Resilience Report (2005: para A7) as they were in the Inquiry into the Sarin attacks and the 9/11 Commission Report. However recognising the necessity of such provisions is not enough; Exercise Atlantic Blue, as well as other smaller exercises were designed and run. It is the level of commitment and engagement with the exercises that is the issue that must be addressed. There is again the danger that this could become

merely a ‘tick box’ exercise, whose value is not realised, let alone captured. Senior management must fully support the use and value of such training, endorsing its value within the organisation. The idea that the investment in risk or crisis management provisions is money and resources wasted because the incidents may never happen, must be removed.

8.2.2 Classification of Dangerous Events

Associated with the problems of communication is the issue of defining events. In Chapter Two, the challenge of agreement of a unified definition of dangerous events was considered and agreed upon as an important way forward in managing such incidents. However, the degree of agreement required following analysis of the three incidents considered here is now suggested to be less than originally perceived. Why would this be so? Flexibility is one of the most important attributes of any crisis management methodology. If we are intent upon reaching consensus on the nomenclature of events then by definition we are becoming rigid in our interpretations and removing, or at least reducing, the potential for growth or adaptation. It is therefore suggested that it is the general principles of what constitutes each type of dangerous event that should be agreed upon rather than a watertight definition for each, or else we increase the risk of suffocating creativity and flexibility in responses. Worse still, without this the propensity for an event to escalate to the next level of events, such as that proposed by Turner’s model, may be increased. Such escalation should not however be assumed, as arguably the model takes a simplistic view that if certain actions are not taken then it is inevitable the situation will escalate; something which is not always the case. Similarly a contemporary definition of an act of terrorism that is appropriate for the threat that now exists should broadly be agreed upon. The definition offered by the UK government within the Terrorism Act 2006 (c.11) (Appendix IX) goes some way to achieving this.

The ability to recognise and declare a dangerous event is also of paramount importance as Borodzicz (1997:230) recognised. Without agreed definitions, the ability to achieve this will be compromised.

Such confusion, albeit on a lesser scale than in 9/11 and 7/7 was seen following the Sarin attacks where it took some time for the situation to be understood and then accurately communicated. Within the 9/11 context, this was a much more serious issue: the lack of awareness as to the imminent danger from the total building collapse as at 5.5.1 is a prime example of this. At 5.5.2 there is explicit recognition that command and control decisions were affected by a lack of knowledge. These are just two examples of such instances: Chapter Five considers many more. It is evident that in the 9/11 case the three key skills required for crises: declaration, negotiation and communication (Borodzicz, 1997:230) were severely impeded, directly affecting the response to the incident.

7/7 is no different. At 6.3 of this thesis it is clear that declaration, negotiation and communication were also not in evidence through discrepancies between emergency services in their assessment of the situation and later in Chapter Six in the communication to the public. The fact that each emergency service declared a major incident is also of concern as it merely complicates and confuses the management of the response and makes establishing an IMS far harder. It is argued that in this instance also, the confusion as to what was faced hindered the response.

8.2.2.1 Recommendations in Response to Classification of Dangerous Events

In the aftermath of the Sarin attacks, it was recognised that the IMS was not properly established due to the delay in recognising the severity and magnitude of the problem. To counter this, simulation training with a focus on inter-agency working has been introduced more widely and attitudes towards sharing information are slowly changing. This thesis would argue that such a programme needs to continue but furthermore, learning from past experiences or rather Isomorphic Learning should be an integral part of the resilience strategy. In the Japanese context, this may be somewhat more problematic than in Western cultures due to the culture of respect and the implications of admitting failure. It is strongly argued however that in utilising Isomorphic Learning theory, that the implications of ignoring what has gone before may be understood more fully.

Following 9/11, New York City adopted a new emergency response plan that expressly contemplated two or more agencies jointly acting as lead agency. However, as with many of the responses that have been reviewed within the course of this research, it did not go far enough: a comprehensive and unified command was not mandated, highlighted at 5.9 of this thesis. The official report suggested that this should be addressed (9/11 Commission Report, 2004:322) and this research echoes that recommendation. Again, the argument of this thesis that a new framework is necessary and that risk and crisis methodologies can greatly benefit this is supported: if learning from past experiences is ensured, combined with a rigorous simulation programme, supplemented by a Risk Communication approach to preparedness, it is argued that a comprehensive, not partial, improvement to present arrangements would be achieved.

The review of 7/7 also highlighted the confusion that arose as each emergency service declared a major incident. The Review Committee Report (2006:128) stated that once on emergency service has declared a major incident, units from all three services should automatically be mobilised and their major incident procedures put into action. This would go some way to clarifying responses during such an event but again this thesis contends that this does not go far enough and that risk and crisis methodologies would be of benefit in this instance also.

In each of the terrorist incidents considered within this thesis, it is clear that the classification of events was an important factor that affected their management, supporting one of the central tenets of this research that this is an important area to be addressed by response agencies. The practical implications are clear following review of the incidents; the review of the literature and risk and crisis management theory demonstrates how it can generate more robust responses and help to reduce confusion. The contention of this thesis, that a new methodological framework is necessary and that risk and crisis management methodologies have much to offer in this development is apparent.

8.3 The Methodologies: The Secret to Success?

This thesis is not suggesting that by incorporating risk and crisis management methodologies into existing frameworks, all of the issues that were evident in the three terrorist incidents reviewed here will be rectified. It is suggesting however that through informed and tactical use of these, analysis of events and responses will be more comprehensive and cognisant than that which is achievable using current arrangements. Several elements of different methodologies are clearly applicable however two key methodologies in their entirety are argued to be of value in developing a new framework. These are:

- Risk Communication Theory
- Isomorphic Learning Theory.

8.3.1 Risk Communication Theory

Effective communication is critical for translating risk management knowledge into effective practice (Maule, 2004: 17). Such an observation was proved beyond doubt in each of the three case studies reviewed in earlier chapters. However, in each case, effective communication was clearly lacking despite such issues being observed in earlier incidents. The blindness to the issue reinforces the argument that current methods for developing communications during such events are falling short of what is necessary. This thesis therefore expounds the utility and value of a Risk Communication approach to the management of the response to terrorist incidents.

Such an approach would firstly address the status quo, before an incident occurred. The focus would be on informing the public of the actual nature of the threat that is faced and would move away from some of the sensationalist-type messages that have appeared in recent times. Through the explanation of some key terminology and reasoning behind decisions that are made, it is argued that the gap between the experts and lay people would be reduced, without increasing the vulnerability to terrorist attack or jeopardising security: at times it would appear that agencies are hiding behind such an excuse as a reason for not informing the public of what is occurring. This is also argued to be an

approach that should be adopted when engaging in dialogue with relevant parties. If such an approach were to be adopted, panic would be reduced within the general populous, hence reducing one of the risks that would need to be managed. This is also the time when people should be informed of what they should do and what to expect if an incident does occur. This would be invaluable, for example in preventing the misuse of the 999 telephone line or mobile telephone networks being overloaded as was evident in each case. Furthermore, it would also reduce the number of people who used treatment centres when this was not necessary.

The concept of reducing panic is an important one within the context of this research as it is argued that a skewed view exists of the scale of the threat that is actually faced both within the UK and the USA. In no way is this thesis suggesting that the attacks considered in the earlier chapters have been over stressed: these were appalling acts of terrorism that cannot be condoned. What it is suggesting is that it is important to try to maintain a balanced view of the threat and ensure that moral panics do not ensue where people feel the need to curtail their everyday activities for fear of attack. As was suggested in Chapter One at 1.9 it is often the fear of attack and the disruption to everyday life that terrorists seek to bring about rather than actual bloodshed. The ensuing broadcasts of injuries and fatalities may be an objective but it is not an aim. The aim is to limit freedom and coerce behaviour.

If the number of attacks is considered within the global context, it is apparent that there are far more countries affected by terrorism around the world, facing far more frequent attacks than the UK, USA or Japan. In the case of the UK, the majority of the attacks noted on the map at Appendix X were as a result of IRA attacks rather than the more recent terrorist threat.

While it is important not to become complacent, the scale of the threat should not be overstated; the goal of improved understanding amongst the population, which Risk Communication seeks to achieve in order to develop a more realistic view of risk management, cannot be achieved if the reality is not accurately portrayed.

However, it is not only the traditional one-way communication that is suggested by this thesis. Two-way communication is also argued to be of value for developing a new methodological framework. This approach allows for more open interactions, such as shared decision making, discussed at 2.3.2. The knowledge and understanding that lay people possess should not be underestimated; they may have expertise that is of benefit to updated procedures for example or local knowledge or understanding that has not been captured previously. Greater communication with relevant groups can be generated, clarifying information and reassuring communities. This is another example of the two-way Risk Communication approach where it operates between governments and local populations. This is suggested to be a useful tool in anti-terrorism strategy.

Risk Communication theory is also beneficial when managing the media in a crisis and indeed in times of calm. The media reflect the nature of definitions of risk. As Denney (2005:83) asserts in 2.3.2 of this thesis, the four key areas of control, legitimacy, trust and precedence joust for supremacy when conveying a message. These, together with the social amplification of risk, impact upon the media's message pertaining to risk. Despite the importance of the media, no indisputable evidence exists that establishes a link between media messages and the public perception of risk. However, it is still important to present a trustworthy illustration of the situation as perceptions of risk are shaped by cultural, social and psychological factors. Through being open with the media, good relations are also engendered that can help to disseminate or dispel information during dangerous events.

The adoption of any Risk Communication approach must be carefully managed as, like any other approach, there are caveats to its potential success. Individuals' frame of reference must be taken into account in order to determine why risks have been perceived as they have and how their worldview is constructed: something that was first considered at 2.3.2 of this thesis. It is when this is done and without any manipulation of the meaning to achieve a specific aim, that any form of mutual understanding may occur. From this

foundation, a more useful and reasoned dialogue concerning risk and its management may be opened up.

This is clearly not a short-term fix to the challenges of risk management and understanding of the threats, nor is it something that can begin in times of crisis. Such approaches are about looking to the longer term, moving away from the short-term accounting view that has plagued risk management for so long and about bringing about a paradigm shift in the way in which society views and responds to risk.

8.3.2 Isomorphic Learning Theory

Isomorphic Learning Theory is also argued to be a valuable tool in developing a new methodological framework for managing the response to terrorist incidents. Part of the utility of this theory is its innateness; human beings initially manage unknown situations through heuristics, or 'rules of thumb' amongst other things. These rules of thumb are based on facts that we already know, experiences we have had. We therefore naturally recall past experiences to help us to understand our present condition. Isomorphic Learning theory is merely an extension of this, developing the idea to apply it explicitly, not just implicitly and to extrapolate it beyond the like with like, to things that may be externally dissimilar but ultimately internally similar.

Despite the obvious benefits of utilising such an approach, it has not been comprehensively adopted as this research has found. Some elements may be seen at a superficial level but this thesis strongly contends that this risk methodology has an invaluable part to play in improving the analysis of events and in designing the responses to these. Blindness to specific risks or groups of risk is argued to be likely to be reduced, providing more resilient arrangements in the future. As Fink recognised:

> 'The best predictor of future events is past events' (Fink, 2002:43).

There is of course a danger that Isomorphic Learning is merely hindsight, as Borodzicz asserted (2005:27) but this thesis contends that with the right debriefing, capture and sharing of information and knowledge this theory can go far beyond this.

8.4 Terrorist Incident Response Vs. Crisis Response

In the course of this research, it was recognised that much of the existing literature considered terrorism and crisis events separately and that very few academic resources linked the two areas in order to provide a more cohesive and holistic approach to understanding events and developing management frameworks for the response to these. The two areas appeared to be viewed as distinct with little overlap between them. It is one of the contentions of this thesis that this is failing to capture valuable knowledge and understanding that would move the development of the management of the response to such events into the twenty-first century and would embed within it the flexibility and ability to adapt to scenarios as they unfolded. It is the rigidity of existing SOPs and the lack of scope for flexibility and innovation in dealing with dangerous events that frequently makes them harder to manage.

It is useful at this point to consider the views on crisis management and the management of responses to terrorist attacks to illustrate some of the concerns that may exist and perhaps what the rejoinder to these may be. Before this is explored however, we need to revisit some earlier considerations presented in Chapter One as the perceived starting point of the response to terrorist incidents should be considered: why is it happening and what are the motivations?

This thesis has already stated at 1.3 that if the drivers and preconditions can become to be understood, the more the nature of the current threat may be understood and policies designed to match these. However, the idea of root causes, this research concurs, is somewhat simplistic as it assumes that single factors may drive individuals to perform a terrorist act or make them more likely to do so. It is contested that the concept of trigger causes, rather than root causes, is more appropriate as Bjorgo (2005:3) suggests.

This is however, an issue that runs in parallel to the main aims and objectives of this thesis and is therefore not the main focus. The way in which situations and past events are analysed and frameworks are developed, together with a focus on improving current resilience is what this research is centred upon. This does however increase our understanding of the overall picture of the terrorist threat and is something that risk and crisis methodologies can help to take advantage of. It is argued that understanding of Perrow's Normal Accident Theory (explored at 2.3.4.3 of this thesis) can help to explore the looser coupling of terrorist cells (referred to at 1.2) and begin to determine the ways in which this may be exploited. Without such theoretical underpinnings, it is contested that comprehension of the whole situation is hindered and ways forward may not be apparent. Risk and crisis management theory can therefore be of assistance here.

At 2.6 of this thesis, barriers to effective crisis management were considered that on review of the three terrorist attacks, they could also be barriers to effective terrorist response management. The first barrier was identified as difficulty between the balance of the high potential impact of crisis against the low priority of crisis management. Within this barrier, the word 'crisis' could easily be replaced with the word 'terrorism' as although there is clear recognition of the potential impact of a terrorist attack, terrorism response management as an ongoing preparedness concern is not of high priority. Much may be made of resources such as more CCTV or strengthened glass or even evacuation procedures but little is done to recognise more of the continuity element of this, in that one-off actions or purchases are not enough. This is another example of the tick-box approach to readiness.

The second barrier that is also applicable within the terrorism context is the juxtaposition of planning and order versus the uncertainty of disorder in a crisis. The value of training and simulation plans have been advocated throughout this thesis just as they have been for crisis management. Yet both events often require improvisation that has not been trained for (McConnell and Drennan, 2006:64). This thesis argues that for both crisis management and terrorism incident management, training for a generic response is still of great benefit as it ensures that the standard elements of response are so ingrained in

participants' psyches that they do not have to think about this part of the plan. This will then release them mentally to think outside normal, learned responses which should result in flexibility being far easier to achieve and far quicker to implement. In order to achieve this, it is clear why the merely symbolic readiness of some organisations is of no use. This barrier interacts with the fourth and final barrier: the difficulties in training for crises and dangerous events which will be considered after the third barrier.

The third barrier which was identified at 2.6 is that expertise and networks within organisations should be utilised to harness this and improve crisis management yet this rarely happens as many departments are virtually shut-off from the rest of the organisation. Making use of such knowledge is obviously beneficial within the terrorist incident management context and furthermore, reinforces the validity of the contention of this thesis, that a Risk Communication approach should be adopted when developing plans.

The fourth and final barrier was, as referred to above, concerned with the challenges surrounding crisis training. The three main points associated with this barrier are the cost of a realistic simulation, the concern that participants do not always put what is learned into practice and lastly that the events that may be faced do not fit the practiced scenarios. Again this could equally be levelled against the use of these within the anti-terrorism context. However, if the benefits of such preparedness could be conveyed to organisations and the normal operating advantages of such training demonstrated, such as improved performance and efficiency, potential increases in profitability due to efficiency improvements and a responsive, flexible organisation, then resistance to such training would gradually be reduced. The emergency services clearly practise emergency scenarios quite regularly however it is argued that even they fall into the trap at times of not learning enough from these exercises, or not implementing enough changes in some cases. Furthermore, as was observed in Exercise Atlantic Blue, the fidelity of an exercise can sometimes be compromised for seemingly public relations-type reasons: a good example of short-termism and a tick box approach to the utility of such exercises.

8.5 New Developments

In 2006, the UK Government published CONTEST2, The United Kingdom's Strategy for Countering International Terrorism. This strategy updated that which was previously published in 2003 and did take account of some of the lessons learned from the 7/7 attacks. However, whilst it spoke of engaging in communication with communities and being more open, the overriding feature of the strategy was one of dictating to the public and of referring to terrorism and the threat from this in overly emotive terms that could be seen by some as scaremongering. It could be argued that some of the phrasing within the strategy would have the opposite effect to that which was intended and alienate communities still further. Such strategies and thinking are firmly based in old ways of thinking that do not sit comfortably with the new order. A genuine understanding of this and adopting the lessons learned over the last decade are a must.

It is the suggestion of this thesis that such a strategy is a useful starting point but still does not go far enough or heed enough of the lessons learned from past events to be of as much use as it should be.

8.6 Moving Forward

During a crisis, communication is unlikely to be simple or orderly hence clarity and information sharing and exchange become central to the successful management of an event. It is contended that the approaches recommended in the course of this thesis would improve both intra- and inter-agency communication and hence improve the likelihood of a successful management outcome to such events.

The crux of the recommendations rest on organisational learning and the willingness and ability to put this into practice. However this is no easy task as Smith and Elliott (2006:519) concur due to growing evidence that organisations are resistant to learning from crisis. They go on to recognise that although there may be some reflection and analysis following a crisis, this is often only on a superficial or first-order learning basis which addresses purely technical and procedural issue amendments (2006:526). Such a

view echoes the findings from the three case studies reviewed earlier. It is this mindset that this thesis hopes to challenge in order to bring about second-order learning within organisations which is realised ultimately through the paradigm shift and resulting full cultural readjustment.

This is of course no short-term aim. Such changes will take years to realise. This does not mean that it should not be attempted however. As was clear particularly in Chapter Six, the same issues can arise eighteen years apart because the lessons have not been learned; we are not dealing with a quick fix. It is the longevity of this issue that must also be realised and appreciated as if the short-term view that has been evident continues to dominate risk and crisis management thinking, the real lessons will never be learned, let alone acted upon.

The aims of this thesis have largely been achieved through the course of this research and it is asserted that if the lessons identified here and the recommendations for the adoption of risk and crisis management methodologies are heeded, the opportunities for learning from incidents and improving the response to them are more likely to be realised.

What is clear is that this is an area where attention will continue to be focused and will constantly adapt and evolve. Human beings will continue to behave irrationally and there will always be financial constraints limiting available courses of action. But what is a downside to this research area is also its most attractive feature as it offers a genuine opportunity to examine individuals and organisations at their most vulnerable and it is arguably at this time when they are most conducive to accepting scrutiny and ultimately recommendations for change.

8.7 Contribution of this Thesis to Existing Knowledge

This research contributes to the existing body of knowledge in several ways. Firstly, it contributes to the literature in the fields of terrorism and crisis management and, to the practice within these.

