Fit to Fight or Unfit for Purpose? A Review of the Effectiveness of the Intelligence Cycle in UK Counter-Terrorism, 2003-2013.

By

Paul Burke

Submitted in partial fulfilment of the requirements for the award of the degree of Professional Doctorate in Policing, Security and Community Safety at London Metropolitan University.

Copyright

This is the sole work of Paul Burke. This is not a resubmission.

Table of Contents

Copyright 2

Table of Contents iii

List of Tables viii

List of Figures ix

Abstract xi

Acknowledgements xiii

Chapter 1 Introduction 14

1.1 Rationale for study 14

1.2 Overview of Research 19

1.3 Thesis Question 21

1.4 Guide to Chapters 21

1.5 Theoretical Framework 25

1.5.1 The Composition of the UK Intelligence Community. 25

1.5.2 How the UK Intelligence machinery functions 30

1.5.3 Legislation and oversight of the UK Intelligence Community 34

Chapter 2 Methodology 39

2.1 Theoretical Framework and Argument 39

2.2 Operationalising the Research Question................................40

2.3 Ethical Issues and Problems Encountered.............................41

2.4 Literature Review..44

2.5 Collecting the Raw Data and Methods of Analysis...54

2.6 Interview structure and interview questions.........................55

Chapter 3 Theoretical Framework: Defining Intelligence and Terrorism 60

3.1 Defining Intelligence...61

3.1.1 Intelligence Failures or Intelligence Gaps? 81

3.2 Defining Terrorism...84

3.3 Problems with terrorism definitions.....................................103

3.4 Summary...107

Chapter 4 CONTEST: The UK Counter-Terrorism Policy...................111

4.1 PURSUE...114

4.1.1 Covert Detection & Investigation 116

4.1.2 Effective Prosecution 125

4.1.3 Non-prosecution Actions 128

4.1.4 Disruption of Terrorist Activities Overseas 133

4.1.5 Capacity Building 136

4.1.6 Inter-Agency Co-ordination 138

4.1.7 SUMMARY 140

4.2 PREVENT 141

4.2.1 The Ideological Challenge of Terrorism 141

4.2.2 Prevent the Recruitment of Individuals 143

4.2.3 Addressing Radicalisation 146

4.3 PROTECT.. 156

4.3.1 Critical National Infrastructure 156

4.3.2 Transportation, Border Security and Crowded Places 157

4.3.3 Operation CREVICE – 2004 164

4.3.4 Operation RHYME - 2006 167

4.4 PREPARE.. 171

4.4.1 The CBRN Threat 171

4.4.2 Interoperability 174

4.5 Summary.. 186

Chapter 5 The Intelligence Cycle.. 191

5.1 Direction 193

5.2 Collection.. 198

5.3 Collation.. 206

5.4 Evaluation.. 211

5.5 Analysis.. 217

5.6 Dissemination 223

5.7 Summary 229

Chapter 6 Strengths and Weaknesses of the Intelligence Cycle 234

6.1 Weaknesses of the Intelligence Cycle 234

6.1.1 Challenges and vulnerabilities in Intelligence 256

6.1.2 Pathologies of Intelligence Sharing 264

6.2 Strengths of the Intelligence Cycle 274

6.3 Summary 291

Chapter 7 Conclusions 293

Annex A - Example of a Priority Intelligence Requirement 304

Annex B - Participant Consent Form 306

Annex C – UN Conventions 310

Annex D – Example Intelligence Collection Plan 312

Annex E –Financial investigation infographic 313

Annex F – Example Tear Line Report 314

Annex G - Community Engagement to Counter-Terrorism (Metropolitan Police Authority 2007, sec.G) 315

Annex H – Relevant Public Authorities – RIPA 2000 316

Annex I – The Eight Attributes of Intelligence Excellence, as considered by the U.S. Joint Chiefs of Staff 319

Index 322

Bibliography 324

VITA 357

List of Tables

Table 1: Categorisation of Intelligence definitions on a Broad-Narrow continuum, according to Davies (2005). 17

Table 2 List of interviewees and their primary agencies 58

Table 3 O'Connor's Ten Reasons for Intelligence Failures 83

Table 4 Sample of closed databases 210

Table 5 Breakdown of the evaluation variables in the National Intelligence Report (5x5x5) 215

Table 6 Intelligence Analysis Challenges and Vulnerabilities 259

Table 7 Intelligence challenges and vulnerabilities listed by taxonomy 261

List of Figures

1 The earliest known version of a printed Intelligence cycle, 1948 15

2 Harfields' triptych conceptualisation of Intelligence, based on Ratcliffe (2003). 80

3 The CONTEST Strategy 112

4 The relationship between CONTEST and the policing pillars 114

5 Directed surveillance authorisations for law enforcement agencies over past ten years (Rose, 2014:11) 119

6 Intrusive surveillance authorisations over past ten years (Rose, 2014:10) 120

7 Property interference authorisations over past ten years (Rose, 2014:10) 121

8 Charity Commission Counter-Terrorism Strategy: The Four-Strand Approach (2012:8) 132

9 The CHANNEL process (Peters, 2012:15) 153

10 Graph showing number of individuals referred to CHANNEL from 2006-2014 155

11 The INSTINCT concept 163

12 Three phases of Critical Incident Management (College of Policing, 2013) 179

13 Workstreams of the UK Resilience Capabilities Programme 181

14 British Army Intelligence Cycle, circa 1984 192

15 The 6-stage Intelligence Cycle 192

16 Example of a National Intelligence Report (5x5x5) 212

17 Intelligence cycle with single-stage feedback loops 239

18 Intelligence cycle with hand-drawn, multiple-stage feedback loops 240

19 Treverton's forms of politicisation 242

20 A systems approach to the Intelligence cycle 250

21 Clark's Hierarchy of Models 252

22 Clark's target-centred view of the Intelligence Process 252

23 Treverton's "Real Intelligence Cycle" 254

24 Engineering and production functions isolated in their own separate functional silos 272
25 The SARA model 277
26 The Intelligence Triosphere 300

Abstract

The Intelligence process has increasingly found itself in the public eye in modern times. The Al Qa'eda attacks against the USA in September 2001 led to a rapid spread of other international terrorist attacks. The invasion of Afghanistan occurred soon afterwards, followed by the invasion of Iraq in 2003. All of this resulted in the Intelligence community and their processes being pushed into the spotlight of the global media. Central to all Intelligence work is the Intelligence cycle, in whatever form it might take.

This thesis investigates the effectiveness of the UK's 6-stage Intelligence cycle in counter-terrorism work. Definitions of two key terms, Intelligence and terrorism are dissected at length, and the merits and shortcomings are outlined. Accusations of Intelligence failure have been levelled at both the UK government and at the country's law enforcement, Intelligence and security agencies. Intelligence gaps and Intelligence failures will be described, and the differences between these key terms highlighted.

All counter-terrorism work in the UK takes place within the environment of the government's counter-terror strategy called CONTEST. The six pillars of the strategy are explained, and examples are used to show where Intelligence fits into it. Two UK-based case studies (Operation CREVICE and Operation RHYME) are used to highlight how Intelligence is used to protect the public from terrorist attacks.

A thorough examination of the Intelligence cycle is conducted and some of the common difficulties and challenges encountered in the cycle are presented. It shows what can, and sometimes does, go wrong in the Intelligence cycle, and why this happens. Various models of the Intelligence cycle are compared and their intrinsic components discussed.

The thesis benefits from a unique collection of personal insights from a number of serving and retired Intelligence specialist, all with personal experience of working in counter-terrorism. This adds valuable material to the considerations of the strengths and weaknesses of the model. The conclusion

provides some recommendations for the enhancement and strengthening of the Intelligence cycle, resulting in a more robust and applicable model for the UK's counter-terrorism work.

Acknowledgements

Dr. Dan Silverstone

Dr. Nicholas Ridley

For Fiona, always.

Chapter 1 Introduction

1.1 Rationale for study

> *"Intelligence merely provides techniques for improving the basis of knowledge. As with other techniques, it can be a dangerous tool if its limitations are not recognised by those who seek to use it"* (Butler, 2004:14).

The Intelligence cycle in some form or other has been used for decades as a tool by the Intelligence agencies of most countries in the world. The earliest pictorial representation of a model of the Intelligence cycle appears to be one published in 1948, in a book written by two U.S. Army Lieutenant Colonels who had both seen service in World War 2 and were both instructors at the U.S. Command and General Staff College (Glass & Davidson, 1948:5).[1]

[1] There are earlier references to various Intelligence processes, but the Davidson-Glass model is the earliest known pictorial depiction of a cyclical model. Omand, for example, cites Wheaton in positing that a cycle may have existed in training delivered at Fort Leavenworth, but there is no evidence of this to confirm the theory (Omand 2013, p.62).

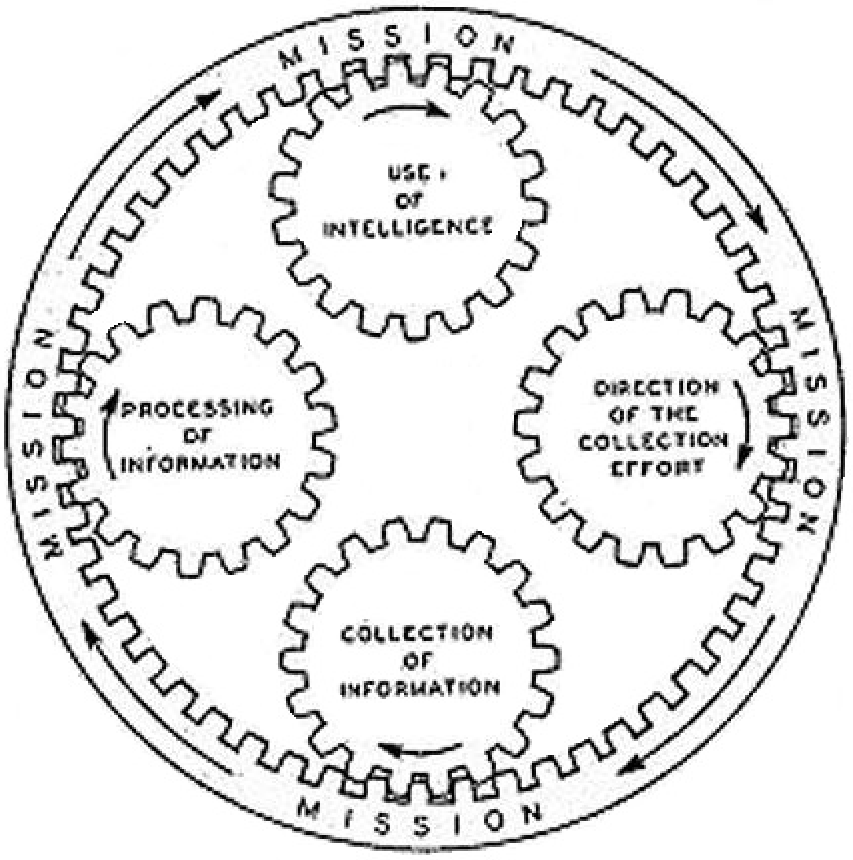

MISSION
USE OF INTELLIGENCE
DIRECTION OF THE COLLECTION EFFORT
COLLECTION OF INFORMATION
PROCESSING OF INFORMATION
MISSION
MISSION
MISSION

PLATE 1. The Intelligence Cycle.

1 The earliest known version of a printed Intelligence cycle, 1948

The Davidson-Glass model of the Intelligence cycle from 1948 contained four components: direction, collection, processing and use. Nowadays, there are many versions of the Intelligence cycle and even different agencies within the same country often use different models, such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) in the USA. The role of the Intelligence cycle is paramount to this study, as it has formed the theoretical basis of the Intelligence process for several decades. Counter-terrorism work is absolutely dependent upon Intelligence, without which it cannot function. It is Intelligence-led, more so than other areas of Policing or

Law Enforcement. If the Intelligence cycle is flawed, or is unfit for purpose, it follows that Intelligence-led operations will suffer, either by going awry, by being ineffective, or even being directed against the wrong target. In counter-terrorism, the potential stakes are very high and the impact of mistakes for the authorities can be large-scale loss of life.

This study investigates the effectiveness of the 6-stage Intelligence cycle as a valid model, specifically examining its utility within counter-terrorism work carried out by the Intelligence, security and law enforcement community of the UK. It will conduct a thorough examination of the Intelligence process, analysing the typical difficulties encountered by the various agencies in their efforts to produce Intelligence. It will consider what can, and often does, go wrong in the Intelligence cycle, and why this happens.

The concept of Intelligence-led counter-terrorism contains two words which are notoriously difficult to satisfactorily define, either academically or legally - Intelligence and counter-terrorism. Both of these terms will be unpacked in detail, and a wide selection of the various definitions for each term will be considered. Defining Intelligence has become something of an academic pursuit, and entire essays have been devoted to this subject, such as those by Warner (2002) and Davies (2002). Attempts to frame the concept of Intelligence encounter difficulties with scope, boundaries, politicisation, process and structure to name but some. Academic discussion, especially by Davies (2012), has also tried to place these definitions on various axes, such as “broad-narrow”, “informational-organisational” and “analytical-operational”, some of which are briefly outlined in this paper. In a lecture given by Davies (2005) he categorised a number of Intelligence definitions using the following spectrum:

BROAD	INTERMEDIATE	NARROW
Kent	Godson (Considered by Davies to slide from Broad to Intermediate)	Elliott
Hoover / US DoD		Robertson
Wilensky		Herman
Sims		Butler
US DoD (1979)		Schulsky
Richelson		
Capel-Dunn		
J.B. Lockhart		

Table 1: Categorisation of Intelligence definitions on a Broad-Narrow continuum, according to Davies (2005).

Attempting to define terrorism is even more contentious than attempting to define Intelligence and the debate arouses strong opinions. Any effort to define terrorism will necessarily be done through one conceptual lens or another and this debate will continue for the foreseeable future. Chomsky (2003) captured the essence of the debate on terrorism probably more concisely than anyone, when he wrote :

> “*It is important to bear in mind that the term "terrorism" is commonly used as a term of abuse, not accurate description.*

> *It is close to a historical universal that our terrorism against them is right and just (whoever we happen to be), while their terrorism against us is an outrage. As long as that practice is adopted, discussion of terrorism is not serious. It is no more than a form of propaganda and apologetics.*"[2]

As one journalist wrote, shortly after the 11 September 2001 attacks in the USA: "*Immediately beyond Al Qaeda, the high moral condemnations of global terrorism rapidly become relative, and the definition blurred*" (Schmemann, 2001:2). The politicisation of the issue is almost inescapable and yet it constitutes one of the most globally recognised crimes. Before considering the UK's counter-terrorism policy and the role that the Intelligence cycle plays in it, the concepts of Intelligence and terrorism must first be taxonomically dissected if we are to gain a deeper understanding of these issues, particularly the highly polarised topic of terrorism.

Interviews have been used as a valuable and unique primary source of experience and knowledge regarding the role of Intelligence in counter-terrorism. These interviews were conducted with serving and retired practitioners with a spread of experience including the UK's Intelligence agencies, the Armed Forces and law enforcement. This material adds a richer insight into the actual experiences of Intelligence practitioners who use the cycle in their daily counter-terrorism work.

This study makes a comparison of some models of the Intelligence cycle in use by different agencies, not only those within the UK. The component elements of the Intelligence cycle are dissected and discussed in turn, examining common problems encountered in Intelligence work, and how these relate to the cycle. The collection, analysis and use of Intelligence by the law enforcement, security and Intelligence agencies is a complex process

[2] From an interview printed in an unidentified Kurdish newspaper.

which has come under increasing scrutiny in the UK since the invasion of Iraq in 2003. Accusations of Intelligence failure have been levelled at both the UK government and at the country's Intelligence community. Intelligence gaps and Intelligence failures are described, and the differences between these key terms highlighted. The paper draws conclusions from these findings, regarding the suitability of the current UK Intelligence cycle and it proposes some changes to strengthen the model and to make it yet more robust for its function within UK counter-terrorism. Finally, some recommended areas for future research are identified, to help pave the way for other scholars who may wish to build on this paper's new contributions to the corpus of existing knowledge in this area.

1.2 Overview of Research

This paper answers a number of research objectives. The Intelligence cycle is described, and an examination is made of some different models in use. To further explore the differences, various models are analysed, comparing and contrasting them to the model used by the agencies of the UK Intelligence community. This leads to a critical assessment that answers the question of whether the 6-stage model of the Intelligence cycle, as described in detail in this paper, is still an effective tool for UK counter-terrorism work. The sources and methods used by Intelligence agencies are examined, and an assessment made of their relative merits and weaknesses, with particular reference to how they contribute to the Intelligence cycle, and how they interact with other sources and methods. Some of the inherent problems faced in conducting and managing the process of Intelligence analysis are scrutinised, examining whether it is possible to factor out these problems and, if this is considered possible, to what degree.

A wide range of vulnerabilities and issues has been identified by scholars such as Heuer (1999), Sheptycki (2004), Heuer & Pherson (2011), Krizan

(1999), Trent (2007) and Hutchins (2007), which are all of relevance to an analysis of the Intelligence cycle's effectiveness. These vulnerabilities can include bias (which can take many forms, such as hindsight, cognitive, selective), interpretation, group-think, expressions of uncertainty, anchoring, perception of correlation, competing hypotheses, persistence of impressions and evidence. A full analysis of these vulnerabilities is beyond the scope of this thesis, as it constitutes a very large research topic in itself, but the general nature of vulnerabilities is discussed, and this paper groups them in three taxonomical sub-classes to show that the majority of them are actually human factors.

The differences between an Intelligence gap and an Intelligence failure are described, in an attempt to explain why the use of these two terms is so commonly mistaken in the mainstream media. Definitions by Schulsky (Schulsky & Schmitt, 2002:63) together with O'Connor's taxonomic classifications (O'Conner, n.d.) are the key works in this area.

While the collection of Intelligence is conducted by the organs of the UK's Intelligence machinery, it is crucial to consider that both the finished Intelligence product and, on occasion, the raw Intelligence material, may find their way into a senior politician's in-tray. The politicisation of Intelligence can have a significant impact upon national security and community safety, both real and perceived. Various forms of politicisation are covered, along with some of their academic definitions (Treverton, 2008), which then provides a summary of the dangers posed by such politicisation, and the concomitant effects that this has upon the effective utility of Intelligence-led counter-terrorism.

All Intelligence communities are hampered by "stovepipes" or "silos" to some degree, and this affects the releasability and dissemination of Intelligence to customers.[3] The problem of such stovepipes is a recurrent one for many

[3] While the term "releasability" is not found in the dictionary, its use is widespread in the "five eyes" community comprising the UK, USA, Canada, Australia and New Zealand. It describes whether an agency or country can release the Intelligence to another agency or country.

commercial organisations (Ensor, 1988b) and for most Intelligence communities. This report will consider the impact of this in relation to the effectiveness of the UK's counter-terrorism policies, capabilities and operational capacity.

Having considered these factors, and using a variety of lenses such as transparency, legality, proportionality, oversight and the public interest, this paper will identify and propose recommendations for the collective improvement of the use of the Intelligence cycle by the UK's Intelligence community, in order to enhance national security and community safety in the UK.

1.3 Thesis Question

The thesis of this paper is that the 6-stage UK Intelligence cycle, insofar as it is used within the UK Intelligence community, remains a valid and effective model for use in counter-terrorism.

1.4 Guide to Chapters

Chapter one presents the overarching topics of the thesis and it contextualises the rationale for the work covered. The chapter begins by explaining the reasons for writing this thesis. An overview of the research is provided, followed by a framing of the thesis question. The theoretical framework of the research is also outlined. Chapter one also explains some important background information about the UK Intelligence community. Since the Iraq war of 2003, the UK Intelligence agencies have been subjected to considerable and relatively continuous criticism from multiple fronts, including the British public, world opinion, the media, UK parliamentarians and various groups both inside and outside government. An accurate understanding of this community and its associated machinery is essential to contextualise the thesis question. Without an understanding of the Intelligence agencies, their inter-relationships, the legislation which governs them and the oversight which keeps them as transparent as possible (while at the same time making sure that national security is not compromised), the role of the Intelligence cycle and its effectiveness as a tool in UK counter-terrorism cannot be reasonably assessed. The roles of the three primary UK Intelligence agencies are explained and the overview then moves to the inner workings of the Intelligence machinery.

The JIC is central to this machinery, as it is the JIC papers which carry so much weight when presented to the Prime Minister and his inner circle of advisers. The JIC in particular was singled out for criticism in the Butler Report, after the 2003 invasion of Iraq. The three Intelligence agencies no longer operate in complete secrecy, devoid of oversight or robust and effective legislation. Chapter one describes the genesis of this legislation, how it came into being and why it is necessary for the UK to have such legislation. The legislation of Intelligence activities without the accompanying oversight is, however, something of a toothless tiger. The oversight arrangements of the Intelligence agencies are covered in this chapter, with a brief explanation of how and why they came into being. This introductory chapter also defines the problem statement: “How effective is the Intelligence cycle as a model in UK counter-terrorism?” The relevance of this research paper to the current position of the topic within Intelligence studies is discussed in this chapter.

Chapter two describes the methodology of the research paper, expanding upon the research objectives of the paper. It explains how the paper’s research was operationalised and covers the methods of analysis. This chapter also contains a literature review, which introduces the framework of the paper’s research and its focus. Some of the key writings on Intelligence and counter-terrorism are reviewed, to highlight the current body of academic knowledge in this area of study. This research paper necessarily covers a wide area of academic material, due to the number of essential components that must be covered, in order to ensure that any overview of the Intelligence cycle and the entire Intelligence process is meaningful. Relevant points from the various UK inquiries are extracted and discussed. This chapter also lays out the detailed methodology of the research paper, covering the main source materials and the interviews.

Chapter three provides the theoretical framework of the paper. This includes key academic discussions on the attempts to define Intelligence and terrorism, the difficulties these attempts encounter, and the academic and political landscape in which some of these definitions have been crafted. A selection of definitions is pictorially represented using models with varying axes, to provide some explanation of the academic arguments surrounding many of the definitions. It compares a wide range of definitions and examines what, if anything, is missing. It further considers how the definition of Intelligence used by an agency can affect the Intelligence it collects and the processes it is subjected to. Current thinking on the Intelligence cycle and Intelligence-led counter-terrorism are also dissected. These two areas are brought together later in the paper, to prepare for a more detailed examination on the effectiveness of the Intelligence cycle as a model. The concept of terrorism and the various definitions of it are examined in detail in this chapter and it describes the problems which have been faced by the many attempts to encapsulate a definition of terrorism. A brief summary is provided at the end of the chapter on the differences between an Intelligence gap and an Intelligence failure, using a combination of academic definitions and real-world experience.

Chapter four describes CONTEST, the UK government's counter-terrorism strategy that was first introduced in 2006. The principles of the strategy are examined, including the latest policy update announced in June 2011. The four central pillars of the CONTEST strategy are known as PREVENT, PURSUE, PROTECT and PREPARE, and these are described in detail, explaining the aims of each pillar and providing examples of the work involved in each of them. The CONTEST strategy is a crucial backdrop to the use of the Intelligence cycle in counter-terrorism, as this policy underpins the model as used by the UK Intelligence community. Some aspects of the CONTEST policy have been subjected to intense media scrutiny, especially when high-visibility raids (such as Operation VOLGA in Forest Gate, London, in June 2006) have not culminated in a successful prosecution (Glass, 2006).

Chapter five concentrates on a deep analysis of the cycle itself, examining the Intelligence process and the difficulties which agencies face in their collection, production, reporting and use of Intelligence. It begins with direction, detailing the process that takes place before an agency or an asset can be tasked with collecting Intelligence. The collection process is described, covering overt and covert sources. Some of the strengths and limitations of these sources and methods are also covered. Collation is often overlooked or even ignored by some Intelligence staff, yet it is a fundamental piece of the Intelligence cycle. It brings together all available material already held on a target, and puts it into a format or formats best suited to assist with the analytical process. More than any other aspect of the Intelligence process, evaluation was singled out for criticism in the UK government's inquiry (Butler, 2004) and considerable space is devoted to the importance of evaluation within the cycle. Analysis forms the core of Intelligence work and it usually receives the most attention, especially in the area of published works, yet it is co-dependent upon the other aspects of the cycle. Inaccurate direction can lead to the collection process being misdirected, and following the collation of material already held, the analysts can only work with the material provided. Incorrect, faulty or incomplete analysis likewise has a direct result on the production of a finished Intelligence product that may then be disseminated to customers.

Chapter six presents for discussion some of the strengths and weaknesses of the Intelligence cycle. In this chapter, common problems with analysis are examined, and their potential impact discussed. It also takes the recurrent problems and accepted pathologies of Intelligence sharing, as well as the wider Intelligence process and discusses them in detail, with examples provided where practicable. Intelligence "stovepipes" or "silos" are often necessary for the protection of sensitive Intelligence, but they can also be a contributing factor to Intelligence failures. The strengths and weaknesses of the cycle are described, with the additional benefit of primary source material. This is derived from personal, semi-structured interviews with retired and serving Intelligence officers covering a wide spectrum of agencies and departments. Most of these have considerable experience in counter-terrorism Intelligence and have been personally involved in all aspects of the cycle. Their opinions and experiences are a valuable resource of first-hand understanding of how the cycle functions in the real world, and how effective it is in counter-terrorism.

Chapter 7 consolidate the essential elements of this research and details the paper's conclusions, returning to the thesis question of how effective the Intelligence cycle is, as a model for UK counter-terrorism. Suggested changes are provided, which make the Intelligence cycle still more robust for its continued deployment in the field. This final chapter also identifies areas for future research in this field of study.

1.5 Theoretical Framework

1.5.1 The Composition of the UK Intelligence Community.

The UK's Intelligence machinery is made up of the three primary Intelligence collection agencies (SIS, GCHQ and the Security Service), together with the Joint Terrorism Analysis Centre (JTAC), Defence Intelligence (DI) and the centralised Intelligence machinery of the Cabinet Office (Cabinet Office, 2010b:1).[4]

The three primary agencies are responsible for the collection of secret intelligence. The first two are the Secret Intelligence Service (SIS), often referred to as MI6, and the Security Service, often referred to as MI5. Both these agencies are covert and the identities of the majority of their staff are not released publicly. The majority of the UK's mainstream media agrees to abide by a voluntary code regarding publication of material concerning the national security of the UK. Defence Advisory Notice 5 (often referred to as a "D Notice") specifically covers, amongst other topics:

> "*the identities, whereabouts and tasks of people who are or have been employed by these services or engaged on such work, including details of their families and home addresses, and any other information, including photographs, which could assist terrorist or other hostile organisations to identify a target*" (Ministry of Defence, 2008).

The third agency is the Government Communications Headquarters (GCHQ). Whilst the nature of GCHQ's work is also secret, it is not classed as a covert agency but an overt one. That is not to say that the work it carries out is overt, rather that the UK's Intelligence machinery classifies it differently because GCHQ staff are not subject to same rules on disclosing where they work, as officers from SIS and the Security Service.

SIS works primarily as a HUMINT Agency, collecting secret intelligence abroad and mounting covert operations abroad to support the UK government in areas such as counter-terrorism, national security and interdicting serious crime. In addition, it has a highly developed technical intelligence collection

[4] In 2009, the organisation known as Defence Intelligence Staff (DIS) was renamed to Defence Intelligence (DI).

capability. The activities conducted by SIS are legislated by the Intelligence Services Act 1994 (ISA), (Parliament, 1994). SIS (2011) describes its missions as:

> "*to give the UK advantage, acting secretly overseas to make the country safer and more prosperous…by… obtaining secret intelligence on critical security and economic issues to inform better policy decisions…operating overseas to disrupt terrorism and proliferation and helping to prevent and resolve conflict…using covert contacts overseas to shape developments and exploit opportunities in the UK's interests*".

The Security Service is the national security Intelligence agency of the UK and is responsible for "*protecting the UK against threats to national security from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means*" (Security Service, 2011). The agency is legislated by the Security Services Act 1989 (Parliament, 1989). It also holds an advisory capacity, providing advice on a range of security threats to other organisations, and this function extends to installations designated part of the UK Critical National Infrastructure (CNI).[5] The Security Service has been carrying out a gradual expansion beyond the physical confines of London and to date it has eight regional centres in the UK, plus an additional Headquarters in Northern Ireland, based in Belfast.

Of these three primary intelligence collection agencies, officers from the Security Service work more closely and more frequently with the UK Police than the others, yet officers from the Security Service have no powers of

[5] The UK's Critical National Infrastructure is broken down into ten key areas. These are: communications, emergency services, energy, finance, food, government and public services, health, public safety, transport and water. See chapter 4.3.1

arrest, have no executive powers and are not issued warrant cards. Officers from the Security Service have traditionally worked in very close co-operation with Special Branch officers, (especially during the height of the terrorist campaigns in Northern Ireland, and more recently with the rise of Islamist terrorism).

GCHQ has two primary roles. The first is to conduct Signals Intelligence (SIGINT) in support of UK national security and the economic well-being of the UK, as well as supporting the operational capacity of the UK Armed Forces and the UK Law Enforcement community. The second role is conducting Information Assurance (IA), which aims to secure and protect the sensitive information of the UK government and its associated entities. This role falls to the Computer Electronic Security Group (CESG) which holds the responsibility of being a national technical authority on IA within the UK. A key role of CESG is in protecting UK government and defence computer networks from external attacks and intrusions, from cyber-vandals, Hostile Intelligence Services (HIS) and hackers (GCHQ, 2011). Together with SIS, the operational activities of GCHQ are covered by the ISA, and the Regulation of Investigatory Powers Act 2000 (RIPA).

The Joint Terrorism Analysis Centre (JTAC) is the newest organ of the UK's formal intelligence machinery, having been created in June 2003, and its role is described as follows:

> "*JTAC analyses and assesses all intelligence relating to international terrorism, at home and overseas. It sets threat levels and issues warnings of threats and other terrorist-related subjects for customers from a wide range of government departments and agencies, as well as producing more in-depth reports on trends, terrorist networks and capabilities*" (Security Service, 2015).

JTAC was a ground-breaking body when it was formed, as it brought together for the first time a truly multi-agency workforce in a centralised location, all of which had access to their own agencies' intelligence products, systems and procedures. A key strength of JTAC is that in addition to its full-time, core workforce from sixteen agencies and government departments, it can draw upon other agencies and assets, depending upon the nature of the work it carries out. The London terrorist attacks in July 2005 were an example of this, when several other agencies contributed staff to the post-incident work of JTAC. Some of these agencies are not traditionally involved in intelligence work, but their sector expertise was necessary in the post-attack phase.

Defence Intelligence (DI) is a component part of the UK Ministry of Defence (MOD) and not an independent organisation. It is headed by a serving 3-star officer of the UK Armed Forces, who also holds the post of Chief of Defence Intelligence (CDI). Until 2009, DI was called the Defence Intelligence Staff (DIS). DI staff members are either civilian or military, and the military staff members are drawn from all branches of the Armed Forces.[6] The official website (MOD, 2015) describes DI and its role thus:

> "…*an integral part of the Ministry of Defence (MOD) and the main provider of strategic defence intelligence to the department and the Armed Forces. It provides timely intelligence products, assessments and advice to guide decisions on policy and the commitment and employment of the Armed Forces; to inform defence research and equipment programmes; and to support military operations*".

The primary function of DI is not to serve as an intelligence collection agency *per se*, but to conduct all-source analysis across a wide range of intelligence

[6] In 1964, the Intelligence staffs of the Army, Navy and Air Force were combined with the civilian-staffed Joint Intelligence Bureau (JIB) to form the Defence Intelligence Staff.

feeds, both overt and covert. Notwithstanding this, it does fulfil some intelligence collection functions, though these are usually in support of either military operations conducted by the UK Armed Forces, or in support of the 3 primary intelligence collection agencies. An additional key function of DI is the provision of Geospatial Information Services (GIS).

1.5.2 How the UK Intelligence machinery functions

In the UK, the primary Intelligence agencies (SIS, Security Service and GCHQ) are tasked by a central core of Cabinet Office inner machinery which is led by the Chairman of the Joint Intelligence Committee (JIC), who also holds the position of Permanent Secretary for Intelligence, Security and Resilience. The tasking is carried out according to the intelligence priorities agreed by the JIC, and is conducted according to the agreed requirements, which are subject to approval by the NSC Committee for Threats, Hazards, Resilience and Contingencies.