Secondly, although there is much written on the subject of terrorism and about crises, very few academic resources link the theory and the practice of the two areas. This thesis addresses this under-researched link.

Thirdly, it takes a qualitative rather than a quantitative approach to the study of terrorism and crisis management and uses the sociological systems and Risk Communication methodology approaches to analyse and evaluate current practices.

The final contribution of this research is to identify new directions for future research to consider. Such directions include a large-scale research project analysing responses to smaller terrorist attacks and those which do not have such distinguishing features as the attacks assessed within this thesis. Investigation into attacks within different cultures would also be particularly valuable in light of the Risk Communication theory recommendations made here. This could provide new insights to help to identify ways to overcome cultural barriers that may impede emergency responses in the future. More research into the debriefing process following simulations and training exercises is also suggested in order to better ascertain how to capture lessons learned.

Practices and policies have clearly been improved since the events of 7/7. However, little has been changed to address the way in which lessons are learned or how the concept of preparedness is bettered. The majority of the changes have been practical changes: new ways of performing actions and improved equipment. This thesis contends that this is not enough as the underlying issues identified within this research have still not been addressed. Those concerns that the risk and crisis theory methodologies have begun to tackle are even now not dealt with by the practical changes recommended in the inquiry reports. There needs to be a paradigm shift in the way in which terrorist incidents and response to these are viewed and this thesis strongly contends that this can only be brought about through adoption and understanding of the key methodologies reviewed and recommended within this research. It is only when the existing methodological

framework is amended to reflect these recommendations that a more comprehensive analysis of events and development of the response framework will emerge.

9. Conclusion

In Chapter One, the contemporary literature on terrorism was considered to chart its evolution, causes, possible responses and the role of the media. Possible future directions for terrorism were also expounded to highlight the dynamic nature of the threat that we now face. The inclusion of this information was intended to help to develop risk and crisis management arrangements for terrorist incidents that were presented in Chapter Seven. It was proposed that terrorism mirrors global politics and hence responses must be regularly updated to keep pace with these.

Contemporary academic and government definitions of terrorism were considered historically and internationally in order to develop a more coherent and complete picture of different perceptions and interpretations of terrorism in the global context. This has potentially great implications for international co-operation and prevention of terrorist events; if we cannot agree what it is that we face and if it does constitute terrorism, then how can we improve resilience? This was echoed by Quarantelli (1995:224) in his disquiet surrounding the lack of consensus regarding the terminology of dangerous events. However, as this thesis argued, perhaps it is in fact the response that we need to agree upon and define, rather than the event itself. After all, if the act of terrorism does not fit our understanding or definitions, how are responders to choose the appropriate response?

Much of the research regarding terrorism is strongly focused on the idea that it is a different sort of risk from other forms of dangerous event that may be faced. It was argued here that such attempts to reduce the complexity and interactionist nature of the events and ignore the congruence within risk and crisis management that are clearly evident, hinders the resilience to and success of the management of the aftermath of such events; something that was clearly evident in the consideration of the July 7th bombings in Chapter Six. A seeming reluctance to learn from past experiences still appears to exist despite obvious advantages from learning from experience.

In the deliberation on the possible future direction of terrorism, it was recognised that social reform may be a valuable tool in the fight against terrorism, particularly if in partnership with improved international co-operation. A moderating influence with humanist principles as Bandura (2005) in Moghaddam and Marsella (2005:150) supports was emphasised as an important way forward in the fight against terrorism.

The focus on developing new legislation against terrorism was touched upon as an area for concern as it is argued that existing legislation is appropriate, it is the way in which it is applied which is not always the in the most effective manner. Review of the key pieces of terrorism legislation were referred to in Appendix I. From this, overall, it can be seen that the anti-terrorism laws can have a ratchet effect on the operation of the criminal justice system, where the distinction between minor and more serious offences becomes blurred in terms of their punishment, returning to a crime control model of criminal justice (McEldowney, 2005:773). It is that which this thesis does not support.

What is clear from all of the legislation is the impact that September 11th 2001 had on national and international approaches to terrorism and, most importantly, the relationship between the state and society. The important caveat underlying all of this, as Haque (2002:178) asserted, is that alternative perceptions of the causes of terrorism warrant serious consideration, not least because in order to effectively combat terrorism, it is necessary to understand the causes and motivations behind it. Without this, governments run the risk of counter-productive measures as their legislation makes terrorists "victims" of executive power (McEldowney, 2005:780); something which they cannot afford.

In concluding this chapter, a considered response was stressed as imperative to maintain credibility and to achieve success. Ultimately any government should consider what they perceive as the trigger causes of terrorism, rather than focusing on root causes that it is a dangerously simplistic view of a situation. They should also seek to agree clear definitions and include all government levels to avoid piecemeal adoption of anti-terrorism measures; three principles highlighted in Sinai's (2005) work in Bjorgo (2005:18).

In the second chapter of this thesis, literature on conceptual approaches to risk and crisis management were reviewed from the sociological perspective. Through this research and review, it was determined that the most relevant and important risk theories for the purpose of this thesis were risk communication, systems theory and that of safety culture. Each of these is equally valid and if combined, could in some cases, achieve a type of synergy whereby the results are more far reaching and have greater effect than if applied in isolation.

By understanding and incorporating these into the recommendations stemming from this research, it is intended that responders to crisis events will have a more rounded approach to the situation and greater flexibility; something which was seen to be key in such events. Arguably, incorporating such theoretical considerations may also help to prevent such instances due to increased awareness of how to create a more flexible and aware environment prior to the event occurring. This also augments understanding of how potentially, it may escalate. It is also important to consider the theoretical concepts, as Burke (2005:639) recognises that terrorism and terrorist threats to organisations and individuals are affecting organisational behaviour.

It was suggested in this chapter that Beck's view of a risk society was still highly influential however and could be considered pessimistic, rationalistic and could be better served in taking account of the differences that may exist between individuals, building on the work of Denney (2005:32). This chapter also determined that although such approaches were largely qualitative, they were still of use and furthermore, were not mutually exclusive, as some theorists would suggest. By combining two or more of these, a more comprehensive approach to understanding risk and crisis scenarios is likely, as Borodzicz (1997:254) supports.

The literature review concluded that flexibility was the key to successful risk and crisis management. The need for preparedness and familiarity with plans was also highlighted to limit the impact of the 'unknown' on individuals and thus their behaviour. As known risks were less frightening than unknown risks, it is clearly pertinent to obtain as much

information about the environment and situation as is possible. This is not helped however by the continuing debate regarding nomenclature of risks and dangerous events. The relevance and importance of organisational learning and training for crises was also found to be a vital consideration here, in order not to destabilise an organisation in times of crisis.

Following review of the crisis literature, it can be seen that the previous classifications of man-made, natural and social causation are no longer appropriate in today's environment. Due to the likelihood of multiple causations, it is almost impossible to separate these into distinct events. It was however possible to classify dangerous events as emergencies, crises and disasters and hence, their management can be tailored for the circumstances.

A mounting interest and theorisation in the field of crisis management was also increasingly apparent. This was felt to be a positive move in promoting good crisis management practice. Despite all of these positive aspects, the lack of agreement regarding terminology still poses many problems for those involved. What can be taken and learned from this chapter is that crises have identifiable phases and the identification of these enables more effective management, which should be viewed as a holistic process. They are merely times of risk and uncertainty that may not necessarily be bad. It is this change in mindset that needs to be brought about in order to capitalise on the opportunities that crises can offer.

Some clear tensions can exist between the ideal and reality of crisis management as McConnell and Drennan (2006:62) and Smith (2006) in Smith and Elliott (2006:99) highlighted. Organisations must understand the existence of such issues in order to counter them before they arise. This is a further endorsement of the value of simulation training as long as it goes beyond 'symbolic readiness', as Chapter Two discussed.

Overall, the chapter highlighted a move towards resilience, bringing together all of the components of the disaster cycle from response, to recovery, mitigation and preparedness as the most appropriate, working with communities. Despite the obvious need for a

holistic approach, this was at times undermined through government focus on particular areas rather than the process as a whole. The importance of good media relations and a long term view were also identified as two key features of successful crisis management.

Chapter Three reviewed the philosophical perspective adopted for this study, the research design and the multiple case study methodology. Justification and rationale for the chosen methods were provided with express attention given to validity, reliability, generalisation and ethical considerations. The highly emotive nature of the topic under consideration was also reflected upon together with the implications for the researcher in undertaking such a study.

Chapters Four to Six of this thesis comprised the empirical section of this thesis and were secondary case studies considering unique terrorist attacks that posed particular problems for those tasked with responding to them. Each provided a strong descriptive framework which helped to identify valuable potential lessons, furthering and adapting Toft's (1994) Isomorphic Learning theory, introduced in Chapter Two. All three case studies were secondary analyses of the Tokyo Sarin attack in 1995, the World Trade Center attack in 2001 and the July 7th bombings in 2005. Their inclusion allowed analysis and a deeper understanding of the issues associated with responding to terrorist incidents that helped to produce more robust event preparedness. Each incident demonstrated ill-structure and socio-technical weaknesses and interactions that went unnoticed or were poorly managed, arguably leading to the events included here.

Although each scenario was quite different, it could be argued that each was largely successfully managed in the circumstances although there was room for improvement in each of the contexts. Both good and bad practice can clearly be identified and used for future reference: the value of simulation training in the 9/11 evacuation procedures, attempts to proactively use the media in 7/7 and keeping people moving in the Sarin case study were all examples of some good practice, albeit misguided in some instances.

Chapter Four was based on the report and investigation of the Sarin attack in Tokyo, 1995. The study analysed how the incident rapidly evolved from an emergency, if the definitions in Chapter Two are applied, to a crisis with the potential for disaster. Many lessons are gleaned here, cementing its utility as a model for crisis learning and highlighting the utility of Turner's Incubating Disaster Aetiology.

The Japanese authorities' response to focus on dismantling the cult rather than pretending that the vast transport network could be realistically protected, was a brave step in terms of public relations; better communications with the public would however have been advisable here.

The Sarin attack response does however reinforce the suggestion that a generic disaster response with an adaptive and flexible range of additional measures, is an advantageous approach.

Chapter Five considered the World Trade Center attacks on 9th September 2001. The symbolism of the attack changed the face of the global perceptions of terrorism and heralded a new approach to both performing acts of terrorism and responding to them. However, the lessons learned from this event highlight a central point in improving resilience and the response to such attacks: planners should not overestimate the complexity and resources required by terrorists to carry out an attack as 9/11 was perpetrated with only box cutters, some flying experience and an ability to book tickets and read airline timetables, as Borodzicz (2005:12) asserted. By overestimating the complexity and preparedness required, potential opportunities for those who may seek to carry out such attacks may be overlooked. It would seem that the KISS (Keep It Simple Stupid) anagram so often propounded by management gurus may equally be applicable to both terrorists and those responsible for safeguarding our countries alike.

Perhaps one of the strongest lessons to learn from this incident was how invaluable the support of senior management both in the immediate aftermath and following the attacks

really was. If we are to strengthen resilience this support is vital to ensure flexibility and robustness of response and preparation plans.

Chapter Six contemplated the 7th July 2005 bombings in London. Review of the comprehensive Inquiry Report suggested that one of the key lessons to be learned from the attack was that emergency plans should focus on the individuals rather than impersonal incidents (Review Committee Report, 2006:120); something that was also echoed in Chapters Four and Five.

The confusion that occurred at the incident sites around London highlighted the importance of the three key skills for crisis management, those of declaration, communication and negotiation (Borodzicz, 2005:156). Had these more clearly been understood and applied, the management of events may have been less problematic. However, the purpose of the analysis of these case studies, as discussed earlier in this thesis, is not to retrospectively advise those involved with the management of these events but instead to learn lessons for the future management and preparedness for such incidents and it is the proactive stance that should be taken forward from this analysis.

It is the researcher's intention that these case studies should be viewed together as a learning process, with a nascent theoretical core that runs throughout this thesis and can be seen to work towards building a sound management framework.

The third and final part of this thesis presented the findings from this research. Chapter Seven presented the conceptual groundings for this thesis and included a conceptual model and a theoretical model. The models related the thinking behind the research with the literature and thesis findings in order to link them more fully. Discussion of the models was included to further justify the recommendations and conclusions drawn from this work.

In Chapter Eight, the lessons learned from analysis of the literature and the three case studies on terrorist attacks were brought together. It was contended that the adoption of

both Isomorphic Learning Theory and Risk Communication Theory by those responsible for designing response frameworks for such incidents would result in more effective methodologies. This was supported by the lack of evidence of learning from previous crises and disasters and illustration of how such theories could be utilised.

The challenges facing organisations were also recognised and it was conceded that any changes would not happen in the short-term. However, it was argued that the potential benefits of such an approach would yield such benefits that adoption of this was still desirable. Overall it was recognised that a cultural change was required regardless of organisation size, sector or age and that although some organisations appear to be learning from crises, this is largely only superficial and classed as first-order learning.

The challenges of responding to the current terrorist threat are not to be underestimated. Today, terrorism is directed at people rather than governments as it aims to bring about a change in lifestyle and beliefs. As Newman in Freilich and Newman (2009:42) recognises:

> 'modern terrorists cannot lose a war in the traditional sense, since the fight is not over occupying territory but rather over occupying the minds of people everywhere'.

If not for any other reason, the importance of Risk Communication and media skills are clear for all to appreciate.

The continuing failure of organisations to learn from crisis has many costs ranging from social to financial as Elliott (2009:157) recognises. He argues that it is the separation of policy development from practice that is the major contributor to a failure to learn from crises and the cause of a seeming lack of an all-embracing framework of organisational learning (Elliott, 2009:158). The evidence following the research within this thesis would appear to concur. It is also the lack of apparent ability for organisations to 'unlearn' bad practice that is a major hindrance to learning from crises (Elliott, 2009:161).

At the start of this thesis, it was acknowledged (at 2.3.3) that it is impossible to eliminate risk: it can only be minimised and if it is seemingly removed, it has merely been transferred elsewhere. The probability of risk is therefore, always equal to 1. For this reason, a long-term view of risk, crisis and terrorism management must be taken. Without this, the same issues will keep arising and the same inquiries will come to the same findings. A paradigm shift in how crisis management and the response to terrorist incidents are viewed is therefore imperative: second-order organisational learning must be achieved.

Overall it can be recognised that an awareness and understanding of conceptual approaches to the management of dangerous events can broaden the toolkit available to those responsible for preparedness and responding and perhaps, they are no longer the sole domain of academics.

Bibliography

Adams, J.G.U. (1995). *Risk*. London: UCL Press

Alavosius, M.P., Braksick, L.W., Daniels, A.C., Harshbarger, D., Houmanfar, R. and Zielstra, J. (2002). The Impact of Terrorism on the US Economy and Business. *Journal of Organizational Behavior Management*. 22, 3-2

Alexander, D. (2002). *The Principles of Emergency Planning*. Harpenden: Terra Publishing

Alexander, D. (2005). Towards the Development of a Standard in Emergency Planning. *Disaster Prevention and Management*. 14(2), 158-175

Alvarez, A. and Bachman, R. (2008). *Violence: The Enduring Problem*. London: Sage Ltd

ANSCI (1993). *Human Factors Study Group*. Third Report: Organising for Safety. London: Stationery Office

Apgar, D. (2006). *Risk Intelligence: Learning to Manage What We Don't Know*. Boston: Harvard Business School Publishing

Atlantic Blue Tests International Readiness. 15 April 2005. *The Job*. Metropolitan Police Service. 38 (951). Retrieved 24 April 2010 from http://www.met.police.uk/job/job951/live_files/2.htm

Attacks on London Transit System. (n.d.). Retrieved on 22 July 2010 from www.globalsecurity.org/security/ops/images/london-jul7.htm

Augustine, N.R. (1995). Managing the Crisis You Tried to Prevent. *Harvard Business Review*. Boston: HBR

Bandura, A. (1998). Mechanisms of Moral Disengagement. In W. Reich (Ed). *Origins of Terrorism: Ideologies, Theologies and States of Mind*. Washington D.C.: Woodrow Wilson Center

Barkan, S.E. and Snowden, L. L. (2001). *Collective Violence*. Boston: Allyn and Bacon

Barnett, A. And Bright, M. (2004, 21 April) Straw Ordered Probe Weeks Before Coup Bid. Retrieved 10 April 2010 from http://www.guardian.co.uk/politics/2004/nov/21/uk.equatorialguinea

Beaton, R., Stergachis, A., Oberle, M., Bridges, E., Nemuth, M. and Thomas, T., (2005) The Sarin Gas Attacks on the Tokyo Subway – 10 Years Later/Lessons Learned, *Traumatology.* 11(2) June 2005, 103-119

Beck, U. (1992). *Risk Society: Towards a New Modernity*. London: Sage Publications

Beckett, M. Rt Hon (2000) Modernising Government in Action: Realising the Benefits of Y2K, London: The Stationery Office, Cm 4703

Bernhardt, J. (1970). Society *and the Assassin: A Background Book on Political Murder*. New York: MacMillan Publishing

Birkland, T. (2006) *Lessons of Disaster*. Washington: Georgetown University Press

Bjorgo, T.(2005). *Root Causes of Terrorism*. London: Routledge

Blalock, G. Kadiyali, V. and Simon, D.H. (2005, 10 February) The Impact of 9/11 on Road Fatalities: The Other Lives Lost to Terrorism. Retrieved 2 February 2009 from http://ssrn.com/abstract=677549 or doi:10.2139/ssrn.677549

Boin, A. and McConnell, A (2007) Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. 15(1) 50-59 *Journal of Contingencies and Crisis Management*

Borodzicz, E.P. (1997). *Risky Business: Crisis Simulations Examined in the Context of the Safety People*. PhD, London University

Borodzicz, E.P. (1999) The Terminology of Dangerous Events: Implications for Key Decision Maker Training. *International Journal of Police Science and Management*. 2(3), 348-359

Borodzicz, E.P. (2005). *Risk, Crisis and Security Management*. Chichester: John Wiley and Sons Ltd

Bousquet, A. (2009). *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. London: Hurst Publishers Ltd

Bryman, A. and Bell, E. (2007). *Business Research Methods*. Oxford: Oxford University Press

Burke, R.J. (2005) International Terrorism and Threats to Security: Implications for Organizations and Management. *Disaster Prevention and Management*.14(5) 639-643

Clarke, R.V.G. and Newman, G.R. (2006). *Outsmarting the Terrorists*. New York: Praeger Publishers

Cohen, L. and Manion, L. (1989). *Research Methods in Education*. London: Routledge

Collis, J. and Hussey, R. (2003). *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*. (2nd ed). Basingstoke: Palgrave Macmillan Ltd.