The JIC was created in 1936 to bring together the Heads of the intelligence collections agencies, plus other related departments such as the Ministry for Economic Warfare. The responsibility of compiling the strategic Intelligence assessments for the government has lain with the JIC for more than 60 years. The role of the JIC is to provide the Prime Minister, Cabinet Ministers and other senior government officials with "*co-ordinated inter-departmental Intelligence assessments on a range of issues of immediate and long-term importance to national interests, primarily in the fields of security, defence and foreign affairs*" (Cabinet Office, 2010b:23). A report written for the JIC in 1945, on the future composition and direction of the group in the post-war world, used a term which had as much relevance for the JIC in 1945 as it still does today. The report, entitled "The Intelligence Machine", considered that all of the departments producing Intelligence should have no reason to refrain from sharing their material at "*the anvil of discussion and appreciation*" (Herman, 2011:17).

The JIC Chairman also holds two other posts: Professional Head of Intelligence Analysis (PHIA) and Head of the Joint Intelligence Organisation (JIO). As Chairman of the JIC, he reports directly to the Prime Minister for the overall supervision of the JIC's output. His role as Head of the JIO charges him with the supervision of the Assessments Staff (AS). The AS are responsible for producing draft JIC papers, as well as other all-source assessment papers covering issues relating to UK national security. The AS is made up of analysts from a range of government bodies and departments, and they have access to intelligence reports produced by SIS, Security Service and GCHQ, plus diplomatic cables, military reports and relevant open source reports.

The Chief of the Assessments Staff is responsible for the "provision of timely, accurate and objective all-source intelligence assessments and through provision of a tailored service of policy-relevant intelligence to senior readers", and also acts as the leader of the Assessments Staff team.(UK Government 2015). According to Davies, the Chief of Assessments Staff is "of "three-star equivalent" seniority, hence of roughly the same rank as Chief of Defence Staff" (Davies 2012a). The Chief's primary customers are the JIC Secretariat, the Cabinet, the NSC, COBR and ultimately the Prime Minister.

These draft JIC assessments are themselves subject to further assessment conducted by Current Intelligence Groups (CIGs), in a similar manner to that of a peer review in the academic community. The CIGs are staffed by analysts and experts from the intelligence agencies as well as from other government departments. A former Director of GCHQ described the JIC process as follows:

> "*The JIC process is, as far as I know, unique around the world. One reason may be that the process involves close interaction between the senior policy makers and the intelligence community, examining the most sensitive intelligence in the course of producing JIC papers. But the reason the JIC emerged during the Second World War as it did was to bring greater rationality into bitter strategic debate*" (Omand, 2005:7-8).

In March 2005 a report was presented to Parliament, outlining the changes which were to be made in the field of Intelligence and security. One of these was the establishing of the post of PHIA. According to the report (Cabinet Office, 2005:09-10), the role of PHIA is to:

> "*advise in the security, defence and foreign affairs fields on gaps and duplication in analyst capabilities, on recruitment of analysts, on their career structures and on interchange within and beyond Government; to advise on analytical methodology across the intelligence community; and to develop more substantial training than hitherto on a cross-Government basis for all analysts working in these fields*".

The role of PHIA came about because of a recommendation from Lord Butler's review. He saw a need for an Intelligence analysis professional to "*provide a "champion" for analysts, and to establish a distinct career specialism for this group*" (Howells, 2009:32-32). The role of PHIA is clearly a key one and the ISC were keen that this should constitute an independent role. Butler's review generated intense public interest in the various issues around the Intelligence upon which the decision to invade Iraq was ultimately based. It was therefore surprising when the government of the day decided not to make the PHIA post an independent one, but to leave it combined with the role of JIC Chairman. Given the accusations of politicisation which were prevalent at the time, it was a curious decision. The ISC (Howells, 2009:para.114–115) made their disagreement and displeasure very clear in a strongly worded paragraph of their Annual Report which stated:

> "*We are therefore very concerned that the post remained vacant since Jane Knight (the first post-holder) retired in August 2007. We are particularly concerned that the progress achieved during the previous two years may be lost. Although we note that the Deputy Professional Head has been covering both posts during this time, we question the extent to which one person can adequately cover two demanding posts at the same time. The JIC Chairman told us in January 2008 that thought was being given to the future of the Professional Head post – whether it should be a separate post, or whether it should be amalgamated within the JIC Chairman role. The Cabinet Office has since told us that a decision has been made to subsume the role within the JIC Chairman role.* ***Given the importance of the Professional Head of Intelligence Analysis (PHIA) post, we are very concerned by the plan to subsume the role within the Joint Intelligence Committee Chairman's post as this may actually lessen the priority given to this crucial role. The Committee is disappointed that the PHIA post has not been maintained as a distinct and separate role***".[7]

The concept of professionalising a top-level role at the apex of the Intelligence analysis community is not new. Lord Franks made the same point in his

[7] Text in bold as emphasised by the ISC in the original report.

review for the government of the day, of the circumstances which led to the Argentine invasion of the Falkland Islands (Aldrich, 2009:238).

1.5.3 Legislation and oversight of the UK Intelligence Community

Whilst the covert agencies of the UK Intelligence machinery (SIS and the Security Service) have been in existence for over a century at the time of writing, the concept of wider accountability for the UK intelligence machinery is a relatively new one. Gill (2011:46-47) defines Intelligence oversight as "*the scrutiny of agencies' actions, whether contemporaneously or after the event, in order to ensure their effectiveness, legality and propriety on behalf of the public*". A key driver in the push for greater oversight of the Intelligence machinery was the growing concern across Britain's left-wing political landscape that the Security Service was employing its powers of investigation and surveillance to intrusively monitor left-wing political entities under the umbrella of countering subversion of the State. During the 1970s and the 1980s, this concern focused on some of the major political issues of that era. Allegations were made that bodies targeted by the Security Service included the Campaign for Nuclear Disarmament (CND), the National Union of Miners (NUM), the Associated Society of Locomotive Engineers and Firemen (ASLEF), a number of Labour Members of Parliament and even Prime Minister Harold Wilson. The situation was not helped by the response of former Prime Minister Jim Callaghan when giving evidence before the Treasury and Civil Service Committee. When questioned on whether he felt that the accountability of UK intelligence agencies was satisfactory or not, he replied:

> "*I am not sure what its accountability is to Parliament…….I am going to give you a very unsatisfactory answer, I do not know…..I think the ethos of those particular services is*

> *probably as important as the degree of accountability that you can visit upon them…….I am going to give you a very unsatisfactory answer, I do not know"* (Norton-Taylor, 1995:1; Griffith, 1987:982).

The Interception of Communications Act 1985 (IOCA) was introduced in the UK as a result of a challenge in the European Court of Human Rights (ECtHR) in Strasbourg, after the case of *Malone v. UK* in 1984(European Court of Human Rights, 1985).[8] The introduction of IOCA covered only the lawful intercept of postal mail and telephone calls, thus leaving additional interception methods (such as intrusive bugging) outside this legislation and thus regulated only by Home Office guidelines (Phythian, 2009:338). The legal case of two prominent Labour Party members taking their complaint to the European Commission of Human Rights in 1985, plus other cases, prompted the UK government to enact the Security Services Act of 1989 which placed the Security Service on a statutory footing for the first time.[9]

[8] The case of *Malone v UK* went before the ECTHR in 1984 and the verdict was delivered in Strasbourg on 26 April 1985. The complainant, Malone, "*asserted that his telephone conversation had been tapped on the authority of a warrant signed by the Secretary of State, but that there was no system to supervise such warrants, and that it was not therefore in 'accordance with law'. The taps were based on a non-binding and unpublished directive from the Home Secretary to the Director-General of the Security Service. The directive did not have the force of the law, nor did its contents constitute legally enforceable rules governing the operation of the Security Servic*e". It was held that "*the interception pursuant to such a warrant was an 'interference by a public authority' with the right to a private life. English law did not meet the requirement that any interference must be 'in accordance with the law'. The law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference. English law does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking. The Court would reiterate its opinion that the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law*" (SWARB, 2014).

[9] Harriet Harman was a Labour MP in 1985, and a practising Solicitor. Patricia Hewitt was a former Secretary General of the National Council for Civil Liberties, an organisation which MI5 had classed as subversive. Following the revelations from an MI5 whistle-blower, Cathy Massiter, that MI5 had placed both Harman and Hewitt under surveillance (which included intercepting their telephone calls), both Harman and Hewitt began a joint action in 1986 to take the UK government to the European Commission of Human Rights, claiming that the surveillance breached the following rights: the right to privacy (covered in Article 8); the right to freedom of expression (covered in Article 10); the right to freedom of association (covered in Article 11); and the right to an effective remedy for breaches (covered in Article 13). in respect of the violations arising from the nature and consequences of the surveillance to which they had been subjected by MI5. In May 1988, the legal application for the case was declared admissible. In its final report, the Commission found in favour of Harman and Hewitt, concluding by a majority verdict, that: "….*given the existence of practices in the United Kingdom permitting secret surveillance and given further the reasonable likelihood that the applicants were the subjects of surveillance the compilation and retention by the Security Service of information concerning the private lives of the applicants constituted an infringement of their right to privacy under Article 8 (1) of the Convention. The Commission further concluded that the domestic law of the United Kingdom contained neither legal rules formulated with sufficient precision nor a framework indicating with the requisite degree*

SIS was not formally acknowledged as an Agency until 1992, when the Prime Minister at that time, John Major, admitted its existence openly. The Intelligence Services Bill of 1993 was enacted into UK law as the ISA on 26 May 1994 and it included mechanisms for additional oversight of SIS and GCHQ, plus some additional caveats on Security Service warrantry. The purpose of the Act, as described in the long title, is:

> *"to make provision about the Secret Intelligence Service and the Government Communications Headquarters, including provision for the issue of warrants and authorisations enabling certain actions to be taken and for the issue of such warrants and authorisations to be kept under review; to make further provision about warrants issued on applications by the Security Service; to establish a procedure for the investigation of complaints about the Secret Intelligence Service and the Government Communications Headquarters; to make provision for the establishment of an Intelligence and Security Committee to scrutinise all three of those bodies; and for connected purposes*" (Parliament 1994, p.3).

Section 10 of the Act (Intelligence Services Act, 1994:7) legislated for the establishment of an Intelligence and Security Committee (ISC), the remit of which was to provide an oversight and investigative function, regarding the "*expenditure, administration and policy of (a) the Security Service; (b) the Intelligence Service; and (c) GCHQ*". The introduction, composition, responsibility and reporting lines of this committee generated spirited debate in Parliament at the time. There was resistance to the validity of the ISC from the leader of the Labour opposition, who accused the government of the day

of certainty the scope and manner of the exercise of discretion by the Security Service in the carrying out of secret surveillance activities to render interference "in accordance with the law" within Article 8 (2). Finally the Commission concluded that since no information was forthcoming in relation to how the United Kingdom had chosen to provide an effective remedy under its domestic law that the applicants did not have an effective remedy as required by Article 13" (ECHR, 1993) of creating Prime Ministerial oversight as opposed to parliamentary oversight, stating:

> *"Whatever the status of the committee, it should not be able to interfere in operational matters….I am also concerned that the committee will apparently not have the power to call witnesses and commission papers to be brought before it. That is another weakness for a committee that is seriously expected to deal with scrutiny or oversight…Furthermore, it is proposed that the committee should not report to Parliament but to the Prime Minister. I do not regard that as parliamentary scrutiny or oversight, because the Prime Minister has the right to veto sections of its report—I call it prime ministerial oversight and scrutiny. If we are to have an effective parliamentary watchdog to oversee such matters and to probe and scrutinise, it should report to Parliament. It cannot legitimately be called a parliamentary committee unless it does so"* (HC Deb, 22 February 1994:col.171)*.*

The government countered this argument, pointing out that the ISC would be free to make public their displeasure with the way in which things were being handled by the Intelligence agencies, stating:

> "*Somebody asked earlier where the teeth were. The teeth consist of the fact that the committee, staffed by very senior Members of the House, will have the right not to publish stuff that would damage national security—which it would not want to do—but to write a report saying, "We believe that things are not being handled properly, and that Ministers are not responding properly." No Government in their senses*

> *would want to risk such criticism. That is why the committee will be powerful*" (HC Deb, 22 February 1994:col. 240).

The ISC published its first annual report in 1995 (King, 1995) and it has carried out this function each year since its inception.

Chapter 2 Methodology

2.1 Theoretical Framework and Argument

> "*If you want to understand what a science is you should look in the first instance not at its theories or findings and certainly not at what its apologists say about it; you should look at what the practitioners of it do*" Geertz (1973:5).

The Intelligence cycle was developed as a model to describe the Intelligence process and, with various refinements, has been taught within the UK Intelligence community for several decades. Following the 11 September terrorist attacks in the USA in 2001, and the subsequent invasions of Afghanistan and Iraq, considerable criticism has been levelled at the Intelligence processes which underpinned the decisions to go ahead with offensive military action against the regimes in Afghanistan and Iraq. The Intelligence agencies also conducted their own internal reviews of their processes, their checks and balances, even their very structures. External criticisms have been levelled at the Intelligence cycle and questions have been raised about its suitability for purpose (Hulnick, 2006; Warner, 2002; Treverton, 2001). In order to conduct a meaningful examination of the Intelligence cycle's effectiveness as a model in UK counter-terrorism, the intricacies of the various concepts of Intelligence and terrorism need to be examined.

2.2 Operationalising the Research Question

The methodology employed in this thesis will include both primary and secondary sources of data. The UK's Intelligence machinery and the systems and processes which it uses have been described in considerable detail within several UK government inquiries (Butler, 2004; Hutton, 2004; Taylor, 2003; Foreign Affairs Committee, 2003). The material contained in the various reports was provided by the Intelligence agencies and other government departments to these inquiry bodies in response to formal requests. Collectively this public record of information now comprises an accurate and concise insight into the inner workings of these agencies, including organisational structures, inter-agency co-operation, the tasking process, limitations of various Intelligence sources, and other areas of interest to this paper.

In writing this paper, the author has also drawn extensively on the personal experiences gained during his 30-year career in Intelligence, national security and counter-terrorism work. Since the author retired from the Intelligence community in 2009, he has continued to engage in the academic study of Intelligence, allowing him to straddle both the internal and the external viewpoints of the wider Intelligence community. His own personal knowledge and experience have been combined with the knowledge and experience of other Intelligence practitioners. A number of practitioners agreed to give personal interviews to the author, to provide unclassified and non-sensitive background material covering the key areas of the paper's research. This has provided the author with unique access to the views of officers deeply involved in Intelligence and counter-terrorism work on behalf of the UK government. This type of first-hand experience is seldom published.

2.3 Ethical Issues and Problems Encountered

As this research is centred on a topic which is sensitive in nature, the ethical considerations were carefully taken into account. After working for many years in a classified area, it is only natural that a classified body of knowledge is built up by anyone in this position. When this thesis was begun, the author was working in an Intelligence role overseas. The need to ensure that classified information did not inadvertently stray from the realms of memory into the body of the research was of paramount importance. This paper has been rigorously checked before submission, and has also been reviewed by more than one of the practitioners interviewed, to ensure that no sensitive information was contained within it. The author's personal experiences of using the Intelligence cycle, together with his impressions of the relative strengths and weaknesses of the model, have been incorporated into this research. These are more general observations and they do not rely on sensitive examples which would require an unacceptable level of detail to be revealed.

All of the respondents who provided interview material are either currently working in, or have previously worked in, areas including Intelligence collection, analysis, reporting, law enforcement, covert surveillance, policing, customs or the Armed Forces. All have long experience in their fields and a number of them have had training in media handling, under whichever term it falls within the various organisations (e.g. Public Information, media relations, defence media, etc.) The start of each interview consisted of a lengthy summary provided by the author, regarding the boundaries of the research, and the fact that the research itself was unclassified. The Author agreed with all interviewees that any audio recordings would be securely scrubbed electronically, after the interviews were transcribed. It was also agreed with interviewees that all written transcripts would be securely shredded after the thesis was submitted. The shredding was completed using a 1mm diamond-cut shredder, resulting in the same level of physical destruction as that employed within government establishments. This meant that all interviewees were assured of the data security measures implemented around the recording of interviews.

Compared with many Western countries, the UK has now placed into the public domain a substantial amount of previously classified documentation relating to the Intelligence world. Much of this has come from several government inquiries, some of which are covered in detail in this paper (Butler, 2004; Hutton, 2004). Some documents have been declassified in the public interest while others have been leaked and are now widely available on the internet (Rice, 2010).[10] This has resulted in a previously unavailable body of classified material being made available to the academic corpus which studies Intelligence processes. Some of the declassified material, such as the "Downing Street Memo" (Rycroft, 2002) was singularly illuminating in informing public opinion of the perceptions of senior UK policy makers involved in discussions with the U.S. government, prior to the Allied invasion of Iraq in 2003.[11] The unauthorised release by Chelsea (formerly Bradley) Manning, of classified material into the public domain, through the Wikileaks website, was previously unprecedented. The scale of the leaks and the viral spreading of the information on global "mirror sites" has meant that almost a million classified documents are now permanently located in the public domain. As one Intelligence officer remarked about these massive leaks: "*we can't put the genie back in the bottle this time*" (Source_12, 2011).

The potential for personal bias was also considered, due to the Author's previous work. A large quantity of academic literature was reviewed before the writing of this thesis began, to provide as neutral an assessment as possible of the current and previous academic landscapes in the area of study. The thesis question was deliberately designed to cover a review of the model, to keep the outcome and conclusions open until all the research had

[10] See Annex A for an example of a leaked U.S. Government report

[11] See chapter 6.1.1

been completed. The subject of personal bias in research presents a field of study in itself, but it would be useful to note some key points here. Denzin (1989:12) believes that "*interpretive research begins and ends with the biography and self of the researcher*", arguing that our own personalities dictate how we approach our research. According to this theory, removing all personal bias is impossible as our experiences have already preconditioned the ways in which we think about things. Mehra (2002:1) takes the argument further, arguing that even if the researcher tries to stop personal bias from entering their research, it will ultimately still affect it:

> "(*the*) *qualitative research paradigm believes that (the) researcher is an important part of the process. The researcher can't separate himself or herself from the topic/people he or she is studying, it is in the interaction between the researcher and researched that the knowledge is created. So the researcher bias enters into the picture even if the researcher tries to stay out of it*".

The framing of the thesis question was aimed at assessing whether or not the model of the Intelligence cycle remains effective. An assessment of this type is subjective by nature, but this does not necessarily imply a negative connotation. Heuer (1999:41–42), one of the most influential voices on the psychology of analysis, states that:

> "*One might speculate that the analyst who seeks greater objectivity by suppressing recognition of his or her own subjective input actually has less valid input to make. Objectivity is gained by making assumptions explicit so that they may be examined and challenged, not by vain efforts to eliminate them from analysis*".

The sourcing of opinion and comment from a range of senior and experienced practitioners from the Intelligence field adds a deeper and richer context to the academic framework of this study. Several academics have written papers on the Intelligence cycle, but a number of them are written with no practical insight into this area. The addition of personal insight from a spectrum of Intelligence disciplines brings a unique layer of context within which this assessment can be viewed. The value of practitioner experience was highlighted by Geertz (1973:5) who said: “*If you want to understand what a science is you should look in the first instance not at its theories or findings and certainly not at what its apologists say about it; you should look at what the practitioners of it do*”.

2.4 Literature Review

There are several journals and publications which concentrate on Intelligence studies, counter-terrorism, and the government organisations which carry out this work. These include, but are not limited to, “*Studies of Intelligence*”, “*Cambridge Review of International Affairs*”, “*International Journal of Intelligence and Counter-Intelligence*”, “*Intelligence and National Security*”, “*Journal of Policing, Intelligence and Counter-Terrorism*”, “*Journal of Peace Research,* “*Journal of International Law*” and the “*Journal of Strategic Studies*”. Additionally available material includes individual academic papers on Intelligence studies, position papers, newspaper articles, television documentaries, academic and non-academic books, UK legislation, political discussions in the Houses of Commons and Lords, and internet-based articles covering Intelligence and terrorism.

One of the biggest difficulties in Intelligence research has always been the availability of official documents relating to this subject matter. In addition to the UK governmental inquiries mentioned previously, the past decade has seen an increase in academic research in the field of Intelligence studies. This paper, although focused on the UK, draws on personal experiences in using Intelligence within an operational context in the UK and overseas. This provides an additional degree of context regarding the peculiar difficulties encountered in using the Intelligence cycle in hostile environments such as Iraq and Afghanistan, compared to UK-based operations.

The review of literature gives a high-level view of the current body of knowledge around the area of the thesis and serves three purposes. First, it identifies the extent of the key writings from the current literature available. Second, it was very useful in ensuring that there was no case of information overload when the research for the thesis began, as the key writings and findings had already been identified and extracted. Third, this body of key literature was assessed to elicit what areas it covered, the gaps which it did not cover at all (or covered but not to a satisfactory degree) and it was critically analysed for its relevance and contribution to the thesis question.

The "*Review of Intelligence on Weapons of Mass Destruction*" published by Lord Butler in July 2004 described the Intelligence process in some detail in its first chapter (Butler, 2004:7-16). In its conclusions, the report covered broad topics such as general summaries about the UK Intelligence machinery, Intelligence assessments and the use and validation of Intelligence. The enquiry focused on "*Intelligence coverage available in respect of WMD programmes in countries of concern*" among other areas (Butler, 2004:1). While some areas of the Intelligence process were put under the microscope by this enquiry, the scope of the report was more broad than narrow.

The "*Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly C.M.G.*" published by Lord Hutton in January 2004 (Hutton, 2004) contained a critical analysis of the provenance of Intelligence in the so-called "September dossier". This was a declassified summary of the UK Government's evidence that Saddam Hussein was developing a WMD programme. As the provenance of Intelligence is a key factor in the Intelligence cycle, the Hutton Inquiry also provided a wealth of source material for scholars and academics of Intelligence studies (Hutton, 2004:119–124). The Hutton Inquiry dissected the circumstances surrounding the death of Dr Kelly, but stopped short at voicing concrete recommendations. Lord Hutton explained his reasons for this, in the final chapter of the report, stating that: "*I* *have decided that it is unnecessary for me to make any express recommendations because I have no doubt that the BBC and the Government will take note of the criticisms which I have made in this report*" (2004:327). The Hutton Inquiry did, however, further ignite the public debate about the government's use of Intelligence, the "spin" that was believed to have been put on it, and the wider politicization of Intelligence.

Lefebvre's paper (2004), "*A Look at Intelligence Analysis*", is a suitable start point for looking at the process of analysis, covering ground such as the role of the Intelligence analyst and how analysts deal with uncertainty. He also asks a pertinent question, whether terrorism should be analysed differently, although the paper is not detailed enough to attempt anything more than a brief consideration of this question.

A RAND paper from 2008, "*Assessing the Tradecraft of Intelligence Analysis*", covers similar ground to Lefebvre's paper, but with a distinctly US-centric approach (Gabbard & Treverton, 2008). Most of the paper's recommendations only concern the U.S. Intelligence community and the training and productive employment of Intelligence analysts therein. The recommendations themselves are more conceptual than practical, such as "*a set of basic software tools common to the analytic community would facilitate joint analysis. An analyst from one agency could move to a task force or another agency and be able to "plug and play," without first having to master a new analytic workstation*" (Gabbard & Treverton, 2008:37).[12]

A useful collection of academic essays is contained in "*Secret Intelligence: A Reader*" (Andrew et al., 2009). Warner's essay (2002) dissects the problem of concisely defining Intelligence and he compares and contrasts a selection of definitions from narrow to broad, dating from 1955 to the present day. He concludes with his own definition of Intelligence as: "…*secret, state activity to*

[12] When this author worked in a national Intelligence agency, he had login details for almost 30 separate software tools and programs, and in addition, used another 20 or so which did not require a login. Many tools, as defined within the RAND report, are specific to task, discipline or repository. A SIGINT agency, for example, has extremely specific tools which would not be suitable for use in other agencies, such as a HUMINT agency.

understand or influence foreign entities" (Warner, 2002:21).[13] Davies presents a paper discussing some of the differences in British and U.S. definitions of Intelligence, and the importance this makes, specifically in how the Intelligence agencies of the two countries have traditionally approached the business of Intelligence collection and use (2002). Davies (2009:13) provides a detailed consideration of his topic, although some statements are inaccurate, such as "*While U.S. Intelligence analysis is professionalized, in British practice it is really no more than the ordinary work of government departments and ministries*". A highly detailed and well-researched paper by Aid (2009:40–77) examines the use of SIGINT in the field of international counter-terrorism, in which he usefully draws on examples of both U.S. and UK SIGINT collection against terrorist targets such as Al Qa'eda operatives. Aid's paper is all the more interesting for providing this detailed technical analysis on the topic of SIGINT, which is so rarely written about with such factual credibility. Aid also covers more wide-ranging topics related to SIGINT and counter-terrorism, such as the issues surrounding the dissemination of SIGINT material to customers, the problems encountered within inter-agency co-operation and the analytic shortcomings of the system due to problems such as a shortage of trained linguists.

Two essays by Jervis (2006:193-228) and Aldrich (2009:229–244) respectively cover Intelligence failures and four of the recent enquiries in the UK within which Intelligence became a key factor. Jervis (2006:193) introduces his paper with a hard-hitting statement on the Iraq WMD issue:

> "*The investigations are marred by political bias and excessive hindsight. Neither the investigations nor contemporary Intelligence on Iraqi WMD followed good social science practices. The comparative method was not utilized, confirmation bias was rampant, alternative hypothesis were*

[13] See chapter 3.2 for a detailed analysis of various definitions of Intelligence

> *not tested, and negative evidence was ignored. Although the opportunities to do better are many, the prospects for adequate reform are not good*".

Jervis discusses two types of Intelligence failure, both equally important and equally relevant in counter-terrorism Intelligence. The first type of failure he classes as "*the mismatch between the estimates and what later information reveals to have been true*" (Jervis 2006:197), and he classes the second type as "*a falling short of what we could expect a good service to have done*" (2006:198). The term "Intelligence failure" is now widely used in the media when reporting on both failed and successful terrorist plots. The questionable usage of the term by the media has resulted in the public perception of this word being critically distorted. What is often reported in a media report as an Intelligence failure is actually an Intelligence gap, and the distinctions between these terms, are covered in this paper.[14]

Aldrich's essay examines the approaches taken by, and the conclusions of, four separate Intelligence inquiries undertaken by various elements of, or on behalf of, the UK government between July 2003 and July 2004. Aldrich's work (2005; 2009) has direct relevance to a number of areas in this research paper, as he states:

> "*Although the enquiries have been useful in underlining the extent of genuine "Intelligence failure", wider reflections about the nature and direction of UK Intelligence have been conspicuously absent. None of the enquiries has dealt with the difficult issue of how Intelligence analysis might interface with modern styles of policy-making. More broadly, it is argued that there is a growing mismatch between what*

[14] See chapter 3.2.1 and chapter 6.

> *Intelligence can reasonably achieve and the improbable expectations of politicians and policy-makers*" (2005:1).

Another detailed collection of essays lies in "*Learning from the Secret Past: Cases in British Intelligence History*", edited by Dover and Goodman. The essays cover four central themes: the organisation and oversight of Intelligence; political interference in Intelligence; counter-insurgency and counter-terrorism; avoiding surprise. The essays include work by notable academics including Aldrich, Gill, Goodman, Herman, Phythian and Scott, among others. Adding particular interest to this collection is the inclusion of actual Intelligence documents upon which each essay is based. This lends an additional, historical focus to the work and brings academic insight to important documents such as "*The Intelligence Machine*" (Cavendish-Bentinck & Capel-Dunn, 1945) and "*The JIC and Warning of Aggression*" (Nicoll, 1981), known as the Nicoll Report.

Schindler (2009) writes on the relationship between Intelligence and strategy in respect to counter-terrorism and the Islamist threat. He briefly examines three case studies in counter-terrorism: Yugoslavia, Israel and Algeria. Even though specific links to Intelligence material within these campaigns are very thin, it is Schindler's conclusions that they are of more interest and relevance. Schindler muses on "*the way ahead*" (2009:255), pondering the limits of countering terrorism through offensive measures such as financial interdiction, the targeted assassination/detention of top-tier terrorist figures, and a publicity drive to counter the propaganda message of the salafist-jihadist publicity machine. He advocates the covert penetration of terrorist groups to prevent them co-operating with other groups and to deny them the opportunity of increasing their operational capability and effectiveness. He also makes a valid point that has direct relevance to UK counter-terrorism. Discussing President Bush's call for a 50% increase in CIA operations officers, Schindler comments: "*Mere numbers cannot compensate for missing expertise or ability, nor will it fix a broken tradecraft model*" (2009:256). His statement is of equal relevance to the directive that the UK's Security Service should increase its manpower by 50%, as a post-incident response to the London bombings of July 2003. A director of the Security Service, speaking in a public lecture, confirmed in 2006 that this increase had been achieved (Manningham-Buller, 2006).

In "*Intelligence-Led Policing*", Ratcliffe introduces the origins of the concept (2008:16–40), before delving into the tricky issue of actually defining it (2008:65–88). His work examines the analytical frameworks surrounding Intelligence-led policing, and he covers several useful models, such as Gill's cybernetic model (2000:22), the UK National Intelligence Model (NIM) (NCIS, 2000) and Ratcliffe's own 3-i model (2003:109). As Ratcliffe's work focuses on policing and not counter-terrorism specifically, he understandably places a greater emphasis on the UK's National Intelligence Model. He provides a thorough and detailed examination of the components of the NIM, how it is deployed, the composite products enshrined by it and what benefits it should provide. Much of his writing equally applies to policing and to counter-terrorism. Writing on the relationship between Intelligence and the general public, Ratcliffe (2008:49) considers the situation in the US, describing:

> "*a growing recognition of the need to redefine community policing (where it is still practised) within an Intelligence-led policing framework for counter-terrorism purposes, even though most local law enforcement officers have never had intelligence training and thus would be hard-pressed to recognise, or know how to share, information pertaining to terrorism that they may receive from the public*".

A duo of well-regarded writers on various aspects of policing and Intelligence, Clive and Karen Harfield, have produced a detailed work on the role of Intelligence in Policing, and the relevant legislation pertaining to it. Their work starts with a discussion of the concepts of Intelligence-led Policing (Harfield & Harfield, 2008:4–5), before moving on to a deeper examination of the problems with trying to define Intelligence (2008:50–68). Only four pages are devoted to a description of the Intelligence cycle itself (Harfield & Harfield, 2008:63–66), but their deeper discussions surrounding the use of Intelligence are most useful. The book deals with the Intelligence process and it devotes an entire chapter to the UK National Intelligence Model, as it is central to Intelligence-led Policing and to counter-terrorism in the UK (Harfield & Harfield, 2008:91–93).

An educational research consortium called the Transnational Terrorism, Security and the Rule of Law (TTSRL) was established by the European Commission (EC) in Brussels. One area of their research for the EC is on "Citizens and Governance in a Knowledge-Based Society" and a TTSRL-authored paper covers the difficult issue of defining terrorism (TTRSL, 2008). This policy brief begins by stating the case for arriving at a common definition of terrorism, recognising that "*in today's globalized world, it is impossible to fight terrorism effectively without functional cross-border cooperation*" (2008:1). It explains why an agreed definition is essential, in areas such as extradition or cross-border prosecution, and also makes a relevant connection between defining terrorism and ensuring transparency in deciding upon eligibility for refugee status. The report is hard-hitting and practical, and it does not shy away from criticising EU member states which it considers could do more. The UK is included in this category by the TTSRL consortium (2008:3). The most useful addition the policy brief makes is the identification of six key points, referred to as definitional elements, which the TTSRL considers necessary inclusions for any sound definition of terrorism. The brief also highlights why the EU's current "framework" definition is not effective, and why it needs to be strengthened (TTSRL, 2008:2).

As a writer on terrorism, Richard Jackson is prolific and controversial and he considers that terrorism is poorly defined and poorly characterised (2007:1). Jackson adds that the field of critical terrorism studies (CTS), on which he writes, is "*characterised by a set of core epistemological, ontological and ethical commitments*" (2007:1). He expands on this theme, analysing what he calls the "*politically constructed nature of terrorism*", and provides harsh criticism of four weaknesses which he contends have had a continual and negative effect upon the academic study of terrorism (Jackson, 2007:1).

The targets of Jackson's criticism are: poor and/or weak research methodology in the previous academic studies of terrorism, its root causes and definitions; the "*accepted*" body of knowledge being "*highly contestable and largely unsupported by empirical research*"; the linkages between many researchers of terrorism and the State-funded institutions which support them, and the lack of perceived neutrality or transparency which this can portray (the RAND corporation, for example, is singled out for particularly harsh criticism for what Jackson perceives as its lack of neutrality); finally, current models of approaching terrorism come from a "problem-solving" perspective, which assumes that the current status quo of the global political arena remains stable, a fact which Jackson sees as being a major contributory factor to the lack of a clear definition of terrorism (Jackson, 2007:1-7). Although there is a clear academic grievance in Jackson's criticisms, especially against the various works of Schmid, Silke, Jongman and other academics of Intelligence studies, he does make some valid points and justifies them accordingly. He presses for a "*broad, epistemological orientation*" in the field of terrorism studies, demanding to know who the research is primarily for, and how it will assist (Jackson, 2007:3).

A paper by Jones (2007) on terrorism studies takes as the centre point for its study the failure of the academic branch of terrorism studies to have satisfactorily moved the debate on to an explanatory level. On the contrary, the report, consisting of a critical examination of the literature in the field of terrorism studies in the period 2000-2007, suggests that the study of terrorism has not benefited from the amount of academic effort which has been put into it.

Schbley's paper (2003) on "*Defining Religious Terrorism*" recommends an interesting change in emphasis in the search for an acceptable, academic definition of terrorism. While retaining the focus on the methods used by terrorists, she proposes examining the *actus reus* of terrorist actions, rather than continuing with the more usual focus on the *mens rea* of those actions (Schbley, 2003:106).[15] Schbley considers that a definition of terrorism needs to be "*removed from politics and placed into the realms of criminal justice and future international criminal court(s)*" (2003:106) and she provides her own definition of terrorism as: "*Terrorism is any violent act upon symbolic civilians and their properties*" (2003:107).

While the detail of Schbley's paper adds much to the academic debate, her definition of terrorism adds less. Under the above definition, for example, an attack by a gang of hooligans upon a city Mayor and his official vehicle would be construed as terrorism. Schbley argues that the *jus in bello* of any such attack can never be justified by the counter-theory of *jus ad bellum*, although this leaves her own definition somewhat open to question (2003:107).[16] Furthermore, she postulates that any definition of terrorism must "*focus on a corpus delicti of irrefutable and uncontroverted facts that constitute its spirit and parameters*" (Schbley, 2003:106).[17] From Schbley's perspective, this would remove any possibility for legitimacy or justification of the terrorist

[15] The terms *actus reus* and *mens rea* refer respectively to concepts usually translated as "guilty act and "guilty mind". The concepts have their genesis in a legal principle stated by Edward Coke (1552-1634) which declared "*actus non facit reum nisi mens sit rea*". Roughly translated, the principle states that the act alone does not make someone guilty, unless the mind also is guilty.

[16] Laws such as the 1949 Geneva Convention stipulate certain conditions which warring nations must abide by in the engagement of war, such as the wearing of a standardised and easily recognisable uniform, the treatment of prisoners of war and the safeguarding of historically significant buildings. These constitute the *jus in bello*, or the acceptable limits of conduct during war. The justification on which it is considered acceptable to go to war constitutes the *jus ad bellum*.

[17] The term *corpus delicti* (meaning "body of crime" in Latin) relates to the principle that, before an individual can be convicted of committing a crime, that crime itself must be proven to have taken place. According to Black's Law Dictionary, *corpus delicti* is defined as "the fact of a crime having been actually committed".

offence being claimed, and ultimately, she considers that: "*a terrorist for one must be perceived as a terrorist for all*" (2003:106).

2.5 Collecting the Raw Data and Methods of Analysis

The primary question which this thesis seeks to answer is whether the Intelligence cycle is still an effective and fit-for-purpose model for the UK's counter-terrorism needs. A major benefit of the author's previous experience is the access to a wide-ranging network of practitioners, retired and serving, who all have long experience in the fields of counter-terrorism and/or Intelligence. To exclude personal bias as much as possible, none of the people who were approached to be interviewed had at any time acted in a work capacity as either the superior or the subordinate of the author. None of the interviewees are related to the author. Each individual was approached because they had the necessary experience and knowledge to make a valuable and unique contribution to the further study of the Intelligence field.

A total of eighteen individuals were approached, and all agreed to participate in the interviews. Of these, three were unable to do the interviews, either due to travel abroad, operational commitments and workload, or a combination of both these factors. It was accepted from the outset by the author that such a small number could not be described as constituting a representative sample, and indeed this was not the aim of the interviews. Rather, the aim was to use the filter of the personal perception of actual practitioners in Intelligence. This provided a unique perspective on the opinions of people who are or were recently actively engaged in counter-terrorism and/or Intelligence, regarding the effectiveness of the Intelligence cycle.

The majority of interviews were conducted in 2012, with a small number being done in 2013 and 2014. All interviewees were asked if they consented to the interview being recorded, for the sake of accuracy and transcription. All agreed, with the majority requesting that the audio recordings be securely erased after the interviews were transcribed, and the written transcripts destroyed after the thesis was submitted, due to the nature of the topic. In the event, this policy was implemented for all of the audio and written records, to ensure fairness and parity.

While it would undoubtedly add to the clarity of the interview material if every comment was referenced to a particular interviewee, it was agreed with the interviewees that this would only be done in the case of generic comments which did not reveal any of their personal backgrounds. The interviewees' combined amount of service totals almost 300 man-years of work in the areas of policing, security, sensitive Intelligence, counter-terrorism, counter-narcotics and law enforcement. In order to preserve the anonymity of the sources, no ranks, grades, appointments or seniorities have been divulged in this thesis, and neither have their exact number of years' service or experience been given. What can be said, however, is that none of the people interviewed have less than twenty years of operational experience in their respective fields and they have current or previous experience working in the following organisations: Security Service; SIS; GCHQ; the Police forces of the UK; Her Majesty's Customs and Excise; Serious Organised Crime Agency (SOCA) (now the National Crime Agency); Special Forces; Intelligence Corps (British Army); Foreign and Commonwealth Office (FCO); Defence Intelligence Staff (DIS) (now Defence Intelligence (DI)). Some have experience in more than one agency but this has not been disclosed in the thesis, to preserve their anonymity. Each interviewee was carefully selected for their experience, knowledge and field of operational activities. The author knows each of them personally.

2.6 Interview structure and interview questions

All interviewees were provided with an interview background form prior to the interviews being conducted. A sample of the form is provided at Annex B. The form was designed by another Doctoral Student on the same course, who generously provided permission to use this template after his successful graduation (Bhayani, 2013). This form explained a number of key areas. The abstract of the thesis was provided, which explained the aim of the paper and highlighted why the interviews were a key component of the research. As the interviewees all come from operational backgrounds, the principles of confidentiality and anonymity were very important, both to them and to the author. The form explained that any information which they might provide would only be included in the thesis if they agreed to its inclusion, having been made aware of the context in which the information would be used. It also reassured them that their identities, ranks/grades and other identifying information would be omitted, to ensure that any aggregated background information could not be analysed in the future, to reveal their identities or their specific roles at a defined point in time. These conditions were related verbally to the interviewees when they were initially approached about their willingness to contribute to the research, and they were related again at the start of the interview process.

It was agreed that an audio recording would be made of each interview, for the purposes of accuracy. On several occasions, a number of interviewees asked for the recording to be stopped so that they could discuss a sensitive topic, usually concerning an operation. On some occasions, it was requested that both the audio recording was stopped, and that no written notes were made. On other occasions, it was requested only that the audio recording was stopped, but the making of written notes was permitted, as the topic was less sensitive. As all of the interviewees are known personally to the Author, none of them requested to see a transcript of the finished interview.

It was initially planned to conduct each interview for around 90 minutes, to allow sufficient time to discuss the Intelligence cycle and its effectiveness. Two interviews lasted just under an hour, due to time constraints of the interviewees. Several lasted in excess of three hours, with one being conducted over a period of two weeks, due to the sheer amount of material covered. Geographic location and operational availability meant that two people were interviewed on more than one occasion. The interview was structured around seven questions, which were listed by the author at the start of each interview. The questions were asked as follows:

1. What model of the Intelligence cycle do you use in your workplace?
2. Is Evaluation included as a stage in the model which your workplace uses?
3. In your experience, what are the things which go wrong in the use of the Intelligence cycle?
4. Do you feel that the things which go wrong are usually in the same parts of the cycle?
5. In your opinion, could the Intelligence cycle be improved? If so, how?
6. Is the Intelligence cycle fit for purpose in your area of work, and in UK counter-terrorism?
7. Do you have any final thoughts on what has been discussed?

The breakdown of the interviewees was as follows:

Source	**Agency**
Interview 01	Police
Interview 02	Police
Interview 03	GCHQ
Interview 04	Police
Interview 05	SIS
Interview 06	SIS
Interview 07	Special Forces
Interview 08	Security Service

Interview 09	Defence Intelligence
Interview 10	Army
Interview 11	GCHQ
Interview 12	GCHQ
Interview 13	SOCA (now NCA)
Interview 14	FCO

Table 2 List of interviewees and their primary agencies

This chapter covered the methodology of the research, outlining the theoretical framework and the sources of information used. The importance was described, of using individual perspectives from serving and retired officials experienced in working with the model. Ethical considerations were then covered, with emphasis given to the care which has been taken to ensure that sensitive information was not inadvertently included in the finished research. The issue of personal bias in research was discussed and examples were quoted from notable academics in this field, describing the academic conflict inherent in conducting research, yet trying to ensure that personal bias does not exert an undue influence on the material collected, the interpretation of it, or the final conclusions of the research. A copy of the participant consent form was included and discussed, to demonstrate the information provided to each individual for reasons of disclosure and transparency. Finally, the process of the semi-structured interviews was outlined, showing where the conversations flowed from.

The next chapter describes the theoretical framework in detail. Two key terms are used in the thesis question: Intelligence and terrorism. While it is standard practice to define such terms, it is clear that these two key terms have inherent difficulties associated with defining and using them, especially the label of terrorism. The theoretical framework conducts a deep analysis of both terms. Many different definitions are provided as examples, and the merits of each are discussed. Defining the term of Intelligence has challenged government agencies and experienced academics equally. Some academics have employed various continua to contrast different definitions, while others have considered whether Intelligence is a structure, a process, a product, or a combination of any or all of these three concepts. Still others, primarily from government bodies, have crafted definitions which are products of the age in which they were made, such as those written in the immediate years after the Second World War or at the height of the Cold War.

Definitions of terrorism are even more politically, socially, legally and morally charged. The examination of the concept of terrorism takes in a wide range of thinking, of definitions, of academic argument and of the use of the term as an accusation. The cases of individuals are discussed, all of whom were directly associated with, or participated in, terrorism. Two of them were subsequently awarded the Nobel Price for Peace. These cases are included to illustrate the sheer complexity involved in attempting to define terrorism. Even the combined resources of the United Nations have been unable to craft an agreed definition of terrorism. It appears to be something which most of us think we recognise, but would struggle to describe it accurately, inclusively, fairly and succinctly.

Chapter 3 Theoretical Framework: Defining Intelligence and Terrorism

> "*And Moses sent them to spy out the land of Canaan, and said unto them, Get you up this way southward, and go up into the mountain: And see the land, what it is; and the people that dwelleth therein, whether they be strong or weak, few or many; And what the land is that they dwell in, whether it be good or bad; and what cities they be that they dwell in, whether in tents, or in strong holds; And what the land is, whether it be fat or lean, whether there be wood therein, or not*".[18]

Chapter 2 provided a brief outline of the methodology of this thesis, starting with an introduction to the theoretical framework. Some of the problems encountered in the research were described, such as the problem created with the unauthorised release of a huge quantity of classified documents to the Wikileaks website, together with their usefulness to the academic study of Intelligence. An extensive literature review followed, providing an assessment of a curated selection from the current landscape of academic writing in the areas of terrorism and Intelligence. The mechanism of collecting and processing personal experiences from interview subjects was then described, as this primary source material constitutes a critical part of the thesis. The personal insights collected from serving and retired counter-terrorism and Intelligence professionals constitute a unique body of knowledge in a subject which has relatively few practitioners studying it academically. The ethical considerations of the interviews were described, with considerable detail explaining the necessary security measures taken to safeguard the identities

[18] King James Bible, Numbers 13:17-20. This quote is often seen on the desks and walls within the UK intelligence community. It is also an excellent example of the "direction" phase of the Intelligence cycle.

of the interviewees, as well as the original records of the interviews, some of which were audio and some written. Chapter 3 advances this overview by moving into a detailed study of the definitions of the two key terms in the thesis question: terrorism and Intelligence. It also considers the inherent problems encountered with trying to define these terms and with the subsequent employment of them.

No serious analysis of the Intelligence cycle in counter-terrorism can be conducted before a thorough examination of the various definitions of these two terms has first been carried out, including the component parts of the definitions and the issues which revolve around them. The first half of this chapter takes the definition of Intelligence as its subject, looking at a number of definitions, analysing the component parts of them and considering their effectiveness in terms of practicality and employability. A brief summary is then provided, of the difference between an Intelligence gap and an Intelligence failure. Some definitions and causes are considered, using examples from works by Schulsky (Schulsky & Schmitt, 2002), O'Connor (n.d.), Laquer (1985), Lowenthal (2003) and Treverton (2008). The second half then considers the definition of terrorism, a highly political topic and one which is regnant in the academic communities of terrorism studies and Intelligence studies. A wide selection of terrorism definitions is then examined, and a number of issues are identified and discussed, which primarily emanate from the vagaries of these definitions.

3.1 Defining Intelligence

Attempting to define concepts as complex as terrorism and Intelligence creates problems which have troubled writers and practitioners for decades. It is often written, incorrectly, that the eminent military strategist von Clausewitz considered Intelligence to only add to the "fog of war", thus consigning Intelligence to the bottom drawer. While this maxim has now entered contemporary perceived wisdom, particularly in the military community, the phrase “fog of war” was not actually used by von Clausewitz in his book “*On War”.* He wrote: “*all action takes place, so to speak, in a kind of twilight, which, like fog or moonlight, often tends to makes things seem grotesque and larger than they really are*” (Clausewitz, 1976:140). Clausewitz’ main point, however, is directly relevant to the area of study concerned with definitions of Intelligence.

Although the collection of Intelligence has been around for millennia, it can be argued that we are no closer to a generally accepted definition of the concept. Gill (2009) states that there are three compelling reasons for a comparative study of Intelligence. First, the rationale for even conducting such a comparative analysis in the first place is a prerequisite, and he uses Bayley’s argument (1999:3–4), that: “…*all science is comparative in the sense of depending upon analysis of multiple cases. Science is the systematic observation of many instances of a phenomenon*”. Second, he considers classification to be “*the first step of any science*”, thus the classification of Intelligence and its related systems is of importance (Gill, 2009:83). Finally, the empirical body of evidence regarding the various definitions, systems, agencies, etc. should produce both differences and similarities which can be further studied and more deeply analysed (Gill 2009, p.83). He uses a thought-provoking comment from Herman (2001:138), namely that intelligence is not “*an isolated activity. It is an integral part of government. It reflects the character of national constitutions and the societies in which it is set*”. This comment is of direct relevance to the chapter on the UK’s counter-terrorism strategy (CONTEST) for Herman’s point is very true; it is impossible to separate the Intelligence process from the governmental processes of the country conducting it.

An oft-quoted maxim in Intelligence agencies says that “*Intelligence is finding out other people’s secrets*”, but while this encapsulates a core principle, it does not suffice as a definition.[19] Many definitions of Intelligence can be placed on an axis stretching from broad to narrow. At the broader end of the spectrum, definitions tend to include the entire intelligence process, up to and including all-source fusion, while at the narrower end of the spectrum, definitions focus more upon the actual collection itself. Warner (2002), Davies (2002) and others argue that this also provides a roughly equivalent spectrum upon which can be mapped the differing definitions of Intelligence which are held by the U.S. and UK. This theory holds that U.S. definitions generally tend to the broader end of the scale, while UK definitions tend to lean towards the narrower end. Davies writes at great length on this particular continuum and holds the opinion that broad definitions are less desirable as he believes that the resultant product from agencies using broad definitions will be competitive instead of complimentary. The end result, according to Davies, is "*conflict, not consensus*" (Davies cited in Treverton et al. 2006:21).

Another method expresses these definitions in a span ranging from "analytical" at one end, to "operational" at the other. Additional axes have been employed to assist with the mapping of definitions of Intelligence, such as the one spanning from "informational" at one end, to "organisational" at the other. Warner (2002:16) in particular considers some definitions being firmly entrenched at the informational end of the spectrum, something he considers ironic as these definitions are all the product of elements of the U.S. Intelligence community, or reports prepared on their behalf. Davies (2009:14) goes one stage further, arguing that the U.S approach considers information as "*a specific component of Intelligence, while Britain approaches Intelligence as a specific type of information*".

While these models only place a definition of Intelligence somewhere between two ends of a scale, Kent's position (1949:60) as early as 1949 was that Intelligence comprises three distinct types of substantive content, which he named as "*descriptive*", "*current-reportorial*" and "*speculative-emulative*".

[19] The author first heard this in 1984 and it has continued to be quoted since then. No attribution has been found for this maxim.

Descriptive was identified as being essential to the other two components, adding that descriptive is "*the groundwork which gives meaning to day-to-day change and…without which, speculation into the future is likely to be meaningles*s" (Kent, 1949:60) and he considered it the "*most important complicated element of strategic intelligence*" (Kent, 1949:viii). Current-reportorial he described as "*keeping track of the modalities of change*" (Kent, 1949:30), thus encouraging the analyst to constantly update his or her own knowledge on a target or subject as the picture changes. This is behaviour which is still strongly encouraged to this day within GCHQ, SIS and the Security Service. Kent's speculative-evaluative component is the trickiest of the three to describe and assess, focusing as it does on the analyst's ability to answer the fundamental question of the entire Intelligence process: "*so what?"* Kent's own description (1949:39–40) of the speculative-evaluative aspect states that it is "*far more speculative than…the basic descriptive and current reportorial…*" adding that it "…*puts a very high premium on the seeker's power of evaluation and reasoned extrapolation*".

It is a useful exercise to examine some definitions to compare and contrast them, and to understand the difficulties in trying to define Intelligence. The following definition comes from the U.S. National Security Act of 1947 (Senate, 1947:sec.3): "*The term foreign intelligence means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons*". This definition was cast in the immediate post-war years and carries with it the introspective focus, even the obsession and paranoia, then prevalent regarding U.S. concerns about the Soviet threat. Particularly in the aftermath of the post-2001 September attacks upon the USA and the terrorist threat which many countries now face from within the ranks of the population of their own nationals, the above definition does not bound the concept of Intelligence with sufficient inclusiveness. The terrorist attacks on the London transport system on 07 July 2005 (and the subsequent foiled attacks on 21 July 2005) were a stark reminder of the domestic terrorist threat which the UK faces. A definition exclusively focused on foreign elements falls far short of what is now required for an effective and workable definition of Intelligence for the UK.

Two years after the introduction of the National Security Act 1947, Kent attempted to frame Intelligence in a paper on U.S. foreign policy in 1949, writing (1949:vii) : "*Intelligence, as I am writing of it, is the knowledge which our highly placed civilians and military men must have to safeguard the national welfare*". This definition was rather vague but to be fair to Kent, the focus of his paper was not an academic discussion of what Intelligence consists of, rather it was a broader look at strategic Intelligence, within the context of U.S. foreign policy in the highly charged years immediately following the end of World War Two, and the descent of the "iron curtain" across Eastern Europe.

Six years later in 1955, the Clark Task Force (1955:26) made the following definition: "*Intelligence deals with all the things which should be known in advance of initiating an action".* This definition is so broad as to be of almost no practical use. Intelligence has a major role to play in informing decision-making, and the Intelligence cycle functions to provide the required product which can assist decision-making. Intelligence agencies, however, are rarely (if ever) in possession of all the facts desirous of being known by those directing the Intelligence process. Intelligence only assists the decision-makers. It does not, and cannot, make the decision by itself. The Clark Task Force definition considers that all things needing to be known prior to beginning a course of action fall under the term "Intelligence" yet this definition presages accusations of Intelligence failures because of its very wording: if we *should* know something prior to taking action, and we *don't* know it, this would be termed as an Intelligence failure by the Clark definition, rather than an Intelligence gap.

Some things on the Intelligence "shopping list" will never be known, despite the Intelligence community throwing all its resources at a problem. This leads to a discussion perennial in the world of Intelligence analysis: the topic of secrets and mysteries. Secrets are those things which the Intelligence community tries to uncover through all the means at their disposal. Mysteries are much less straightforward and may never be known. Nye (1994:88) provides a slightly different description of the distinction, that: "*a secret is something that can be stolen by a spy or discerned by a technical sensor … A mystery is an abstract puzzle to which no one can be sure of the answer*".

A simplified example of the difference between a mystery and a secret could be as follows: a secret is the disposition of Soviet strategic rocket forces during the Cold War, while a mystery is the mind-set of the Soviet leader at that time, and how he was expected to react, given a particular scenario. Andrew (2004:4) considers that collectively, analysts need to consider the past before trying to predict the future, noting that: "*during the twentieth century we were frequently very good at discovering our opponents' secrets when it mattered most but more confused than we should have been by the mysteries of what they intended to do*". Treverton (2009:9) notes a particular difficulty in collecting Intelligence for counter-terrorism, stating that: "*Cold War espionage practices will not work against terrorist targets because ... Al Qaeda operatives do not go to embassy cocktail parties*". Butler (2004:14) contributed to this argument, taking the discussion further by considering how a mystery cannot be converted into a secret by the Intelligence process, stating:

> "*A hidden limitation of intelligence is its inability to transform a mystery into a secret. In principle, intelligence can be expected to uncover secrets. The enemy's order of battle may not be known, but it is knowable. The enemy's intentions may not be known, but they too are knowable. But mysteries are essentially unknowable: what a leader truly believes, or what his reaction would be in certain circumstances, cannot be known, but can only be judged. JIC judgements have to cover both secrets and mysteries. Judgement must still be informed by the best*

> *available information, which often means a contribution from intelligence. But it cannot import certainty*".

The Clark Task Force definition is very broad in its terms of reference and it focuses on Intelligence as information, as opposed to Intelligence as process, or even as activity. Yet it also introduces the idea of action, something which has become a prime focus of the UK and U.S. Intelligence agencies since the 11 September attacks by Al Qa'eda. This focus was borne out of the need to take what was initially highly classified Intelligence and to sanitise it sufficiently that it could actually be used by those closer to the front-line operational areas, often described by soldiers as "where the flesh meets the metal".[20]

Vernon Walters (1978:621) was Deputy Director of U.S. Central Intelligence when he crafted the following definition in 1975: "*Intelligence is information, not always available in the public domain, relating to the strength, resources, capabilities and intentions of a foreign country that can affect our lives and the safety of our people*". Walters joined the Army as a soldier and was quickly commissioned, becoming an Intelligence officer and subsequently a diplomat. The influence of these different careers can be seen in his definition which encompasses the politico-military and economic spectrum while retaining the inclusion of the intentions and capabilities of other powers. Another former U.S. military Intelligence officer provided a definition in his published dictionary of Intelligence terms (Carl, 1990). In his book, Carl (1990; cited by

[20] The need for Intelligence to be sanitised to the lowest possible level was arguably driven by the U.S. Intelligence community prior to Operation Desert Storm, the Allied invasion of Iraq in 1991. The U.S. rolled out a wide-ranging effort called "Intelligence Support to the War Fighter", aimed at sanitising Intelligence to provide it down to as low as Squad level (This is roughly equivalent to Platoon level in UK parlance, consisting of approximately 30 fighting troops). When briefed into Orders for a forthcoming operation, the Intelligence contributed to the "Actions On" section, such as "actions on enemy forces" or "actions on ambush". When briefed into "Orders" for a forthcoming operation, the Intelligence contributed to the "Actions On" section, such as "actions on enemy forces" or "actions on ambush". Even before the Iraqi invasion of Kuwait, the UK had already introduced the "Tear Line Report" as a mechanism to provide an immediate, sanitised version of a sensitive Intelligence report. The idea was to be produce a report at SECRET or TOP SECRET classification, and at the end of the highly classified section a dashed "tear line" was printed, below which was a sanitised version, usually CONFIDENTIAL (before this was replaced in the UK by the new classifications of OFFICIAL in 2014), which could literally be torn off and given to others who were only cleared to this lower level of access. This was the forerunner of what subsequently came to be known as the "Action On" report used so frequently in the Iraqi and Afghan theatres of operations post-2001.

Muskingum University n.d.:para.2) describes Intelligence as: "*the product resulting from the collecting and processing of information concerning actual and potential situations and conditions relating to domestic and foreign activities and to domestic and foreign or U.S. and enemy-held areas*". His definition begins with clarity but ends with a slightly mangled bounding of the definition, which renders it cumbersome.

The Central Intelligence Agency took a radical step in 1993, with its publication of "*A Consumer's Guide to Intelligence*" (CIA, 1993). This publication was designed to assist Intelligence customers in using, digesting and operationalising the Intelligence produced by the CIA. As the Intelligence community takes on new staff each year, many of whom have little or no understanding of Intelligence sources and methods, collection capabilities or the limitations of Intelligence, it is important for the CIA to educate the analysts and other staff in the agencies and departments of the areas of U.S. government which are customers of CIA Intelligence reporting. The guide included explanations of important topics such as the language of probability and possibility and it provided definitions on some key terms, one of which was a definition of Intelligence: "*Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us. The prelude to decision and action by U.S. policymakers*" (CIA, 1993:vii).

This definition feels closer to the essence of Intelligence, and feels more useful in the everyday work of the Intelligence process. The terms "*knowledge and foreknowledge*" encompasses two important concepts. Knowledge of the world around us can consist, in Intelligence agency terms, of a large volume of material which shows us the *status quo* as far as it is believed to be accurate, of a country, an area, a situation or similar. The term "knowledge" implies that we have a body of reference material available, which can paint a sufficient background picture to allow us to form a detailed view of an Intelligence target. More important than this, however, is the term "foreknowledge", as this concept lies at the heart of Intelligence work. UK and U.S. Intelligence agencies expend a significant proportion of their efforts (in terms of manpower, budget, assets and time) on obtaining and refining actionable intelligence. During the Cold War, a large part of Intelligence collected by both sides consisted of initially discovering, then repeatedly confirming, the locations and dispositions of troops and equipment holdings of the adversary. Contemporary Intelligence, especially in the UK's counter-terrorism sector, has an intense focus on this actionable Intelligence, as it is of critical importance in the combined work of the agencies in carrying out the work of the PREVENT strategy. As one senior member of a UK Intelligence agency was fond of saying, "*the only Intelligence is actionable Intelligence, everything else is history*".[21]

This informal definition is a close relation to a short and very succinct definition by Professor John Grieve CBE QPM who has made major contributions to the field of Intelligence, both in UK policing and in the academic study of Intelligence. Grieve (2004:25) defines Intelligence simply as: "*information designed for action*". A former national co-ordinator for the Anti-Terrorist Squad, he was also the first Director of Intelligence for the Metropolitan Police, so the influence of his operational experience upon his definition is quite clear.

The CIA definition does not include the element of secret information, which some scholars such as Herman consider necessary. In contemporary Intelligence collection, open source Intelligence (OSINT) is now considered a discipline in itself and it can be argued that a focus on exclusively secret material is now outdated and inappropriate. The counter-argument to this is that the discipline of OSINT *can* be excluded from a definition of Intelligence, due to the fact that, by its very nature, OSINT material is in the public domain and attempts have not been made to conceal it. Where OSINT can really make a difference is in the identification of a piece (or multiple pieces) of information in the public domain which may not appear significant in Intelligence terms, but actually is significant. The subsequent analysis of such

[21] Anonymous.

information can allow the analyst to draw a reasonable conclusion about something which either was not contained in the original information, or which inadvertently leads to such a conclusion, unplanned by both the author of the material and the party with something to hide.

A classic example occurred in March 2010, when an analyst studying open-source defence contracts and tenders read about a planned shipment of military ordnance from the U.S. mainland to the island of Diego Garcia in the Indian Ocean. The consignment consisted of 387 bombs of the nomenclatures BLU-110 and BLU-117, commonly known as “bunker busters”. The most powerful of these weapons, designated the “super penetrator”, is designed to pierce up to 6 metres of reinforced concrete before detonating. The explosion of this weapon creates a *camouflet*, and the resulting debris buries the subterranean target in a massive quantity of displaced earth. The U.S. Air Force maintains a large airbase on Diego Garcia, which it leases from the UK. At the time of the shipment, tensions between the U.S. and Iran were especially high, following repeated Iranian non-compliance with United Nations nuclear inspection requirements. This was in addition to increasing friction between Israel, the U.S. and Iran. All of this took place against the backdrop of the publication by the US, the UK and France in September 2009, of a summary of their secret Intelligence concerning the construction of a covert uranium enrichment facility called the Ferdo nuclear site, near to the city of Qom. The island of Diego Garcia has previously been used as a launch base for U.S. airstrikes in several conflicts and the researcher examining the defence contracts and tenders realised that such a large consignment of “bunker buster” bombs had a high probability of being used in contingency planning for airstrikes on Iranian targets (Middle East Security Ltd, 2011). The story was published and resulted in considerable embarrassment for the U.S. administration, but it clearly illustrated the value of OSINT. The parties involved in releasing the contract information saw nothing compromising in the tender. All that was required was the background knowledge of an analyst, together with some educated guesswork, to put the pieces together and to produce an accurate supposition.

The collection of secret Intelligence usually relies on covert methods to carry out the collection. The analysis of the collected material must also be classified, to prevent the target from realising that the material has been successfully collected. Otherwise, the target would almost certainly close the gaps to prevent future collection, either using the same method or using the same point of entry, whether physical or virtual. The difference with OSINT is that the material has already been placed in the public domain, or is at least freely available.

Macartney (1995:3–4) defined Intelligence as "*a dedicated and usually tailored foreign information support service for government policymakers, planners and implementers*". This definition also has an exclusive focus on foreign targets, similar to previous ones. It includes the concept of a product being tailored, which could be considered to include an analytical process but could likewise be considered to simply be filtered, having undergone no analytical process. This definition also excludes non-governmental customers. The absence of any domestic aspect of the U.S. government's Intelligence needs is also a major omission.

The next definition, also organisational, was produced by the Aspin-Brown Committee between 1995 and 1996 in the US. The commission was established for the purpose of conducting a government inquiry into the status of the U.S. Intelligence community and its agencies, with a particular focus on how those agencies should be adapted (if necessary), to respond to the new global dynamic which followed the demise of communism and the break-up of the Warsaw Pact. The Commission (Brown & Aspin, 1996:5) defined Intelligence: "…*simply and broadly as information about things foreign – people, places, things and events – needed by the Government for the conduct of its functions*".

In order to contextualise the Commission's definition, it is important to understand the key drivers taking place contemporaneously, which resulted in the decision to appoint a commission to examine the U.S. Intelligence community. Two incidents were of specific importance. On 26 February 1993, the World Trade Center in New York was attacked, when a massive truck bomb was detonated beneath the North Tower by a group of terrorists (FEMA, 1993). Later that same year, U.S. forces were deployed to Somalia in support of a United Nations intervention there, aimed at establishing sufficient security to enable the distribution of humanitarian aid to the areas most affected by famine and drought (UNSC, 1993).[22] A contingent of U.S. Forces found themselves cut off in surrounded in the Baraka Markets area of Mogadishu, while attempting to capture General Mohammed Farah Aidid (UN, n.d.). In a 48-hour battle between U.S. forces and militia forces loyal to General Aidid, 19 U.S. troops and between 1,500 and 2,000 Somalis were killed (Stewart, 2003). The American public saw news footage of the corpses of several U.S. soldiers and aircrew being dragged behind pickup trucks through the streets of Mogadishu. Public opinion in the U.S. rapidly swung towards a withdrawal of U.S. forces from Somalia.[23] In the aftermath of "the battle for Mogadishu", questions were asked about whether Task Force Ranger (the main body of U.S. troops involved in the operation) had sufficient and accurate Intelligence before the failed operation to capture Aidid took place.[24] The Aspin-Brown inquiry took place against the backdrop of this deployment and the subsequent withdrawal of U.S. troops from Somalia. President Clinton announced the end of the U.S. deployment to Somalia just 2 months after the

[22] A mission under the auspices of the United Nations, designated UNOSOM II (also designated Operation CONTINUE HOPE by the U.S. Armed Forces) was created by the United Nations Security Council on 26 March 1993, under the authorisation of UN Resolution 814. The UNOSOM II mission formally began on 04 May 1993, when the preceding UNITAF force was disestablished.