CONTEST2. (2006). *A Strategy to Counter the Threat to the United Kingdom and to Overseas Interests from International Terrorism*. London: The Home Office

Coolican, H. (1992). *Research Methods and Statistics in Psychology*. London: Hodder and Stoughton

Corbin, J. and Strauss, A. (2007). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks: Sage

Covello, V.T. (1991) 'Risk Comparisons and Risk Communication: Issues and Problems in Comparing Health and Environmental Risks' in R.E. Kasperson & P.J.M. Stallen (eds) Communicating Risks to the Public, Dordrecht: Kluwer

Cox, S. and Tait, R. (1991). *Safety, Reliability and Risk Management*. London: Butterworth Heinneman,

Crenshaw, M. (1990). The Logic of Terrorism: Terrorist Behaviour As A Product of Strategic Choice In W. Reich Ed (1998) Origins of Terrorism: Ideologies, Theologies and States of Mind, Washington D.C.: Woodrow Wilson Center

Crenshaw, M. (1992) in *Psychology of Terrorism* (2010) Center for International Research on Terrorism. Retrieved 22 March 2010 from www.terrorismresearchcenter.org/psych-of-terrorism.html

Crenshaw, M. (1995). (Ed.) *Terrorism in Context*. Pennsylvania: Pennsylvania State University Press

Cresswell, J.W. (1998). *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*. Thousand Oaks: Sage

Dake, K. (1991) Myths of Nature: Culture and Social Constructions of Risk: An Analysis of Worldviews and Cultural Biases. *Journal of Social Issues*. 48(4), 21-37

Davis, R. and Owen, D. (1998). *New Media and American Politics*. New York: Oxford University Press

Denney, D. (2005). *Risk and Society*. London: Sage Publications Ltd

Dombrowsky, W. R. (1995) 'Again and Again: Is a Disaster What We Call "Disaster"? Some Conceptual Notes on Conceptualizing the Object of Disaster Sociology' *International Journal of Mass Emergencies and Disasters*, 13(3):241-254.

Douglas, M. & Wildavsky, A. (1982). *Risk and Culture: An Essay on the Selection of Technological and Environmental Danger*. Berkley: California University Press

Dubai Hamas Killing Pledge by UK Foreign Secretary, (2010, 18 February). Retrieved 25 February 2010 from http://news.bbc.co.uk/1/hi/world/middle_east/8521246.stm?ls

Dynes, R. (1994) Community Emergency Planning: False Assumptions and Inappropriate Analogies. *International Journal of Mass Emergencies and Disasters*. 12(2) 141-158

Dynes, R. and Drabek, T. (1994) 'The Structure of Disaster: Its Policy and Disciplinary Implications', *International Journal of Mass Emergencies and Disasters*, 12(1):5-24.

Ehrenfeld, R. (1990). *Narco-Terrorism*. New York: Basic Books

Elliott, A. (2002). Beck's Sociology of Risk: A Critical Assessment. *Sociology*. 36(2) 293-315

Elliott, D. (2009) The Failure of Organizational Learning from Crisis – A Matter of Life and Death? *Journal of Contingencies and Crisis Management*. 17(3), 157-168

Elliott, D. (2008) *Modelling Learning from Crisis*, Proceedings of the British Academy of Management. Harrogate. September 2008

Elliott, D. and Smith, D. (1993) Learning from Tragedy: Sports Stadia Disasters in the UK. *Industrial and Environmental Crisis Quarterly*. 7(3) 205-230

Elliott, D. and Smith, D. (2006). Patterns of Regulatory Behaviour in the UK Football Industry. *Journal of Management Studies*. 43(2), 291-318

Fennell, D. (1988). *Investigation into the King's Cross Underground Fire*. (Dept. of Transport), London: HMSO

Fierke, K.M (2007). *Critical Approaches to International Security*. Cambridge: Polity Press

Fink, S. (2002). *Crisis Management: Planning for the Inevitable*. Lincoln, N.E,: iUniverse Inc

Franklin, J. (Ed). (1998) *The Politics of Risk Society.* Oxford: Polity Press

Freilich, J.D. and Newman, G.R. (Eds.) (2009). *Reducing Terrorism Through Situational Crime Prevention*. New York: Criminal Justice Press

Friedland, N. (1992). Becoming a Terrorist: Social and Individual Antecedents. In L. Howard. (Ed.) *Terrorism: Roots, Impact and Responses*. New York: Praeger

Frosdick, S. (1995) 'Organisational Structure, Culture and Attitudes to Risk in the British Stadia Safety Industry'. *Journal of Contingencies and Crisis Management*. 3(1):43-58

Gilbert, C. (1995). Studying Disaster: A Review of the Main Conceptual Tools' *International Journal of Mass Emergencies and Disasters*, 13(3):231-40

Global Terrorist Incident Report Map. Retrieved 19 July 2010 from https://wits.nctc.gov/FederalDiscoverWITS/index.do?t=Map&N=0

Global Security (2001) World Trade Center – New York City 9-11 Terrorist Attacks. Retrieved 2 February 2007 from www.globalsecurity.org/eye/wtc.htm

Guelke, A. (2009). *The New Age of Terrorism and the International Political System*. London: I.B. Tauris and Co. Ltd.

Gumm, P. (2007, 7 August) New London CCTV Control Room Designed to Thwart Terrorists. Retrieved 11 May 2010 from

Gundel, S. (2005) Towards A New Typology of Crises. *Journal of Contingencies and Crisis Management*. 13(3), 106-115

Hayenhjelm, M. (2006) Asymmetries in Risk Communication. *Risk Management: An International Journal*. (2006), 8, 1-15

Healy, S. (2006) Risk as Embodied Circumstance: Some Organisational Observations. *Risk Management*. (2006), 8, 77-91

Heymann, P.B. (1998). *Terrorism and America: A Commonsense Strategy for a Democratic Society*. Cambridge: MIT Press

Hillyard, M.J. (2000). *Public Crisis Management: How and Why Organizaions Work Together to Solve Societies Most Threatening Problems*. Lincoln: Writers Club Press

Hoffman, B. (1998). *Inside Terrorism*. New York: Columbia University Press

Holden, M.T. and Lynch, P. (2004) Choosing the Appropriate Methodology: Understanding Research Philosophy. *The Marketing Review*. 4, 397-409

Home Office Press Release (2005) Atlantic Blue – International Counter-terrorism Exercise, 17th March 2005

Horlick-Jones, T. (1990) *Acts of God? An Investigation into Disasters,* Association of London Authorities.

Hussey, J. and Hussey, R. (1997). *Business Research: A Practical Guide For Undergraduate and Postgraduate Students*. Basingstoke: Palgrave MacMillan

ICAEW (Institute of Chartered Accountants in England and Wales) (1999) *Internal Control: Guidance for Directors on the Combined Code*. London: ICAEW

Ignatief, M. (2004). *The Lesser Evil*. Princeton: Princeton University Press

Intelligence and Security Committee Report into the London Terrorist Attacks on 7 July 2005, Cm6785, (2006) London: TSO

Irwin, A. (1989) 'Deciding About Risk: Expert Testimony and the Regulation of Hazard' in J. Brown (Ed.) *Environmental Threats: Perception, Analysis and Management*, London: Belhaven Press

Irwin, A. (1995). *Citizen Science: A Study of People, Expertise and Sustainable Development*. London: Routledge

Jenkins, B.M. and Gersten, L.N., (2001) Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices, September 2001, San Jose: Mineta Transport Institute, College of Business, San Jose State University

Johnson, P. (2004) Analytic Induction in C. Cassell and G. Symon (Eds) *Essential Guide to Qualitative Methods and Analysis in Organizational Research.* London: Sage. pp165-179

Kahneman, D. and Tversky, A. (1979) 'Prospect Theory: An Analysis of Decision Making Under Risk', *Econometrica*, 47(2):263-291.

Kaplan, D.E. and Marshall, A. (1996). *The Cult at the End of the World*. London: Crown

Kasperson, R.E & Stallen, P.J.M. (Eds.) (1992) *Communicating Risks to the Public*. Dordrecht: Kluwer

Kegley, C.W. (Ed.) (1990). *International Terrorism: Characteristics, Causes, Controls*. New York: St Martin's

Kelly, R.J. and Maghan, J. (Eds.) (1998) *Hate Crime: The Global Politics of Polarization*. Carbondale: Southern Illinois University Press

King, N. (2004) Using templates in thematic analysis of text, in C. Cassell and G. Symon (Eds) *Essential Guide to Qualitative Methods and Analysis in Organizational Research.* London: Sage. pp. 256-270

King's Fund (1992) *Too Many Cooks.* London: King's Fund.

Lagadec, P. (1982) *Major Technical Risk: An Assessment of Individual Disasters*, Pergammon Press.

Lakha, R. and Moore, T. (Eds.) (2002) *Tolley's Handbook of Disaster and Emergency Management: Principles and Practice*. London: Reed Elsevier Ltd.

Laqueur, W. (1999). *The New Terrorism: Fanatacism and Arms of Mass Destruction* New York: OUP

Lee, T. (1993). 'Seeking a Safety Culture'. *ATOM Journal* (429):20-23.

Lia, B. and Skjolberg, K. (2004) *Causes of Terrorism: An Expanded Review of the Literature*. Norwegian Defense Research Establishment

London Assembly Report of the 7 July Review Committee (2006) June London: Greater London Authority

London Resilience Forum (2006). Looking Back Moving Forward: The Multi-Agency Debrief, Lessons Identified and Progress Since the Terrorist Events of 7 July 2005. (September 2006).Retrieved 02 February 2010 from http://www.continuitycentral.com/news02800.htm

Lopes, L.L. (1987) 'Between Hope and Fear: The Psychology of Risk'. *Advances in Experimental and Social Psychology.*, (20):255-295.

Lupton, D. (1999). *Risk*. London: Routledge

Martin, G. (2010). *Understanding Terrorism: Challenges, Perspectives and Issues*. London: Sage Publications

Martin, G. (2003). *Understanding Terrorism: Challenges, Perspectives and Issues*. London: Sage Publications

Maule, A.J. (2004). Translating Risk Management Knowledge: The Lessons to be Learned from Research on the Perception and Communication of Risk. *Risk Management: An International Journal*. (2004) 6 (2), 17-29

McConnell, A. and Drennan, L. (2006). Mission Impossible? Planning and Preparing for Crisis. *Journal of Contingencies and Crisis Management*. 14(2), 59-70

McEldowney, J.F. (2005) "Political Security and Democratic Rights". *Democratization*. 12(5),766-782

Miles, M.B. and Huberman, A.M. (2004). *Qualitative Data Analysis: An Expanded Source Book*. London: Sage Publications

Mileti, D. (1999). *Disasters by Design: A reassessment of Natural Hazards in the United States*, Washington D.C: Joseph Henry Press

Moghaddam, F.M. and Marsella, A.J. (2004). *Understanding Terrorism: Psychosocial Roots, Consequences and Interventions*. Washington D.C.: American Psychological Association

Musson, G. (2004) Life Histories in C. Cassell and G. Symon (Eds) *Essential Guide to Qualitative Methods and Analysis in Organizational Research.* London: Sage. pp. 34-44

N.A. UK Terrorist Threat Level Raised to Severe, (2010, 23 January 2010). Retrieved 2 February 2010 from http://news.bbc.co.uk/1/hi/uk/8476238.stm

O'Brien, G. and Read, P. (2005). Future UK emergency management: new wine, old skin? *Disaster Prevention and Management.* 14(3) pp. 353–361.

OECD (1987) *Nuclear Agency Chernobyl and the safety of Nuclear Reactors in OECD Countries*. Paris: OECD

OECD (2003) *Emerging Risks in the 21st Century: An Agenda for Action*. Paris: OECD

Paletz, D.L. and Schmid, A.P. (1992). *Terrorism and the Media*. Newbury Park: Sage Publications

Pangi, R. (2002) Consequence Management in the 1995 Sarin Attacks on the Japanese Subway System. *Studies in Conflict and Terrorism*. 25, 2002, 421-448

Pargeter, A. (2008). *The New Frontiers of Jihad: Radical Islam in Europe*. London: I.B. Tauris and Co. Ltd.

Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books Inc.

Perrow, C. (2006) Disasters Ever More? Reducing US Vulnerabilities in H. Rodriguez, Quarantelli, E.L. and R.R. Dynes. (Eds.) *Handbook of Disaster Research*. New York: Springer, pp521-533

Perry, R.W. and Lindell, M.K. (2006). *Emergency Planning*. Hoboken: John Wiley and Sons

Perry, R.W. and Quarantelli, E.L. (2004). *What is a Disaster? New Answers to Old Questions*. Philadelphia: Xlibris Press

Peterson, D.M. and Perry, R.W. (1999). The Impact of Disaster Exercises on Participants. *Disaster Prevention and Management*. 8(4), 241-254

Petts, J., Horlick-Jones, T., Murdock, G., Hargreaves, D., McLachlan, S. and Lofstedt, R. (2001). *Social Amplification of Risk: The Media and the Public*. Contract Research Report 329, Health and Safety Executive

Pidgeon, N. (1991) 'Safety Culture and Risk Management in Organisations'. *Journal of Cross-Cultural Psychology*. 22(1):129-140.

Pidgeon, N., Kasperson, R.E. and Slovic, P. (Eds) (2003). *The Social Amplification of Risk*. Cambridge: Cambridge University Press

Post, J.M. (1998) Terrorist Psycho-Logic: Terrorist Behaviour as a Product of Psychological Forces in W. Reich. (Ed.) *Origins of Terrorism: Psychologies, Ideologies, States of Mind*. Washington D.C.: Woodrow Wilson Center

Powell, D.A. and Leiss, W. (1997). *Mad Cows and Mother's Milk: The Perils of Poor Risk Communication*. Canada: McGill-Queen's University Press

Quarantelli, E. L. (1995) 'What Is a Disaster'. *International Journal of Mass Emergencies and Disasters*. 13(3):221-229.

Quarantelli, E.L. (1992) The Case for a Generic Rather than Agent-specific Approach to Disasters. *Disaster Management*. 2, 191-196

Reich, W. (Ed.) (1998). *Origins of Terrorism: Psychologies, Ideologies, States of Mind*. Washington D.C.: Woodrow Wilson Center

Renn, O. (2003) Social Amplification of Risk in Participation: Two Case Studies, In N. Pidgeon, R.E. Kasperson and P. Slovic (Eds.) *The Social Amplification of Risk*. Cambridge: Cambridge University Press

Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World*, London: Earthscan

Report of the 7 July Review Committee, London Assembly (2006) London: Greater London Authority

Report of the Official Account of the Bombings in London on 7th July 2005, (May 2006) HC1087, London: TSO

Riege, A.M. (2003) Validity and Reliability Tests in Case Study Research: A Literature Review with 'Hands-on' Applications for Each Research Phase. *Qualitative Market Research: An International Journal*. 6(2), 75-86

Robertson, S. (2006, 6 July) News Analysis: London's Tourism Revival Post-7/7. *PR Week*. Retrieved 1 May 2010 from http://www.prweek.com/uk/news/search/567823/News-Analysis-Londons-tourism-revival-post-7-7/

Robson, C. (2002). *Real World Research*, Oxford: Blackwell Publishing

Rosenthal, U. (1996) Crisis Management: Second-order Techniques. In T. Horlick-Jones and A. Amendola. (Eds.) *Crisis Management and Decision Making*. The Netherlands: Kluwer

Roux-Dufort, C. (2007) Is Crisis Management (Only) a Management of Exceptions? *Journal of Contingencies and Crisis Management*. 15(2)

Royal Society Group (1992). *Risk: Analysis, Perception and Management*. London: The Royal Society

Saunders, M. Lewis, P. and Thornhill, A. (2009). *Research Methods for Business Students*. London: Pearson Education

Schmid, A.P. and Jongman, A.J. (1988). *Political Terrorism*. Amsterdam: North Holland

Schneir, B. (2006). *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York: Springer

Sellers, K.G. (2002). The Perception of Risk. *Catalyst*. 3(5), 18-22

Sheffi, Y. (2001) Supply Chain Management Under the Threat of International Terrorism. *International Journal of Logistics Management*. 12, 1-11

Shrivastava, P. (2005). Managing Risk in the Age of Terror. *Risk Management: An International Journal*. 7(1), 63-70

Sikich, G.W. (1993). *It Can't Happen Here: All Hazards Crisis Management Planning*. Tulsa, OK: PennWell Books

Silke, A. (2004). *Research on Terrorism: Trends, Achievements and Failures*. Frank Cass Publishers

Simonsen, C.E. and Spindlove, J.R. (2000). *Terrorism Today: The Past, The Players, The Future*. Upper Saddle Rive: Prentice Hall

Sjoberg, L. (2003). *Trust and Antagonistic Relationships*. Paper presented at the Annual Meeting of the Society for Risk Analysis. Baltimore, MD, December 2003

Sjoberg, L. (2005). The Perceived Risk of Terrorism. *Risk Management: An International Journal*. 7(1), 43-61

Slovic, P. (1987) 'Perceptions of Risk', *Science*, (236):280-285

Slovic, P., Fischoff, B. and Lichenstein, S. (1980) Facts and Fears: Understanding Perceived Risks. In R.C. Schwing and W.A. Albers (Eds.) *Societal Risk Assessment*. New York: Plenum Press

Smith, D. and Elliott, D. (Eds.) (2006). *Key Readings in Crisis Management: Systems and Structures for Prevention and Recovery*. London: Routledge

Starbuck, W. and Farjoun, M (Eds.) (2005). *Organization at the Limit*. New York: Blackwell Publishing

Suder, G.G.S. (Ed.) (2006). *Corporate Strategies under International Terrorism and Adversity*. Gloucester: Edward Elgar Publishing Ltd

t' Hart, P. (1993). Symbols, Rituals and Power: The Lost Dimension in Crisis Management. *Journal of Contingencies and Crisis Management*. 1(1), 36-50

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (2004) New York: W.W. Norton and Company Inc.