[23] Although not academic books, two works that adequately cover the "Battle for Mogadishu" are first-hand accounts. One is "*Blackhawk down*" (Bowden, 2000), the other is "*In the Company of Heroes*", written by one of the U.S. helicopter pilots who was shot down, captured and tortured by the Somali militia (Durant, 2004). The battle, the capture of the U.S. pilot and the rescue attempt dominated the military-political landscape in the UK and U.S. headquarters for several months afterwards and is still used as a case study in military operational planning, especially in the subject of "centres of gravity".

[24] Although much internal debate took place, there have been no open source reports on this.

Battle of Mogadishu, and on 03 March 1994, U.S. forces completed this withdrawal (1998:33).

The Aspin-Brown Commission was open about the fact that it considered its definition to be simple and broad. In the same way as the Clark Task Force's definition focused on foreign targets, the Aspin-Brown definition contains no reference to domestic Intelligence targets, concentrating only upon "*things foreign*". The Aspin-Brown definition is vaguer than the Clark Task Force one, which is strange. When considering that the purpose of the Aspin-Brown Commission was to evaluate the status of the U.S. Intelligence agencies, it would be natural to assume that this body would devote significant effort to the understanding and defining of Intelligence, before beginning any examination of the community tasked with providing it. If this definition provides the foundation for an inquiry into the Intelligence agencies, it is a shaky foundation. The Aspin-Brown definition contains no reference to the collection of Intelligence or to the dissemination of it. It does, however, specify that the ultimate customers of the product are the Government, although it does not contain any reference to the expectation or otherwise that the Intelligence process itself is conducted by government elements. The definition does not add anything of substance to the debate and it was a missed opportunity for an influential U.S. body to compose a useful and encompassing definition of Intelligence for the U.S. Intelligence community.

The Council of Foreign Relations (CFR) describes itself as "*an independent, nonpartisan membership organization, think tank, and publisher*" (CFR, n.d.). It is an influential and established think tank, covering a wide range of the international political spectrum. In 1996, the CFR published a paper (Haas,1996:8-9) on "*Making Intelligence Smarter*", which included the Council's own definition: "*Intelligence is information not publicly available, or analysis based at least in part on such information, that has been prepared for policymakers or other actors inside the government*".

The CFR definition retains the focus on the end product being provided to policymakers and other governmental entities, and includes the fact that information used to produce Intelligence is either not in the public domain, or if it is, that this has been taken into account. As a definition, it is more useful but still lacks the wider perspective which has become more necessary in the present day, due in large part to the way in which the terrorist threat has morphed in the last 20 years or so.

Another user guide was published in 1997 and it defined Intelligence as "…*the knowledge – and ideally, the foreknowledge – sought by nations in response to external threats and to protect their vital interests, especially the well-being of their own people*" (Jentleson et al., 1997:365). This definition was fixed firmly at strategic level, placing Intelligence at national level and focusing on external threats, yet establishing the aim of such Intelligence as protection of national interests. Once again, the domestic aspect is missing but the well-being of the population has been included. Today, the protection of CNI is a national priority for the UK's National Security Strategy, as the national livelihood could be significantly disrupted by a successful terrorist attack against infrastructure such as the national grid, the water supply and other elements of the CNI (CPNI, 2010:5).[25]

In the USA, The Joint Chiefs of Staff (JCS) comprise the Chairman of the Joint Chiefs of Staff (CJCS), the Vice Chairman of the Joint Chiefs of Staff (VCJCS), plus the Heads of the various branches of the U.S. Armed Forces - the Navy, the Marine Corps, the Army, the Air Force and the National Guard. As in the UK, the U.S. Armed Forces are a primary collector, producer and user of Intelligence. The JCS produced their own, all-arms definition of Intelligence in 2001 just five months before the Al Qa'eda attacks against the USA in September of that year. Their definition differs from most of the previous ones in that it considers more fully the actual process of Intelligence, including the composite elements of the U.S. military Intelligence cycle (as it was at that time). It also did not restrict itself to external threats only. The irony is that the U.S. Armed Forces could be expected to have had a more external-

[25] The UK's Critical National Infrastructure, and the Intelligence requirements pertaining to the safeguarding of it, is covered in Chapter 4.3.1.

looking focus at that time, while some of the previous crafters of definitions could conversely have been expected to consider domestic and external threats equally. Yet the opposite was in fact the case. The JCS (Gortney, 2014:208) defined Intelligence in two ways:

> "*1. The product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas.*
>
> *2. Information and knowledge about an adversary obtained through observation, investigation, analysis or understanding*".

The Al Qa'eda attacks against the USA in September 2001 resulted in evaluations of the entire U.S. Intelligence landscape in the aftermath. These included the organisations, cultures, structures and processes, plus an analysis of any and all relevant Intelligence which could have been available prior to the attacks. A paper was presented to the U.S. Congress in 2004 outlining various options for changes within the FBI, in the wake of the Al Qa'eda attacks. Instead of attempting to use various layers of aspects, as other definitions had done, this paper framed Intelligence in three categories, which it extracted from existing U.S. legislation:

> "*Three formal categories of intelligence are defined under statute or regulation:*
>
> *Foreign Intelligence. Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons.*
>
> *Counterintelligence. Information gathered, and activities conducted, to protect against espionage, other intelligence*

> *activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.*
>
> *Criminal Intelligence. Data which has been evaluated to determine that it is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity. (Certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area)*" (Cummings & Masse, 2004:appx.1).

The definition is haphazard and while it does provide some principles, it implies that some factors are exclusive to the domain under which they are described. The category of criminal Intelligence, for example, is the only category which makes any mention of an analytical process, including evaluation, of the Intelligence. The implication is that analysis and evaluation counter-Intelligence, and in what this definition describes as foreign Intelligence.

The RAND Corporation is a US-based think-tank and describes itself as independent and non-partisan (RAND, n.d.). The origins of RAND come from the military research and development programmes which were still running as the Second World War came to a close in 1945. A part of the Douglas Aircraft Corporation was spun off into a separate project which took its name from a contraction of the terms "research and development" and its aim, as specified in the Articles of Incorporation for the new entity, were stated as follows: “To further and promote scientific, educational, and charitable purposes, all for the public welfare and security of the United States of America (RAND n.d.). At the time of its inception, all RAND staff would have had a US government security clearance. Today RAND publishes frequent papers in the area of defence and national security. In 2005, RAND UK published a paper (Hannah et al., 2005) focused on the legislation of Intelligence and security, within the context of security sector reform (SSR). Within this paper (Hannah et al., 2005:iii) RAND provided their own definition of Intelligence as:

> “*a special kind of knowledge, a specialised subset of information that has been put through a systematic analytical process in order to support a state’s decision and policy makers. It exists because some states or actors seek to hide information from other states or actors, who in turn seek to discover hidden information by secret or covert means. Within a security sector reform context, intelligence has also been defined as the ‘production of unbiased information about threats to the national vision*”.[26]

This definition includes the analytical process, and includes the term “systematic” when describing it, indicating that some model of process is followed, whether cyclical or otherwise. Its focus is once again on Intelligence being used to support State actors, and it adds an interesting dimension to the

[26] Despite its claims to be independent and non-partisan, RAND’s independence has been seriously questioned in the academic arena, most notably in an academic paper by Burnett and Whyte, writing in the Journal for Crime, Conflict and the Media (2005:9). In their paper, the authors described the nexus between the RAND Corporation and the St. Andrews University Centre for Studies in Terrorism and Political Violence (CSTPV). They question the validity of peer-reviewed research articles published by the Centre, writing that: “*Many of the top editorial positions of this journal are occupied by RAND employees, and Magnus Ranstorp and Paul Wilkinson of the CSTPV have positions on the editorial committee of the journal. What this effectively means is that, in this context, peer reviewed publications are dominated by academics connected by this nexus of influence. Whilst we are by no means suggesting that the system of peer review being used is in any way corrupted or less rigorous than it is in other publications, if we consider that two of the key journals in the discipline are dominated by scholars from the RAND-St Andrews nexus, then this does say something about their ability to impose their influence upon the field*” (Burnett & Whyte, 2005:9).

definition by including the fact that Intelligence comes from information which others necessarily want to keep secret. It follows up on this by adding that the discovery process itself is covert. The final part of the definition was included as the paper's focus was on SSR. The inclusion of the word "unbiased" is of note, as it did not feature in any of the previous definitions described. The principle of the information being unbiased is sound, and is one which any credible Intelligence agency should strive for. As we have seen, however, this principle is not always upheld.

In July 2004, the UK government published its "*Review of Intelligence on Weapons of Mass Destruction*", referred to as the Butler Report (Butler, 2004). The report provided a valuable repository of information for those involved in the academic study of Intelligence, as it included not only previously classified Intelligence material, but also the resulting Parliamentary commentary upon this Intelligence. As could be expected, the Butler Report included a section wherein it defined Intelligence. It also discussed the component parts of the Intelligence cycle and it highlighted some of the common problems encountered in the world of Intelligence, notably including validation in this section (Butler, 2004:99–102). Butler's (2004:7) definition of Intelligence was:

> "*Information acquired against the wishes and (generally) without the knowledge of its originators or possessors is processed by collation with other material, validation, analysis and assessment and finally disseminated as 'intelligence'.*

Like the Rand definition, this one also includes the idea that the collected raw product is something which its owners do not want to be revealed. Similarly, this definition clearly states that the information, once acquired, is subjected to a process before it can be considered to be Intelligence, but it goes one step further than RAND, adding crucial elements of validation and assessment to it. In the UK, the AS play a crucial part in assessing the most sensitive Intelligence for UK government customers and it is highly likely that the familiarity with the work of the AS coloured this definition. It also makes a distinction between information and Intelligence, placing information at the start of the process and Intelligence at the end, implying that the actual end product of Intelligence only comes at the end of the cycle.

It may be more useful to consider Intelligence not just as a process but as a combination of factors, regardless of how we define it. Ratcliffe (2003:3) considers that: "*a broader view of intelligence could incorporate the view that intelligence is a structure, a process and a product*". While accepting the six stages of the Intelligence cycle form the process, Ratcliffe considers that the cycle produces a product, in the form of finished Intelligence, and also has to have a structure for it to operate. The Harfields (2008:60) develop this concept, describing it as a "*triptych conceptualisation of Intelligence*" which they describe in more detail through the use of a table, shown below:

Intelligence as:	**Defining Characteristics**
Structure	The existence of an Intelligence unit or department as an individual entity within an organisational framework, equipped with people, skills, methods and organisational structure
Process	A continuous cycle of tasking, information collecting, analysis, evaluation, dissemination leading to intervention action or the identification of an Intelligence gap requiring further tasking.
Product	The output of the Intelligence process, the processed information, such as a Subject Profile or a Tactical Assessment, intended to inform decision-makers.

2 Harfields' triptych conceptualisation of Intelligence, based on Ratcliffe (2003).

The Harfields (2008:60) make an important observation in their conclusions, which helps to explain why different people may have different ideas of what Intelligence is, when they are discussing it:

> "*even within a single theoretical model, Intelligence can have more than one conceptual (as well as literal) meaning and that it is important, when debating issues and considering strategy and tactics to be certain that all parties understand which meaning is under consideration at any given moment*".

Clearly, much of this debate is primarily of relevance to the English-speaking world, and there will be other interpretations of the definition of Intelligence in other languages which are more difficult to assess and compare, partly due to the fact that they will necessarily also be influenced by the particular translation selected. There remains a considerable gap between the Intelligence concepts, methods and definitions used by the UK and the USA and a detailed description of these differences is beyond the scope of this work.[27]

3.1.1 Intelligence Failures or Intelligence Gaps?

In addition to defining Intelligence itself, another closely related but key distinction needs to be examined: the difference between an Intelligence gap and an Intelligence failure. This is relevant because, as Chapter 6 explains, Intelligence failures are often held up as examples of a weakness in the Intelligence cycle or process, but such so-called Intelligence failures are often Intelligence gaps. The subject of Intelligence failures has become a common topic for discussion in the UK, largely as a result of media coverage which tends to see almost any negative development in the counter-terrorism space as an Intelligence failure. Schulsky's definition of an Intelligence failure is frequently cited by writers such as Warner (2002), Phythian (2008) and others. Schulsky defines an Intelligence failure as: "*any misunderstanding of a situation that leads a government or its military forces to take actions that are inappropriate and* counterproductive *to its own interests*" (Schulsky & Schmitt, 2002:63). The definition does not have the all-encompassing characteristics one might expect to find, based on some of the definitions of terrorism. The inclusion of the word "misunderstanding" does not, for example, permit the classification of Intelligence failure in circumstances where the necessary information was already residing in the data repositories of one or more agencies, but through human error or linkage blindness, connections and resultant conclusions were not made which should have or could have been. Nonetheless, it provides a useful start point of reference.

[27] For a detailed examination of the differences between the UK and the US approaches, see Davies' two-volume work (Davies 2012a; Davies 2012b)

A CIA definition of Intelligence failure (2005:6) is given as "*systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses*", compared to an "*Intelligence error*" which it describes as "*factual inaccuracies in analysis resulting from poor or missing data*". Gormley (2004) considers an Intelligence failure "*to be virtually assured when a predisposed analytic mindset is combined with predictable overhead collection systems*".

O'Connor (n.d.) adds considerably to an understanding of Intelligence failures by drawing together multiple strands of research such as that done by Laquer (1985) and Lowenthal (2003) and categorising what he considers to be the ten root causes of Intelligence failures, shown below in table form.

Reason for Failure	**Symptoms and Examples**
Overestimation	This is perhaps the most common reason for failure, and one which, if uncorrected, can lead to the continuation of error for a long time. Examples include the long Cold War period in which the U.S. consistently overestimated the "missile gap" between the U.S. and Soviet Union. Critics of the Iraq invasion say this was the main kind of error that happened in the estimation of Saddam Hussein's warfare capability.
Underestimation	This occurs when intelligence or political leadership seems unwilling to be receptive to warnings, or completely misreads the enemy's intentions. A classic example is Stalin in 1941, who didn't want to hear about the possibility of Hitler invading Russia, even though the British and Americans tried to tip him off.
Subordination of Intelligence to Policy	This happens when judgments are made to produce results that superiors want to hear instead of what the evidence indicates. It is the most widely discussed and analyzed type of intelligence failure, although some discussions talk about a related error, bias.
Lack of communication	The lack of a centralized office often creates this problem, but it more typically results from when you have different officials from different agencies who have different rules on who and how they communicate, or few analysts who work on-the-fly for different agencies and don't have full-time intelligence responsibilities.

Unavailability of Information	Regulations and bureaucratic jealousies are sometimes the cause of this, but the most common problem involves restrictions on the circulation of sensitive information. When there is virtually no intelligence at all, this is called something else, ignorance.
Received Opinion	This is also called "conventional wisdom" and consists of assertions and opinions that are generally regarded in a favourable light, but have never been sufficiently investigated.
Mirror-Imaging	This is technically defined as "the judging of unfamiliar situations on the basis of familiar ones," but most often involves assessing a threat by analogy to what you (your government or a similar government) would do in a similar position.
Over-confidence	This occurs when one side is so confident of its ability that it projects its reasoning onto the other side and believes that since it would not do something itself, neither will the other side. The classic case is the Yom Kippur war of October 1973.
Complacency	This happens when you know the enemy might do something, though you are not sure what or when, and yet you do nothing anyway. The classic example is the British who did nothing in the weeks leading up to the Falkland War of 1982.
Failure to connect the dots	This occurs when the connections between bits of intelligence are not put together to make a coherent whole. It is most easily observed in hindsight.

Table 3 O'Connor's Ten Reasons for Intelligence Failures

O'Connor's category of "subordination of Intelligence to policy" seems to be identical to the vulnerability usually classed as politicisation. Interestingly, Treverton (2008:93-94) defines five categories of politicisation, which if we accept that O'Connor and Treverton are writing about the same issue, would make five taxonomical sub-categories of politicisation. The vulnerability of politicisation of Intelligence is discussed in chapter 6.

Intelligence gaps, by contrast, can be created as a result of human, system or process failures. They can also simply be absences of information due to the inability of the agencies to collect against a particular target or group, or to break into a particular source of information. A target could change its methods of passing information, rendering conventional methods unworkable. Such was the case in the immediate post-invasion period in Iraq in 2003 and for several years afterwards, when insurgent groups moved to the use of human couriers on motorbikes and bicycles, in an attempt to defeat the surveillance methods used by some of the allied agencies.[28] One of the reasons for creating an Intelligence collection plan, and the breaking down of these requirements into primary and secondary requirements, is to help with establishing what gaps in collection capabilities exist. Another reason for the plan is to then work out how to close those gaps, to enable the fullest collection coverage possible, within the limits of available resources, mapped against priorities.

3.2 Defining Terrorism

> *"One man's terrorist is another man's freedom fighter*".[29]
>
> "*Terrorism is a term without any legal significance. It is merely a convenient way of alluding to activities, whether of States or of individuals, widely disapproved of and in which either the methods used are unlawful, or the target protected, or both"* (Higgins, 1997:28).[30]
>
> "*We have cause to regret that a legal concept of terrorism was ever inflicted upon us. The term is imprecise; it is*

[28] Information provided by several Intelligence officers with experience of working in Iraq during that period.

[29] Anonymous.

[30] Judge Rosalyn Higgins was the first female judge to be elected to the International Court of Justice (ICJ).

> *ambiguous; and, above all, it serves no operative legal purpose*" (Baxter, 1974:380).[31]

The long-standing failure to compose a globally acceptable definition of terrorism, even by the United Nations, highlights the intensely political, deeply divisive and insoluble nature of the concept of terrorism. Few other words are so loaded with such strongly opposing viewpoints and yet repeated attempts to encapsulate terrorism in an all-inclusive, internationally agreed upon, practical and legally acceptable definition all appear to have failed. At one extreme end of the spectrum, some definitions have been spectacularly incomplete. Following the Al Qa'eda attacks upon the U.S. on 11 September 2001, the UK Ambassador to the United Nations, Sir Jeremy Greenstock, famously remarked that: "*what looks, smells and kills like terrorism is terrorism*" (Collins, 2002:167–168).[32] It is difficult to imagine Greenstock's definition being accepted in a UK court of law. Likewise a famous U.S. legal statement on a definition of pornography is often paraphrased into a simplistic yet equally inaccurate definition on terrorism: "*when one sees terrorism, one recognises it*".[33]

The degree to which the concept of terrorism suffers from politicisation was highlighted by Weiss when he compared the backgrounds and subsequent international elevation of four prominent figures in world politics. The four individuals mentioned by Weiss provide interesting case studies. They were all actively involved in terrorist offences, yet all went on to become significant

[31] Prof. R. Baxter is a former Editor-in-Chief of the American Journal of International Law, a Member of the U.S. Permanent Court of Arbitration and a former consultant to the U.S. Dept. of Defense, Dept. of State and the Naval War College.

[32] Greenstock's full quote was "Increasingly, questions are being raised about the problem of the definition of a terrorist. Let us be wise and focused about this: terrorism is terrorism. What looks, smells and kills like terrorism is terrorism".

[33] The original "non-definition" was given by a U.S. Supreme Court Justice, Potter Stewart who was presiding over the case of Jacobellis v. Ohio (1964). The case centred on a movie theatre which was alleged to have shown a hard-core pornographic film. Stewart's written notes on the case stated that hard-core pornography was difficult to define, but, he added, "*...I know it when I see it…and the motion picture involved in this case is not that*".

political leaders, two of them winning the Nobel peace prize. Weiss (2011) stated:

> "*What do we make of terrorism when we consider what Nelson Mandela, Menachem Begin, Gerry Adams, and Yasir Arafat have in common? They were all regarded as terrorists at one time. Then two of them got the Nobel Peace Prize and all were eventually regarded as great leaders of their people. So terrorism is a difficult concept to get hold of".*

Menachim Begin was a former member of the Jewish underground group Irgun, and was personally responsible for conducting several terrorist operations aimed at forcing a British withdrawal from the British Mandate of Palestine, prior to the declaration of the State of Israel in 1948. One of Begin's operations, a terrorist bombing in 1946 of the King David Hotel in Jerusalem, resulted in the deaths of 91 civilians (Kushner, 2002:181). Elected as Prime Minister of Israel in 1977, Begin signed the Camp David peace treaty with Egyptian President Anwar Sadat in 1979 (Stein, 1999:228-229). Both Begin and Sadat were awarded the Nobel Prize for Peace in 1978 (Nobel Prize, n.d.).

As leader of the *Umkhonto we Sizwe* (usually translated as "Spear of the Nation" or known as "MK"), Nelson Mandela planned and directed sabotage operations against the apartheid government of South Africa, for which he was jailed for life in 1964. Released from prison in 1990, he was eventually elected as President of South Africa in 1994. He was awarded the Nobel Prize for Peace in 1993, in conjunction with Prime Minister FW de Klerk (Mandela, 2004:63–68).

Gerry Adams was a member of Sinn Fein since at least 1970, and was interned in 1971 under the Special Powers Act 1922. Released in 1972 to participate in secret talks with the British government, he is alleged to have played a direct and central role in planning the bombing campaign in Belfast in July 1972, which became known as Bloody Friday.[34] Twenty-two explosive devices were detonated in Belfast, in just over an hour, resulting in nine dead and 130 injured (Lalor, 2003:7–8).[35] Adams was re-arrested in 1973 and was subject to internment at Long Kesh internment facility. Following two escape attempts, he was subsequently convicted and jailed. In 1983, he became the President of Sinn Fein and was elected as Member of Parliament. Taking part in secret talks with both the Irish Taoiseach and the British Northern Ireland Office, he was deeply involved in the negotiations which led to the 1994 IRA ceasefire and later the 1998 "Good Friday Agreement" (UK Government, 1998). He was present at the inauguration of U.S. President Barack Obama as a personal guest of U.S. Congressman Richard Neal. In 2011 he was elected as member of the Irish Parliament. He was also a Westminster Member of Parliament (although abstentionist) from 1983-1992 and 1997-2011.

Yasir Arafat founded the FATAH movement (The Palestinian National Liberation Movement) in 1959 and was actively involved in the fight for Palestinian statehood for most of his life, personally leading several paramilitary incursions of FATAH commandos into Israeli territory (Aburish, 1999:33–67). Throughout his life, he was dogged by allegations of direct and personal involvement in a number of major terrorist incidents. These included the hijacking of five airliners and the subsequent destruction of three of them in Jordan, the operations of the FATAH sub-group "Black September", which kidnapped and killed 11 Israeli athletes during the Olympic Games in Munich in 1972 and the murder of U.S. diplomats in Khartoum (Karam, 2006).[36] Later

[34] In 2010, a convicted IRA bomber, Doloures Price, said that she had told researchers from Boston University that Gerry Adams was her Officer Commanding, when she was a member of the IRA's Belfast Brigade.

[35] Adams denies the allegations of IRA membership as libellous, although he has never fought a libel action against it (cf. Taylor (1997:140), English (2003:110), Moloney (2002:140) and Urban (1993:26)).

[36] One of the Palestinians involved, Daoud, gave several interviews after the opening of Steven Spielberg's film "Munich", which reignited the issue of the Munich massacre. Daoud remained unrepentant on his role in the Munich attacks. During a televised interview on the German TV channel "Spiegel TV", he stated "*I regret nothing. You can only dream that I would apologize*. (Karam, 2006)" In an Associated Press interview, he justified the Munich operation, considering that its success legitimised it, saying "*Before Munich, we were simply terrorists. After Munich,*

in life, Arafat entered into secret talks with the government of Israel, concerning Palestinian self-rule in the West Bank and the Gaza Strip. These negotiations resulted in the 1993 Oslo Accord (or the "Declaration of Principles on Interim Self-Government Arrangements"), which paved the way for the creation of the Palestinian National Authority (PNA), a Palestinian Police Force and the withdrawal of the Israeli Defence Forces (IDF) from areas of the West Bank and the Gaza Strip (Mattar, 2005). In 1994, Arafat became the Prime Minister and the President of the PNA, as well as the Commander of the Palestine Liberation Army and the Speaker of the Palestinian Legislative Council. In the same year, Arafat was jointly awarded the Nobel peace prize together with the Israeli Prime Minister Yitzhak Rabin, and the Israeli Foreign Minister, Shimon Peres (Nobel Prize, n.d.).

Schmid (2004:375–395) identifies four primary reasons why terrorism is difficult to define:

> "*1. Terrorism is "a contested concept" and political, legal, social science and popular notions of it are often diverging;*
>
> *2. The definition question is linked to (de-)legitimisation and criminalisation;*
>
> *3. There are many types of "terrorism", with different forms and manifestations;*
>
> *4. The term has undergone changes in meaning in the more than 200 years of its existence*".

The first point is significant, that terrorism is one of the most fiercely contested words. The terrorist label is polemical and it has now become almost

at least people started asking who are these terrorists? What do they want? Before Munich, nobody had the slightest idea about Palestine. (Mostyn, 2010)" weaponised, carrying strong and vivid connotations and implying criminality, lawlessness and public condemnation. More importantly, perhaps, it also implies that the protagonist using the label has some kind of moral right, or at least holds the moral high ground. A comment by Jenkins (1980:2) captured this neatly when he wrote that the use of the word terrorism: "*implies a moral judgment; and if one party can successfully attach the label terrorist to its opponent, then it has indirectly persuaded others to adopt its moral viewpoint*". The last part of Jenkins' statement points to an important factor in the debate: that applying the label against one's opponent can help to change the wider perception of the public. This can result in increased support against those labelled terrorists and more sympathy for those using the label. In this case, much can depend on the marketing and publicity power generated in support of the labelling protagonist.

The second point centres on (de-)legitimisation. If one can successfully de-legitimise one's opponent, it makes it considerably more difficult for the opponent to make their political points in a public forum. It also decreases the likelihood that any meaningful negotiations can take place between the two sides. By successfully criminalising one's opponent, it can make it more difficult for them to operate effectively, and it allows for more robust judicial proceedings against them in the event that they are arrested. This has been a powerful tool used repeatedly in the Palestine-Israel conflict, where both sides have consistently accused each other of conducting terrorist acts and of committing war crimes. Palestinian suicide bombings against Israeli targets have been declared as terrorist actions by the Israeli government. Israeli military reprisals in the form of airstrikes resulting in civilian casualties, or the demolition of houses lived in by suspected terrorists, are likewise labelled as acts of state terror by Palestinian leaders. De-legitimisation can also lead to dehumanisation, another powerful weapon which can be deployed in support of one side or the other. When one side dehumanises the opposing side, it can be much easier to take robust action or to justify what would otherwise appear to be a disproportionate response.

Schmid’s third point brings up the pluralist nature of terrorism and the resultant debate on terrorism not being a concept, tangible or easily identifiable, but a web of interconnected typologies of terrorism. This issue of terrorism typologies has been the subject of considerable academic debate (Kaplan, 2003; Schmid, 2004b; Schmid, 2004a; Hoffman, 1986), yet it also has implications for a country’s legislation and its counter-terrorism policies and responses. The fourth point raises the debate on how terrorism is defined now, and how it has been defined in the past.

Schmid (2004a:197–221) also proposed five conceptual frameworks which could be used as lenses through which terrorism could be viewed: crime; politics; warfare; propaganda/communication; religion/fundamentalism. These frameworks were not designed to be taken as a definitive or exhaustive list, but more of a sample of potential frameworks. Such frameworks could assist in examining how individuals enter into terrorism (radicalisation and/or recruitment), progress to conducting terrorist actions (operational involvement) and how and whether they leave terrorism behind (disengagement). Schmid and Jongman (2005:40) took this dissection of terrorism still further by defining ten distinct typologies seemingly in an effort to produce an etiology of terrorism, should such a thing be considered to exist. Schmid (Schmid, 2004b:198) considers the two distinctions of *mala prohibita* and *mala per se*, before coming down on the side of *mala per se*, stating:

> “*Some offences are so serious that they are considered morally wrong in all civilised societies. In particular, this applies to murder—the premeditated, unprovoked killing of a human being. When it comes to terrorist crimes, a narrow definition of terrorism that would focus on mala per se crimes appears desirable, since there is widespread international*

> *consensus about the latter as constituting a gross violation of accepted rules*".[37]

Writing specifically on the problems encountered in defining religious terrorism as opposed to terrorism in general, Schbley (2003) recognises the conundrum that an apolitical definition of terrorism is the most desirous, and would also be the most effective type of definition, yet accepts that such a definition would also be the most problematic in defining. She ambitiously proposes (Schbley, 2003:106) that the academic community must provide "*legislators, policymakers, soldiers, and intelligence and law enforcement officers with defining tools, legal précis, and concepts that will redress this costly and painful misunderstanding*". It is unrealistic to expect that this would provide a workable solution for the UK government, in respect of its counter-terrorism policy, but it would be a distinct step in the right direction for the UK government to host a conference, and a post-conference working group, on defining terrorism. This would ideally enjoy the participation of serving and retired Intelligence practitioners, and academics from the forefront of terrorism and legal studies.

All of this academic discourse leads to a vexing question: is it possible to successfully and accurately define terrorism? Some academics disagree (Schmid & Jongman, 2005:2-3), arguing that "*the study of terrorism can manage with a minimum of theory*". Others (Ganor, 2002:287) see the defining of terrorism as a central and crucial foundation for that study, arguing that "*an objective definition of terrorism is not only possible: it is also indispensable to any serious attempt to combat terrorism*". This leads to an interesting *erotema*: if we cannot define terrorism, can we realistically expect to craft a meaningful, international response to combat it? At the same time,

[37] *Mala in se* (what Schmid calls *mala per se*) comes from the Latin which means "*wrong in itself*" and is used to denote behaviour which a civilised society considers inherently wrong. Commonly quoted examples include murder and rape. *Mala prohibita* is behaviour which is prohibited by law, as opposed to being considered as fundamentally wrong. This is similar to the Roman legal principles of *iussum quia iustum* (that which is commanded because it is just) and *iustum quia iussum* (that which is just because it is commanded). See Deffains and Fluet (2014) for a fuller description.

an additional question must be asked: is it reasonable to expect to achieve a single, all-encompassing definition of terrorism, fit for all circumstances, covering all possible situations? There is an argument which suggests that the mechanisms for successfully prosecuting perpetrators of terrorist offences are diminished by the continuing absence of such a global definition. This argument follows the legal principle known as *nullum crimen, nulla poena sine praevia lege poenali*, which states that no crime can be committed, and thus no corresponding punishment can be administered, without there already existing at the time of the offence, a penal law which was violated. This is employed to prevent *ex post facto* laws being introduced. Article 7 of the Human Rights Act (Parliament, 1998) prohibits criminal laws being introduced retrospectively.[38] The absence of a clear definition of terrorism can impact upon extraditions and other international co-operation agreements. The inability to clearly define terrorism carries with it the issue that different countries have different thresholds for what constitutes a criminal act. This is an area in which the UN could make a considerable contribution, by bringing together the legal and professional expertise necessary to discuss and eventually create an international definition of terrorism. Such a definition would not, admittedly, provide an immediate solution to the problem of defining the act, but it would at least provide an internationally crafted framework upon which the individual countries could use as a foundation for their own, national definitions. Analysis of selected terrorism definitions

From as early as the 1930s it can be seen that the problem of defining terrorism was a difficult one. In its 1937 Convention, the League of Nations (1937:sec.1) defined terrorism in Article 1.1 as: "…*criminal acts directed against a State and intended or calculated to create a state of terror in the minds of particular persons or a group of persons or the general public*".[39] At

[38] Schedule 1, Article 7 of the Human Rights Act 1998 (Parliament 1998b) states that "*no one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the criminal offence was committed*"

[39] This statute was never formally enacted by the League and thus never entered into force.

the time, it was an ambitious attempt at encapsulating the offence of terrorism. The Convention went further in Article 2, which subsequently attempted to clarify exactly what could constitute a terrorist action. If an action was already covered by the above definition in Article 1.1, and if the action was directed at another State, then the 1937 Convention (League of Nations, 1937:sec.2.1–2.5) considered the following to constitute terrorist acts:

> "*1. Any wilful act causing death or grievous bodily harm or loss of liberty to:*
>
> *a) Heads of State, persons exercising the prerogatives of the head of the State, their hereditary or designated successors;*
>
> *b) The wives or husbands or the above-mentioned persons;*
>
> *c) Persons charged with public functions or holding public positions when the act is directed against them in their public capacity.*
>
> *2. Wilful destruction of, or damage to, public property or property devoted to a public purpose belonging to or subject to the authority of another High Contracting Party.*
>
> *3. Any wilful act calculated to endanger the lives of members of the public.*
>
> *4. Any attempt to commit an offence falling within the foregoing provisions of the present article.*
>
> *5. The manufacture, obtaining, possession, or supplying of arms, ammunition, explosives or harmful substances with the view to the commission in any country whatsoever of an offence falling within the present article".*

It is prescient that even today the United Nations remains unable to agree on a formal definition of terrorism, despite the fact that there are several UN resolutions condemning terrorism.[40] This absence of acceptable definition is not for lack of trying, however. The United Nations General Assembly (UNGA) has been formally deliberating a “Proposed Comprehensive Convention on International Terrorism” since at least 2000. The UN’s most comprehensive attempt at a definition of terrorism is arguably that from 2002 (2002:sec.2.1) and reads thus:

> "*1. Any person commits an offence within the meaning of this Convention if that person, by any means, unlawfully and intentionally, causes:*
>
> *(a) Death or serious bodily injury to any person; or*
>
> *(b) Serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or the environment; or*
>
> *(c) Damage to property, places, facilities, or systems referred to in paragraph 1 (b) of this article, resulting or likely to result in major economic loss, when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act.*"

The problem causing the log-jam on formal ratification is not the definition itself. The main issue is bifurcated and the two sides are closely related, yet mutually opposing: should the UN definition apply to a State’s armed forces,

[40] See Annex C for a list of relevant UN Instruments.

and should it also be applied to liberation or self-determination movements? The often diametrically opposed relationship between these two groups constitutes the kernel of the problem. It raises questions which have to date been indeterminable by the international community. Examples of these include:

1. What are the defining characteristics of a terrorist group or organisation?
2. What are the defining characteristics of a liberation or self-determination movement?
3. Should activities of nations' Armed Forces be included or excluded?
4. Should there be a separate definition of "state terrorism"?

On 08 October 2004, the United Nations Security Council (UNSC) unanimously passed Resolution 1566 (UNSC, 2004) which condemned terrorist acts defined as:

> "*criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by*

> *considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature*."

The definition adds nothing to strengthen previous definitions and makes no attempt to address the perennial issue of the inclusion or otherwise of self-determination groups, liberation movements or the acts carried out by a State's armed forces. Less than one year later, the United Kingdom drafted Resolution 1624, aimed at combating international terrorism by enhancing international passenger security. The Resolution was unanimously adopted by the UNSC on 14 September 2005, yet despite many references to fighting terrorism and the member states' obligations in doing so, it did not add any new additions to the definition of terrorism (UNSC, 2005). Thus the UK failed to take advantage of an opportunity to influence the definition of terrorism and to shape the international debate on this. The United Nations now has nineteen international conventions on terrorism, yet an internationally agreed UN definition on terrorism continues to be elusive.[41]

In addition to the United Nations, the European Union has also devoted considerable energy to carving out its own definition of terrorism. Article 1 of the EU's "Framework Decision on Combating Terrorism (2002)" (European Council, 2002:sec.1.1) directs EU member States to:

> "*take the necessary measures to ensure that the intentional acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:*
>
> *— Seriously intimidating a population, or*

[41] The nineteen UN specialised international conventions on terrorism to date consist of 14 major universal legal instruments and five amendments to prevent terrorist acts. A summary of these is provided at Annex C.

— unduly compelling a Government or international organisation to perform or abstain from performing any act, or

— seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation, shall be deemed to be terrorist offences:

(a) attacks upon a person's life which may cause death;

(b) attacks upon the physical integrity of a person;

(c) kidnapping or hostage taking;

(d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;

(e) seizure of aircraft, ships or other means of public or goods transport;

(f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;

(g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life;

(h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life;

(i) threatening to commit any of the acts listed in (a) to (h).

The EU definition has a number of interesting additions. The inclusion of clauses such as "*seriously intimidating a population*" together with "*unduly compelling a Government or international organisation to perform or abstain from performing any act*" bring the definition more up to date by recognising the intimidation of a state, or its people, by another state. While the EU definition is only binding for EU member states, clauses (d) and (h) have particular significance for the international community, in particular regarding conflicts which have a terrorist component. One such example was the 2006 war in Lebanon, which began as a retaliatory conflict between the Israeli Defence Forces on one side and Hizbollah on the other, and turned into a full-scale war resulting in thousands of dead and the displacement of just under a quarter of Lebanon's population (UNHRC, 2006). During this conflict, Israeli military aircraft conducted raids against Beirut Rafic Hariri International Airport, destroying all three runways and forcing the diversion of international flights to Cyprus. Other installations targeted included power plants and water infrastructure (BBC, 2006). Under the EU definition, such attacks would be classified as terrorist actions even though they were conducted by the Armed Forces of a state. It is exactly this conundrum which poses the most difficult issue for the UN in trying to create a definition of terrorism which is meaningful, robust and inclusive, yet is globally acceptable among member states (Bures, 2011:pt.3).

The EU Transnational Terrorism, Security and the Rule of Law (TTSRL) body studied the available academic discourse on defining terrorism and published a paper in which they identified "*six key qualities (definitional elements) that a sound definition of terrorism must contain*" (2008:2). The paper considered that for a definition of terrorism to be sound, the following criteria have to be met:

1. *It should render the intentional character of the committed acts.*

> 2. *It should be clear on the purpose of the act.*
>
> 3. *It should qualify the act itself.*
>
> 4. *It should specify the target….*
>
> 5. *…. as well as the perpetrators.*
>
> 6. *It should define the scope of the act, including the exceptions*" (TTRSL, 2008:2–3).

In addition to its list of definitional elements, the report also noted that that there was one central principle it had identified which all academic definitions of terrorism contained. Calling this the "*nodal point*", the report identified it as the principle of double victimization (TTRSL, 2008:2). This holds that the actual target of a terrorist attack is not the "real target", instead it is a secondary target, "*connected or not with the victims*" which is the real target. Furthermore, this principle states that this is the case regardless of whether or not the secondary target is in any way connected with the actual target, as it is the secondary target which the attack seeks to influence.

This is an important point and it captures the concept that a terrorist attack rarely seeks to "only" cause terror or casualties. Instead, the terror is intended to act as an indirect lever of influence upon a secondary group, usually one which either holds power or which is close to the power-broking circle. The report is blunt in describing the lack of commitment from some EU member states in adopting the EU definition of terrorism. The UK is singled out for criticism, along with a handful of other member states. As the report pointedly states:

> "*Unfortunately, the implementation in the member states has passed with mixed results.....Above all, Italy, Poland, Spain, Sweden, and the United Kingdom have not incorporated the*

> *second part of the EU definition – the specific list of criminal acts that should be considered terrorism when motivated in the particular manner.....The inconsistent implementation hinders the full exploitation of the common EU definition of terrorism. It opens up room for law suits on extradition, complicates cooperation between the member states, and thus casts doubts on the whole EU counter-terrorism cooperation*" (TTRSL, 2008:3).

The EU report makes one final salient point: "*Efficient counter-terrorism policy will inevitably rest on many factors, but above all, the countries must agree on what terrorism is*" (TTRSL, 2008:3).

Tiefenbrun takes a similar approach to the EU's TTSRL, but arrives at different conclusions. She identifies five structural elements to which all definitions of terrorism can be reduced (Tiefenbrun, 2003:367). These primary elements she identified thus:

> "*1. The perpetration of violence by whatever means;*
>
> *2. The targeting of innocent civilians;*
>
> *3. With the intent to cause violence or with wanton disregard for its consequences;*
>
> *4. For the purpose of causing fear, coercing or intimidating an enemy;*
>
> *5. In order to achieve some political, military, ethnic, ideological, or religious goal*".

Tiefenbrun subsequently unpacks these elements, examining the deeper issues coming from her search for a semiotic definition of terrorism and she asks a number of questions. What constitutes terrorism? Who can and cannot be considered as an innocent civilian? What can legitimately be considered as an unintentional killing in wartime? While the TTSRL list has an emphasis on legal aspects, Tiefenbrun's paper is more philosophically focused. This resonates clearly with a central topic of this section, namely how can we fight something which we cannot seem to accurately define? The current UK definition of terrorism, as provided by the Terrorism Act 2000 (Parliament, 2000:sec.1) states:

> "(1). "*terrorism" means 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 purpose of advancing a political, religious, racial or ideological cause.*
>
> *(2) Action falls within this subsection 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 seriously to interfere with or seriously to disrupt an electronic system*".[42]

[42] This definition is the current one, which was slightly updated by the Terrorism Act 2006 (Parliament, 2006b) and the Counter-Terrorism Act 2008

Having stated that the EU's TTSRL list of six essential points is a valid concept, it would be apposite to map the UK's definition of terrorism, as contained in the Terrorism Act 2000, against the TTSRL criteria. First, it should "*render the intentional character of the act*". Section 1(a) of the Terrorism Act includes an "*act which either does, or threatens to, influence the government, or intimidate the public*" (2000, sec.1a). This seems to meet the threshold for the first criteria, but other parts of the definition also meet it adequately. Section 1(c) carries a fairly comprehensive selection of some of the more usually considered elements of motivations for terrorist acts, namely "*advancing a political, religious, racial or ideological cause*" (Parliament, 2000:sec.1c). Both of these sections carry implicit intention within them, and fulfil the requirement for *mens rea*.

The second point from the TTSRL paper states that a definition must be "*clear on the purpose of the act*" (2008:2). Sections 1(a) and 1(b) of TA 2000 (2000:sec.1a, 1b), described previously, seem to cover this point, and even if one considers the purposes in 1(c) as an inconclusive list (2000:sec.1c), it does nevertheless signpost the most common and most serious purposes of terrorist actions. The third TTSRL point states that a definition must "*cover the act itself*" (2008:2), and on this point the definition from TA 2000 is lacking. While section 2 of the Act includes rather broad offences such as "*involving serious violence against a person*" and "*involving serious damage to property*", there is no detailed list of specific actions included (2000:sec.2). Earlier in this chapter, an overview was provided of Article 1 of the EU's Framework Decision (2002). This provides a list of specific actions and it extends to acts such as kidnapping, hostage taking, seizure of aircraft, release of dangerous substances, and more. Yet the requirement to include an exhaustive list is itself the subject of debate in the academic community, as evidenced in works by Roy (2002), Green (2001), Holmes (2001), Saul (2006:2), Zunes (1988), Burns(2001) and Jackson (2009).

The fourth point requires that a definition "*specifies the target of the terrorist act*". Various subsections cover this requirement: Section 1(b) stipulates that the use, or threat, is designed to influence the government, an international government organisation, the public, or a section of it, while section 2(e) includes the more recent phenomenon of electronic attack. The fifth point requires that the perpetrators should be specified in addition to the target, and this requirement is not fulfilled by the Terrorism Act 2000 definition. Finally, the last requirement is that the definition should "*define the scope of the act, including the exceptions*". The UK definition places the offence within the boundaries described in Terrorism Act 2000, but it cannot be said to define the scope of the act, nor the exceptions to it. Burke (2004:22), in a study of Al Qa'eda, surmised how loaded with meaning and counter-meaning a definition can become:

> "*despite the shifting and contested meaning of "terrorism" over time, the peculiar semantic power of the term, beyond its literal signification, is its capacity to stigmatize, delegitimize, denigrate, and dehumanize those at whom it is directed, including political opponents. The term is ideologically and politically loaded; pejorative; implies moral, social, and value judgment; and is "slippery and much-abused." In the absence of a definition of terrorism, the struggle over the representation of a violent act is a struggle over its legitimacy. The more confused a concept, the more it lends itself to opportunistic appropriation*".

3.3 Problems with terrorism definitions

> "*After September 2001, problems of definition became acute, since the Council adopted general legislative measures against terrorism—with serious legal consequences—without defining it. The Council has encouraged States to unilaterally define terrorism in national law, permitting wide and divergent definitions*" (Saul, 2008b:2).

> "*the question of a definition of terrorism has haunted the debate among States for decades*" (Schmid (1992) cited in Burns, 2001:1–2).

The absence of an internationally accepted definition can arguably solicit abuse of the term by both sides in a conflict. In the uprising in Libya, the former leader Colonel Muamar Gaddafi continually denounced Libyan protestors as foreign terrorists, calling on his supporters to fight them as such. Until the situation in Syria deteriorated into entrenched fighting, and was followed by the rise of the Islamic State (aka. ISIS, aka. ISIL), the Libyan conflict, of all the uprisings during the Arab Spring, was the one which more closely evolved into a classical armed struggle. The protagonists were the various anti-Gaddafi rebel groupings (mostly under the umbrella National Transitional Council (NTC)) on one side and the Libyan Armed Forces on the opposing side. The carrying out of NATO airstrikes in support of the rebels had a significant impact on making the conflict a more even-handed one, but it also resulted in the questioning of the legitimacy of that NATO support (Abass, 2011). The NATO military intervention was dragged into the wider debate on terrorism and on state-sponsored actions which may or may not be classified as such. Güngör (2013:2) goes so far as to state that NATO involvement in Libya exceeded its legitimate authority as it brought about "regime change", something prohibited by international law.

This military application of NATO force was primarily conducted through the medium of targeted airstrikes against the Libyan Armed Forces. Viewed through the lens of the EU's Article 1 mentioned previously, two of the identified "*terrorist offences*" bear closer scrutiny. First, "*unduly compelling a Government or international organisation to perform or abstain from performing any act*" (European Council, 2002:sec.1.1). An implicit aim of the NATO air support to the TNC forces was to limit the ability of the Libyan Armed Forces to fight an effective campaign against the rebel forces of the TNC. The second offence recognised by the EU Framework's Article 1 as a "*terrorist offence*" is listed as "*seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation*". Güngör (2013) and Abass (2011) make the argument that this is what the application of NATO military air power in the Libyan conflict has resulted in. Thus the argument of whether to include or exclude acts committed by the Armed Forces of a State (or States), in an effective and acceptable definition of terrorism, was brought to the fore in the Libyan conflict, despite the fact that the use of force was authorised by the UNSC (UNSC, 2011:para.4).[43]

Without the effective criminalisation of terrorism, it becomes more difficult to combat it on an international level. This criminalisation is regularly purported to strengthen the policies related to dealing with terrorism. These include, but are not limited to: punishment or other retributive designs; incarceration of the offender(s) to prevent further acts being committed; rehabilitation of the offender(s) [44]; the deterrent effect which nations generally wish to project, in order to minimise the probability of an attack taking place.[45]

Cultural context is extremely important in the area of criminalisation. A report by the Australian Law Reform Commission, for example, notes that criminalisation can reinforce deterrence of and retribution for a crime, as it

[43] UNSCR 1973 had five explicit aims: Protection of civilians; No Fly Zone; Enforcement of the arms embargo; Ban on flights; Asset freeze.

[44] This is a contentious topic, particularly in light of recent programmes to rehabilitate Al Qa'eda terrorists in some countries. For specific research on rehabilitation experiences in Indonesia, see "*Deradicalisation and Indonesian Prisons*" (ICG, 2007). Other relevant research in this area is by Christmann (2012) and Disley (Disley et al., 2012).

[45] Honderich (1984) provides a deeper discussion of this topic.

encourages the revulsion of the community while simultaneously adding to the resultant "*social censure and shame*" (2002:65).

In a community which has a strong level of support for the person carrying out a terrorist attack, the dynamic switches. At the height of the internecine violence between Shia-Sunni communities in Baghdad during 2004-2007, even though Iraqis not involved in terrorism were losing members of their family and their wider community to suicide bomb attacks conducted by the opposing sect, many expressed strong support for members of their own sect conducting similar attacks upon their opponents in reprisal. In these cases, there was virtually no social stigma or community repulsion, even for extremely violent and deadly terrorist attacks, as each side felt under mortal attack from the other. It was common at that time to hear both sides express the belief that they were fighting a war of survival and were threatened with extermination.[46] Unless the overwhelming majority of the community feel the sense of revulsion and disgust mentioned by the Australian report, then a significant aspect of the criminalisation policy fails.

Saul (2008d; 2008b; 2008a) has written extensively on the complex nature of the legal issues associated with our inability to define terrorism effectively, and the resulting implications this has for the criminalising of terrorism. He highlights the emotive aspect of terrorism and the tendency of criminal law to avoid the motive, resulting in an inevitable discord. His description (Saul, 2007:sec.5) of the problem, though lengthy, is an excellent summary of the issues inherent in attempting to define terrorism within law. :

> "… "*Terrorism" currently lacks the precision, objectivity and certainty demanded by legal discourse. Criminal law strives to avoid emotive terms to prevent prejudice to an accused, and shuns ambiguous or subjective terms as incompatible with the*

[46] Based on discussions between the author and a large number of Iraqi Intelligence officers and other government officials of both Shia and Sunni persuasion, while the author was working in Baghdad during this period.

> *principle of non-retroactivity. If the law is to admit the term, advance definition is essential on grounds of fairness, and it is not sufficient to leave definition to the unilateral interpretations of States. Legal definition could plausibly retrieve terrorism from the ideological quagmire, by severing an agreed legal meaning from the remainder of the elastic, political concept. Ultimately it must do so without criminalizing legitimate violent resistance to oppressive regimes – and becoming complicit in that oppression*".

Saul identifies one problem clearly: the need to de-couple a legal meaning of terrorism from the politicised concept of it. Solving this problem, however, is much more difficult than identifying it. The academic community alone cannot fulfil the remit to construct a suitable, workable and acceptable definition of terrorism for the government, nor would they be the most appropriate body to carry out this task. A round-table audience, however, consisting of relevant experts from the Police, the judiciary, the Department of Public Prosecutions, the Intelligence services and the academic community who research and write on terrorism, would provide a forum for a very useful exchange of viewpoints, and would raise the debate on defining terrorism to a new level within this community. It is only through deeper discussion that we can more closely approach a practical, effective, inclusive and relevant definition of terrorism for the UK.

3.4 Summary

In this chapter the two crucial terms of the thesis question, Intelligence and terrorism, have been taxonomically unpacked to highlight the difficulties inherent in defining these two terms. Even before any definitions were examined, a more fundamental issue was raised: that there is a difference of opinion among those writing on Intelligence and terrorism matters, as to whether the rationale for defining these terms is a sound premise. This study highlighted some of the definitions which have been constructed and employed since as early as 1949. The various constituent parts of these were considered, and a summary of each was provided. Some of the various continua were also described, as some writers have referred to them in their academic work on defining Intelligence. It is no surprise that the scope and scale of these definitions has changed considerably since 1947. At that time the main threat to the national security of the UK and the USA was viewed as twofold. Externally, the Soviet Union and its Warsaw Pact allies constituted the primary threat, which was military in nature. The second dimension was an internal one, consisting of domestically conducted espionage, subversion and sabotage. In the Cold War period, countering these two threats absorbed the bulk of the Intelligence efforts of the UK and the USA.

The threats which the UK faces now include domestic terrorism carried out by its own citizens and residents, as well as other less deadly but economically damaging ones. An example of this would be the various anti-globalisation protests which have necessitated enormous deployments of Police officers and which have resulted in damage to commercial and residential areas and disruption to major city centres. As society and the global community have changed, the threat of terrorism is now one of the most important challenges for the UK government. The Intelligence work required to counter this threat must be efficient, in terms of resource deployment, and effective, in terms of preventing attacks.

The second half of this chapter continued with the taxonomical examination, this time looking at specific definitions of terrorism. The examination opened with a quote from Greenstock, and this was compared to a definition of pornography from a U.S. Supreme Court Judge, as both definitions were similarly vague and assumptive in nature. Next, in order to demonstrate some of the difficulties in defining terrorism, a brief summary was provided on four globally renowned individuals: Nelson Mandela, Menachem Begin, Gerry

Adams and Yasir Arafat. All four became international leaders in their own right, two of them were recipients of the Nobel Peace Prize, and yet all four had also been previously regarded as terrorists.

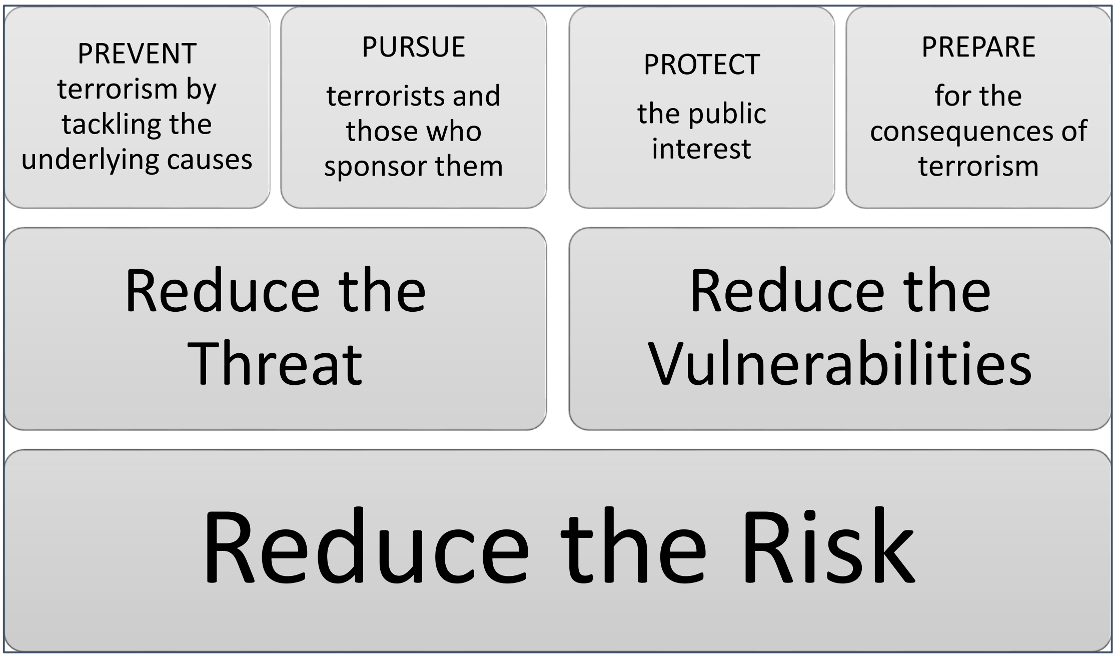
These biopics reinforced the fact that the concept of terrorism is very difficult to consider without some form of politicisation also being inherently present. The topic of the politicisation of Intelligence has been writ large in the media of the UK and the USA in particular, following the invasion of Iraq in 2003. Both Hulnick (2006:968) and Ott (2003:69-94) agree on the continuing need for analysts and Intelligence officials to speak truth unto power. Hulnick considers it the perennial challenge of the industry, while Ott laments what he sees as a gradual decline in the presence of oversight within the Intelligence sphere.

The work of authors such as Schmid and Schbley were introduced to explain the contemporary thinking from the academic community writing on terrorism studies. Schmid provided us with four reasons why terrorism is a difficult concept to define, while Schbley presses her readers to accept that defining terrorism is of paramount importance. The lack of any UN-wide, accepted definition of terrorism was discussed at length as this issue features in much of the critical literature surrounding the topic. Research from Tiefenbrun and others has contributed much to the debate, especially in attempting to identify the key components which a terrorist action should contain, in order to be so labelled. This brings us back to the initial question raised in the introduction, *viz*. can we fight something which we cannot truly define? As Stern (2000:12–13) notes, the way in which governments respond to terrorism is directly influenced by the way in which governments perceive and define terrorism.

Defining the two concepts of Intelligence and terrorism is clearly a task beset by difficulties on all sides, but what of the implications of such difficulties? The activities of the UK Intelligence agencies are now governed by the legislation which also placed them on a statutory footing (The Security Services Act 1989 and the Intelligence Services Act 1994) as well as by other legislative instruments (e.g. the Regulation of Investigatory Powers Act 2000, among others). The nature of Intelligence collection is heavily weighted towards secrecy and covertness, which is necessarily more difficult to legislate than prosecuting individuals for terrorism offences. In order to collect Intelligence to assist in safeguarding the domestic security of the UK, legislation governing the UK Intelligence agencies authorises them to conduct activities which would otherwise be unlawful, such as the intercept of personal communications. This important distinction is often overlooked by media reporting on Intelligence cases and accusations are levelled at the agencies (and by extension, against the government of the day), that their activities are unlawful. The various legislative instruments authorise them to conduct activities otherwise unlawful, such as the intercept of communications, subject to stringent checks and balances (e.g. warrants, either judicial or Ministerial), specific guidelines (e.g. Regulation of Investigatory Powers Act 2000 Guidance), and other legislation (e.g. the Human Rights Act 1998, *et al*) (Parliament 1998b; Home Office 2013; Parliament 1994; Parliament 1989; Parliament 2000b). The importance of defining terrorism, however, has an arguably greater impact as the ability to clearly state the parameters of a terrorism-related offence under law is essential to enable the State to successfully prosecute a person or persons actively involved in supporting terrorism. An inability to clearly define Intelligence has a greater impact on the agencies carrying out the work than on public safety, whereas the inability to clearly define terrorism could result in the inability to successfully prosecute an evidentially sound case in a court of law.

Chapter 4 CONTEST: The UK Counter-Terrorism Policy

Before examining the Intelligence cycle in UK counter-terrorism and assessing its effectiveness, the UK's counter-terrorism policy first needs to be understood, as the collection, analysis and use of Intelligence takes place within this context. This chapter examines this policy, explaining the environment within which the UK's intelligence work takes place. The UK's strategy for combating terrorism is known as the CONTEST strategy. First introduced in 2006, the current version was approved in 2011 (Home Office, 2011) and a subsequent update to the policy is next due in 2016. The aim of CONTEST is "*to reduce the risk to the UK and its interests overseas from international terrorism*" (Johnson, 2010:4) and it is divided into four distinct work-streams or strands. These strands are named PREVENT, PURSUE, PROTECT and PREPARE. The PURSUE and PREVENT strands are focused on reducing the terrorist threat, while the PROTECT and PREPARE strands aim to reduce the vulnerability of the UK to terrorist attacks. Working in conjunction, the four strands reduce the threats and the vulnerability which as a result reduces the overall risk of a successful terrorist attack against the UK.

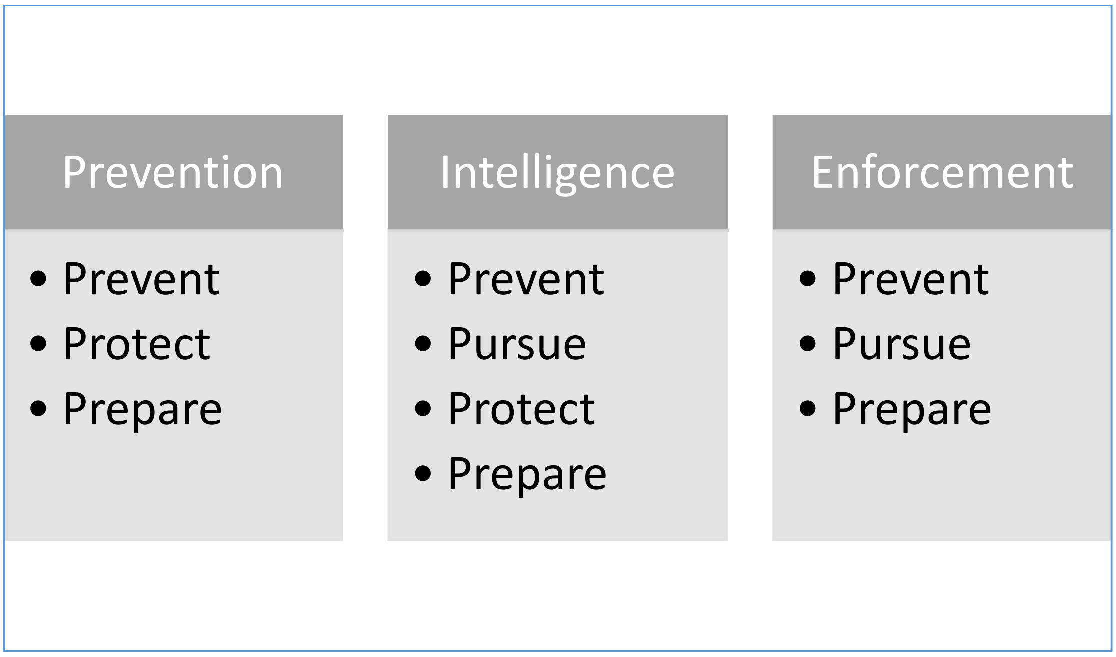

PREVENT terrorism by tackling the underlying causes
PURSUE terrorists and those who sponsor them
PROTECT the public interest
PREPARE for the consequences of terrorism
Reduce the Threat
Reduce the Vulnerabilities
Reduce the Risk

3 The CONTEST Strategy

The CONTEST strategy dovetails with the three primary pillars of the Control Strategy in the UK National Intelligence Model: Prevention, Intelligence and Enforcement. Prevention is encompassed by the PREVENT strand through the development and delivery of a co-ordinated, cross-government response for preventing violent extremism. Three of the strands, PROTECT, PREPARE and PREVENT all contribute to the production of risk assessments and security advice for the Police, government departments and key partners from the public sector. These include financial institutions and those estates designated as elements of the Critical National Infrastructure. The pillar of Intelligence is covered by all four of the CONTEST streams, as the Intelligence cycle functions in each of these.

The mechanics of the Intelligence cycle in the PREVENT strand are very similar but the primary focus here is on stopping individuals or groups becoming sufficiently radicalised to begin attack planning. Direction in this case is more likely to come from warnings by agencies and key partners, such as the CHANNEL programme, the Prison service, community Police officers, youth groups and other organisations at a more grass-roots level within society. Collection may be carried out in a much more overt manner, such as face to face meetings with youth leaders, housing officers, concerned friends, family or neighbours, even a personal meeting with the target of the investigation. Collation will take place at the same time, and will help to enrich the overall picture of the case, adding data from a range of potential partners such as housing, social services, police, prisons, MAPPA, CDRP, etc. Analysis and evaluation are more likely to be collegial in PREVENT cases with a high degree of multi-agency collaboration, less focused on stopping an attack than on preventing a person or persons from crossing a line into a dangerous stage of radicalisation. As PREVENT targets the twin threats of terrorism as well as violent extremism, it has a necessarily wider focus than the PURSUE strand.

Once Intelligence has been produced, all four CONTEST streams are involved with the Intelligence-sharing among the relevant agencies and trusted key partners. The enforcement pillar encompasses both the PREVENT and PURSUE strands through the disruption of terrorist individuals and networks as well as violent extremist groups and individuals, using arrests where applicable and appropriate. This also generates a deterrent effect through the publicly visible disruption of such networks and groups. Enforcement is also covered by the combination of PREPARE and PURSUE. These continually add to the development of Counter Terrorism capacity, while at the same time extending the capability to respond to terrorist incidents and to move as rapidly as possible to the post-attack recovery phase. The relationship between the CONTEST streams and the UK policing pillars can be looked at from a different angle, mapping the CONTEST strands against the components of the NIM's Control Strategy, as seen below:



4 The relationship between CONTEST and the policing pillars

4.1 PURSUE

The PURSUE strand of CONTEST aims to stop terrorists from conducting attacks, and this work includes disrupting cells actively engaged in attack planning. There are 6 main priorities under PURSUE:

> "*increasing covert detection and investigation capability and capacity; improving the effectiveness of the UK prosecution process; developing more effective non-prosecution actions; improving capability to disrupt terrorist activities overseas; strengthening the coherence between our counter-terrorism work and counter-insurgency and capacity building overseas; and enhancing inter- agency coordination*" (Johnson, 2010:2).

PURSUE relies very heavily on intelligence for it to be effective and there is a close relationship between PREVENT and PURSUE. In an ideal world, this would result in a virtuous circle. The PREVENT strand would reduce the numbers of those involved in terrorism, while the PURSUE strand would disrupt, dismantle and where applicable, convict those involved in terrorism. This would result in a further reduction in physical plotters, and an increase in public awareness of the deterrent effect of such operations. The importance of this work is reinforced by statistics from the annual Intelligence and Security Committee annual reports. In the period 2012-13, the Security Service devoted 68% of its resources to international counter-terrorism, a figure which the report says was broadly similar to the preceding two years (Rifkind, 2013:12). Likewise, SIS devoted 35% of its resources to the same challenge and GCHQ made a similar contribution of resource allocation (Rifkind, 2013:14).