Thompson, M., Ellis, R. and Wildavsky, A. (1990) *Cultural Theory*, Westview, Boulder

Thorpe, R. Easterby-Smith, M., Lowe, A. and Jackson, P.R. (2008). *Management Research*. London: Sage

Tissington, P. and Flin, R. (2005). Assessing Risk in Dynamic Situations: Lessons from Fire Service Operations. *Risk Management: An International Journal*. 7(4), 43-51

Tobin, G.A. (1999) Sustainability and Community Resilience: The Holy Grail of Hazards Planning? *Environmental Hazards.* Vol 1 13-25

Toft, B. and Reynolds, S. (1994). *Learning from Disasters: A Management Approach*. Oxford: Butterworth Heinemann

Townsend, M. and Hinsliff, G. (2005, 10 July) Anti-terror Drill Revealed Soft Targets in London. *The Guardian*. Retrieved 11 May 2010 from www.guardian.co.uk/uk/2005/jul/10/july7.uksecurity2

Trist, E.L. and Bamforth, K.W. (1951) Some Social and Psychological Consequences of The Longwall Method of Coalgetting. *Human Relations*. 4(1)

Turner, B. (1978). *Man-made Disasters*. London: Wykeham

Turner, B. (1994) 'Flexibility and Improvisation in Emergency Response' *Disaster Management: Journal of Contingency Planning for Large Scale Emergencies* 6(2): 85-89

Turner, B.A. and Toft, B. (2006) in D.Smith, and D. Elliott. (Eds.). *Key Readings in Crisis Management: Systems and Structures for Prevention and Recovery*. pp193-204 London: Routledge

UK 'Number One al-Qaeda Target'. (2006, October 19). Retrieved 20 November 2008, from http://news.bbc.co.uk/1/hi/uk/6065460.stm

UK resilience (2003) Capabilities Programme available at www.ukresilience.info/contingencies/capabilities.htm. Retrieved 4 April 2009

UK resilience (2005) available at www.ukresilience.info/home.htm. Retrieved 14 April 2009

United Nations (2005). *Know Risk*, Geneva: Tudor Rose

Wahlberg, A.A.F. and Sjoberg, L. (2000) Risk Perception and the Media. *Journal of Risk Research*. 3(1), 31-50

Waring, A. and Glendon, A.I. (1998) *Managing Risk: Critical Issues for Survival and Success into the 21st Century*. London: International Thompson Business Press

Weimann, G. and Winn, C. (1994). *The Theater of Terror: Mass Media and International Terrorism*. New York, Longman

Wester Herber, M. (2004). *Talking To Me? Risk Communication to a Diverse Public*. Doctoral Dissertation. Orebro University

Whittaker, D. (2004). *Terrorists and Terrorism in the Contemporary World*. London: Routledge

Whittaker, D.J. (Ed.) (2002). *The Terrorism Reader*. New York: Routledge

Wilcox, L. (1996) What is Extremism? Style and Tactics Matter More Than Goals. In J. George and L. Wilcox (Eds.) *American Extremists: Militias, Supremacists, Klansmen, Communists and Others on the Fringe*. New York: Amherst

Wilde, G. (1982). 'The Theory of Risk Homeostasis: Implications for Safety and Health'. *Risk Analysis*. (2):209-225

Wolf, F. and Sampson, P. (2007). Evidence of an Interaction Involving Complexity and Coupling as Predicted by Normal Accident Theory. *Journal of Contingencies and Crisis Management*. 15(3)

Worcester, K, Bermanzohn, S.A. and Ungar, M. (Eds.). (2002). *Violence and Politics: Globalization's Paradox*. New York: Routledge
www.info4security.com/story.asp?storycode4113985

Wynne, B. (1992). Risk and Social Learning: Reification to Engagement, In S. Krimsky and D. Golding (Eds.). *Theories of Risk*. New York: Praeger Publishers

Yin, R.K. (1994).Discovering the Future of the Case Study in Evaluation Research. *Evaluation Practice*. 15, 283-290

Yin, R.K. (2009). *Case Study Research: Design and Methods*. London: Sage Ltd

Zenko, M. (2009, 30 June) Collateral Damage in Afghanistan is Unavoidable. *The Guardian*. Retrieved 12 March 2010 from www.guardian.co.uk/commentisfree/cifamerica/2009/jun/24/mcchrystal-usa-afghanistan-air-attacks

Appendices

Appendix I: Terrorism Legislation: A Consideration

A1.1 Introduction

This appendix will consider the current legislation in place in the UK to address terrorism and terrorist activity. It will describe the four main Acts and how they came to evolve, as well as highlighting legislation that they replaced. In addition, the Civil Contingencies Act 2004 (c.36) will be reviewed as it established key procedures and responsibilities in civil defence, including in response to terrorist acts. Allied to the legislation is London's Strategic Emergency Plan which is the strategic response to emergency events. The document lays down protocols and plans for such events and as such, should be considered with the legislation. This will be considered at the end of the chapter and will be used to inform the interviews with key responders to the 7th July 2005 terrorist incidents.

It is intended that this appendix will exemplify the parliamentary provisions for managing and preventing terrorist acts, in order to highlight the legislative resilience available to the authorities for coping with such matters. It will therefore not describe every part, schedule and subsection but will instead highlight that which is directly relevant to the issue of resilience to terrorism. As McEldowney (2005:772) commented, the UK's approach to terrorism has developed along both an idealistic and a pragmatic approach, the former of which emphasises due process, justice equality and the democratic process. The latter has a much stronger focus on the authoritarian processes which support the sovereignty of Parliament. This can clearly be seen in the three distinctive threads that run through the terrorism legislation.

The first is the clear aim to differentiate between supporters of terrorism and those active terrorists, therefore creating a clear distinction between terrorist and criminal acts. The second is to enact strong laws that aim to reduce the terrorist threat and make it easier for the law enforcement agencies to infiltrate terrorist groups. The third is the attempt to balance both the needs of the security forces with the crucial need to develop political dialogue. The result of this has been the creation of a Human Rights Commission,

constitutional reforms, police reforms and changes to laws against religious discrimination, among other measures (McEldowney, 2005:773).

A1.2 Legislative Background

Prior to the Terrorism Act 2000(c.11) (the TACT), the Anti-Terrorism, Crime and Security Act 2001 (c.24) (the ATCSA), the Prevention of Terrorism Act 2005 (c.2) (The PTA), and the Terrorism Act 2006 (c.11), most anti-terrorism legislation had been designed in response to terrorist activity connected with Northern Ireland. This legislation was largely temporary and was periodically reviewed. Similarly, emergency legislative powers were shaped by the two World Wars in addition to the Northern Ireland situation.

The Terrorism Act 2000 (c.11) was passed on 20th July 2000 and came into force on 19th February 2001. It reformed the legislation, not least through making it permanent. Previous legislation had been extended to cover certain types of international terrorism, but now all forms were covered by the Act. The main purpose of this legislation was to deal with the proscription of terrorist groups, the appeals process by which a proscription order may be challenged, offences relating to terrorist property, both used for terrorism and the proceeds of acts of terrorism, and police counter-terrorist groups (Anti Terrorist Legislation, 2006:para 3). The enactment of this Act was particularly significant as it broke the mould of operating distinct legal regimes designed to deal with Northern Irish terrorism and the rest of the UK (McEldowney, 2005:766).

Each year Parliament receives a report from an independent reviewer, Lord Carlile of Berriew QC, on the use of the Act in order to monitor its effectiveness and to ensure that is being appropriately interpreted and applied.

The ATCSA was passed following the attacks on the World Trade Center, New York in September 2001. This Act built on the Terrorism Act consolidating the powers of the authorities and increasing their effectiveness in combating those involved in, or supporting, terrorist activities.

The Act has four main provisions covering terrorist funding, access to information, aviation, chemical, biological and nuclear security, immigration provisions and police powers, which will be discussed in more detail later in this chapter. The Act essentially covers asset freezing by the authorities, identity establishment by the police and access to information by the relevant authorities. The immigration provisions that made up Part 4 of the Act have been replaced by the Prevention of Terrorism Act 2005 (c.2) which was the culmination of events that began in the House of Lords in December 2004. It was then that the Law Lords delivered their ruling in the case of A v. Secretary of State for the Home Department [2004] UKHL56 and declared that s.23 of the ACTSA 2001 was incompatible with the Convention right in Article 5 of the European Convention on Human Rights (ECHR), which related to liberty of the person. This referred to the provision for the Home Secretary to detain terrorist suspects who could not be deported from the UK for legal or practical reasons (Hickman, 2005:655).

The Prevention of Terrorism Act 2005 (c.2) came into effect on 11th March 2005 and gives the Home Secretary the power to make Control Orders in respect of suspected terrorists. The Control Orders can include restrictions such as bans on internet use, tagging in order to monitor curfews, restrictions on movement and fraternising with named individuals.

On the 30th March 2006, the Terrorism Act 2006 (c.11) received Royal Assent. The Act created a number of new offences and also altered the existing legislative framework by amending the TACT 2000 in several ways. It is therefore relevant to include a review of the original TACT in order to see how it has been updated and the relevance of the changes brought about with the new Terrorism Act 2006.

To supplement the specific terrorism Acts, the Civil Contingencies Act (c.36) 2004, (CCA) replaced existing civil defence legislation and incorporated the new threat from terrorism within it. The Act received Royal Assent on 18th November 2004 and forms the backbone of civil defence and emergency planning legislative measures in the UK. The CCA is therefore also central to any review of terrorism-related legislation.

A1.3 The Terrorism Act 2000 (c.11)

This Act is the centrepiece of counter-terrorist legislation and was introduced to reflect the changing nature of the terrorist threat posed internationally, no longer just from domestic shores. Three pieces of previous legislation were reformed and extended through the introduction of this Act and were put on a permanent basis. These were the Prevention of Terrorism (Temporary Provisions) Act 1989 (c.4) (the "PTA"), the Northern Ireland (Emergency Provisions) Act 1966 (c.2) (the "EPA") and sections 1 to 4 of the Criminal Justice (Terrorism and Conspiracy) Act 1998 (c.40).

Previously, the measures in place to prevent terrorist activity and investigate it could be divided into three categories which were a power for the Secretary of State to proscribe terrorist organisations, backed by a series of offences relating to membership of these organisations or fundraising for them; other specific offences that were connected with terrorism such as training in the use of weapons for terrorist purposes; and a range of police powers (Terrorism Act 2000 Explanatory Notes, 2000: para 5).

Four specific measures were introduced in the new Act to counter terrorism. Firstly, it created new criminal offences including inciting terrorist acts, seeking or providing training for terrorist purposes at home or overseas and providing instruction and training in the use of firearms, explosives or chemical, biological or nuclear weapons.

It also proscribed certain terrorist groups and specifically ensured that international groups were included in the proscribed list. It was argued by the government that this highlighted the seriousness with which they regarded the fight against terrorism and was hoped to serve as an effective deterrent against would-be terrorists. In addition, police were given enhanced powers which included wider stop and search powers and the power to detain suspects following arrest for up to 14 days, although any longer than two days requires approval by a magistrate (Counter Terrorism Strategy, 2000: para 3)

The Act also provides temporary powers in relation to Northern Ireland but these are renewed annually and are time limited to five years. It is intended that such provisions

will not be needed indefinitely and are kept under review in the context of the security situation.

In order to better understand the provisions of the Act and to establish the powers that is bestows, a more detailed review of each of the eight parts listed below will now be discussed.

- Part 1 – Introductory
- Part 2 – Proscribed Organisations
- Part 3 – Terrorist Property
- Part 4 – Terrorist Investigations
- Part 5 – Counter-terrorist Powers
- Part 6 – Miscellaneous
- Part 7 – Northern Ireland
- Part 8 – General.

A1.3.1 Part 1 - Introductory

This Part defines terrorism for the purposes of the Act, building on that used by the PTA. Under the PTA, terrorism was "the use of violence for putting the public or any section of the public in fear" (Section 20). This was limited to terrorism relating to Northern Ireland, Irish and international terrorism. The new Act widened the definition to incorporate the new motivations such as religious and ideological motivations rather than political motives alone. In addition, actions were also covered that may not be violent acts themselves but do have a crushing impact on society were they to occur, for example interfering with water supplies (Explanatory Notes, 2000:para10). Technological advancements are also covered in subsection (2)(e) where disruption of key computer systems is also legislated for.

Within the old PTA the definition of terrorism was covered globally not just within the United Kingdom (UK); this was an implicit assumption. The new Act made this explicit to reflect the new levels of threat and its scope. Subsection (1) repeals the PTA and EPA

while subsection (2) together with Schedule 1, addresses the continuation of certain temporary provisions of the EPA until Part 7 of the Act is brought into force (Explanatory Notes ,2000: para 9).

A1.3.2 Part 2 – Proscribed Organisations

This is based on Part 1 of the PTA and Sections 30-31 of the EPA. It allows the Secretary of State to proscribe organisations and details associated offences. A list of affected organisations is included in Schedule 2 and details regarding the operation and function of the Proscribed Organisations Appeal Commission (POAC) which was established by the Act are given in Schedule 3.

The Act differed from previous legislation in several ways. Firstly, prior arrangements were separated between Great Britain and Northern Ireland. The new Act applies to the UK as a whole. Secondly, proscribed organisations no longer are only concerned with Irish terrorism but also international and domestic terrorism. Thirdly, originally, any organisation wishing to challenge the proscribed status could only do so via judicial review, which no organisation ever did. Now, application can be made to the Secretary of State and if refused, can appeal to POAC. At present, forty organisations are listed.

The matter of deproscription can be particularly important for individuals convicted of terrorist offences. If an individual was convicted in respect of an organisation which was deproscripted , as long as the offence was committed after the date of the refusal to deproscribe then in England and Wales, can appeal against the conviction. Compensation may also be available. Corresponding provision also exists for Scotland and Northern Ireland (Explanatory Notes, 2000: para 20).

Sections 11 and 12 address membership and support of organisations. Subsection 4 of Section 12 however does ensure that genuinely harmless meetings are still permitted.

A1.3.3 Part 3 – Terrorist Property

Offences relating to fundraising and other financial terrorism support are covered here, in addition to providing the court with the power to order the forfeit of any money or other property that has any link to the terrorist offence. It corresponds to Part 3 of the previous PTA which only affected Irish and particular kinds of international terrorism. Part 3 of the new legislation applies to all forms of terrorism.

In order to further reflect the changing nature of the terrorist threat, Part 3 also gives power to the police, Customs and Immigration officials to seize cash at borders (Section 25) and request that cash be surrendered in civil proceedings (Section 28). The Drug Trafficking Act 1994 (c.37) was used as the model for this within which Part 3 provides similar powers to the authorities. The Anti Terrorism Crime and Security Act 2005, Section 1, Schedule 1 has since expanded and replaced this.

The definition of terrorist property includes not only property used for terrorism but also proceeds of acts of terrorism. In addition, proceeds of acts of terrorism covers not only money stolen in a terrorist robbery, for example, but also money paid in connection with the commission of terrorist acts (Explanatory Notes, 2000: para 27). Subsection (2)(b) of Section 14 furthers this by making it explicit that any resources of proscribed organisations are also fully covered, from weapons to the money to pay rent. Any money that is seized can be detained for up to 48 hours after which application must be made for continued detention of forfeiture (Explanatory Notes, 2000:para 36). Detention can continue for up to 3 months and can then be renewed to a maximum of two years. If an individual makes a successful appeal for the return of the funds, then it will be returned together with any accrued interest (Explanatory Notes, 2000: para 38).

The issue of fundraising is an important point that legislation must address. Within the Terrorism Act 2000, Section 1(5) includes the phrase “for the purposes of terrorism” which can also be accepted to mean for the benefit of the proscribed organisation. Therefore, fundraising, using and possessing money and involvement in any sort of funding arrangements connected to a proscribed organisation have now been covered by

Sections 15-17 of the Act (Explanatory Notes, 2000: para 28). Money laundering and any other type of laundering, such as property laundering, is also addressed within Section 18.

A duty to disclose information is covered in Section 19. This is a particularly important part of the Act as without as much intelligence as possible, the fight against terrorism is made nearly impossible. Banks and other financial institutions are required to report any suspicions they may have that terrorist money is being laundered or that any of the other "terrorist property" offences are being committed. Subsection (1)(b) exists to ensure that the focus is on those suspicions that arise at work but, legal advisers' confidential information remains so and this is protected by Subsection (5). Businesses can disclose information to the police without breaching the law. Subsection (1) of Section 21 protects individuals who may innocently become involved and also those who act as informants and may have to continue to be involved with terrorist activity in order to be able to continue to provide information. In addition, as long as individuals report suspicions to the police as soon as it is reasonably practicable then they may be able, under Subsections (2-4) of Section 21 to avoid prosecution as long as they desist in their activities if asked to do so by the police. Suspicions arising at home are not covered following Lord Lloyd, differing from Section 18 of the PTA (Explanatory Notes, 2000: para 31).

A1.3.4 Part 4 – Terrorist Investigations

Part 4 addresses terrorist investigations and allows the police to set up cordons, obtain search warrants, production orders, search premises and seek explanations of items that may be found. Section 39 also creates an offence of "tipping off" in relation to a terrorist investigation to act as a deterrent. Sections 33-36 also make it an offence to breach a cordon.

A1.3.5 Part 5 – Counter-Terrorist Powers

Part 5 provides for counter-terrorist powers. Sections 14 and 15 of the old PTA made provision for the arrest and detention of terrorist suspects. Sections 41-43 of the new Terrorism Act 2000 build on these and also give the police special arrest powers. The reasoning for this is that it is claimed that experience continues to show the necessity for

provision to be made for situations where, at a point where police feel an arrest should occur, there is insufficient evidence to charge an individual, even though reasonable suspicion may exist regarding the suspect's involvement (Explanatory Notes, 2000: para 45).

Sections 42 and 43 allow police to search people liable to arrest under Section 41. Two subsections, subsection (9) of Section 41 and subsection (5) of Section 43, authorise police officers to arrest suspects under Section 41 (1) of the Act, anywhere in the UK and to search them under Section 43, which implies cross-border powers for the authorities. In terms of stop and search, police can stop pedestrians, vehicles and their occupants in order to prevent terrorist acts being committees. Authorisations have to be confirmed or amended by the Secretary of State within 48 hours else they cease to have effect. These powers are conferred under Sections 44-47 (Explanatory Notes, 2000: para 46).

A1.3.6 Part 6 - Miscellaneous

Part 6 of the Act addresses miscellaneous issues, some of which are detailed in the Government's Consultation Paper under "Ancillary Offences". These include weapons training for terrorism purposes, including recruitment for such training, directing terrorist organisations, possessing articles for terrorist purposes and incitement of overseas terrorism. In addition, provisions are also made to address extra-territorial jurisdiction and extradition in order for the UK to ratify the UN Conventions for the Suppression of Terrorist Bombings and for the Suppression of the Financing of Terrorism (Explanatory Notes, 2000: para 9.6).

Sections 54-55 of the Act address the issue of weapons training and include chemical, biological and nuclear weapons and materials. Those who are acting for non-terrorist purposes are defended from prosecution by Subsection (5) of Section 54. This would apply to the Armed Forces, for example. The evidential burden is, however, on the defendant. Subsection (1) of Section 54 has evolved from the EPA in that a recipient of weapons training is not necessary; it is enough that an individual could make weapon

instruction available for terrorist purposes, such as via the Internet (Explanatory Notes, 2000: para 51).

Section 56 of the Act is an important section as it makes is an offence to direct a terrorist organisation. The most important caveat here however, is that the organisation does not need to be listed as a proscribed organisation.

Sections 59-61 address the issue of incitement to commit acts of terrorism. These sections make it an offence not only to conspire in the UK to commit terrorist acts abroad but also to incite them. Although other parts of the Act provide for this, in addition to extra-territorial jurisdiction, this provision seeks to cover any remaining gaps in the law (Explanatory Notes, 2000: para 56).

Sections 62-64 enable the UK to meet it's obligations regarding the UN Conventions mentioned above in relation to the extradition or prosecution provisions of these Conventions.

A1.3.7 Part 7 – Northern Ireland

Part 7 relates to Northern Ireland. It provides additional Police and Army powers and regulated the private security industry in Northern Ireland. In addition, it provides for a system of non-jury trials for certain offences (Explanatory Notes, 2000: para 9.8).

A1.3.8 Part 8 - General

Part 8 contains a list of terms defined in the Act and provides general powers for police, customs and immigration officers include powers to facilitate the exchange of information between the authorities. Consequent amendments and repeals are also included under Sections 15 and 16.

It can be seen from the above that the Terrorism Act 2000 has moved to address the changing face of the terrorist threat that now faces the world. The legislation did not stop

there however and in the following year, the Anti-Terrorism, Crime and Security Act was passed to greater strengthen the United Kingdom's resilience to the terrorist threat.

The Act will now be considered.

A1.4 The Anti-Terrorism, Crime and Security Act (ATCSA) 2001

The Act received Royal Assent on 14th December 2001 in response to the terrorist attacks in the United States of America on 11th September 2001. It was intended to achieve eight main objectives which were to cut off terrorist funding, ensure that government agencies can collect and share information in order to countering the terrorist threat, streamline the relevant immigration procedures and ensure the security of the nuclear and aviation industries. In addition, it was also intended to improve the security of dangerous substances that may be targeted or used by terrorists, extend police powers available to relevant forces, ensure that the UK can meet it's European obligations to counter bribery and corruption and lastly, to update parts of the UK's anti-terrorist powers (Explanatory Notes, 2001: para 3).

The Act has five main provisions addressing terrorist funding, access to information, aviation, chemical, biological and nuclear security, immigration provisions and police powers. Overall, it is divided into fourteen parts, listed below.

- Part 1 – Terrorist Property
- Part 2 – Freezing Orders
- Part 3 – Disclosure of Information
- Part 4 – Immigration and Asylum
- Part 5 – Race and Religion
- Part 6 – Weapons of Mass Destruction (WMD)
- Part 7 – Security of Pathogens and Toxins
- Part 8 – Security of Nuclear Industry
- Part 9 – Aviation Security
- Part 10 – Police Powers

- Part 11 – Retention of Communications Data
- Part 12 – Bribery and Corruption
- Part 13 – Miscellaneous
- Part 14 – Supplemental.

A1.4.1 Part 1 - Terrorist Property

Part 1 and Schedules 1 and 2 focus on obstructing access by terrorists to their funds. These work alongside the provision in the Proceeds of Crime Bill. The provisions work to ensure that the authorities have the power to investigate and freeze funds that may be used to finance terrorism. Schedule 1 which is contained in Section 1 expands upon and also replaces the provision established in the Terrorism Act 2000 regarding the seizing and forfeiture of terrorist cash at borders. Assets can also be frozen at the start of any investigation in order that the chance that funds may be used or moved before they can be frozen is largely reduced.

For the purposes of the Act, terrorist cash is defined as that "which is intended to be used for the purpose of terrorism, cash which is or represents property obtained through terrorism" (Explanatory Notes, 2001: para 42).

Subsections 1to 3 have also now amended the Access to Justice Act 1999 so that Community Legal Service funding is available to finance proceedings under Schedule 1 (Explanatory Notes, 2001: para 45). In addition, account monitoring orders are available to the police in order to receive information on suspect accounts for a maximum of 90 days. It is now also an offence for financial institutions not to report to the authorities where there are "reasonable grounds" for suspicion (Explanatory Notes, 2001: para 6).

A1.4.2 Part 2 – Freezing Orders

Provisions have also been made in Part 2 to address the possibility of overseas governments, not just individuals, executing acts that may be detrimental to the UK economy. The chance of the threat of such an action also being a threat to either the property or life of a UK national or resident is also covered. Should such actions occur,

the Treasury is empowered to freeze the assets of the foreign government or the individual concerned. These provisions replace section 2 of the Emergency Laws (Re-Enactments and Repeals) Act 1964. In order for the Treasury to make such an order, two conditions have to be satisfied which are that firstly, the Treasury must reasonably believe that action threatening either all or part of the UK economy, or the life of property of a UK national or resident has either occurred or is likely to take place. Secondly, the persons involved must be either resident outside the UK or be an overseas government. The orders prevent funds from being made available to those specified in the order or to be of benefit to them.

The Treasury must monitor the order to determine whether it should be kept in place or amended. Any freezing order ceases to have effect two years after it was invoked (Explanatory Notes, 2001: para 54). In addition, any freezing order will cease to have effect 28 days if each House of parliament has not approved it. Freezing orders must be made by statutory instrument (Explanatory Notes, 2001: para 56).

Part 2 also enables the UK to impose sanctions in cases where it is appropriate for them to do so unilaterally, and where the United Nations (UN) or European Union (EU) has not yet agreed a course of action (Explanatory Notes, 2001: para 50).

A1.4.3 Part 3 - Disclosure of Information

Section 18 of the Act is particularly important as it affects the disclosure of information. This section provides the Secretary of State with the power to prohibit disclosure of information for the purpose of overseas criminal investigations (Explanatory Notes, 2001: para 64). Explicitly, the Act states that no obligation of secrecy prevents voluntary disclosure of information except the Data Protection Act 1998. The Commissioners must also give their authority and the disclosure should assist a criminal investigation or proceedings in the UK or abroad or to determine whether they should continue (Explanatory Notes, 2001: para 66). Once information has been disclosed, it cannot be further disclosed except for criminal investigation proceedings.

In order to build on the powers bestowed by the Terrorism Act 2000, Section 19 of the Act makes provisions to allow the disclosure of information to security and intelligence agencies and Law Enforcement Agencies by HM Revenue and Customs. In addition, provisions have been made to improve access to information held by passenger and freight carriers and the ability to share information between agencies.

A1.4.4 Part 4 – Immigration and Asylum

Sections 21-32 of Part 4 of the Act allow those who have been declared threats to national security by the Secretary of State, or suspected of being international terrorists, to be detained when they cannot be removed at that time. Regular independent review occurs but these powers will no longer have effect from the 10th November 2006.

The asylum process is also speeded up but not in breach of the 1951 Refugee Convention as suspected terrorists are not included for protection (Explanatory Notes, 2001: para 9). In addition, judicial review is also prevented for decisions made by the Special Investigation Appeals Commission (SIAC). It is, however, possible to appeal to the Court of Appeal on a point of law. Part 4 of the Act addresses Investigation and Asylum procedures and their capacity to deal with those whose presence in the UK is not regarded as conducive to the public good for national security or international relations. Other reasons of a political nature may also be valid (Explanatory Notes, 2001: para 70). A provision also now exists through the Act whereby the Secretary of State can keep fingerprints for up to 10 years, taken in particular asylum and immigration cases that previously were destroyed when the case was decided (Explanatory Notes, 2001: para 71).

Sections 21 to 23 covering certification, deportation and detention of terrorist suspects, build on the powers contained in the 1971 Immigration Act. Detention powers are extended to those instances where the Secretary of State seeks the removal of a suspected international terrorist but is not currently able to do so. It must be possible within a reasonable period else it is deemed that detention is unlawful (Explanatory Notes, 2001: para 73). In the wake of September 11th 2001, the Government decided that such

provisions are necessary in order to safeguard national security and that a public emergency exists.

To ensure that the UK is not in breach of the Human Rights Act 1998, on the 18th December 2001, the UK informed the Secretary General of the Council of Europe of a derogation from the right to liberty and security (Article 5) in order to ensure that sections 21-23 do not breach the obligations of the European Court of Human Rights (ECHR).

Public emergency is addressed through Article 15 of the ECHR which allows such a derogation to the extent that is strictly required by that emergency (Explanatory Notes, 2001: para 75).

Although sections 21 to 23 work very closely together, supporting each other within a very specific area, it is useful to consider each of the sections in turn. Section 21 enables the Secretary of State to certify an individual as a "suspected terrorist". This is defined as someone whose presence in the UK the Secretary of State reasonably believes to be a risk to national security and whom is reasonably suspected to be a terrorist. The section also defines terrorism in the same way as Section 1 of the Terrorism Act 2000. CHK. Any individual who has been certified under Section 21 may appeal within 3 months to SIAC, or after 3 months with leave from the SIAC.

Section 22 specifically addresses deportation and removal of suspects. Subsection 3 of this section details those actions which may be taken against individuals if they could not at present be removed from the UK due to practical considerations, for example, no flights are available to the country of intended removal, or if there is a point of law in question that relates to an international agreement. Article 3 of the Human Rights Act 1998 does however prevent removal of individuals where they may be at real risk of torture.

Section 23 considers detention and allows for a suspected international terrorist to be detained even though removal may be temporarily or indefinitely prevented (Explanatory Notes, 2001: para 82).

Within Section 28 exists a requirement for the appointment of a reviewer to monitor the application of sections 21-23. The Secretary of State has responsibility for the appointment. The reviewer must conduct the review within 14 months of Royal Assent and also at lease one month before the expiry date made by an order under section 29(2) (b) or (c). A report is then sent to the Secretary of State who presents it to Parliament (Explanatory Notes, 2001: para 89). The following section, section 29, again relates to the operation of sections 21-23. The Secretary of State must review these sections by order otherwise they will expire 15 months after Royal Assent. Sections 21 to 31 are also applicable in the Channel Islands and Isle of Man, following modification. An Order in Council extends these sections to the above locations.

The non-refoulement provision, Article 33(1), ensures that refugees cannot be removed if their life or freedom was threatened. However, Article 33(2) provides that if reasonable grounds exist to believe that the refugee is a danger to national security, then an exception can be made. Supplementary to this is Article 1(F) that ensures if serious grounds exist that an individual has performed an action proscribed in the Article, then the provisions of the Refugee Convention do not apply. The UN purposes and principles are included here and include acts of terrorism. Article 3(3) of the UN Security Council Resolution 1373 is often referred to which requires that countries "take appropriate measures in conformity with the relevant provisions of national and international law, including internal standards of human rights for the purpose of ensuring that the asylum seeker has not planned, facilitated or participated in the commission of terrorist acts" (Explanatory Notes, 2001: para 94).

The result of these Articles means that if both or either Article 1(F) or 33(2) applies to an individual then the Refugee Convention is not applicable and they can be removed from

the UK without contravening the Convention. Immigration provisions have now been replaced by the Prevention of Terrorism Act 2005.

A1.4.5 Part 5 – Race and Religion

Part 5 of the Act addresses race and religion. This part both amends the provisions made by the Public Order Act 1986 relating to incitement to racial hatred and also increases the maximum sentence by five years to seven years imprisonment. Provisions under the new Act now include cases where hatred is directed against groups abroad (Explanatory Notes, 2001: para 102). In addition, the Crime and Disorder Act 1998 is also amended to include offences in which religious hostility is also an element (Explanatory Notes, 2001: para 104).

A1.4.6 Part 6 – Weapons of Mass Destruction

The issue of Weapons of Mass Destruction (WMD) has become more prominent in recent years. To reflect this, Part 6 of the Act moves to considerably strengthen the existing legislation regarding chemical, nuclear and biological weapons.

One of the most important sections of the Act in Part 6 is Section 44. This section extends UK jurisdiction over offences under section 1 of the Biological Weapons Act 1978 so that if in offence is executed overseas by a UK person, then UK jurisdiction will be applicable (Explanatory Notes, 2001: para 118). Section 48 ensures that military actions are not affected.

A1.4.7 Part 7 – Security of Pathogens and Toxins

Part 7 of the Act addresses the issue of control over pathogens and toxins. Section 59 provides that should occupiers keep or use dangerous substances at premises then the Secretary of State must be notified. Managers must also disclose to the police, if requested, the details of anyone with access to those substances and also details of the security of such substances (Explanatory Notes, 2001: para 135-137).

A1.4.8 Part 8 – Security of Nuclear Industry

Civil nuclear security is directly addressed in Part 8 of the Act. In addition to updating the regulation for this, the Act also extends the jurisdiction of the UK Atomic Energy Authority Constabulary (AEAC). In practical terms, this latter point enables AEAC constables to be deployed at any licensed nuclear site, not just the UKAEA, British Nuclear Fuels and Unrenco Ltd sites. It is important to note that AEAC will not operate on defence sites, only civil installations. Their powers are applicable up to five kilometres from any site (Explanatory Notes, 2001: para153).

Importantly, sanctions have been strengthened via Part 8, against any unauthorised disclosure of sensitive information pertaining to nuclear sites, material or technology. In light of this, the Attorney General, and Attorney General for Northern Ireland must consent for any prosecution to be brought under section 79 or 80 relating to disclosure in relation to nuclear security and uranium enrichment technology respectively.

A1.4.9 Part 9 – Aviation Security

Aviation security has also been directly addressed in this Act via Part 9. This part not only relates to aircraft but also to airports and has also introduced a new offence of falsely claiming to be a security approved air cargo agent (Explanatory Notes, 2001: para 23). Increased police powers regarding this are provided through the addition at the end of Section 24(2) of the Police and Criminal Evidence Act (PACE) 1984. Although the maximum penalties for the offences are not high enough o allow for an automatic power of arrest (Explanatory Notes, 2001: para 175).

A1.4.10 Part 10 – Police Powers

Part 10 of ATCSA addresses police powers and much of it amends PACE 1984. Section 90(2) specifically builds on the powers provided by PACE through enabling police officers to take the fingerprints of an arrested person to establish or check their identity Explanatory Notes (2001:para 197). In addition, photographs can be taken without consent as long as force is not used.

In order to address the issue of face coverings, whether paint, masks or other coverings, and the problems associated with photographing individuals wearing such items, section 92 can be invoked to require the removal of these to aid in identification and to photograph them. Reasonable force is also permitted - Explanatory Notes (2001:para 199). This is furthered through section 94, although caveats are in place to try to avoid exploitation of this section through the requirement that a senior officer must give authorisation and that the senior officer must reasonably believe that activities may occur in the area that involve commission of offences and that such authorisation would prevent or control them - Explanatory Notes (2001:para 200).

Section 98 addresses the subject of the jurisdiction of the Ministry of Defence police (MDP). The MDP is a civilian force which is governed primarily by the Ministry of Defence Police Act 1987. Following the events of September 11th 2001, the limits of their jurisdiction were extended. Section 2 of the 1987 Act was amended in order to provide for this. MDP also had additional jurisdiction in relation to defence personnel. Originally, this was limited to offences by defence personnel, now, subsection (3) extends it to offences against defence personnel (Explanatory Notes, 2001: para 250).

Section 99, adds a new section (2A) in the 1987 PACE Act, which allows the MDP to provide assistance if chief police officers request it, to enable a force to meet special demands on their resources. In such circumstances, MDP will work under the direction of the chief officer of the force (Explanatory Notes, 2001: para 249).

The British Transport Police (BTP) have similar jurisdiction to the MDP under the ATCS Act by virtue of sections 98 to 101 and Schedule 7. In order to improve the effectiveness of the BTP, section 100 empowers their officers by allowing them to act outside railway jurisdiction. BTP officers can also, through a provision in subsection (1), assist local forces, MDP or UKAEAC officers on request, but only in relation to a specific incident, as is the case for MDP officers (Explanatory Notes, 2001: para 253). The overarching aim of section 100 can be seen as trying to enable the BTP to respond to terrorist threats and to better protect the public from other crimes.

A1.4.11 Part 11 – Retention of Communications Data

This addresses the issue of the retention of communications data for access by security, intelligence and law enforcement agencies in the course of protecting national security. The ATCS Act provisions work with the Regulation of Investigatory Powers Act 2000 (Part 1, Chapter 2) through clarification of the legal requirements for the retention of data by communication service providers. Communications data, for the purpose of the Act, relates to international, postal and telephone communications but importantly, does not include the substance of the communication itself (Explanatory Notes, 2001: para 257).

In order to avoid exploitation, a statutory code of practice which provides a clear structure has been drawn up in consultation with both industry and the Information Commissioner. The code has been subject to Parliamentary approval by affirmative resolution procedure (Explanatory Notes, 2001: para 28). Although the Code of Practice is voluntary, if this proves ineffective, the Act provides that the Secretary of State may impose mandatory retention directions on providers through the use of affirmative order (Explanatory Notes, 2001: para 259). Subsection (4) confirms that the code is voluntary, nevertheless, strict procedures have been put in place to govern the code. It can also be revised and reissued but would need to be approved by both Houses of Parliament. Any direction must also be explicitly brought to the attention of those to whom it applies (Explanatory Notes, 2001: para 273). Non-compliance may be penalised through civil proceedings brought by the Secretary of State against the communications provider.

In order to try to prevent protests from the providers, the Secretary of State has a duty, under section 106, Arrangements for Payments, subsection (1), to establish arrangements to pay what is deemed to be an appropriate contribution towards the costs that the provider may incur through compliance with either the code or any agreements. Parliament can provide the money for this (Explanatory Notes, 2001: para 283).

A1.4.12 Part 12 – Bribery and Corruption

Part 12 of the ATCS Act addresses the issues of bribery and corruption and seeks to strengthen the law regarding international corruption. This part of the Act goes much

further than previous legislation through confirming that the bribery legislation applies to officials of foreign public bodies, ministries, MPs, judges and agents of foreign principals. The acts of UK nationals and UK incorporated bodies are also included, giving the courts jurisdiction over these Explanatory Notes (2001:para 32).

A1.4.13 Part 13 - Miscellaneous

One of the first areas to be considered here is the implementation of the 3rd pillar in section 111. Paragraph 33 notes that prior to the ATCSA, measures regarding police and criminal judicial co-operation agreed by the Justice and Home Affairs Council of the European Union (3rd pillar) could only be implemented within the UK through primary legislation, Section 111 enables specific measures that are included in the EU's anti-terrorism "road map" to me implemented through secondary legislation by the affirmative resolution procedure. The road map is a list of measures that were identified following September 11th 2001 that required rapid agreement and implementation in order to create better resilience to such events should they occur again. This is not that unusual as measures agreed by the EU on, for example, the internal market or the environment can already be implemented by secondary legislation.

In light of the contemporary issue of Part 13, WMD, the Act also addresses dangerous substances in terms of their use and hoaxes involving them, in sections 113 and 114. The Act also made it an offence to send hoax powders or liquids through the post, not just explosives, and to claim that they were harmful (Explanatory Notes, 2001: para 299).

Section 116 amends the Intelligence Services Act 1994. Overall, the provisions intend to provide greater flexibility for gathering intelligence outside the British Islands. Furthermore, the scope and definition of serious crime is also adapted through the Act's provision for the extension of the powers of the Government's Communication Headquarters (GCHQ).