The PURSUE strand employs the entire Intelligence cycle to meet its aims. Direction could come from the Security Service, the JIC, from Special Branch or other departments or agencies acting on information received. Collection is carried out in accordance with the direction received, to provide the raw material required to start building up a picture. This is simultaneously enhanced by the collation of existing information already held in a variety of data repositories. Analysis is conducted within the relevant agencies such as the Security Service and GHCQ, and it is evaluated in-house and at multi-agency level. The more serious the case, the more involved this evaluation process becomes. The dissemination of interim and polished Intelligence reporting will aim to provide actionable Intelligence to the executive bodies tasked with intervention, to prevent a terrorist action from taking place. This could be done by Special Branch and/or other Police assets such as specialist firearms and forensics teams, or it could require action by SIS overseas. As PURSUE is aimed at stopping an attack from happening, there is a much tighter tactical focus in this area. The authorities, especially the Police and the Security Service, constantly have to balance two opposing requirements. On the one hand, there is the desire to collect as much Intelligence as possible, to derive an evidentially solid case for a successful prosecution. On the other hand, there is the need to protect the safety of the general public.

4.1.1 Covert Detection & Investigation

The first PURSUE priority is increasing the capability and capacity of covert detection and investigation. The regulation, use and governance of covert surveillance in the UK are covered by RIPA. Covert surveillance comprises two main categories: directed surveillance and intrusive surveillance. Part 2 of RIPA governs the way in which authorised public sector organisations classed as RIPA Authorities (e.g. councils, police, and some government departments and agencies) carry out directed surveillance. This is tightly defined in RIPA (Parliament, 2000a:sec.26 (2)):

> "*Surveillance is directed for the purposes of this Part if it is covert but not intrusive and is undertaken (a) for the purposes of a specific investigation or a specific operation; (b) in such manner as is likely to result in the obtaining of private information about a person (whether or not specifically identified for the purposes of the investigation or operation); and (c) otherwise than by way of immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.*"

Intrusive surveillance is thus named as it permits a much higher degree of intrusion by the State into the right to privacy of an individual or individuals. Intrusive surveillance includes techniques such as the covert deployment of cameras in residential dwellings, and the covert deployment of listening devices into privately owned vehicles. Intrusive surveillance is defined in RIPA (Parliament, 2000a:sec.26 (3)) thus:

> "*surveillance is intrusive for the purposes of this Part if, and only if, it is covert surveillance that —*
>
> *(a) is carried out in relation to anything taking place on any*
>
> *residential premises or in any private vehicle; and*
>
> *(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance devic*e".

As covered in chapter 4.2, the proposed use of directed and intrusive surveillance must take into consideration the factors of the mnemonic "PLAN", i.e. that it is proportionate, legitimate, authorised and necessary (Johnson, 2010:para.2.04).[47] The regulatory mechanisms for the application of authorisation to conduct covert surveillance are contained in the Codes of Practice for RIPA (Home Office, 2010). The use of directed and intrusive surveillance is an increasingly emotive topic in the UK media, more so since the release of highly classified material into the public domain by the revelations of Edward Snowden (BBC, 2013). A frequent topic of discussion in the global media is the balance between the intrusion of the State into the private lives of citizens, as part of the State's attempts to secure and protect society, versus the individual and collective freedoms which citizens expect to enjoy. The most important of these are enshrined in the Articles of the Charter

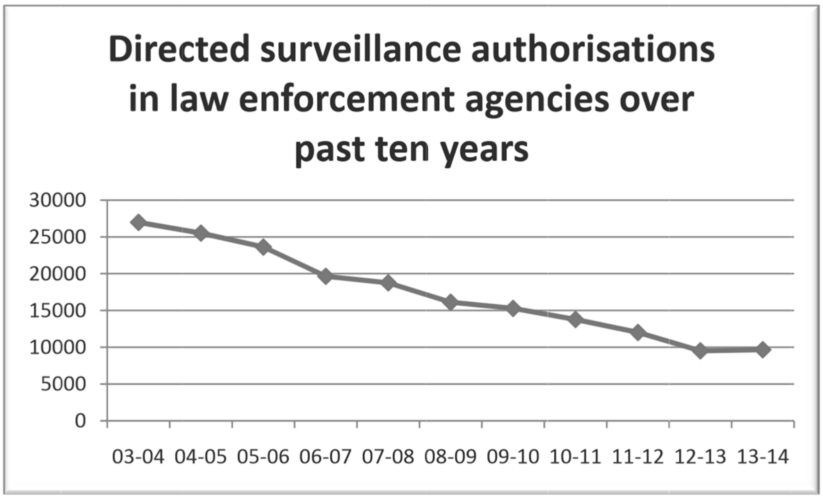
[47] A consultation was launched in April 2009 to ensure that techniques are used only when they are strictly necessary and proportionate to the offence under investigation. Following this consultation, the Government took seven statutory instruments through Parliament. These set out exactly who in each public authority may authorise certain covert techniques and for what purpose. They give clear guidance on when authorisation under RIPA is – and when it is not – required, and provide enhanced controls for local authority use of RIPA.

of the United Nations (1945). A former Director General of the Security Service commented on this distinction during a Reith lecture, stating

> "*I am often asked to speak at conferences and in debates on the theme of security versus liberty. I always refuse because I do not see these as opposites. They are different but there is no liberty without security. I wish to argue for liberty, not be falsely characterised as its opponent*" (Manningham-Buller, 2011:3).

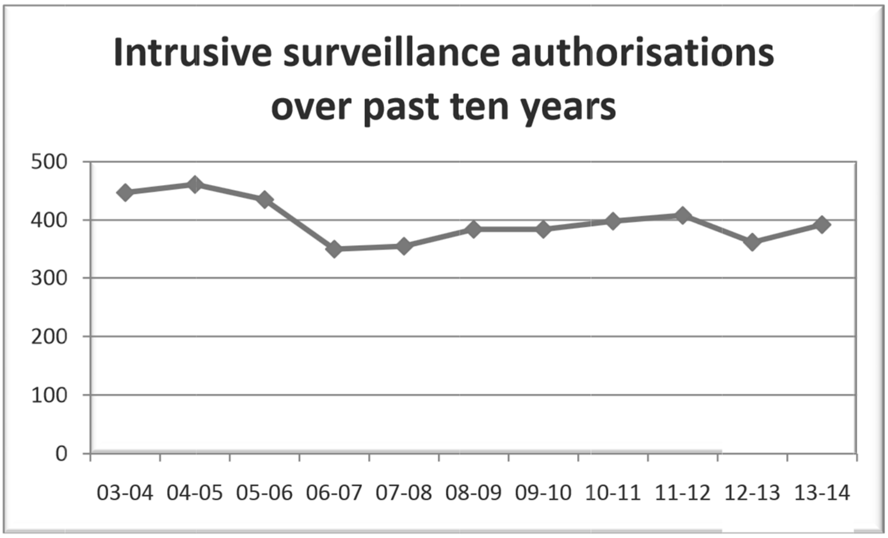
It would be useful to briefly mention the most recent statistics related to authorised property interference, and to directed and intrusive surveillance requests by law enforcement agencies in the UK, and to view these figures graphically, in the context of the previous decade.

In the Annual Report of the Chief Surveillance Commissioner for 2103-2014 (the most current at the time of writing), authorised requests by Law Enforcement agencies in the UK to conduct directed surveillance increased marginally to 9,664 applications in the period 2013-14, compared to 9,515 for 2012-13, following a continually downward trend from more than 25,000 applications in 2003. (Rose, 2014:para.4.8).



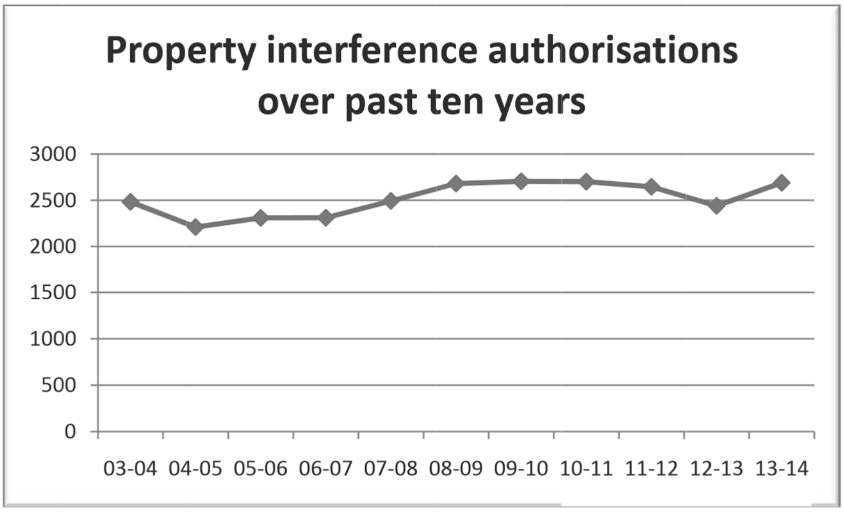
5 Directed surveillance authorisations for law enforcement agencies over past ten years (Rose, 2014:11)

Authorised requests by Law Enforcement agencies to conduct intrusive surveillance showed a slight increase for the period 2013-14, to 392, compared to 362 for 2012-13 and 408 for 2011-12 (Rose, 2014:para.4.6).



6 Intrusive surveillance authorisations over past ten years (Rose, 2014:10)

Authorisations for property interference were granted on 2,689 occasions for the period 2013-14, also an increase compared to 2,440 for 2012-13.(Rose, 2014:para.4.5).



In the report for 2011-2012, the Surveillance Commissioner commented that the use of a tracking device in a vehicle is often "*more proportionate, more accurate and safer than using scarce surveillance personnel*" (Rose, 2012:para.4.3). Many individuals engaged in terrorist activity are now much more familiar with the tactics, capabilities and technical tools used by law enforcement and Intelligence agencies than they were a decade ago. Recent terrorist plots have shown a higher degree of this knowledge than previously. Terrorist groups, organised crime groups and narcotics traffickers have also engaged in the transfer of knowledge in this area, making the work of the agencies more difficult. They are now much more "surveillance aware" than previously.[48]

7 **Property interference authorisations over past ten years (Rose, 2014:10)**

[48] See Chapter 4.3.4, *cf.* Operation RYHME.

In his 2011-12 annual report (Rose, 2012:11) the Chief Surveillance Commissioner made an observation which has implications for covert Intelligence work in counter-terrorism. He wrote that the course of his department's inspections had shown a distinct reluctance by local authorities to authorise covert operational elements such as surveillance, which he attributed to their unwillingness to be expose themselves to potentially adverse media coverage. He saw three possible explanations for this. The first was that local authorities could be conducting fewer investigations, with the associated impact that this could be contrary to the public interest. The second was that these local authorities may be employing traditional, overt methods which also carry an intrinsic risk of infringing upon an individual's right to privacy (European Court of Human Rights, 2010:10). The third was the most concerning, that local authorities were carrying out the activities without the necessary authorisation, and therefore without the legal protection of an authorised operation conducted under the auspices of RIPA (Rose, 2012:11).

A key difference between the law enforcement community and the non-law enforcement agencies such as the Department of Work and Pensions (DWP) is the level of knowledge and experience in covert surveillance and the relevant but extremely necessary legislation which governs its use. The senior leadership of the UK's Police forces are now more aware of the requirements enshrined in RIPA and other Acts, which govern the requests for, and deployments of, human surveillance teams, technical surveillance, CCTV and CHIS. The process of applying for a warrant to conduct such activities is strictly laid out and a request is submitted through a recognised and clearly defined chain of command which expects to see satisfactory justification for the granting of a warrant to conduct covert surveillance. Agencies other than Intelligence or law enforcement do not generally have this level of knowledge, awareness or experience. It can be argued, however, that covert surveillance is not their core business.

Yet any organisation or body which is authorised by RIPA to conduct such covert activities, (defined as "relevant public authorities" (Parliament, 2000b:sched.2)), has been vested with these powers because it is considered that they may have a legitimate need to use such covert methods.[49] Indeed, in the period 2011-12, 66.86% of requests for authorisation to conduct directed surveillance came from the DWP (Rose, 2012:11). As the Surveillance Commissioner highlights, there are a number of factors which engender reluctance by many of these relevant public authorities to request authorisation for the deployment of covert surveillance. This is one area in which inter-agency collaboration can help. Cross-pollonisation of officers between agencies such as GHCQ, SIS, Security Service, Special Branch and others can increase the skill sets in areas such as covert legislation, warranty and case management.[50] RIPA is not a "silver bullet" for covert Intelligence, however, and on its own it cannot be expected to cover any and all possible eventualities for covert collection.[51] While RIPA is the primary legislation governing covert surveillance, other instruments of legislation also impact on the process. The Freedom of Information Act (FIA) (Parliament, 2000a) and the Data Protection Act (DPA) (Parliament, 1998a) both have a direct relevance upon covert surveillance for relevant public authorities. The Human Rights Act (HRA) (Parliament, 1998b) also mandates the obligations of an agency employing covert surveillance, to ensure the protection of individuals who willingly pass information to that agency. The UK law enforcement agencies are also governed by the Criminal Procedures and Investigations

[49] See Annex H for a list of relevant public authorities

[50] The author has worked alongside embedded officers from a variety of agencies and has also been embedded in foreign agencies. While such cross-pollonisation can help in raising skill levels, it is also highly dependent upon the personalities involved.

[51] The question of whether RIPA is sufficient for the task of collecting covert Intelligence is one which cannot be answered in this paper, as it is a subject worthy of its own thesis, such is the depth and the breadth of the field covered. An excellent introduction to some of the issues surrounding RIPA are contained in a collection of essays edited by Billingsley (2009). Particularly relevant are Harfield's chapter (2009) on "The Regulation of CHIS", Buckley's chapter (2009) on "Managing Information from the Public". Gillespie's writing on "Juvenile Informers" (2009) take an interesting diversion for those interested in a more in-depth examination of RIPA's suitability for purpose in highly specific areas. Gillespie posits, for example, that a juvenile informant who is used covertly to conduct a test purchase of narcotics is currently covered by RIPA, yet he believes that such use cases would never have been envisaged by the authors and creators of the RIPA legislation. Indeed, Gillespie considers that this is an area best directed to the Home Office RIPA Review Group.

Act (CPIA) (Parliament, 1996) which mandates when information received in confidence by those agencies must be disclosed to the defence.

This combination of legislative instruments can result in the decision being taken by a relevant public authority that the requesting of authorisation for covert surveillance is either too risky (in terms of negative publicity and liability) or too complex (in navigating the legislation) to embark on. The path of least effort, and therefore least perceived risk, is to simply avoid requesting authorisation. For the law enforcement and Intelligence agencies, the option to take the path of least effort is rarely, if ever, available. In addition, the topic of surveillance is now very much in the national agenda of the UK media, particularly in light of the unauthorised releases of classified information by Edward Snowden.

These revelation have had negative impacts upon the Intelligence community's efforts to track and disrupt terrorists (Moore & Whitehead, 2014) and have also had an international impact in the political sphere. For example, a major breakdown occurred in the political relationship between Germany and the USA following allegations of a sustained intelligence collection effort by the USA against German governmental targets, including Germany's Chancellor Merkell (Pond, 2013; Martin, 2014). This relationship breakdown culminated in the expulsion of the CIA Head of Station, an act usually reserved for only the most serious diplomatic incidents involving Intelligence matters (BBC, 2014).

Covert detection and investigation contributes primarily to the collection part of the cycle, but it cannot start without direction, whether it is initial or ongoing. The stringent legal requirements involved in being granted a warrant for directed or intrusive surveillance ensure that individual or collective human rights are not adversely affected with just cause, and with sufficient supporting evidence to convince a Judge or a Minister of State. The cycle supports this legislative foundation, requiring direction to be given and allowing from the necessary supporting evidence to be produced during the application for a warrant. This ensures that without the necessary warrant in place, collection cannot begin, or in the event of an ongoing case, cannot continue unless an existing warrant is approved for extension or re-issue.

4.1.2 Effective Prosecution

The second PURSUE priority is to improve the effectiveness of the UK prosecution process. The primary aim of any Intelligence cycle is to produce actionable intelligence and in counter-terrorism this can take various forms. Intelligence is collected on a terrorist target in order to build up a picture of the individuals involved, the location of materials, the roles and hierarchical functions of those involved, their motivations and capabilities, the details of any attack planning and critically, what stage that planning has reached. As in the PREVENT strand there is a balance to be maintained between continuing to collect Intelligence to complete the overall picture, and to ensuring that public safety is maintained. This is particularly important to ensure that control of weapons, explosives or individuals is not lost by law enforcement or Intelligence officers. Disrupting a terrorist cell too early can mean that prosecutions are unsuccessful due to a lack of *prima facie* evidence. Allowing a terrorist cell to continue to operate, in order to conduct further Intelligence gathering, carries a risk that the cell will evade surveillance and successfully carry out an attack.

Some of the improvements in effectiveness of legislation derive from the introduction of laws such as the Counter-Terrorism Act 2008 (CTA) (Parliament, 2008). This Act introduced a number of strengthened provisions which PURSUE benefits from. Schedule 2 provides extended sentencing for offenders convicted of offences which, although non-terrorist in nature, are nonetheless deemed to have a terrorist connection, an example being the possession of explosives (Parliament, 2008:69). Certain restrictions on foreign travel can be applied in Schedule 5 to those convicted of terrorist offences, if necessary preventing offenders convicted under the CTA from travelling abroad (Parliament, 2008:76-81). Domestically, new requirements now ensure that those convicted of terrorist offences are monitored on their release from prison. In an effort to target the funding of terrorism, the Treasury Department is now empowered to order institutions in the financial sector to take direct action against suspect transactions, where a suspicion of money laundering or terrorist financing exists. UK legislation, such as the Terrorist Asset-Freezing Act 2010 (Parliament, 2010) is intended to strengthen the interdiction of terrorist financing and those engaged in it. It restores the asset-freezing capabilities previously authorised by the Terrorism (United Nations Measures) Order (Parliament, 2006) and the Al-Qaida and Taliban (United Nations Measures) Order (Parliament, 2006a) which were previously authorised under the United Nations Act 1946 (Parliament, 1946). These two Acts were subsequently deemed unlawful and *ultra vires* by the UK Court of Appeal in the case of *R v Ahmed* (Supreme Court, 2010:, para.177).[52] The Court concluded that the 1946 United Nations Act had not been intended to provide authorisation for the conduct of "coercive measures" which would, in the Court's opinion, unjustly interfere with human rights, without the requisite degree of Parliamentary oversight. TA 2006 established offences which support both PURSUE and PREVENT, such as the offence of encouraging terrorism (2006a:sec.1) or disseminating publications that seek to encourage terrorism (2006a:sec.2). These offences of incitement to terrorism have become known as "glorification" offences.

The role of intercept in counter-terrorism work is a central one and this is clearly recognised at the highest levels of UK government policy-making. The Privy Council in their review on the role of intercept as evidence (Chilcot et al., 2008:10), highlighted the importance of intercept in counter-terrorism cases worked on by SIS, GCHQ and the Security Service. The report concluded that there was considerable support for the admission of intercept as evidence but it stated that a satisfactory legal model could not be agreed upon by the key stakeholders (Chilcot et al., 2008:pp.48–51). Gordon Brown summarised the

[52] *Ultra vires* is a legal maxim, the meaning of the Latin phrase being traditionally translated as "*beyond the powers*". Its antonym is *intra vires*, usually translated as "*within the powers*". If something is *ultra vires* it is usually considered to be invalid from a legal standpoint. For a detailed explanation of this legal principle, see Dobson (2013).

dilemma in Prime Minister's Question Time, noting that the report supported the use of intercept as evidence in principal, but also had concerns about the potentially negative impact which disclosure of such material could result in (Anon, 2008:col.959).

It is exactly these conditions which prove most problematic and continue the divide between select Parliamentarians on one side, and the Intelligence community on the other. This debate is an example of the dichotomy facing a democratic government – ensuring that citizens' rights (to privacy, freedom of speech, freedom of expression, etc.) are safeguarded and remain protected from institutional abuse, while at the same time making every effort to ensure that national security and public safety are maintained. It is a delicate balance and can only be maintained if the requisite components of legislation, oversight, transparency and trust are present, and are employed satisfactorily.

The subject of lawful intercept is an extremely sensitive one in the UK but as the Home Secretary confirmed in 2014, the UK's counter-terrorism work relies heavily on the capability of intercept (2014b). This fact is now widely known and technical details regarding intercept techniques are now available on the internet (May, 2014a; BBC, 2003).[53] May (2014) also told Parliament that communications data has been used as evidence in "*95 per cent of all serious organised crime cases handled by the Crown Prosecution Service*", and that intercept has been a significant part of every counter-terrorism operation undertaken by the Security Service in the past 10 years.

The Home Office continues to take the stance that it is the Government's desire to find a method or system for the use of intercept as evidence in UK courts. In the 2013 CONTEST Annual Report (May, 2013:15), the Home Secretary stated that the government would continue to seek a workable solution which would enable intercept to be used evidentially in UK courts, but

[53] The BBC report describes the mobile telephone evidence presented by the Prosecution, in the case of the Soham murders of Holly Wells and Jessica Chapman in 2002. This case shows how forensic evidence derived from the signal data and call records of a mobile telephone are used in law enforcement. Summers (2012) describes the technical aspects of the analysis of the mobile phone handset in relation to the various cell towers.

would not reduce the value of the intercepted information as Intelligence or reveal too much about the capabilities of the Intelligence services. Given the difficulties surrounding this issue, it is unlikely that such a legally viable model will be introduced in the near future.

Effective prosecution can only take place once the cycle has been completed for at least one iteration. Intelligence alone is not enough to secure a successful prosecution; it requires solid evidence to support the prosecution in a court of law. The "sterile corridor" helps to ensure that Intelligence is used correctly and does not inadvertently encroach on the investigation itself, which could lead to evidence being dismissed, or having to be withdrawn, or being proven as unsound. All the parts of the cycle work to generate evidence, and finished product reports together with technical evidence, as depicted in many court cases with the support of graphical charts such as that in Annex E, are used to lay out the arguments of the prosecution's case. The cycle supports effective prosecutions by ensuring that the necessary analysis and evaluation have taken place before any disseminated reports are released.

4.1.3 Non-prosecution Actions

The third priority is the development of more effective non-prosecution actions, an essential component of the wider PURSUE strategy. Not all cases of suspected terrorist activity can be prosecuted, for a variety of reasons. In cases involving nationals of other countries who pose a risk to the national security of the UK, the stated aim of the UK Government is to deport such people (May, 2013:14). In cases where groups or organisations are deemed to be "concerned in terrorism", the Government's ultimate response lies in the proscription of such organisations (Parliament, 2006a:sec.21). Such proscription makes the organisation illegal in the UK, and also prohibits the organisation from operating in the UK. In addition, several ancillary restrictions assist in cutting off the group's ability to function, such as the inherent consequential offences of actual or professed membership of a proscribed group, which carries a custodial sentence of ten years (Parliament, 2006a:sec.3).

The term “operating space” can used to describe the nebulous concept of a terrorist group’s ability to form, to associate, to communicate, to plan, to gather equipment and to conduct operations (Burke, 2014). In short, it is the degree of operational freedom which the group enjoys. Within this operating space, terrorist groups conduct their own Intelligence cycle, collecting Intelligence, evaluating and analysing it, before eventually using it for attack planning (Burke, 2014). The denial of this operating space becomes a key aim in counter-terrorist planning and operations. Intelligence plays a primary function in building up a rich picture of a terrorist group and how it functions as a network, within its own operating space.

Not all terrorist groups are subjected to prosecution. It is not in the State’s interest to allow an identified group to proceed as far as possible with attack planning, and for the State to intervene at the last moment, in order to maximise the evidence collected. As discussed previously, this carries a high risk that the attack will actually take place, so the duty to maintain public safety is paramount. Second, not all groups are equal in capability and intent. Some groups are little more than two or three disillusioned individuals who may have formed a bond and discuss topics such as armed struggle and conducting attacks, but who may not actually progress beyond this stage. If and when they come to the attention of the authorities, such individuals may be more appropriately dealt with by initiatives such as the CHANNEL programme, which works to help steer such individuals away from extremist viewpoints (ACPO, 2009).

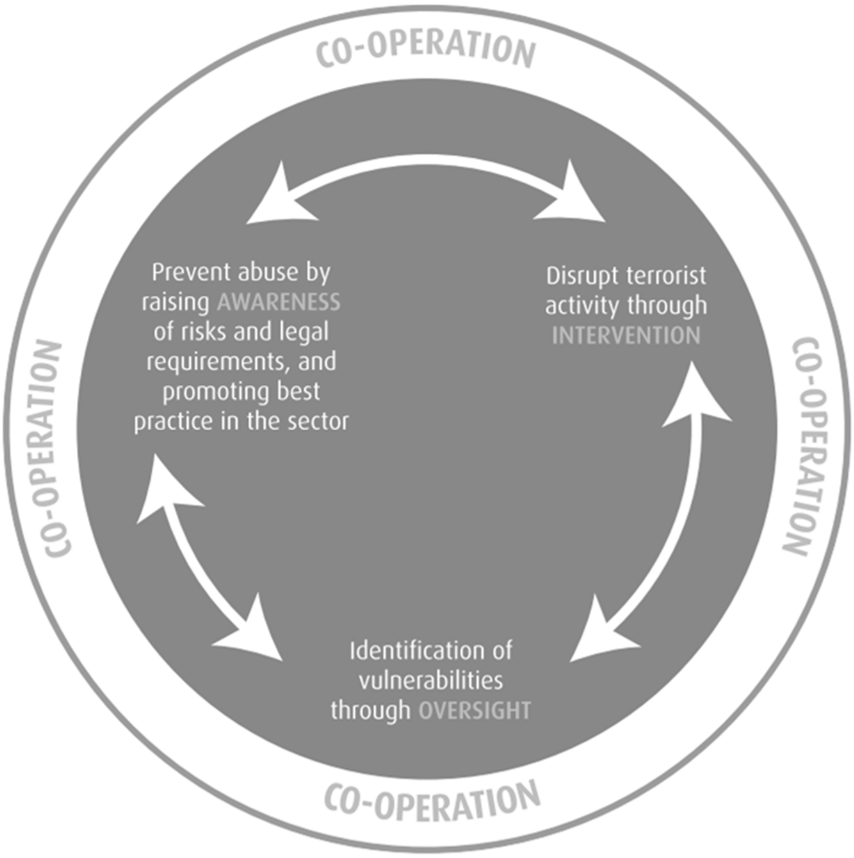
The Terrorism Prevention and Investigation Measures Act (2011) (Parliament, 2011) abolished the previous system of control orders, replacing it with Terrorism Prevention and Investigation Measures (TPIM) against an individual about whom there exists a reasonable belief that the individual is, or has been, involved in terrorism (Parliament, 2011). Control orders were introduced with the Prevention of Terrorism Act 2005 (Parliament, 2005) and have been the subject of a long-running debate in the UK, about the appropriateness of these measures. Former Home Secretary David Blunkett described the use of electronic tagging as being like a "*prison without bars*" (BBC, 2004). A key objection has been the ability for the State to subject an individual to a control order, while withholding the details from the affected individual, of why they are being subject to the control order. Critics have voiced concern about the State's ability to ignore the central tenets enshrined in *habeus corpus* (Parliament, 1679).[54]

The targeting of terrorist financing remains a key weapon in counter-terrorism, as severing a group's access to operational funds can have a disproportionately successful effect upon the group's ability to plan and conduct actual operations.[55] In addition to the UK's own legislation on the combating of terrorist financing, the UK is also bound by some United Nations legislation, such as United Nations Security Council Resolution 1904 (UNSC, 2009), primarily aimed at disrupting Al Qaeda financing. The UK's Charity Commission has produced its own counter-terrorism strategy document, in which it defines its overarching aim as: "*to identify, disrupt and prevent terrorist and other serious abuse of the charitable sector*" (2012:8). After 2007, the Commission was more proactive in its efforts, engaging more with the Metropolitan Police and Counter-Terrorism Command, and creating a greater focus on Intelligence analysis. The first version of the Commission's counter-terrorism strategy (2008) came about as a result of these efforts, plus a wider engagement with the public, canvassing opinion from civil society and other interested bodies on which strategic direction the Commission should take (Jones, 2008).

[54] The legal maxim of *habeas corpus* translates from the Latin as "*you may have the body*". In its full form, the maxim states "*habeas corpus (ad subjiciendum*)", meaning "*you may have the body (subject to examination)*", i.e. a person could only be held in detention if their detention could be proven to be lawful. The Habeus Corpus Act was passed by Parliament in 1679, although the legal principle is believed to have been part of Common Law prior to the publication of the *Magna Carta*, which was published in 1215. Article 39 of the *Magna Carta* stated that "*No freeman shall be taken or imprisoned or disseised or exiled or in any way destroyed, nor will we go upon him nor will we send upon him except upon the lawful judgement of his peers or the law of the land*".

[55] Interviews between the author and U.S. members of a specialist team working to interdict terrorist financing, Kabul, Afghanistan, 2006-2009.

The strategy was revised in 2012 (Charity Commission, 2012) to align it more closely with the findings of Lord Carlile's review (2011) of the PREVENT strategy for the government. In 2014, a draft Bill (Cabinet Office, 2014a) was produced, entitled "Draft Protection of Charities Bill". This legislation, if enacted, will give the Commission wider powers to take more stringent action. These powers include the ability to close down a charity under investigation, in order to maintain the public's confidence (Cabinet Office, 2014a:sec.6). They also include preventing individuals from resigning before they are disqualified, then returning to another charity at a future date (Cabinet Office, 2014a:sec.8–9). The Charity Commission's 2012 strategy (2012:8) still contains the same four-strand approach of awareness, oversight, co-operation, intervention, the model of which is reproduced below:


CO-OPERATION
Prevent abuse by raising AWARENESS of risks and legal requirements, and promoting best practice in the sector
Disrupt terrorist activity through INTERVENTION
CO-OPERATION
CO-OPERATION
Identification of vulnerabilities through OVERSIGHT
CO-OPERATION

8 Charity Commission Counter-Terrorism Strategy: The Four-Strand Approach (2012:8)

In some circumstances, non-prosecution actions can be a deliberate choice for the Police, while in other circumstances, they may be the only course of action open. Despite the work of the Police and the Intelligence agencies, there are occasions when the outputs of the cycle are only Intelligence, and not evidence. When there is a credible risk to public safety, the Police may have to arrest a terrorist suspect, knowing that at the point of arrest, there may be little or no admissible evidence to support a prosecution.[56] This is not a breakdown or a weakness of the cycle as a model, it is simply a reality that despite the best efforts of Police and Intelligence agencies, there will always

[56] See Section 4.3.4 for an example of just such an instance, during Operation RHYME.

be cases where there is a paucity of evidence collected. Some targets are very “surveillance aware” and are meticulous in ensuring that their behaviour, their communications and their actions cannot be used as evidence against them. The Intelligence cycle conforms to the same principle of databases: “garbage in, garbage out”, that is to say, the outputs of the model are highly dependent upon the inputs into it, as well as on the capabilities of the people involved in the cycle’s processes. The cycle supports non-prosecution actions, as it can be very clear that further Intelligence is unlikely, or that despite the Intelligence collected, there is not enough evidence to move to arrest and prosecution. Finally, Intelligence gaps still occur, despite all available resources being devoted to a high-value target.[57]

4.1.4 Disruption of Terrorist Activities Overseas

The fourth PURSUE priority is improving the government’s capabilities to disrupt the activities of terrorists abroad. Countering the threat of overseas terrorism, in addition to being an aim in itself, also contributes to the national security of the UK. Important intelligence is often derived from the disruption of overseas terrorist groups, especially when members of the group are detained or electronic media is captured. This has, however, raised another issue with which the UK government has had to contend, *viz.* the protocols to be followed when British officials observe or take part in the questioning of suspects detained overseas. Detailed debates took place in the House of Commons, regarding British Intelligence officers and their alleged participation in, or observation of, the torture of terrorist suspects detained overseas (Davis & Lewis, 2009). As a result the UK government produced a guidance document in July 2010, detailing the code of conduct to be followed by Intelligence or law enforcement officers involved in overseas questioning (Cabinet Office, 2010). This was legally challenged In July 2011 by the

[57] See Section 3.1.1 for a detailed summary of the difference between Intelligence gaps and Intelligence failures.