The offence of a general failure to disclose information about terrorism is also reintroduced in the Act Explanatory Notes (2001:para 37). The Act also amends schedule 7 of the Terrorism Act 2000 to include internal journeys within the UK.

Further amendments to the Terrorism Act 2000 are also made in Section 120 which addresses the issue of weapons training for terrorists. Subsection (1) of ATCSA adds an addition paragraph to sections 54(1) and (2) of the Terrorism Act to include training relating to radioactive material - Explanatory Notes (2001:para 318). Subsection (2) also amends section 55 of the Terrorism Act by substituting a new definition for a biological weapon to include any biological agent or toxin in such a form that can be used for hostile purposes. Paragraph (a) and (b) add a new definition of a radioactive material, whilst paragraph (c) deletes the definition of a nuclear weapon which is now out of date (Explanatory Notes, 2001: para 319).

Overall, it can be seen that ATCSA sought to modernise definitions and provisions in order to respond to and prevent terrorist acts. A clear progression can be seen from the Terrorism Act 2000 to ACTSA 2001 in terms of amendments and additions. Given this, it could be suggested that the government is taking an iterative approach to anti-terrorism legislation, adapting in response to the changing climate and events. An exceptional feature of all this legislation is the speed in which it has been implemented and amended.

A1.5 Prevention of Terrorism Act (2005)

The Prevention of Terrorism Act 2005 received Royal Assent on 11th March 2005. The Act was designed to replace Section 4 of the ATCS Act 2001 and provides the Secretary of State with the power to make a control order against any suspected terrorist, regardless of whether they are a UK national or not, and, whether the activity is international or domestic. It can therefore be seen that this was a clear move towards increasing preventative measures in order to combat terrorism. For the purposes of the Act, a control order is defined as "an order against an individual that imposes obligations on him for purposes connected with protecting members of the public from a risk of terrorism"

(Explanatory Notes, 2005: para 1). Each order can be tailored to the specific circumstances surrounding the individual.

The Act is divided into three areas covering control orders, appeals and other proceedings and supplemental considerations as opposed to specific Parts as in the other Acts. These will now be considered in turn.

A1.5.1 Sections 1 to 9 - Control Orders

The Act provides the Secretary of State with the power to make control orders, which are known as non-derogating control orders. However, if those orders would be incompatible with Article 5 of the European Convention on Human Rights (ECHR), called derogating control orders, then the Secretary of State must apply to the court for such an order to be made (Explanatory Notes, 2005: para 23). If the matter is urgent however, the Act provides that the Secretary of State may make the order but then refer it immediately to the court for confirmation (Explanatory Notes, 2005: para 11).

There are four conditions that must be satisfied in order for the court to confirm a derogating control order. These are:

- That the court is satisfied, on the balance of probabilities, that the controlled person is or has been involved in terrorism-related activities

- It considers that the obligations imposed as part of the control order are necessary for purposes connected with protecting members of the public from a risk of terrorism

- It appears to the court that the risk arises out of or is associated with a public emergency in respect of which there is a designated derogation from the whole or part of Article 5 of the ECHR; and

- The obligations imposed by the control order are in a list of derogating obligations set out in the designation order (Explanatory Notes, 2005: para 14).

Provisions exist for the courts to quash orders or to modify them. Any obligations that are imposed as part of the control order must be those that are considered necessary for purposes connected with preventing or restricting involvement by the controlled person in terrorism-related activity (Explanatory Notes, 2005: para 23). For the purposes of the Act, "involvement in terrorism-related activity" is defined as:

- The commission, preparation of instigation of acts of terrorism;

- Conduct which facilitates or is intended to facilitate the commission, preparation or instigation of such acts;

- Conduct which gives encouragement or is intended to give encouragement to the commission, preparation or instigation of such acts;

- Conduct which gives support or assistance to those known or believed to be involved in terrorism-related activity and applies to both specific and general acts of terrorism. Section 15(1) ensures that "terrorism" has the same meaning as in the Terrorism Act 2000 (c.11) (Explanatory Notes, 2005: para 25).

The move towards more preventative legislation can also be seen here through subsection 9 which confirms that the obligations laid down in the order do not just relate to the activity which gave grounds for suspicion in the suspect initially, but also to prevent their involvement in any terrorism-related activity.

The non-derogating control orders can be imposed for up to twelve months at a time and at the end of this period, a new renewal application must be made to the court. The Act ensures that there are strict guidelines that must be satisfied if the court is to grant such an order that require that there is reliable evidence on which the court can depend, that

reasonable grounds exist to believe that the obligations within the control order are necessary to protect the members of the public from a risk of terrorism, that the risk to the public is connected with a public emergency in that there is a designated derogation from either all, or part, of Article 5 of the ECHR and also that the obligations match the description in the designation order (Explanatory Notes, 2005: para 42). Derogating control orders will last for up to six months but can also be renewed by the court. The same requirements exist for this type of control order to be renewed as described above. When the order is imposed, if any changes are made to the order, or if it is renewed, subsection (8) requires that the controlled person must be notified in order for it to have effect, unless it is a relaxation or modification with consent Explanatory Notes (2005: para 59).

As can be seen, the purposes of the control orders are to restrict the involvement of the person placed under the control order in terrorism-related activity. In order to ensure that the order can be updated to reflect any changing circumstances, subsection (2) of section 7 allows the Secretary of State to revoke or relax the non-derogation control order to prevent involvement with such activities. Subsection (3) however, ensures that a non-derogating control order cannot be turned into one which imposes a derogating obligation (Explanatory Notes, 2005: para 56). To ensure that the order does not remain in place when it is no longer appropriate, subsection (7) provides that the court must remove the order entirely if the obligations no longer need to be imposed as part of a derogating control order.

If an individual breaches an obligation laid down in a control order, without a reasonable excuse, then they are guilty of an offence by virtue of section 9, subsection (1). Subsection (2) goes on to create an offence if the individual subject to the control order fails to report, without reasonable excuse, to a specified person when first returning to the UK, when the order has ceased to have effect (Explanatory Notes, 2005: para 63). If a person is guilty of an offence under either of the above subsections, then subsection (4) provides that they will be liable, if convicted, of a custodial sentence up to five years or a fine and, in England and Wales, on summary conviction to a prison sentence of up to

twelve months or a fine. In Scotland and Northern Ireland this is slightly more lenient in that the sentence may be up to six months and a fine (Explanatory Notes, 2005: para 64). If an individual is convicted of an offence under section 9(1) or (2), the court in England and Wales cannot make a conditional discharge order. Similar provisions exist for Scotland and Northern Ireland and other jurisdictions. A new offence is also created through sections 9(9) and (10) in that obstructing the service of a control order is an arrestable offence.

A1.5.2 Appeals and Other Proceedings

Should an appeal be lodged against a non-derogating control order, or a decision to not revoke one, the court has to decide whether either or both of two key decisions
made by the Secretary of State were flawed. Section 10, subsection (4) provides that the court must assess whether:

a) his decision that it was necessary to renew or continue the order for purposes connected with protecting members of the public from the risk of terrorism;

b) his decision that it was necessary to renew or continue each of the particular obligations in the control order in question for purposes connected with preventing or restricting involvement by the controlled person in terrorism-related activity (Explanatory Notes, 2005: para 69).

The same principles that are applied to an application for judicial review must be applied when determining if the judgement was flawed. If such an appeal is successful, section 12, subsection (8) amends section 133 of the Criminal Justice Act 1988 (c.33) (compensation for miscarriages of justice) to allow compensation to be awarded.

A1.5.3 Supplemental

Section 13 subsection (1) provides that sections 1 to 9 of this Act will expire one year after the Act received Royal Assent on 11th March 2005. However under subsection (2) it

may be renewed for up to one year by order made by statutory instrument. Prior to this, the independent reviewer, the Intelligence Services Commissioner and the Director General of the Security Service must be consulted (Explanatory Notes, 2005: para 80).

The duration of an order is subject to certain conditions; a draft must be approved by both Houses of Parliament before an order can be approved, but, if the situation is urgent, the Secretary of State may make an order without parliamentary approval. Parliament must subsequently approve the order within forty days else it will not be applicable after that period. Section 13, subsection (7) does however provide that the Secretary of State can make a new order to the same or similar effect as the one which is no longer valid (Explanatory Notes, 2005: para 81).

Section 14 considers reporting and review of the Act. Subsection (1) requires that the Secretary of State must report every quarter to Parliament on the exercise of his powers over that period. A copy of each report must be laid before Parliament. In order to monitor the operation of the Act further, an independent reviewer reviews the Act every twelve months. The subsequent report must be forwarded to the Secretary of State as soon as is reasonably practicable. A copy of this must also be laid before Parliament. Most importantly, the independent review must specifically report on:

a) the implications for the operation of the Act of any amendments to the law relating to terrorism which the Secretary of State has proposed;

b) the extent (if any) to which the Secretary of State has used his power to make non-derogating control orders in urgent cases without the permission of the court (Explanatory Notes, 2005: para 86).

Section 16, subsection (2) of the Act provides for repeals, including the repeal of particular sections of Part 4 of the ATCSA 2001 (c.24).

Paragraph 9 of the Act also makes a key exception to the Regulation of Investigatory Powers Act 2000 (c.23) by allowing the admission of interception evidence in both control order proceedings and any proceedings arising from such proceedings.

Overall, it can be seen that the Prevention of Terrorism Act 2005 sought to take a much more preventative and proactive stance rather than some of the more reactive prior legislation. The key theme throughout all of the Acts is one of flexibility and a move towards making the legislation better able to cope with the far more amorphous threat that terrorism now appears to pose.

A1.6 Terrorism Act 2006

The Act was intended to ensure that the UK law enforcement agencies have the necessary powers to combat the terrorist threat to the country. Although the Act included measures that were considered pertinent prior to the London attacks on July 7th 2005 and July 21st 2005, additional measures were included following these events. The TACT 2006 extends to the whole of the UK except for section 17 which does not apply to Scotland as this is a devolved matter (Explanatory Notes, 2006:para 165).

Four new offences have been created in the Act which are:

- acts preparatory to terrorism, which is intended to stop those planning terrorist acts
- encouragement to terrorism, which makes it a criminal offence to either directly or indirectly encourage others to commit terrorist acts and includes the controversial incitement to commit terrorist acts
- dissemination of terrorist publication, which includes the sale, loan or other methods of disseminating the information
- terrorist training offences, which ensures that both those who give and receive terrorist training can be prosecuted. Attending a location where terrorist training occurs is also now an offence.

Most importantly perhaps, the new TACT amends the definition of "terrorism" from that which was contained in the TACT 2000. This will be considered later in the chapter.

The Act is divided into three parts:

- Part 1 – Offences
- Part 2 – Miscellaneous Provisions
- Part 3 – Supplemental Provisions.

This chapter will now consider the three Parts in more detail.

A1.6.1 Part 1 – Offences

Underlying the Act are a number of definitions found in the TACT 2000 on which it rests. The definition of terrorism that is used in Section 1 of TACT is maintained here and covers the use or threat of action, however, it must meet three conditions that are laid out in section 1(1) and are given below:

- The first element is that the action must meet the conditions of section 1(2)
- Section 1(2) covers serious violence against a person or serious damage to property; it endangers a life (other than the perpetrator's); it creates a serious risk to the health and safety of the public; or it is designed to seriously interfere with or seriously disrupt an electronic system.
- The second element is that either the use or threat of the action is designed to influence the government or intimidates the public or a section of the public. This includes an international governmental organisation. This element does not have to be satisfied however, if the action coming under section 1(2) involves explosives or firearms.
- The third element is that the threat is meant to further religious, political or ideological causes (Explanatory Notes, 2006: para16).

Importantly, section 1(4) provides that this is not limited to events within the UK, or related to things in the UK.

Section 1 addresses the encouragement of terrorism. This offence is introduced in order to implement Article 5 of the European Convention on the Prevention of Terrorism (the "Convention") and hence, offences covered by this section are also known as Convention offences. The Convention specifically requires that member States have an offence of "public provocation to commit a terrorist offence" which supplements the existing provision for incitement to commit an offence (Explanatory Notes, 2006: para20).

Section 1(2) provides that statements that are likely to be understood by some or all of the public to whom they are intended for, either directly or indirectly encouraging or inducing the commission, instigation or preparation of terrorist or Convention offences are in breach of the Act (Explanatory Notes, 2006: para21). The offence occurs if the individual publishes a statement, or encourages another to do so and has the necessary mens rea at the time of publication or encouragement of publication. The mens rea is defined as

"at the time of publishing or causing to publish, he either intends members of the public to be directly or indirectly encouraged or otherwise induced, by the statement, to commit, prepare or instigate acts of terrorism or Convention offences, or he is reckless as to whether members of the public will be so directly or indirectly encouraged by the statement" (Explanatory Notes, 2006: para23).

Indirect encouragement of terrorism includes the controversial glorification of the commission or preparation of acts of terrorism or Convention offences. In order to pass this section of the Act, the caveat was included that stated that the public should be able to reasonably infer that what is glorified in any statement is intended to be emulated by others in the existing context. Glorification includes both praise and celebration. The circumstances and manner of the publication as well as the content are also to be regarded to determine whether or not an individual has acted in breach of the Act.

Section 1(5) provides that it is not necessary for an act of terrorism to actually be instigated or prepared, it is therefore not necessary for an act to be committed for the offence to occur (Explanatory Notes, 2006: para 26).

Section 1(6) provides for the defence that a defendant may plead that the statement neither expressed their views, nor did it have his endorsement. This also needs to be demonstrated at the time of publication. He must however comply with a notice under section 3 which will be discussed later.

Section 2 addresses the dissemination of terrorist publications and includes the internet to ensure that the legislation is contemporary. Dissemination, for the purposes of the Act, covers a range of mediums that includes giving, selling, lending the publication, providing a service to enable others to obtain, read or listen to it, electronic transmission of such material and lastly possession of such material with the intention of making it available via any of the above methods (Explanatory Notes, 2006 :para 31).

In order for a publication to be considered as a terrorist publication, there are two criteria set out in the Act that must be met. The first is if the information in the publication is likely to be understood by some or all of the people to whom it may become available, either as a direct or indirect encouragement or other type of inducement to the commission, preparation or instigation to terrorist acts. The second is whether the publication contains any material that is likely to be useful in the commission or preparation of such acts and is likely to be understood by some or all of those who read it, wholly or mainly for the purposes of being useful for them (Explanatory Notes, 2006: para 32). Only a small part of the publication needs to satisfy the criteria, not the entire document.

Indirect encouragement of terrorism includes the new glorification of terrorism offence however the person who understands the statement to be encouragement could reasonably be expected to infer that the conduct that is glorified is glorified as conduct that should be emulated by him in existing circumstances. Account can be taken of the

nature of the disseminator or seller of the information (Explanatory Notes, 2006: para 33). Section 2(7) provides that the publication need not even be relevant for a specific act of terrorism but that it may instead be an encouragement or inducement, or even merely be useful for, terrorist acts in general. Section 2(9) allows a defence to the offence laid down in section 2. This can be used provided that the defendant can show that the material contained in the publication did not express his views, or have his endorsement.

Publications have been defined within section 2(13) to ensure that the legislation reflects new technologies. Publications are given to include books, films, videos, cassettes, electronic books, material contained on CD-ROMs and photographs. Section 20 contains a different definition relating to articles and records. An article is anything that can be used for storing data, such as a CD-ROM. A record is anything that is not an article.

Section 3 specifically addresses internet activity and provides that any person using an electronic service is deemed to have endorsed a statement if he has received notice under section 3 and has failed to comply. Such a notice can only be given by a constable and must declare that the article or record is unlawfully terrorism-related in the constable's opinion and also must require the relevant person to ensure that the statement is removed from view or amended so that it no longer contravenes the Act. Two working days are allowed in order to comply with the notice, otherwise the individual is deemed to have failed to comply with the notice (Explanatory Notes, 2006: para 44).

Section 5 of the Act establishes a new offence of the preparation of terrorist acts, which supplements existing legislation regarding attempting and conspiring to carry out such acts. The definition of this is that a person possesses items that may be used for terrorism and that they have the necessary intention to use the items for that purpose.

Section 6 implements Article 7 of the Convention. Although Article 7 is already partially implemented by section 54 of the TACT 2000, this new offence covers issues that it does not address in terms of training for terrorism, either giving or receiving such training.

Section 6(3) defines the skills in which it is an offence to give or receive training and divides these into three sections:

- Making, handling or the use of a hazardous or noxious substance
- The use of any method or technique for the doing of anything other than things falling into the first category, that is capable of being done for the purposes of terrorism, or in connection with the commission or preparation of such an act, or assisting with such acts
- The design or adaptation, for the purposes of terrorism or Convention offence, of any method or technique for doing anything (Explanatory Notes, 2006: para 54).

Section 8 of the Act creates another new offence of attending a place, either in the UK or abroad, used for terrorist training, augmenting section 54 of the TACT 2000 and section 6 of the TACT 2006. This appears to be in response to allegations of some suspected terrorists attending training camps before committing terrorist acts both in the UK and abroad.

In order for the UK to ratify the UN Convention for the Suppression of Acts of Nuclear Terrorism, three specific sections had to be included in the Act, which are sections 9, 10 and 11. These cover the making and possession or devices or materials, misuse of devices or material and misuse and damage of facilities and lastly, terrorist threats relating to devices, materials or facilities. All of these relate to radioactive materials and nuclear facilities. This is largely in response to concerns and threats regarding potential terrorist acts involving a nuclear element. Trespassing on nuclear sites is also addressed in the Act in section 12, which amends sections 128 and 129 of the Serious Organised Crime and Police Act 2005. Section 12 makes it an offence to enter or be on a protected site as a trespasser.

Section 13 goes on to further amend the TACT 2000, section 57(4)(a) increases the maximum penalty for 10 to 15 years imprisonment if an item is possessed for terrorist

purposes. This is not retrospective however, so will only apply to offences committed after the Act came into force.

Section 15 of the Act amends section 53 of the Regulation of Investigatory Powers Act 2000. This section set out the penalties for failing to disclose protected information to authorised persons and originally carried a maximum sentence of 2 years imprisonment if a disclosure notice that was issued on national security grounds was contravened. This has now been increased to 5 years (Explanatory Notes, 2006: para 77).

A1.6.2 Miscellaneous Provisions

Section 21 widens the grounds of proscription laid down in the TACT 2000. Section 22(2) amends section 3 of the TACT 2000 by ensuring that should an organisation listed under the proscribed organisations operate under another name, then the Secretary of State can make an order to the effect that the name that does not appear on the list is another name for that organisation (Explanatory Notes, 2006: para 102).

Section 24(1) adds to powers for extending detention. Here, a review officer may extend a detention if they are satisfied that it is necessary whilst awaiting analysis of evidence of anything that may result in relevant evidence being obtained.