Equality and Human Rights Commission (EHRC) in legal action (2012; 2011) against the Prime Minister, the Secretary of State for Defence and two others, arguing that the governmental guidance:" …*leaves officers in the field with the mistaken and unintended expectation that they will be protected from personal criminal liability in situations where they may, unwittingly, be liable for crimes*".[58]

A key instrument in the UK's capability to disrupt terrorist actions overseas is the use of Special Forces (SF). The UK government confirmed in May 2012 that up to 200 SF soldiers would remain in Afghanistan beyond the 2014 withdrawal (Wintour, 2012). Since 2003, the UK SF have been heavily involved in counter-terrorism operations in Iraq and Afghanistan. The deployment in Iraq after the 2003 invasion required a complete SF Squadron to be based in the country for a 6-month deployment. The Squadrons were rotated every 6 months for a period of several years, resulting in one of the most sustained UK deployments of SF since World War 2. The use of the SF in Iraq and Afghanistan has allowed the British government to engage in significant force projection, taking the counter-terrorism battle to the very centre of the operating space of some groups, especially that of the Afghan Taleban and the Iraqi insurgency. In addition to the physical disruption resulting from a counter-terrorism operation overseas, such a capability also generates a psychologically disruptive effect among cell members, as they often feel unsafe, even within their traditional home areas (Source_08, 2011).

A key factor in disrupting terrorism overseas is the Foreign Service liaison work undertaken by British Intelligence officers with their foreign counterparts. Naturally, this is stronger in some countries than others. The Intelligence cooperation between the UK and the USA, for example, is the real heart of what has become known as "the special relationship". The extent of trust in this relationship allows a full and frank sharing of raw and finished product that enables a very effective division of labour between the two partner

[58] Email correspondence between the author and the EHRC.

countries. Other bilateral relationships have also resulted in significant disruptions, such as the information provided by Saudi Intelligence which enabled the UK authorities to eventually discover the so-called “printer bomb” on a commercial cargo plane when it landed in the UK.[59]

Cultural factors play a large part in the benefits gained from international liaison work, especially where there are considerable cultural differences in the host country. Regions such as the Middle East and Southeast Asia can be difficult environments in which to collect Intelligence, without understanding the myriad factors which underpin the cultural framework and the interpersonal relationships which are so vitally important in these locations.

Foreign liaison is not without its difficulties, however. Not all countries follow the same rules on protecting Intelligence sources, so a deeper risk assessment needs to be conducted when sharing Intelligence with certain countries, in order to ensure that sensitive information is not passed on to individuals or agencies not cleared for such information. Even worse is the potential for high-grade, processed Intelligence to be passed on to the terrorist targets themselves, either deliberately or inadvertently. One of the most frequently discussed countries in this regard is Pakistan, and the links between the Inter-Services Intelligence Agency (ISI) and the Taliban / Al Qa’eda. Legal issues also exist in sharing Intelligence with partner countries that may be subject to additional, legal requirements outside of their own national legislation. One such example is that of US Intelligence reports being passed on to an EU partner nation which then faces a legal challenge to disclose such information.

The Intelligence cycle results in reported product which is used as a basis for disruption operations against terrorist groups or individual actors. In many ways, this disruption is the archetypical picture of the cycle in action. Once an individual is named as a target for investigation, this direction results in a collection effort which, together with other collated information, is analysed

[59] See Chapter 4.3.2 for more details on the “printer bomb plot”.

and evaluated, resulting in the requirement to collect additional Intelligence. The subsequent direction then refines the original direction, bringing a narrower aperture of focus on the target. As the picture builds, a target back begins to develop and when this has been sufficiently refined and contains enough accurate information to be acted on, the disruption plan can be formulated and implemented. This is arguably the zenith of the Intelligence cycle in action.

4.1.5 Capacity Building

The fifth priority is to strengthen the coherence between the UK's counter-terrorism work and the capacity-building and counter-insurgency work which is conducted overseas (Johnson, 2010:11). The use of UK intelligence officers overseas is not the only way in which the PURSUE strategy aims to disrupt overseas terrorist activity. The UK devotes considerable effort and financial commitment to capacity-building programmes which aim to raise the capabilities, effectiveness and standards of other countries which the UK considers as partners in the fight against international terrorism (May, 2013:19).

These capacity-building programmes have soft and hard aspects. The soft side can include the provision of specialist training courses on the whole spectrum of the Intelligence cycle, assisting those countries in raising their own standards of Intelligence collection and use. This helps the recipient country to professionalise their systems and processes to higher, more sophisticated and more effective standards of Intelligence collection and exploitation. Raising the standard of counter-terrorism capabilities of other countries such as Pakistan and Yemen contributes directly to increasing the level of public safety in that country and also helps to reduce the potential threat of international terrorism reaching the UK's shores.[60]

The harder side of the equation concentrates on direct action which is carried out when the Intelligence cycle has generated actionable Intelligence and disruptive action is required. This is another area which can fall to the UK SF, who provide training and mentoring in counter-terrorism operational procedures to other nations. For example, in 2010 the UK government sent a contingent of SF to train the Yemeni Armed Forces, following the abortive attempt by Umar Farouk Abdulmutallab to detonate a device on board a U.S. passenger airliner as it prepared to land in Detroit (Rayment & Blomfield, 2010).

In addition to capacity-building programmes, the UK government also provides direct funding to countries which are considered to be key partners in combating international terrorism. In the financial year 2009-10, the budget for overseas counter-terrorism was £36.9 million (Bryant, 2010). The recipient of the largest segment of this funding was Pakistan, followed by Afghanistan, Yemen, Somalia and the Sahel in descending order (Home Office, 2011:11).[61]

Assessing the effectiveness and impact of capacity-building programmes is one of the most difficult areas of Foreign Service work.[62] In terms of mapping this against the Intelligence cycle, this is almost impossible to do. What is more usual is to look at the quality of the product and the skill of the staff, comparing the before and after results. Such comparisons are, however, more subjective than objective, but the key aims are to assess whether the officers trained have absorbed the training sufficiently to be able to deliver a higher-

[60] The author has worked in several such missions overseas and the efforts of the UK are often closely tied in with other bilateral or multilateral arrangements, employing specialists from different nations.

[61] The financial year 2009-10 was the last year in which government spending on overseas counter-terrorism was revealed in the CONTEST annual summary.

[62] Based on the Author's personal experience of delivering such programmes in a number conflicted and post-conflict countries. The Author has called for increased capacity-building in the area of Intelligence, particularly with capable partner countries who have the capacity and willingness to improve, but have been hampered by external factors, such as a historical past which impacted on their current capabilities, in the case of the Baltic States (Burke 2015, pp.21–25)

grade product afterwards. Much of this training focuses on the analysis and reporting aspects of the cycle. The direction and evaluation parts are often either overlooked or given less priority, which is an area in which improvements can and should be made.

4.1.6 Inter-Agency Co-ordination

The sixth and final priority is the enhancement of inter-agency co-ordination. Much has been written about the rivalry between the UK Intelligence agencies, particularly that between SIS and the Security Service. It has been a long-running topic for authors, especially the depth of the rivalry which was perceived to exist during the Cold War (Harrison, 2012; Corera, 2012; Macintyre, 2014). In the past two decades co-operation between the Intelligence, security and law enforcement agencies of the UK has seen great improvement. By 2007 for example, the Director of the Security Service confirmed that his agency had established eight regional centres in the UK, working in tight integration with Police officers, Special Branch and with other regional authorities (Evans, 2007) and by 2011 this had been increased to nine. The Intelligence and Security Committee (Rifkind, 2013:13) noted in 2013 that such inter-agency collaboration had undergone "*a huge change for the better, sweeping away the tired old turf wars of ten or twenty years ago*".

The UK's Intelligence agencies, together with the Police and the Armed Forces, now co-operate to "*an unprecedented degree*" in the counter-terrorism arena, to protect both the UK and its interests overseas (Source_08, 2011). Since the Al Qaeda attacks on the U.S. in September 2001, and the resulting allied military interventions in Afghanistan and Iraq, this co-operation has increasingly included Defence Intelligence (DI), due to the close proximity in which the UK SF and other elements of the Armed Forces operate in this space. A Foreign Secretary illustrated this increased contribution from DI when he described his involvement in the NATO air campaign in Libya, stating:

> "*We really saw as ministers through the last year, through the Libya conflict, the value of Defence Intelligence. We started each day listening to the Chief of Defence Intelligence and then the JIC staff and we couldn't make our political decisions about Libya without really understanding the defence picture. So I think perhaps we have had direct experience, more than would be the case of ministers in recent years, of the value of Defence Intelligence*" (Rifkind, 2012:17 citing Foreign Secretary Hague).

The degree of crossover nowadays, between overseas and domestic counter-terrorism to protect UK interests has increased since the 2001 Al Qaeda attacks on the USA. Domestic terrorist plots would traditionally have fallen to the Security Service to deal with, while a group plotting to attack British targets abroad, for example, would come under the remit of SIS. The rise of the global, interconnected Islamist extremist network has resulted in a blurring of boundaries, both for the terrorist groups and for those who work to defeat them. Taking post-2003 Iraq as an example, one scenario is a group of Iraqi nationals, based inside Iraq but with connections to other individuals within the UK, plotting an attack inside the UK, requiring one or more of the Iraq-based group to travel to the UK. Another scenario is a group of UK nationals planning to travel to Syria to join a jihadist group such as ISIS. The demarcation of previous decades is no longer as clear-cut as it once was. The Intelligence cycle can be employed by an individual or across multiple agencies and in this latter example, SIS, GCHQ and the Security Service would conduct their own iterations of the cycle, providing their own, single-agency direction, resulting in collection, with multi-agency collation, evaluation and analysis, with each agency exchanging semi-finished reports before an all-source, polished report might be issued. The work of JTAC has done much to push forward this inter-agency working, with each agency providing officers and agency-specific IT terminals to enable a truly joint working environment with commentary from all of the key agencies on terrorist-specific. While the JTAC environment is probably more accurately described as multi-agency working, it has an added, spin-off benefit. Staff seconded to JTAC work in a unique environment where Intelligence sharing and partnerships are the norm instead of the exception. When they return to their parent agencies, these experienced officers are much more willing and able to work collaboratively with their colleagues in other agencies and other government departments. Together with cross-fertilisation tours and exchange officer postings, JTAC adds another mechanism to encourage the spread of joined-up working across the Intelligence community.

When two or more agencies are collaborating on a target, the various elements of the cycle may be carried out by more than one agency. In terms of collection, this may be limited to one agency by necessity, given the nature of the target. Collation, analysis and evaluation are more typical areas in which multi-agency work is more usual. When it comes time to produce a report, this may be done by one agency as the lead, or it may be a collaborative work. Both are common, depending on the nature of the task.

4.1.1 SUMMARY

The PURSUE strand of CONTEST is probably the most easily identified with the operation of the Intelligence cycle. This section has described the six key areas of the work involved, and it has been clearly demonstrated how the Intelligence cycle underpins the whole of PURSUE. Without a functional and simple model, these areas would require more resources for planning and for the operational activities carried out within the cycle. All three of the UK's Intelligence agencies, together with the Police, are familiar with the 6-stage Intelligence cycle and this results in a real "force multiplier" effect. Individual officers as well as teams are able to work on a part of the cycle, share the progress, hand over work to others, and pick up the work at a later stage of the cycle if required, without any loss of momentum. Regular liaison, including multi-agency meetings, help to ensure that all parties are regularly updated and that any new developments are shared among the relevant analysts. The Intelligence cycle works very effectively in the PREVENT strand and it is the mission which drives the process.

4.2 PREVENT

The PREVENT stream concentrates on the root causes of radicalisation, to stop individuals becoming violent extremists or terrorists. Radicalisation has been defined by a specialist Home Office department as: "*the process by which people come to support terrorism and violent extremism and, in some cases, then join terrorist groups*" (BSU, 2008). Under this strand, various outreach programs aim to counter the radical, extremist and/or violent ideologies which assist in recruiting individuals to groups which espouse these belief systems (Home Office, 2011:58–77). The PREVENT stream acknowledges that the proactive disruption of terrorist groups can never be solely sufficient to neutralise the terrorist threat, recognising instead that a collective partnership of central and local Government, law enforcement and the wider community is essential. In June 2011, the PREVENT strand underwent a comprehensive review by the UK government (Carlile, 2011). Following this review, PREVENT now comprises three central policy planks.

4.2.1 The Ideological Challenge of Terrorism

The first component of PREVENT is responding to the ideological challenge of terrorism and to the threat from the people promoting it (May, 2011:1). Under this, the current UK government (a Conservative & Liberal Democrat coalition) takes a visibly tougher stance than the previous (Labour) government, stating that this government will not work with groups or organisations who do not accept "*values of universal human rights, equality before the law, democracy and full participation in our society*" (May, 2011:1–2). This plank of the PREVENT policy also tightened up on providing funding to groups working within this sphere, making it clear that funding would be withdrawn unless clear evidence was available that the work of a group was effective and that it provided value for money (Travis, 2011).

The current strategy aims to interdict the ability of extremist and terrorist groups to spread their ideological message, thus limiting their potential ability to successfully radicalise people, especially those individuals more vulnerable to radicalisation. The ideological challenge identified by the Government also raises the issue of community engagement, which spreads across both the first and third priorities of the revised PREVENT strand (ACPO TAM, 2008). In countering radicalisation and extremism, communities are often more effective at identifying vulnerable individuals and attempts at radicalisation, or any increasing trends of such behaviour with the community (Source_08, 2011). The Association of Chief Police Officers considers the involvement of local authorities and other partners to be "*critical…in preventing violent extremism. They are in a good position to talk to their local communities, hear their concerns and help them to reject extremism"* (ACPO, 2015). This resonates clearly with the ACPO stance that PREVENT is not only an initiative of the Police, as ACPO believes that the communities best able to reject extremism are those with "*strong and empowered communities*" (ACPO, 2015).

Fighting an ideological challenge using the Intelligence cycle is more opaque than the work which takes place in the PREVENT strand, and targeting an individual or a group is a more clearly defined task than targeting a belief system. An additional factor is that much of this work takes place in the political sphere and is therefore carried out not by Police or Intelligence officers, but by civil servants who are unlikely to have been trained in the use of the Intelligence cycle. There are inputs into this work-stream which will have derived from the Intelligence cycle's outputs, such as the scale and content of a jihadist website which promotes extremism and exhorts people to take part in terrorist activities. In addition, reporting derived from the Intelligence cycle is used in cross-government initiatives, such as the report by the Prime Minister's Task Force on Tackling Radicalisation and Extremism (Cabinet Office 2013). Other classified reports will derive from direction, resulting in collection, analysis and evaluation, and will be produced as a disseminated product, but may not go through subsequent iterations of the cycle. This does not, however, lessen the contribution of the model in any way.

4.2.2 Prevent the Recruitment of Individuals

The second priority of PREVENT is preventing people from being attracted to terrorism, and making sure that anyone at risk is provided with the "*appropriate advice and support*" (May, 2011:15). The latest PREVENT strategy makes an important assertion, that radicalisation is usually "*a process, not an event*". This is noteworthy for a number of reasons. First, a process generally has a longer timeline than an event, and a process should provide more opportunities for interdiction than an individual event. Second, this identification of radicalisation as a process has allowed the Home Office to compare it with some elements of the processes used in serious crime, together with the associated crime prevention methods, tactics and tools which have been developed to combat it. Whilst acknowledging some similarities, however, the new strategy clearly emphasises that the PREVENT strand is not a Policing strategy, nor should it become one (ACPO, 2015).

The 2011 revision to the PREVENT strategy acknowledges that there has been public concern over the perception that PREVENT-related programmes are being used as a vehicle to conduct intrusive and/or unwarranted surveillance against citizens (May, 2011:56). It has also been the subject of academic criticism (*imprimis* Rogers, 2008:38–61). Another concern was that the strategy could allow programmes to be used in a disproportionate manner

(May, 2011:31), an issue which had been extensively reported on in the mainstream media, primarily in regard to a paper published by the Institute for Race Relations (Kundnani, 2009). While noting this concern, the report stresses that PREVENT-related programmes are not and will not be used as a means to covertly collect intelligence. The report adds that such programmes will be subject to appropriate oversight mechanisms and data protection regulations (May, 2011:8).

The recommended principles for the sharing of PREVENT-related information are stipulated in a Home Office policy document, which clearly establishes the guidelines for such sharing as necessity and proportionality, consent and the power to share (Gupta, 2010:17-20). Consent should be obtained wherever possible, although the guidance recognises that this will clearly not be possible in some cases, and provides mechanisms for instances in this case. The power to share information between departments is legislated mainly by two statutory Acts, the DPA (Parliament, 1998a) and the HRA (Parliament, 1998b).[63] Necessity and proportionality consider that information should only be shared where it is both necessary and proportionate to the outcome desired by the covert action being planned. Both necessity and proportionality are two key requirements in the legislation of covert policing in the UK, as part of the mnemonic "PLAN". This covers four areas which must be considered before undertaking a covert operation:

> 1. "*Proportionality – is it proportionate to obtain the intelligence desired using the planned covert methods?*

[63] In addition, the power to share information is also covered by the common law duty of confidentiality which places an obligation upon a solicitor, for example, to respect the confidentiality of the affairs and statements of their client. A concise explanation of this premise, together with a legal test is as follows: "*Confidential information is any information to which the common law 'duty of confidence' applies. A duty of confidence is created when 'private' information has been passed on in such a way that the person receiving the information was aware, or should have been aware, that the information was being imparted on the basis of confidentiality. (The legal test is whether a 'reasonable' person would think the recipient ought to have known that the information was confidential)*" (London Law School, 2013:1).

2. *Legitimacy – is the purpose of obtaining the desired intelligence a legitimate on, such as national security interest, prevention of crime and disorder, or public safety?*

3. *Authority - what is the lawful basis and the legal authority for undertaking the covert action, and what warrantry is required?*

4. *Necessity – why is the desired activity necessary, and could the intelligence be obtained through other, less intrusive methods?*" (Harfield & Harfield, 2012:102).

Laws (Parliament, 2000b:sec.30) and statutory instruments (Parliament, 2000d) stipulate, for example, that in order to deploy a Covert Human Intelligence Source (CHIS), authorisation must be necessary and proportionate (Parliament, 2000b:sec.29(2)). These prerequisites, originally deriving from the ECtHR, ensure that a citizen's rights, especially the right to privacy (as stipulated under Article 8 of the ECHR (2010:art.8)) are not lightly sacrificed by the Intelligence agencies or the Law Enforcement community. They further ensure that sufficient justification is provided before any covert action is authorised. In particular, the principle of necessity negates the instigation of covert action such as conducting intrusive surveillance or the deployment of a CHIS, simply because it would provide an easier method of collecting intelligence than less intrusive methods. It would be impossible from a Policing point of view to successfully, effectively and efficiently identify all the cases of extremism and terrorism ongoing in the UK by operational Policing tactics and methods, as there are simply not enough resources.

Another highlight of the 2011 PREVENT policy is a more rigorous scrutiny of the funding provided to the various programmes which work in this area of supporting those identified as being vulnerable to radicalisation or extremism. Acknowledging that such programmes wield considerable influence, the

PREVENT strategy stipulates that such organisations must also be "*credible and able to reach and talk to people at risk*", a criticism which has been voiced about previous efforts (Carlile, 2011:sec.6.53–6.70).

The new strategy also emphasises an international dimension to this work, aiming to operate collaboratively with other foreign governments in the areas of research, and to build on the knowledge and understanding of other countries, to better understand radicalisation. While such international co-operation takes place across many areas related to counter-terrorism, it is rarely publicised due to the sensitivities involved in international collaboration. Some countries do not want such participation made public, and this is particularly the case in the regions of the Middle East and Asia-Pacific. Despite this, a number of de-radicalisation programmes have been discussed openly, including programmes in Saudi Arabia (Ezzarqui, 2010), Yemen (Porges, 2010; Berger, 2014) and Indonesia (ICG, 2007). Opinion is divided as to their effectiveness and long-term success rates (Source_08, 2011).

The Intelligence cycle can be applied to a recruitment prevention target in a similar way to an active terrorist target. Although the threat posed may be lower, the same stages can be followed in collecting and reporting, to enable the authorities to decide which course of action to take. This could range from no action and only a monitoring brief, to referral to the CHANNEL programme, e.g. in the case of a vulnerable adult or a young teenager, through to intervention by the Police if deemed necessary. The Intelligence cycle supports recruitment prevention equally well as it does with the PURSUE strand.

4.2.3 Addressing Radicalisation

PREVENT's third priority is to "*work with those sectors and institutions in which risks of radicalisation exist*" (May, 2011:8). Five particular areas of focus are identified by the June 2011 strategy: faith, health, educational institutions, charities and the criminal justice system and the internet has been added as a separate, standalone category (May, 2011:8). The 2011 policy makes the aspirational statement that there should be no "*ungoverned spaces in which extremism is allowed to flourish without firm challenge and, where appropriate, by legal intervention*" (May, 2011:9).

As the Internet is being used more and more by terrorist groups, and by those engaged in radicalisation, it follows that the use of the Internet as a radicalisation vehicle will be a key area for the PREVENT strategy. Indeed, Al Qaeda has been described as the first guerrilla movement in history which made the move from the physical to the virtual space (Coll & Glasser, 2005). Given the size and depth of the internet, however, the battle to deny the internet to radicalising elements is more of an ambition than an achievable policy goal. PREVENT acknowledges that counter-radicalisation programmes need to be proportionate to the actual risk of radicalisation, as resources are limited in this area.

The PREVENT strategy is owned and coordinated by the Office for Security and Counter-Terrorism (OSCT) within the Home Office. The OSCT reports directly to the UK Home Secretary in the capacity of Lead Minister, and also to the Minister of State for Security and Counter-Terrorism (OSCT, 2011). Despite the PREVENT strategy being owned at Ministerial level, the 2011 policy pushes the implementation of it down to the lowest practical level through a wide range of partnerships such as crime reduction groups, local authorities, faith and youth groups, housing offices and others (May, 2011:sec.8.69, 9.7, 11.13).

The UK government has made efforts to raise awareness about the indicators of radicalisation and extremism, highlighting the risks posed to young people in further and higher education institutions, while the problem of radicalisation, particularly within UK prisons, has been an increasing area of concern in UK counter-terrorism (BSU, 2008).[64] A report by the Quilliam Foundation on radicalisation in British prisons identified four individuals who had been radicalised while in prison, and were later convicted and imprisoned for terrorism-related offences (Brandon, 2009:14). The threat of radicalisation being conducted within UK prisons is a serious one which requires more extensive research to better understand the nature of this threat.[65] Neumann, for example, has doubts about certain individuals, such as Jose Padilla, having been radicalised while in prison, as opposed to after their release (2010:29). Two case studies highlight the dangers which successful radicalisation can pose.

Richard Reid, the so-called "shoe bomber", converted to Islam while serving a sentence in Feltham Young Offenders Institution & Remand Centre for various petty crimes. Following his release from prison, he began to attend Brixton mosque and changed his name to Abdel Rahim. According to the Imam there, Reid was influenced to change mosques by people who had established themselves some years ago on the periphery of the mosque's influence. Baker described their beliefs and teachings as much more militant (BBC, 2001). Imam Baker believed that these individuals deliberately targeted weaker, more impressionable individuals and that Reid fitted this profile.

Reid moved on to attend Finsbury Park mosque in London, which at the time was under the leadership of Abu Hamza al Masri, the radical, extremist preacher. Masri was later convicted in the UK of a series of offences, including six counts of soliciting to murder and one offence under the Terrorism Act 2000. He was subsequently extradited to the USA in October 2012 and convicted of a range of terrorist-related offences including hostage taking and conspiracy to provide and conceal material support and resources to terrorists. He was sentenced to life imprisonment in the USA (U.S. District

[64] Part of the report states: "We have noticed that terrorist groups are remarkably tolerant of individuals with serious criminal histories. This is the case even when those individuals continue to be involved in very serious non-terrorist crimes, including drug trafficking, assault and even rape" (BSU, 2008).

[65] The National Offender Management Service (NOMS) business plan provides an insight into its resources, aims and working methods Also see work by Neumann (2010).

Court, 2004). There is strong conjecture, but no hard evidence, that Reid personally met Zacarias Moussaoui, currently serving life imprisonment without parole in the US, having been convicted of his involvement in the 11 September 2001 attacks by Al Qa'eda against the USA (U.S. District Court, 2006). Imam Baker also agrees with the theory that Reid met Moussaoui (Brandon, 2009:14).

Shortly after he ceased visiting Brixton mosque, Reid travelled to Afghanistan and Pakistan in 1999, and spent most of the year 2000 in Pakistan. It was during this visit that he is believed to have attended the Khalden terrorist training camp outside Kabul. Ahmed Ressam, who attended Khalden training camp and was subsequently imprisoned for his part in plotting to detonate explosives at Los Angeles Airport (the "LAX Millennium Plot"), identified Reid as having attended the camp at the same time as him. Another convicted AL Qaeda terrorist, Yacine Akhnouche, also identified Reid as having attended Khalden camp (Elliott, 2002). On 22 December 2001, Reid attempted to detonate an explosive device hidden in his shoes, while on board an American Airlines plane flying from Paris to Miami. He was overpowered by passengers after the device failed to detonate. Reid was subsequently sentenced by a U.S. Court to three life sentences with no possibility of parole (U.S. District Court, 2002).

Muktar Sa'id Ibrahim was the ringleader in the failed 21 July 2005 attacks against the London transport network, and was also one of the attempted suicide bombers in the plot. He was convicted of conspiracy to murder for his part in the attempted bombings and was jailed for life with a minimum tariff of 40 years (CPS, 2007). Ibrahim is believed to have been radicalised during his time in a British prison (BBC, 2005). Convicted of indecent assault at the age of 15, he was later involved in two robberies and like Reid was eventually detained for five years in Feltham Young Offenders Institution & Remand Centre, for a gang-related attack he was involved in. Also like Reid, he began to attend Finsbury Park mosque, listening to sermons preached by Abu Hamza al Masri.

It is still not fully known if Ibrahim actually met with Mohammed Siddique Khan (leader of the 07 July bombings in London) while he was in Pakistan during a visit in December 2004, but counter-terrorism officers believe that the two men either met in person, or that they were both trained by the same person or people. Ibrahim travelled to Pakistan on 11 December 2004, together with two other males named Shakeel Ismail and Razwan Majid. All three men were carrying camping equipment, cold weather clothing and copies of pages from a medical manual, on dealing with ballistic injuries.

Officials at Heathrow airport detained the men and questioned them, as their equipment was similar to that noted being carried by other British males who had travelled abroad to take part in jihad. They were released after questioning and allowed to depart the UK, as they had not committed any offence. Two of the 07 July bombers, Mohammed Siddique Khan and Shehzad Tanweer, departed the UK for Pakistan a couple of weeks before Ibrahim, on 19 November 2004. Tanweer and Khan returned to UK on 08 February 2005 while Ibrahim returned alone, in March 2005. Between 11 December 2004 and 08 February 2005, two of the suicide bombers who later blew themselves up in the 07 July attacks were in Pakistan at the same time as the leader of the failed 21 July attacks (Casciani, 2007).

In addition to their simultaneous location in Pakistan for nearly 4 weeks, the similarity of the explosive devices was an even stronger link. All the devices used in the successful 07 July attacks and the failed 21 July attacks were based on hydrogen peroxide. Although hydrogen peroxide has been used by many terrorist groups for the past two decades, the actual composition of the devices used in both the 07 July and the 21 July attacks was unlike anything previously seen, according to the government forensics experts who examined the devices (Casciani, 2007). Although forensically similar, the main difference was in the organic compound used in the explosive material. The devices used on 07 July, all of which detonated, had black pepper as the organic ingredient. The devices used on 21 July, all of which failed to fully detonate, employed chapatti flour as their organic compound. Government experts stated that the types of devices used in these attacks has not been found in any professional literature, and believed that this kind of device used was too unstable to handle (Casciani, 2007). When a reconstruction of one of the bombs was manufactured by government technicians for testing purposes, it had to be carried out with the use of robotics in a quarry due to the high risks involved in creating such an unstable device (BBC, 2007a). The degree of similarity of the devices makes it almost certain that they were either constructed by the same bomb-maker, or that the same bomb-maker instructed two or more individuals who subsequently manufactured the devices.[66]

There is another possibility, which is that the explosives used in the devices for the 21 July attacks were manufactured at the same time, and in the same batch, as the explosives used in the devices which successfully detonated in the 07 July attacks. If the explosives had degraded due to sublimation in the period between being manufactured and the attempts to detonate it on 21 July, it could have caused the technical failure of the explosives.[67] The scale of the investigation was immense. More than 12,500 statements were taken by the Police in relation to the 07 July attacks; 26,000 pieces of evidence were catalogued, 5,000 of which required forensic examination; 142 computers were seized as evidence, and the amount of CCTV footage which required examination exceeded 6,000 hours (Parliament, 2006a:para.74).

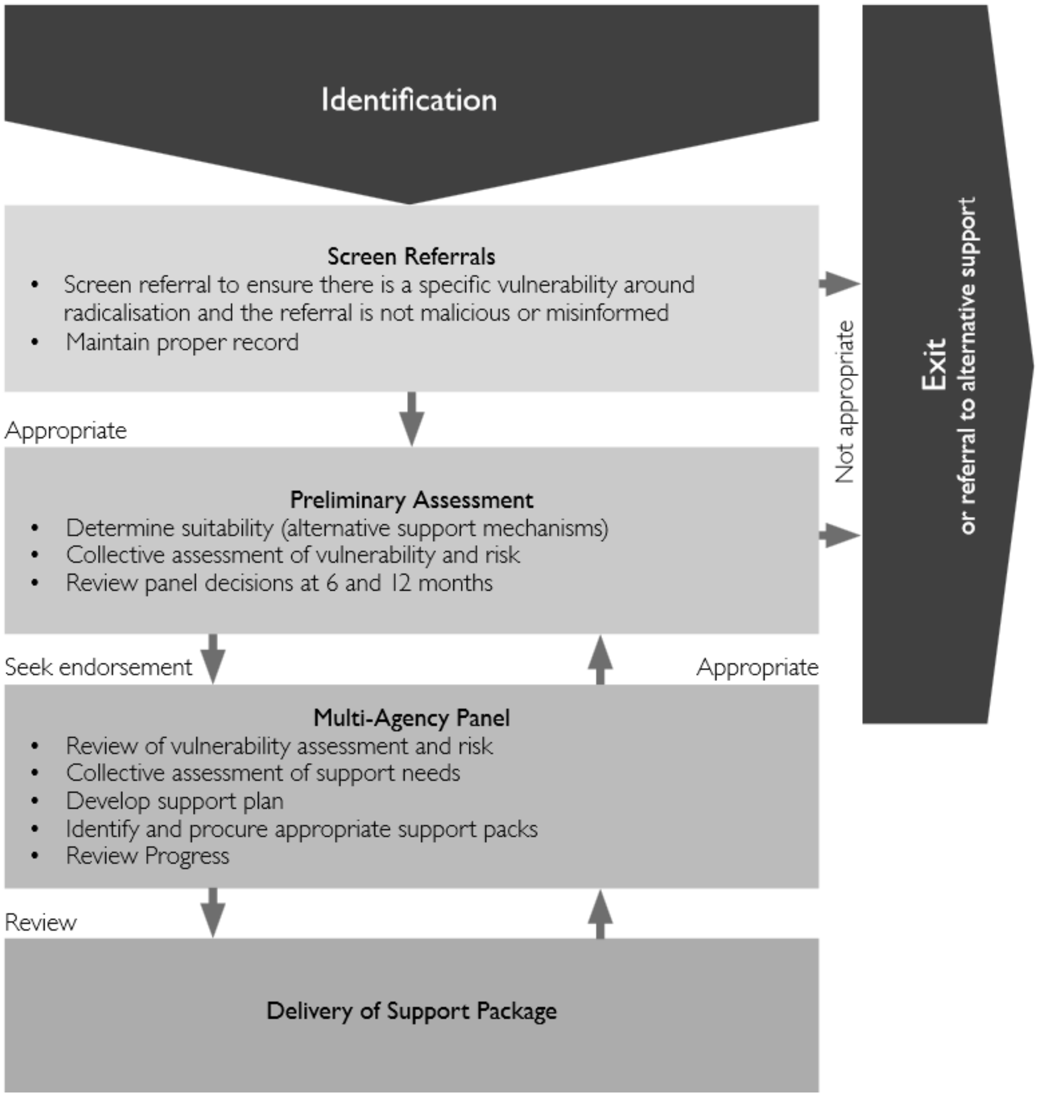
The case studies described above are valuable in helping to understand the path which a radicalised person can take, and how that path can ultimately lead to the person participating in a terrorist attack. Radicalisation is not something which only works for terrorist groups, it is also used across the extremist spectrum from single-issue causes (such as animal rights or anti-abortion activists) to political groups, including both left-wing and right-wing

[66] Comments made to the author by a former government official familiar with the case, who wishes to remain anonymous.