Another amendment by the Act is the provision under section 26 that allows a constable to apply to a District Judge (Magistrates' Courts) for a warrant to enter and search premises as part of a terrorist investigation.

Section 26(2) and (3) amend paragraph 1 of Schedule 5 of the TACT 2000 to provide that search warrants also cover any premises occupied or controlled by a specified person, not only named premises (Explanatory Notes, 2006: para 122). Section 28(6) provides for material seized from premises to be taken away to be read; this was introduced to help manage cases where large numbers of publications were found at a location and time constraints precluded thorough examination of all of the material in the designated time.

Paragraph 2 of Schedule 2 ensures that if terrorist publications are seized, the constable responsible must give notice to every person who is believed to be the owner of any publication. If they are not present, or it is not reasonably practicable, notice must be given to the occupier of the premises from where the publications were seized. In order to make the process more transparent, the notice must describe what has been seized and provide reasons for this action (Explanatory Notes, 2006: para 135).

Section 29 extends the powers conveyed in the TACT 2000, paragraph 8(1) of Schedule 7, to allow an examining officer, which may be a constable, customs or immigration officer, to search a vehicle at a port which is on a ship or aircraft. Prior to the 2006 Act, this power was not available (Explanatory Notes, 2006: para 141). Section 30 goes on to extend the authorisation for stop and search to internal waters.

The Intelligence Services Act 1994 (c.13) is amended by section 31 of the TACT 2006. Now, warrants to carry out acts both in the UK and overseas are possible in relation to the powers of the security and intelligence services. The duration of warrants has also been increased through the Act from 2 to 5 days.

Perhaps one of the most important amendments which the Act makes is the amendment to two definitions of "terrorism". Following the increased focus globally on terrorism, there was some disparity between the various definitions offered in different Conventions and in different UK Acts. An example which clearly highlights such disparity has been given as that between the European Union Framework Decision of 13 June 2002 on Combating Terrorism and the International Convention for the Suppression of Acts of Terrorism. These Conventions allow for actions to be termed as terrorist if, among other tests, the use or threat of action is designed to influence international governmental organisations, in addition to State governments (Explanatory Notes, 2006: para 158).

Section 34 now defines "terrorism" as the use or threat of action where:

(a) the action falls within subsection (2),

(b) the use or threat is designed to influence the government or an international governmental organisation, or to intimidate the public or a section of the public, and
(c) the use or threat is made for the purposes of advancing a political, religious or ideological cause.

Action falls within subsection (2) if it:

(a) involves serious violence against a person,
(b) involves serious damage to property,
(c) endangers a person's life, other than that of the person committing the action,
(d) creates a serious risk to the health or safety of the public, or a section of the public, or,
(e) is designed to seriously interfere with or seriously attempt to disrupt an electronic system (Explanatory Notes, 2006: para 159).

This definition now amends the definition contained in section 1 of the TACT 2000. Section 113 of the ACTSA which made it an offence to use any noxious substance in a way that was likely to cause damage to property, endanger life, make the public fear for their life or cause violence against a person, is also similarly amended. Section 34 of the TACT 2006 extends the provision of section 113 to include international governmental organisations.

A1.7 Civil Contingencies Act 2004 (c.36)

In addition to the specific terrorism legislation it is important to consider this Act as it was introduced to deliver a new framework for civil protection in the UK. The Act comprises two substantive parts: the first lists those persons or bodies subject to duties imposed under or by virtue of Part One of the Act. This Part comprises the first eighteen sections of the Act. Part Two refers to emergency powers and the duty to assess, plan and advise and covers sections nineteen to thirty-one.

In each Part there is a definition of ‘emergency’ that shall be referred to in the following discussions.

The Act also repeals the Emergency Powers Act 1920 and the Emergency Powers Act (Northern Ireland) 1926 and enables Her Majesty or in very limited circumstances a senior Minister of the Crown, to make regulations if an emergency has occurred or is about to. Provision is also made for consultation with and conferral of functions on the devolved administrations (Explanatory Notes, 2004:para 10).

A1.7.1 Part One – Local Arrangements for Civil Protection

The CCA (2004) repealed the Civil Defence Act 1948 and the Civil Defence Act (Northern Ireland) 1950. It ensures that local bodies have a duty to assess the risk of an emergency occurring and maintain plans or response to an emergency amongst other things.

The Act imposes duties on local bodies in England and Wales, now known as Category 1 responders, that are broader than in the previous legislation (Explanatory Notes, 2004:para 6). Such responders must, amongst other duties, maintain plans or the purpose of ensuring, so far as is reasonably practicable, that if an emergency occurs the person or body is able to continue their functions. They should also maintain plans for the purpose of ensuring that if an emergency occurs or is likely to, they are able to perform their functions for the purpose of preventing the emergency, reducing, controlling or mitigating the effects or taking other action in connection with it. Arrangements should also be made to publish all or parts of the assessments and plans. A key point here is to maintain arrangements to warn the public and provide information and advice if the emergency is likely to occur or has done. Duties are also imposed on other local bodies (Category 2 responders) to co-operate with and provide information to Category 1 responders in connection with their civil protection duties.

Part One of the Act also enables Ministers of the Crown to require a Category 1 responder to perform a function to prevent an emergency, reduce, control or mitigate the effects of it (Explanatory Notes, 2004:para 8).
Section 1(1) defines 'emergency' for the purposes of Part One as:

'*…an event or situation which threatens serious damage to human welfare in a place in the United Kingdom; an event or situation which threatens serious damage to the environment of a place in the United Kingdom, or; war, or terrorism, which threatens serious damage to the security of the United Kingdom*'.

Events such as a terrorist attack, disruption of fuel supplies, contamination of land with a chemical matter and an epidemic could satisfy the definition, should they reach the required level of seriousness (Explanatory Notes, 2004:para 13). Subsections (2) and (3) specify exhaustively the kinds of event or situation which may threaten damage to human welfare or the environment. To satisfy the definition, the event or situation must also threaten *serious* damage to human welfare, or in the environment, of a place in the UK.

The definition in Part 2 differs from that here as the situation must threaten serious damage to human welfare in, or in the environment of, the UK or in a part or region, rather than a place in the UK.

Section 2(1) focuses on contingency planning and requires Category 1 responders to assess the risk of an emergency occurring, to maintain plans to respond to this, to publish the assessment and plans insofar as necessary or desirable to deal with an emergency and maintain arrangements to warn, inform and advise members of the public in the event of an emergency.

Section 2(2) provides that the duties under 2(1) only apply in relation to an emergency if it would be likely seriously to obstruct a Category 1 responder in performance of their function or the responder would be unable to take action in relation to the emergency

without changing the deployment of its resources or acquiring additional responses (Explanatory Notes, 2004:para 17).

Section 4 considers advice and assistance to the public and 4(1) imposes a duty to give advice and assistance to the public in connection with the making of arrangements for the continuance of commercial and voluntary activities should and emergency occur (Explanatory Notes, 2004:para 22). The latter only applies to Local Authorities. Section 7 ensures that if Ministers make directions, these cease to have effect 21 days after they have been made.

Section 9 is a particularly important section as it requires Category 1 and 2 responders to provide information on the performance of their functions. This power is likely to be used to support the functions of making secondary legislation under Part One of the CCA.

A1.7.2 Part Two – Emergency Powers

Section 19(1) defines 'emergency' for Part Two of the Act. Here it is defined as:

'*…an event or situation which threatens serious damage to human welfare in the United Kingdom or in a Part or region; an event or situation which threatens serious damage to the environment of the United Kingdom, or of a Part or region, or; war, or terrorism, which threatens serious damage to the security of the United Kingdom'*.

To meet the definition here, the event or situation must threaten *serious* damage to human welfare or the environment of not only the UK but also a part or region of it (Explanatory Notes, 2004:para 40). As in Part One, the same events are specified. 19(5) enables the Secretary of State to update the list of events or situations so that should a supply, system, facility or service become so essential that disruption of it would warrant the exercise of emergency powers, the Act can be amended accordingly. However, a draft must be approved by each House of Parliament as established in 19(5) (Explanatory Notes, 2004: para 41).

Section 20 addresses the powers to make emergency regulations. 20(1) provides that Her Majesty may make emergency regulations by Order in Council if the conditions in section 21 are satisfied. Ministers would be responsible for advising the Monarch and principally would lie with the Secretary of State for the Home Department. 20(2) provides that a senior Minister of the Crown can make emergency regulations if it is not possible without serious delay to arrange for an Order in Council. 20(5) ensures that regulations must be prefaced with a statement that the regulations maker is satisfied with various matters including that they are compatible with Convention rights within the Human Rights Act 1998 (Explanatory Notes, 2004:para 44).

Section 21 refers to the conditions for making emergency regulations, of which three must be satisfied. These are:

- an emergency has occurred, is occurring, or is about to occur
- it is necessary to make the provision for the purposes of dealing with the emergency
- the need for the provision is urgent

(Explanatory Notes, 2004:para 46).

Emergency regulations will not be made where existing legislation is adequate to deal with the emergency.

Section 22(1) provides that the emergency regulations can make any provision which the person making them is satisfied is appropriate for dealing with the emergency (Explanatory Notes, 2004:para 47). 22(5) provides that the maker of the emergency regulations must have regard to the importance of ensuring that Parliament, the High Court and Court of Session are able to conduct proceedings in connection with the regulations or action taken under the regulations (Explanatory Notes, 2004:para 50).

Section 23 is particularly important to consider as it establishes the limitations of the regulations. 23(1), (3) and (4) impose limits on the provisions which may be included in the emergency regulations. The regulations must be in due proportion to the aspect or effect of the emergency to which the provision is intended to address (Explanatory Notes, 2004:para 51).

24(1) states that a Regional Nominated Co-ordinator must be appointed for each region affected by the provisions. The Co-ordinator has responsibility to facilitate and co-ordinate the activities under the emergency regulations (Explanatory Notes, 2004:para 55). After 30 days, the regulations lapse unless the regulations themselves provide for a lapse at an earlier date. New regulations are not prevented (Explanatory Notes, 2004:para 57).

27(1) ensures that the regulations must be laid before Parliament as soon as reasonable practicable and lapse at the end of seven days thereafter unless each House of Parliament passes a resolution approving them (Explanatory Notes, 2004:para 58).

The London Resilience Forum is the chief device for supporting the planning and co-operation requirements of the Act and achieving effective co-ordination with central and regional government (London Strategic Emergency Plan, 2005/7: 5). The London Strategic Emergency Plan will be examined shortly.

The CCA was an important response to the changing environment and illustrated the government's commitment to updating civil protection arrangements, moving away from the more restricted civil defence focus that had previously been adopted. The Act was intended to define more clearly the roles and responsibilities for key responders to enable faster and more effective responses to emergencies. It is the utility and effectiveness of these provisions that shall be considered in response to the London bombings on 7th July 2005 in chapters 7 and 8 of this thesis.

A1.8 The Strategic Emergency Plan

The plan provides an overview of plans in place to respond to emergencies and outlines roles and responsibilities. The document contains specific plans for command and control, mass fatality plan, large scale evacuation, site clearance, communications and a disaster fund. The plan assumes the Civil Contingency Act 2004 definition of 'emergency' but differentiates between types of emergency, classifying them as 'sudden impact' or 'rising tide' (Strategic Emergency Plan, 2005: para 2.1). Thus, alternate responses are designed for each type.

A1.8.1 Types and Scale of Emergency

It is useful to consider the different types of emergency at this point. Sudden impact emergencies occur with little or no warning and the effects are usually noticed immediately. Events such as transportation accidents, terrorist acts and utility failure are all examples of this type of emergency (Strategic Emergency Plan, 2005: para 2.6). Rising tide emergencies has a clear lead time that may extend to months and includes such things as health pandemics, flooding, foot and mouth disease or industrial action. In this instance, the final effect may not be apparent at an early stage. (Strategic Emergency Plan, 2005: para 2.7). For the purposes of this thesis, only Catastrophic Incident arrangements will be considered although brief reference may be made, where appropriate, to Rising Tide protocols.

The scale of the emergency is also categorised and may be local, which is within a London borough, Regional, which affects London, or national, which affects the whole of the UK. The scale of the incident therefore also affects the scope and nature of response as well as the level of co-operation amongst different agencies.

A1.8.2 Major Incident Procedures

For a sudden impact emergency that requires immediate resource deployment on either a regional or national scale, as in the July 7th 2005 bombings, there is one option, the Gold Co-ordinating Group (GCG), that has two levels of response depending on whether it is deemed a major or catastrophic incident for strategic management (Strategic Emergency

Plan, 2005: para 2.12). The Gold Co-ordinating Group will be considered later in this chapter.

A major incident is defined as an emergency that requires implantation of special arrangements by one or all of the emergency services and requires the involvement of large numbers of people (Strategic Emergency Plan, 2005: para 2.12). A catastrophic incident requires central and regional government to work together, along with key organisations at a strategic level. The central government co-ordination and support is usually focussed through COBR (Cabinet Office Briefing Room), led by the Prime Minister or a Senior Minister nominated by the Prime Minister. The Government Liaison Team (GLT) provides the link between the Gold Co-ordinating Group at the Strategic Co-ordination Centre (SCC) and the central government overview and response from COBR. The SCC location is nominated by the Police Gold and is where the teams will convene. Gold level representatives at the SCC must be empowered to make corporate decisions on behalf of their parent organisation. A Government Liaison Officer (GLO) is a member of the GLT and comes from the leading government department at COBR. Their role is crucial, providing the communication link between GCG and COBR through the GLT. If an incident affects the City or Canary Wharf, a finance cell, comprising a Gold member and two support staff from HM Treasury, the Bank of England and the Financial Services Authority.

Should site clearance be necessary following an incident, SO13 (the Anti-Terrorist Branch) should be closely consulted and if sensitive movements of material are necessary, a police escort may be provided. In addition, transport units may require to be cleaned prior to transportation to ensure that contamination of evidence does not occur (Strategic Response Plan, 2005: para 6:14).

A1.8.2.1 Gold Co-ordinating Group (GCG)

The GCG is a key part of the response to an emergency. Its role is to set strategic aims for the incident and to co-ordinate the response organisations. The Chair of the Group has responsibility for its strategic direction and ensuring that this is documented. A Senior

Police Officer will normally take this role. The GCG comprises Gold level representatives in the SCC and the Group must be capable of effective, real-time decision making.

A1.8.2.2 Gold Support at the Strategic Co-ordination Centre (SCC)

The SCC provides Gold Cells comprising Gold level representatives and supporting staff from the organisations and stakeholders that attend in response to a formal Catastrophic Incident. This allows organisations to share information and consider strategic response options in support of GCG decision making. It also ensures that there is a communication point between each Gold representative and their organisation (Strategic Response Plan, 2005: para 2.42).

1.8.2.3 Media and Public Information

A GCG Media Gold, usually provided by the Metropolitan Police will be responsible for co-ordinating media cell activities at the SCC and representing them at the GCG meetings. The media cell, housed at the SCC, will advise and assist in communicating with external news organisations through the News Co-ordination Centre, which is a central government department and located remotely, who will be linked direct to COBR. They will work in conjunction with the GCG. Whatever message is released to the public, it is essential that the information is consistent prior to release to the media. As a result, very close links must exist between COBR and GCG (Strategic Response Plan, 2005: para 2.47-48).

The Mayor of London assumes the role as the 'Voice of London' and will provide clear guidance to the population. In addition, the media strategy ensures that the Mayor is supported by spokespeople from the emergency services, government and other organisations.

At this point it is beneficial to consider the strategic, operational and tactical roles and definitions.

A1.8.3 Gold, Silver and Bronze Operational Roles

Gold, Silver and Bronze are the names given to the Strategic, Operational and Tactical roles, respectively. Gold is the Commander and is in overall charge of each service, formulating the strategy for the incident. Each Gold has overall command of the resources of their own organisation but delegates tactical decisions to their respective Silver(s). At the start of the incident, Gold will set the strategy and record a strategy statement which is monitored and continuously reviewed.

Silver attends the scene, takes charge and is responsible for formulating tactics to be adopted by their service to achieve Gold's strategy. They should not become personally involved in activities close to the incident, remaining detached.

Bronze controls the resources of their service within a geographical sector or specific role and implement Silver's tactics (Strategic Emergency Plan, 2005: para 53).

A1.9 London Regional Resilience Forum

In 2002, the London Regional Resilience Forum was established to address the strategic emergency planning and resilience requirements of the Capital. The Forum brings together Regional emergency planners, responders and other agencies and stakeholders to ensure effective co-ordination and response and several sub-committees exist to support the Forum in its work (Strategic Emergency Plan, 2005: para 81).

Concise terms of reference were established for the Forum to provide focus for its activities. Overall, it was to provide a senior level central focus for co-ordinated and effective emergency planning in London, bringing national government, the Mayor, emergency services and other key business and service communities. It essentially acts as a steering group providing guidance on London's emergency planning as well as regularly scrutinising major threats to safety and public order, security preparations, command, control and inter-agency communication and media communications amongst other areas.

A1.10 Media and Public Information Protocol

As was highlighted in the course of this thesis, effective media management is crucial at times of emergency and crisis. The Strategic Response Plan explicitly recognises this through the inclusion of a media and public information protocol, which intends to ensure that should a Catastrophic Incident occur, there will be an operation in place to, at a minimum, ensure that the flow of public information is overseen, that a capability exists to brief the media on a regular basis, respond to media queries and interview requests so that the media can report the incident safely and fairly. Furthermore, provision is also made so that a multi-agency Media Centre may be established, where appropriate (Strategic Response Plan, 2005: para 3.1). The Metropolitan Police and the Cabinet Office's News Co-ordination Centre (NCC) will jointly run the media operation with the Metropolitan Police taking the operational lead.

To ensure that a coherent message is transmitted to the public, arrangements have been created so that individual 'lines to take' from the emergency services, government and agencies will be shared with the NCC. This is intended to ensure that the highest level of cross-government and cross-organisation co-ordination exists (Strategic Response Plan, 2005: para 3.4).

Additional arrangements exist for 'significant incident' so that press officers for key groups are aware of any incidents as soon as possible and rest on the principle that whoever is aware first of the incident informs the others via text and pager messages. Conference call arrangements are also in place. The following key groups are part of the protocol:

- GICS Operations Unit
- Emergency Services
- ALG
- ODPM Press Office
- Regional Co-ordination Unit
- London Mayor's Office

- London Resilience Team
- Transport for London
- NHS.

Overall it can be seen that the Strategic Response Plan complements the legislation in place to address terrorism and emergencies and provides more detail as to the practicalities of implementing the legislative requirements. It is important to include the Plan in any review of legislation as it also provides a checklist against which to gauge actual actions following an incident with those laid down on paper. The Plan will also be used to design questions for respondents in the interviews included in this study.

A1.11 In Conclusion

Following discussion of the legislation and in some cases, what could be regarded as a fairly speedy enactment, the most obvious concern that arises could be argued to be that fundamental human rights will be overridden and civil liberties will be dangerously eroded. The long-term focus on increased power to the executive, bestowed by the terrorism legislation, for example through the use of control orders, only serves to strengthen this concern.

Prior to the Terrorism Act 2000 there could be argued to have been a twin track basis to the UK legal system whereby ordinary law could be supplemented by extra-legal powers that could be utilised should a state of emergency arise – McEldowney (2005:768). The new anti-terrorism legislation however has extended powers that incorporate emergency action when some, such as Hickman (2005:657) point out that it may actually be more pertinent to defend the integrity of the law through the adoption of the more traditional UK approach. By this he means the adoption of the extra-legal measures model where constitutional systems allow for extra-legal emergency action.

Appendix II: Psychological and Cultural Approaches to Risk

Psychological Approaches

Risk perception is the main area within this area and can be broken down into two main approaches:

- Cognitive/behavioural decision making;
- Psychometric approaches.

Risk perception theorists tended to assume that all risks could be removed or reduced to an acceptable level. However, what was acceptable to experts was not necessarily acceptable to lay people hence the context and culture of those subjected to the risks had to be considered, which eventually gave rise to the theory of risk communication. It has been of interest to researchers since the end of the 1960s when Starr's seminal paper was published (Sjoberg, 2003:19) and is still of interest today as the subjective element of risk can play an important part in policy considerations.

Cognitive Decision Making

Kahnemann and Tversky (1979) pioneered cognitive decision making approaches. Their work showed that individuals rarely displayed rational choice in their decisions on a fairly regular basis, through the use of gambling scenarios with pre-defined conditions. This theory could be argued to be groundbreaking as it challenged the conventional view of human rationality.

Lola Lopes's work built on this as Borodzicz (2005:16) recognised. For him, Lopes's work is significant as it considered the motivations behind individuals' choices. Perhaps the most important element of her work was the identification of 'risky choice' which looked at the context within which a decision was made which would affect it and hence individual behaviour too. Individuals could broadly be divided into two groups: 'risk-seeking' or 'risk-averse' and if the probability of an event could be calculated, it could be seen that individuals' responses to a range of pre-determined scenarios would differ.

Perhaps most interestingly, individuals tended to overestimate death rates for low frequency events and underestimate death rates for high frequency events.

Although decision making theories are fairly reliable, there are possible drawbacks with this approach as Slovic (1987:281) noted. Firstly, individuals' behaviour in a laboratory is likely to be different from their natural behaviour. Secondly, both Kahnemann and Tversky and Lopes approached the notion of risk from a gambling perspective. As Borodzicz (2005:17) argued, can choices in a gambling context inform us about decision making under risk? He argues that gambling as a phenomenon may be more appropriately considered within its own social context and may be a misleading experimental design for other types of risks. After all, there are many social and cultural features to be considered in the use of gambling settings as a representative analogy. Thirdly, the approach does not consider the subjective element of decision making in terms of the weightings which individuals assign to risks. The third concern was addressed by the psychometric approach.

Cultural Approaches

In more recent times, risk theorists have considered the concept of culture within the social sciences. This has divided into two schools of thought: that which considers culture in relation to organisational influences which is known as 'safety culture' and those theorists who took a more anthropological view in their view of risk and developed 'cultural theory'.

Safety Culture

The origins of this theory can be found in the nuclear industry following the Chernobyl incident. Pidgeon (1991) noted that a poor safety culture amongst staff at the plant contributed to the accident. This is because proponents of this approach believe that expert decision makers' work is embedded in the organisation's culture and the safety culture therefore functions at the organisational level.

Again, debate exists regarding what constitutes a safety culture. This was probably best highlighted by Borodzicz (1997:45) when he contrasted the OECD (1987) definition of a safety culture with that of the human sciences approach. The former defined it as a set of administrative procedures including training, emergency plans and attitudes to safety that cannot be regulated. In contrast, the latter described culture as systems of shared meanings or beliefs. Its aim is to improve an organisation's attitude to hazards which should reduce risk.

Lee (1993:21-3) suggested that safety culture provides a way to assess risk management processes in difficult operations. This can then be used to analyse the pre-conditions to many socio-technical disasters. For him, it is one of the most important recent advancements in risk management. Conversely, Pidgeon (1991) is more concerned with how and why a good safety culture may be developed and its benefits for the organisation as a whole.

If it is to be effective, a safety culture must be an integral part of the organisation. As before, the lack of consensus regarding definitions is problematic and may hinder practical use of safety culture and cultural theory however, it could be argued that the more problematic area is to recognise a safety culture and assess it in order to be able to promote good practice. Borodzicz (2005:41) suggests that it is only at times of crisis that a safety culture will be revealed as it is only at this point that the system of shared values and beliefs is truly tested. Safety culture is therefore an important consideration in the field of crisis management. It was a great departure from previous psychological risk research as it no longer considered gambling or psychometric measures. Perhaps one of the most attractive arguments for business regarding creating a safety culture is that both safety and profit in the short and long-term will be enhanced (ACSNI, 1993); an argument also applied to risk management as a whole (ICAEW, 1999:para.13). Such fiscal arguments may help to encourage organisations to adopt this approach.

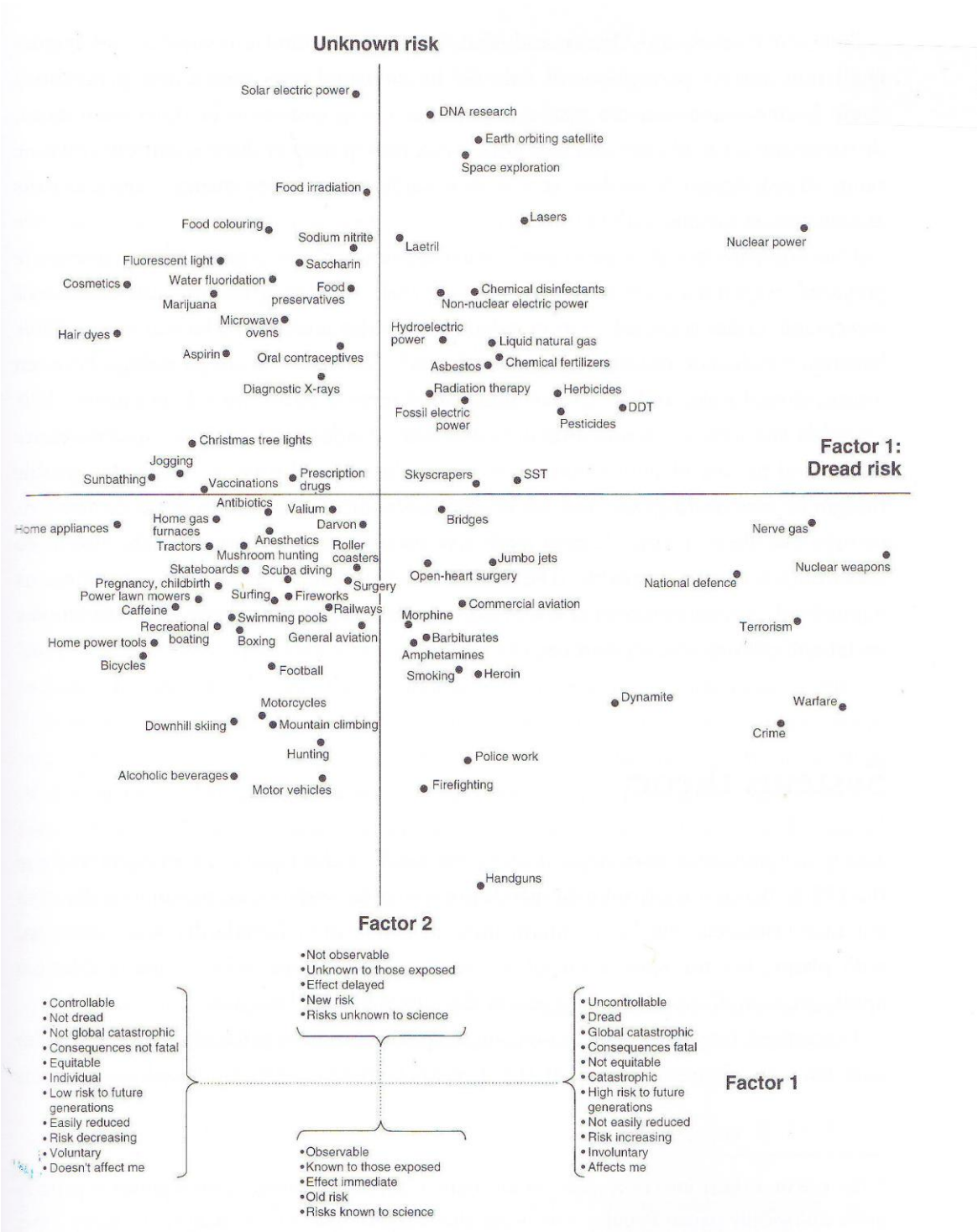
Cultural Theory

For cultural theorists, culture can be divided into two areas: cultural biases, such as shared beliefs and values (group) and social relationships comprising interpersonal relationships (grid). Risk is again regarded as a socially constructed concept. Driving these attributes are four predispositions which affect an individual's perception of risk: hierarchical, individualist, egalitarian and fatalist. An additional fifth category of autonomists is also argued to exist by some (Douglas and Wildavsky, 1982; Thompson et al, 1990; Dake, 1991). This category may be known as 'technological enthusiasts' who believe that technology is the basis for improving society (Maule, 2004:24). Frosdick (1995:4) suggests that where there is low orientation to group and grid attributes then the individualist predisposition will be evident. Individualists tend to accept higher levels of risk as long as this represents entrepreneurial opportunities and freedom for all; we can see evidence of this in the earlier discussion of the development of risk in the nineteenth century at 2.1. If the orientation to both attributes is high then a hierarchical disposition results where individuals are more risk averse. They believe that experts should manage the risks. If group influences are strong but grid influences weak, the egalitarian disposition prevails where risk is viewed as omni-present and caused by others and should be managed by all. This is also the case for fatalists who are high in grid and low in group. Fatalists however accept risk as something that they can do little about, it is pre-ordained (Maule, 2004:24; Lupton, 1999:50). Frosdick (1995) recognises that these dispositions appear throughout the human species in every type of human society and cross cultural, psychological and social boundaries.

Cultural theory is not without its critics, not least as it questions all alternative ways of perceiving the world around us hence has its own belief systems. This is somewhat ironic as it is this that the theory attacks in alternative theories, as Borodzicz (2005:45) supports. Furthermore, it may not be possible to categorise all individuals into four personality types and adding a final 'catch all' certainly raises some doubts as to the validity of the approach. Denney (2005:23) also suggests that it does not consider how risk may change in the future and takes a fairly conservative stance. It is therefore suggested that this theory does have a place within risk management but that it is used as an aid to

understanding the context of risks rather than providing an effective method for risk management.

Appendix III: Unknown and Dread Risks



Source: Slovic, Fischoff and Lichenstein (1980)

Appendix IV: Turner's Incubating Disaster Aetiology

Stage 1 **Notionally Normal Starting Point -** inception of the system

Stage 2 **The Incubation Period** - minor problems and events are overlooked, allowing escalation to Stage 3

Stage 3 **Precipitating Event** - the crisis. This causes decision makers to recognise that their perceptions in Stage 2 were incorrect. If no action or the wrong action is taken, the crisis escalates to Stage 4, leaving an indelible effect on the organisation

Stage 4 **Onset of Disaster** - again, inappropriate actions may lead to further escalation on to Stage 5

Stage 5 **Rescue and Salvage** – here, flexibility and improvisation are required as the situation is outside normal operating procedures

Stage 6 **Full Central Readjustments -** inquiries and assessment of what went wrong. The organisation tries to come to terms with its new understanding of the world.

Source: Turner (1978) in Toft and Reynolds (1997:19-20).

Appendix VI: Jenkins and Gersten's 21 Areas of Concern

A range of issues are covered from more basic, tactical considerations to strategic problem recognition.

1. Contingency planning: for large-scale disasters, accidental or man-made;

2. Chemical/biological preparedness: the Sarin attack was unprecedented but this type of attack must now be accepted as possible in security planning;

3. Co-ordination: between transport authorities and public authorities;

4. On-going threat analysis: to detect an increased threat;

5. The limitations of physical security;

6. The utility of detection and identification technologies: which, if available, may provide immediate warning of a lethal contaminant and its nature;

7. The utility on on-board CCTV: which can alert drivers to the nature of the problem and facilitate prompt diagnosis by central management;

8. The utility of CCTV at subway stations: to further aid diagnosis;

9. The utility of CCTV coverage of the aboveground area around station entrances: which may show the accumulation of casualties and thus aid diagnosis;

10. Anticipation of multiple attacks or a rolling contamination: which must be considered in contingency planning;

11. The necessity of rapid diagnosis;

12. Computerised modelling of airflows and dispersal: in stations and tunnels to aid diagnosis and evacuation (The Tokyo subway had the capacity to reverse the airflow if required);

13. The decision making process for shutdown and evacuation;

14. The necessity of staff training: transport staff will always be first responders and be casualties;

15. The possible utility of special apparatus, such as gas masks, for train staff;

16. The availability of airtight containers: to hold suspicious objects and stop contamination;

17. The development of some type of sealing foam or spray-on substance: to neutralise suspicious liquid patches;

18. Guidance for immediate, on-site treatment of victims: can train staff perform any useful first aid for victims of chemical attacks?;

19. Decontamination, clean-up and all-clear signals;

20. The recovery of transport operations;

21. The restoration of passenger confidence

(Jenkins and Gersten, 2001:64-65).

Appendix VII: The London Assembly's 7th July Review Committee Membership

Richard Barnes AM
Chairman of the Committee
Assembly Member for Ealing and Hillingdon (Conservative Party)

Sally Hamwee AM
Deputy Chair of the Committee and Deputy Chair of the London Assembly
Londonwide Assembly Member (Liberal Democrat Party)

Joanne McCartney AM
Assembly Member for Enfield and Haringey (Labour Party)

Peter Hulme Cross AM
Londonwide Assembly Member (One London Party)

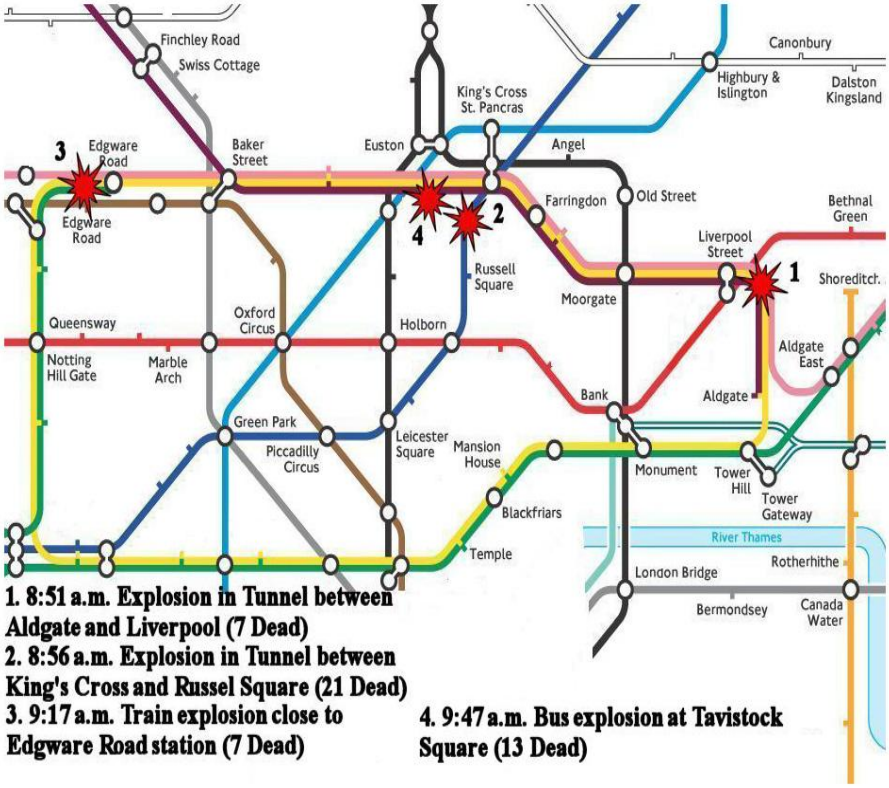
Darren Johnson AM
Londonwide Assembly Member (Green Party)

Janet Hughes
Senior Scrutiny Manager

Dale Langford
Committee Administrator

Kelly Flynn
Senior Media Officer

Appendix VIII: Map of 7th July 2005 Attacks on London Transit System



Source: www.globalsecurity.org/security/ops/images/london-jul7.htm

Appendix IX: The Official Definition of Terrorism in the United Kingdom

The Terrorism Act 2006 (c.11) (TACT) defines terrorism within Section 34 and replaces that originally found in TACT 2000.

Section 34 now defines "terrorism" as the use or threat of action where:

(d) the action falls within subsection (2),
(e) the use or threat is designed to influence the government or an international governmental organisation, or to intimidate the public or a section of the public, and
(f) the use or threat is made for the purposes of advancing a political, religious or ideological cause.

Action falls within subsection (2) if it:

(f) involves serious violence against a person,
(g) involves serious damage to property,
(h) endangers a person's life, other than that of the person committing the action,
(i) creates a serious risk to the health or safety of the public, or a section of the public, or,
(j) is designed to seriously interfere with or seriously attempt to disrupt an electronic system (Explanatory Notes, 2006:para 159).

This definition amends the definition contained in section 1 of the TACT 2000. Section 113 of the ACTSA which made it an offence to use any noxious substance in a way that was likely to cause damage to property, endanger life, make the public fear for their life or cause violence against a person, is also similarly amended. Section 34 of the TACT 2006 extends the provision of section 113 to include international governmental organisations.

Underlying the Act are a number of definitions found in the TACT 2000 on which it rests. The definition of terrorism that is used in section 1 of TACT is maintained here and covers the use or threat of action, however, it must meet three conditions that are laid out in section 1(1) and are given below:

- The first element is that the action must meet the conditions of section 1(2)
- Section 1(2) covers serious violence against a person or serious damage to property; it endangers a life (other than that of the perpetrator); it creates a serious risk to the health and safety of the public; or it is designed to seriously interfere with or seriously disrupt an electronic system.
- The second element is that either the use or threat of the action is designed to influence the government or intimidates the public or a section of the public. This includes an international governmental organisation. This element does not have to be satisfied however, if the action coming under section 1(2) involves explosives or firearms.
- The third element is that the threat is meant to further religious, political or ideological causes (Explanatory Notes, 2006: para16).

Importantly, section 1(4) provides that this is not limited to events within the UK, or related to things in the UK.