[67] Sublimation occurs when a solid converts into a gas without first passing through the liquid stage. It can affect homemade explosives, rendering them highly unstable or rendering them inert.

extremists. The academic study of radicalisation is key to arriving at a clearer understanding of how terrorist groups groom and recruit individuals and some work is already being done in this area (Baker-Beall, 2015). Developing a clearer appreciation of the factors and processes of radicalisation will contribute to a fuller picture on how to prevent it taking place, which lies at the core of the PREVENT strand.

The UK government funds programmes which work to counter the threat of radicalisation, such as the Islam Citizenship Education Project (ICEP), and the CHANNEL project. The approach of ICEP is to provide an Islamic-centred framework which teaches the values and concepts of citizenship, through a series of 44 lessons, all of which have been discussed with the assistance of the Muslim community in the UK (ICEP 2012). The CHANNEL programme was singled out in the June 2011 report as an initiative which has enjoyed successful results (Carlile, 2011:9). CHANNEL is a multi-agency project funded by the OSCT and works as a multi-agency initiative designed to identify and support vulnerable people at risk of radicalisation (Peters, 2012:3). The CHANNEL programme is composed of three stages of process. A diagrammatic model showing the CHANNEL process is shown below (Peters, 2012:15):

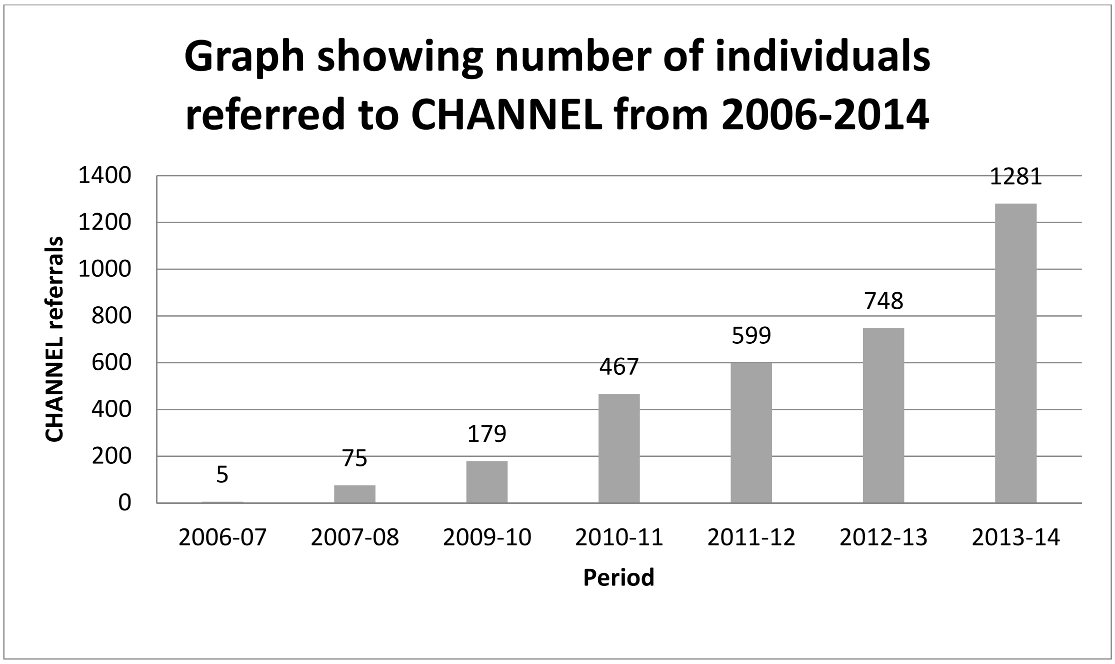

Identification
Screen Referrals
• Screen referral to ensure there is a specific vulnerability around radicalisation and the referral is not malicious or misinformed
• Maintain proper record
Appropriate
Not appropriate
Exit
or referral to alternative support
Preliminary Assessment
• Determine suitability (alternative support mechanisms)
• Collective assessment of vulnerability and risk
• Review panel decisions at 6 and 12 months
Seek endorsement
Appropriate
Multi-Agency Panel
• Review of vulnerability assessment and risk
• Collective assessment of support needs
• Develop support plan
• Identify and procure appropriate support packs
• Review Progress
Review
Delivery of Support Package

9 The CHANNEL process (Peters, 2012:15)

The first stage is the identification of a person or persons vulnerable to radicalisation. This will usually raise the concern that an individual is exhibiting behaviour which leads to believe that s/he is either susceptible to radicalisation, or is closely identifying with radical or extremist ideology. The next step is to conduct a joint risk assessment of the case and to identify the factors/issues of concern which need addressing. Finally there is referral and support, during which a bespoke programme of support measures and intervention will be developed and implemented, with regular reviews of progress. This will provide the necessary assistance to an at-risk person, in order to counter the radicalising influences they are being subjected to. Options which the CHANNEL guidance may suggest as suitable include counselling, faith guidance, civic engagement, support networks and finally the more mainstream services, such as health, housing, education, social services and employment.

A wide range of partners work together in the CHANNEL area, some are statutory partners mandated to be involved, while others become involved as required. Statutory partners include social services, the education sector, children's services, youth services and the various offender management services, such as the Probation Service. Non-statutory partners come from a wider social and governmental landscape and can include the Police service, UK Border Force, Housing, Her Majesty's Prison Service, Youth Offending Services and local authority elements such as the role of "PREVENT Lead". Joining the local and central government bodies are a range of other institutions such as charities, non-governmental organisations (NGOs) and welfare groups. Community policing is a key tool in preventing the radicalisation of young and/or vulnerable individuals, and the willing provision of information by the local community is an underpinning part of such policing.

In the pilot year of 2006 there were just 5 referrals to CHANNEL but by the reporting year of 2013-14, this had increased to 1,281 (ACPO, 2014). The youngest referral to CHANNEL was of primary school age (Ilston, 2014). The following graph shows the number of referrals to the CHANNEL programme from its inception in 2006 to 2014 (the year 2008-20009 is missing as ACPO do not provide any data for this period).



10 Graph showing number of individuals referred to CHANNEL from 2006-2014

Deploying the Intelligence cycle in support of tackling radicalisation is definitely feasible but the operational environment is wide-ranging, encompassing schools, faith groups, religious communities and prisons to name just a few. The difficulties in operating in an environment such as a prison are considerably more challenging than in operating in the wider community so although the model can be employed within this work-stream, the operational environment will have an impact on the effectiveness of the model's deployment, as the environment will produce constraints unique to each. That said, the cycle can still be employed on a target who is at risk of radicalisation, to establish a pattern of life, a circle of associates, meetings with persons of interest, etc., in just the same way as in other work-strands. Conducting the same cycle within the confines of a prison, however, would still follow the same stages but implementing it would be a task of a different magnitude.

4.3 PROTECT

4.3.1 Critical National Infrastructure

The PROTECT stream aims to decrease the UK's vulnerability to terrorist attacks, especially the vulnerability of the UK CNI, the transportation infrastructure, the national borders and those areas designated as crowded places, such as football stadiums. Much of the PROTECT stream takes place in conjunction with the work of the Security Service, especially the protection of the UK CNI. The CNI is defined as: "*those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends*" (CPNI, 2014).

IN the UK, the Centre for the Protection of National Infrastructure (CPNI) is the government body responsible for conducting the site surveys of designated critical facilities. It also provides advice and education to the public and private sectors on the risks to the CNI, and the measures which can be taken to mitigate these risks. The CNI programme encompasses nine distinct sectors constituting emergency services, communications, finance, the food supply chain, energy, the health sector, government, the national transportation network and the water infrastructure (CPNI, 2014).

In the last few years, an extensive programme of work has been conducted to increase the physical security of certain elements of the UK CNI, some of which are very visible. These security upgrades include measures such as heavy-duty, anti-ram barriers installed around the Houses of Parliament, which greatly increase the stand-off distance between a potential vehicle-borne improvised explosive device (VBIED) and the target. This stand-off distance is the primary defence against attack by an Improvised Explosive Device (IED). The over-pressure in a shock wave resulting from a high-order explosion decreases rapidly over two factors - time and distance. The more the distance can be increased between the target and the explosion, the greater the chance that a building will survive against an explosive attack, and the greater the chance that casualties and damage will be minimised.

The threat of explosive attack against buildings generates complex problems for both designers of new-build installations, and for officials responsible for counter-terrorism and critical incident planning. They must contend with multiple threats which include building collapse, flying debris, dust, pollution clouds resulting from destruction of, or damage to, the building infrastructure, secondary hazards caused by damage to utilities and services, such as electrical hazards, flooding, contamination and the ignition of ruptured gas supplies (Gedeon, 2003:pp.4.1–4.19). As the Intelligence agencies have increased their knowledge about how various IEDs are manufactured, this has led to a greater understanding of the potential and actual explosive effects resultant from these devices. This in turn has led to planners, designers and architects being able to design more security measures into a planned building or a piece of infrastructure. Transportation is an area where the Intelligence cycle has made solid contributions and where it works in a continuous iteration of gathering more inputs to be analysed in order to produce a more refined output. As our understanding of terrorist-based explosive devices increases, the ability to build in mitigation measures improves commensurately.

4.3.2 Transportation, Border Security and Crowded Places

Successful large-scale attacks against the public transportation sector have taken place in European cities including London and Madrid, while in the USA, sporting events have also been targeted for attack (FBI, 2010). The unsuccessful attempt in December 2009 by Umar Farouk Abdulmutallab to detonate explosives on board a passenger aircraft while on final approach to land at Detroit airport showed that mass transport remains a priority target for terrorist groups (Office of the Attorney General, 2015). In addition to directly targeting transportation systems, Al Qaeda groups have also employed a considerable degree of lateral thinking in their attempts to inflict large-scale casualties using transportation networks.

Less than a year after Abdulmutallab's failed attack, two IEDs were discovered on board cargo planes bound for the US. The information concerning the existence of the devices, both posted in Yemen, came from Saudi Intelligence. One device was discovered on an aircraft which landed in the UK at East Midlands Airport, while the other was discovered on board an aircraft which landed in Dubai (Hague, 2013). These two devices were expertly concealed as printer cartridges and had even been constructed in such a way that the cartridges would look internally authentic if subjected to X-ray examination (INTERPOL, 2010). The actual printer containing the explosive device at East Midlands was so expertly constructed that the Police and Home Office specialists looking for the device actually disassembled the printer, put it back together again and declared it clear of explosives. Following a second investigation of the printer some 5 hours later, the device was discovered. It transpired that the device had been inadvertently de-activated by the Police during the first inspection when the Printer cartridge was removed (BBC, 2010; INTERPOL, 2010).

Strong Intelligence co-operation between the Intelligence agencies of the UK, UAE and Saudi Arabia helped to ensure that the plot was uncovered, and that the devices were able to be made safe and forensically examined. In the same way that knowledge of IEDs is used to help enhance building design security, so the knowledge gained from the printer bomb plot was also used to strengthen procedures for examining parcels and mail coming from Yemen to the UK. It also resulted in a tightening up of security protocols for the cargo industry (Pistole, 2013).

A more ambitious plot targeting the UK transport sector was the "liquid bomb plot" of 2006. The operation to interdict this complex plot was called Operation OVERT and it culminated with the arrests of 24 people in August 2006, on suspicion of planning to blow up transatlantic passenger aircraft in mid-flight. The plot was centred on the use of the explosive substances TATP and

HMTD.[68] It required up to 18 suicide bombers boarding up to 10 transatlantic aircraft flying from the UK to cities in the U.S. and Canada, carrying with them the necessary equipment and chemical substances necessary to construct IEDs in mid-flight (CPS, 2010). The interdiction of this plot was the culmination of a massive, Intelligence-led operation involving multiple agencies and requiring a very complex framework of co-ordination. The scale of the investigation was similar to that conducted in the 21 July London bomb plot. The Metropolitan Police confirmed the following quantities of evidence seized as part of the investigation: "*26,000 exhibits collected; 102 property searches; 80 computers and other devices seized; 226 (computers) seized from inside internet cafes; 15,000 CDs; 500 Floppy disks; 14,000 Gigabytes of data*" (Casciani, 2009). The ringleader, Abdul Ahmed Ali, was convicted of conspiracy to murder, and was sentenced to life imprisonment with a minimum tariff of 40 years. The plot was described by the Security Service as: "*one of the largest UK-based terrorist plots*" ever (CPS, 2010).

The transport sector, mass-attendance events, the utility infrastructure and the offices of financial institutions are just some of the soft targets which are attractive to terrorist attack planning, and it is these types of target which the PROTECT strand has to encompass. Working together, the Security Service and the Police lead this strand, but local partnerships are also essential for this strand to be successful. Risk assessments cannot be done in isolation from the customers who also constitute terrorist targets. While the Counter-Terrorism Security Advisers (CTSA) from the Police are the primary officials who drive this process, they need a two-way engagement with the public and private sectors (Metropolitan Police Service, 2014). Risk assessments conducted by CTSAs, CPNI staff and others leads to risk management

[68] Triacetonetriperoxide (TATP) is an extremely powerful but unstable explosive. Until relatively recently, TATP was extremely difficult to detect but the requisite technology is now greatly improved compared to the capabilities it offered in 2006, when the London bombings occurred. TATP provides an advantage to terrorist groups over other types of improvised explosives, as it can be manufactured from relatively small amounts of materials which can be purchased without arousing suspicion. The most significant "marker" ingredient is hydrogen peroxide which raises suspicions if bought in sufficient quantity. Some groups have mitigated this problem by purchasing small amounts across a dispersed geography, to lessen any potential suspicion. The explosive power of TATP is assessed to be around 70-85% of the power of the commercial explosive TNT, traditionally used in commercial blasting in the UK. In this particular plot, it is most likely that hexamethylene triperoxide diamine (HMTD) would have been used to trigger the initial detonation which would then cause the TATP to explode.

recommendations. These include advice on vulnerability reduction and, business continuity structures and processes to enable organisations to remain functional in the post-attack phase. As an example of this, the Intelligence gained as a result of Abdulmutallib's failed Christmas Day airliner plot has led to major changes in airport security procedures in the UK and elsewhere, including the dedicated scanning of footwear (Heathrow Airport, 2006). The ratio of passengers being hand-screened was increased from one in four to one in two, a move widely unpopular with the aviation industry but one which the government felt necessary, given the Intelligence derived from the liquid bomb plot, the Christmas Day plot and others (BBC, 2006a).

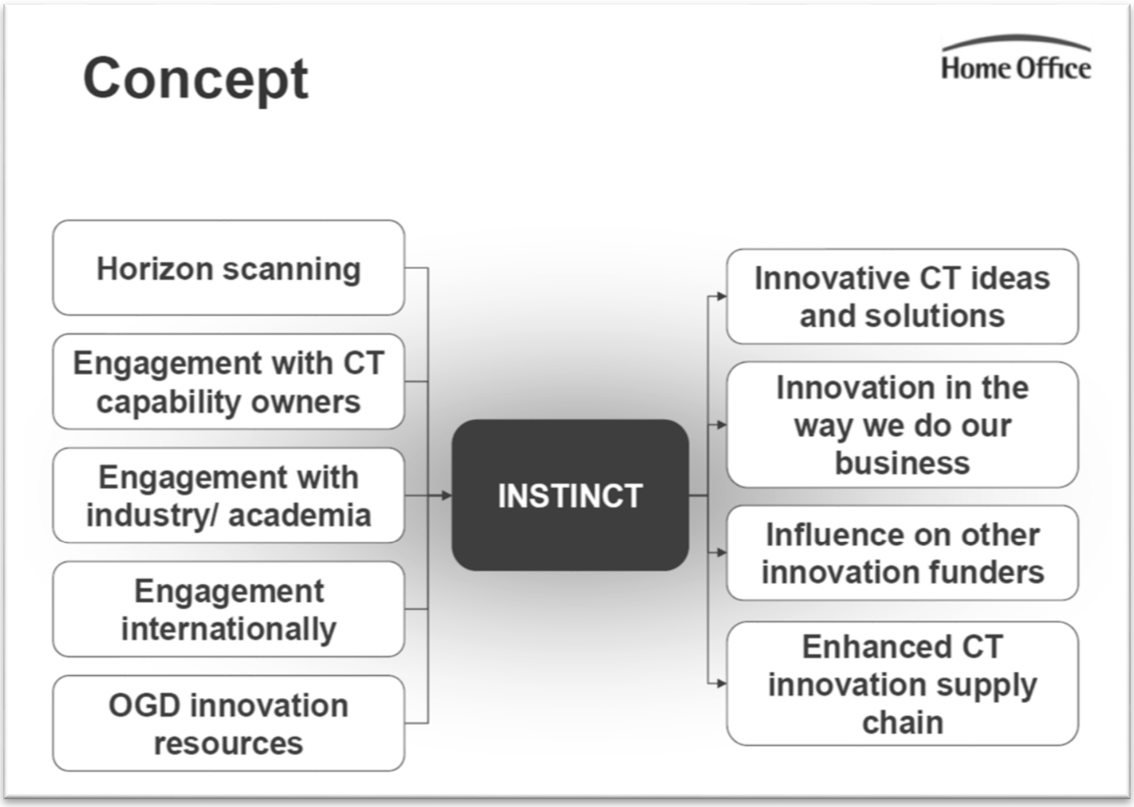
Many of the site surveys undertaken by the CPNI for specific installations or categories of facilities are conducted on a rolling basis, the frequency of which is not publicly disclosed. The terrorist threat is not static by nature, but is dynamic and continues to morph and to be refined. Terrorist groups exchange tactics, ideas and information with other terrorist groups, and also with organised crime syndicates and narcotics networks. In the same way that the UK Intelligence Agencies define their Intelligence requirements and collect against them, so terrorist groups also collect their own Intelligence, for strategic, long-term purposes, for operational requirements and for tactical use in planned attacks (Burke, 2011:pp.16–20; Burke, 2014).

One of the most intelligence-led areas of the whole CONTEST strategy is the operation to secure the UK borders. The provision of Advance Passenger Information (API) and Passenger Name Records (PNR) data generates a massive quantity of raw information which can prove extremely useful to agencies implementing the Intelligence cycle in their efforts to secure the borders (Hardy, 2014). Until 2013, the UK Border Agency (UKBA) had primacy in securing the country's borders and the Agency worked with the Security Service, the Police and the travel industry (UKBA, 2011). In 2012, a highly critical report was released by the Commons Home Affairs Committee which published very strong criticism of the UKBA's senior leadership in particular:

> "*We are astonished that the Agency provided this Committee, and its predecessors, with information that turned out to be patently wrong on so many occasions over the last six years. If it was not attempting to mislead the Committee then it must be a sign that senior officials had no idea as to what was actually going on in their organisation. We find it very hard to believe that no one within the Agency had any idea that checks were not being carried out as they should have been and we expect the Agency to share the findings of its disciplinary investigation with us as soon as it is completed*" (Home Affairs Committee, 2012:39).

After the report was published, the Home Secretary announced the abolition of the UKBA. The core work of the agency was returned to the Home Office, under the UK Visas and Immigration department, while a new agency, the UK Border Force (UKBF), adopted the immigration enforcement responsibilities of the defunct UKBA. One legacy from the UKBA was the opening in 2010 of the National Border Targeting Centre (NBTC), which also contains the Rules-Based Targeting Team. The aim of the NBTC is to act as a central focus for analysing information related to both goods and passengers (Hardy, 2014). It also receives data from the UK e-Borders system. A variety of analytical techniques are used to sift the data provided by these systems and these are combined with watch-lists and no-fly lists primarily from the UK, the EU and the U.S. to proactively enhance the security of UK borders. The e-Borders initiative is designed to "*deliver timely data, information, intelligence and risk assessments to relevant government agencies on all passengers seeking to enter or leave the UK*"(Home Office, 2005:3).

The threat of terrorist attack against crowded places has increased in importance in the last decade. Cutting-edge technology is currently being tried and tested to assist in securing crowded places, with a government initiative called INSTINCT leading the way. INSTINCT stands for Innovative Science and Technology in Counter-Terrorism and is a cross-governmental initiative aimed at identifying and developing new and/or emerging technologies which can assist in the fight against terrorism (OSCT, 2011b). In 2010, a technology demonstrator for INSTINCT was employed by the Home Office under the auspices of the Office for Security Counter Terrorism to highlight the issues surrounding the vulnerability and securing of crowded places and mass-attendance events. It has reportedly been responsible for establishing new standards in the collaborative efforts between the private sector and government, in the area of counter-terrorism. The diagram below shows the concept of INSTINCT, as conceived by the Home Office (OSCT, 2011b).



Concept

Home Office

Horizon scanning

Engagement with CT capability owners

Engagement with industry/ academia

Engagement internationally

OGD innovation resources

INSTINCT

Innovative CT ideas and solutions

Innovation in the way we do our business

Influence on other innovation funders

Enhanced CT innovation supply chain

11 The INSTINCT concept

Attacks on crowded places are a favoured terrorist target as they inflict mass casualties, generate instant media coverage and perhaps more importantly for the attackers, ensure that the terrorist agenda endures in mainstream media reporting. Crowded places have featured as targets in several high-profile, UK-based terrorist plots in recent years. The following case studies cover two of the more ambitious plots in recent years, to launch terrorist attacks against crowded places and to create mass casualties. The disruption of both operations were fully Intelligence-led and required the utilisation of enormous resources from the Intelligence agencies and the Police, to interdict the cells and to secure the convictions of those involved (Source_08 2011). These case studies also demonstrate the scale, complexity and potential lethality of two of these plots, and highlight the importance of the Intelligence cycle in disrupting plots such as these. As an indication, Operation CREVICE required

79,000 man-hours solely dedicated to surveillance, technical monitoring and transcription by the Intelligence agencies (Security Service, n.d:para.13). The Head of Counter-Terrorism Command (CTC) described it as a landmark case, in terms of the resources deployed (Clarke, 2007).

The collaboration between the Saudi and British Intelligence agencies was a prime factor in the successful disruption of the “printer bomb” attack. In this case, it was a foreign Intelligence agency which produced the vital information and without bilateral and multilateral agreements in place, disruptions such as this would be far less probable. The dismantling of the UK Border Force illustrates the fact that even government agencies do not always follow best practice and that without effective leadership and management, processes will not be followed correctly and organisational structures will grow lax. While the NBTC was a step in the right direction, it was too little, too late.

4.3.3 Operation CREVICE – 2004

In March 2004, the Metropolitan Police conducted a series of raids in the UK under the auspices of an ongoing operation, OP CREVICE, which aimed to disrupt an Al Qa’eda-linked terrorist cell in the UK. The cell was plotting to detonate explosives manufactured with ammonium nitrate fertiliser (Hallett, 2011), a technique previously favoured by the Irish Republican Army. The cell was led by Omar Khyam, who at the start of the operation was believed to be involved in providing solely logistical support and facilitation to the Al Qa’eda network, and was not considered to be actively involved in attack planning. Four of the core members of the group were from Pakistani backgrounds and had initially come together over their mutual disillusionment with what they saw as the lack of progress in the Kashmir campaign. All four visited Pakistan and gave their assistance to various Pakistani-led jihadist groups operating in the Kashmir area, as well as to some groups planning operations in Afghanistan. Frustrated at not being able to actively participate in operations there, they decided to target the UK instead. At least Khayam and Ahmed had frequent meetings with members of Al Muhajiroun (the radical Islamic organisation subsequently proscribed under UK law in 2010) (Straw, 2010:1–2).

As early as February 2003, some of the group had begun to discuss the possibility of attacking targets within the UK. Khyam organised a dedicated training camp for the group, which was carried out in secret inside Pakistan in July 2003. The group learned basic skills such as small arms training, and they also received some instruction in explosives (Summers & Casciani, 2007). The culmination of their training was the test detonation of an IED containing around 1.5 kilograms of ammonium nitrate fertiliser, an ingredient frequently used to construct IEDs (U.S. Attorney, 2010). Having successfully demonstrated the capability of the explosive, the group returned to the UK. Garcia purchased a large quantity of ammonium nitrate fertiliser and placed it in a storage facility in West London, in November 2003 (Metropolitan Police Service, 2007). The quantity of fertiliser purchased was 600 Kilograms, which was around a quarter of the amount used by Timothy McVeigh when he carried out the bomb attack in Oklahoma City, killing 168 people (FBI, 1995).

In February 2004, the Security Service gained new information that indicated Khyam and his cell were now actively planning a terrorist attack and he and the core members of the group were placed under more intensive surveillance. On 02 February, Khyam was observed in the company of Mohammed Siddique Khan and Shehzad Tanweer, who carried out the suicide attacks in London in July of the following year. The Police then received a tip-off that a suspiciously large quantity of fertiliser was being stored in London (CPS, 2007b). Following a visit to the storage facility, the fertiliser was identified as the ammonium nitrate variety. It was covertly switched for a similar but inert substance, and the storage facility was placed under surveillance. On 20 February 2004, Mohammed Khawaja arrived in the UK from Canada, where he met with Khyam to show him pictures of detonators constructed by Khawaja, and to discuss the manufacture of detonators in the UK for the group. This meeting was covertly monitored by the Security Service. The following day Khyam again met with Mohammed Siddique Khan and the two had a detailed conversation inside Khyam's car. This meeting was also covertly monitored, but at the time the Security Service were not aware that this was Khan who was present at the meeting. The two discussed a range of topics including attending terrorist training camps in Pakistan, equipment to take for participation in these camps, and details of a fraud scheme which Khyam offered to set up for Khan, to provide funds (BBC, 2007b).

The next day, Khyam discussed potential mass-casualty targets for their UK attack. One of these was the Ministry of Sound nightclub in London. Another was the Bluewater shopping complex, one of the largest in Europe. A third target discussed was the utility sector, where Khyam raised the possibility of getting sympathetic staff within the gas, electric and water companies to provide inside, technical information which would assist with their attack planning. Just over one week later, Khyam was trying to locate a number of CDs which contained technical data about the UK's high-pressure gas pipe network and the related hazardous plant details. The CDs had been stolen and provided to Khyam by a sympathiser working as a gas engineer (BBC, 2007b).

On 19 March, Khyam was recorded discussing a number of possible attack scenarios including a car bomb, a bomb attack against a Police station, and an attack against the Bluewater shopping complex (BBC, 2007b). At this stage, the Police had also been informed by the storage facility that the customer responsible for the fertiliser had notified the company that the storage would no longer be required from the end of March (CPS, 2005:sec.21.14 (iii)). This advancement of the attack planning, together with the new information from the storage facility, meant that the Police and the Security Service had no choice but to move in and arrest the cell, due to the need to ensure public safety (CPS, 2005).

On 29 March, Khawaja was detained in Ottawa by the Canadian RCMP and hours later, six individuals associated with the cell, including Khyam, were arrested in the UK. One more suspect was detained in Pakistan several days later, and eventually returned to the UK (CPS, 2005). Khawaja was sentenced to ten and a half years imprisonment in Canada, subsequently increased to life imprisonment on appeal (Zeldin, 2012). Five of the six members of the British cell were convicted in the UK of terrorist offences and sentenced to life imprisonment (CPS, 2007b).

The description of the Operation CREVICE case, however, provides an excellent example of how the Intelligence cycle can be used to successfully disrupt an advanced terrorist plan to conduct mass casualties. The covert surveillance operation, for example, would have generated a regular stream of Intelligence which would have gradually built up the picture of activities conducted by the group, and would also have resulted in the collection of evidence to be used in the prosecution, once the arrests were made.

4.3.4 Operation RHYME - 2006

Dhiren Barot was a convert to Islam who constructed extremely detailed and sophisticated attack plans for senior Al Qa'eda figures. Having left London to fight as a jihadist in Kashmir around 1995, he wrote a book in 1999 entitled "*The Army of Medinah in Kashmir*" using the pseudonym Esa al Hindi. The book detailed his experiences in this conflict, although most of it portrayed his frustration at what he considered to be an ineffective and almost farcical war. Barot wrote that "*terror works, and that is why the believers are commanded to enforce it by Allah*" (Hindi, 1999:107–108).[69] The book was commissioned by Moazzem Begg, owner of the Islamic bookshop Maktabah al Ansar, in

[69] Barot's book, published under his pen-name Esa al Hindi, was previously downloaded for other terrorism-related research, at http://www.streetdawah.com/books/Kashmir.pdf sometime in 2009.

Birmingham, who was subsequently arrested in Pakistan and detained in U.S. custody in Guantanamo Bay.[70]

Barot compiled a list of what he considered to be the best targets to attack for the creation of mass casualties and the instilling of fear and panic among the population of the UK. One plot centred on the use of stretch limousines filled with propane gas canisters and explosives, which would be parked in underground car parks. The vehicle bombs would then be detonated with the aim of collapsing several major buildings and killing as many people as possible (Barot, n.d.). Another of Barot's plots was to detonate a large bomb underneath London's River Thames to cause a massive flooding of the London Underground network, again with the aim of causing as many casualties as possible (Barot, n.d.:36). Another of his plans included the hijacking of a petrol tanker to be used as a mobile bomb. This would be crashed into a large public building, with the aim of collapsing the building onto others (Metropolitan Police Service, 2006).[71] Barot also researched the potential use of a "dirty bomb" (Barot, n.d.). In addition to targets in the UK, he conducted detailed attack planning on targets within the US. These included financial institutions such as the New York Stock Exchange and various financial headquarters including those of Citigroup bank, the International Monetary Fund and the World Bank (U.S. District Court, 2007).

He was placed under surveillance by UK authorities on 15 June 2004 and displayed a very high degree of surveillance awareness. A senior counter-terrorism officer described Barot as "*probably the most difficult individual to keep under surveillance that we have had in recent times*" (The Guardian, 2006). To facilitate his planning work and to assist with the necessary

[70] Begg's Birmingham bookshop was raided by Police in 2000, under the authorisation of an anti-terrorism warrant. Begg's detention in Guantanamo Bay came after he was arrested in Pakistan on suspicion of terrorism offences. He was released without charge, following the intervention of the UK authorities and he subsequently sued the UK government for their alleged complicity in the case, which was settled out of court.

[71] A detailed summary of the attack plans, including reproductions of some of the trial material, such as recordings of the suspects, copies of their notebooks, sketches etc. were provided on a Metropolitan Police webpage, at http://www.met.police.uk/pressbureau/rhyme/index.htm accessed in February 2010, subsequently removed. A summary of the case was later posted at http://content.met.police.uk/News/Terrorist-jailed-for-life-for-conspiracy-to-murder-in-the-UK-and-US/1260267887712/1257246745756 accessed on 05 August 2014.

logistics, Barot constructed a small cell of at least six people. In addition to their logistical assistance, Barot also utilised their particular skill-sets to enhance his attack planning (BBC, 2007d). Mohammed Naveed Bhatti, an engineering graduate, assisted by researching the effects of explosives, while Zia Ul Haq, an architect, used his knowledge to work out the best way to engineer the collapse of a building (BBC, 2007b). Crown prosecutors detailed how Barot had already evaded his surveillance team and his whereabouts were unknown to the authorities, when his attack plans were discovered on a laptop seized by Pakistani Police during a counter-terrorism raid in Gujarat in 2004 (Sturcke, 2006). Writing of his plan to use gas bottles as improvised explosives in limousines, Barot envisaged the explosion piercing a London Underground tunnel under the river Thames: "*imagine the chaos that would be caused if a powerful explosion were to rip through here and actually rupture the river itself. This would cause pandemonium, what with the explosions, flooding, drowning, etc. that would occur/result*" (Barot, n.d:36).

Despite the fact that there was virtually no admissible evidence with which to secure a conviction, the Police were forced to take the decision that Barot would have to be arrested as soon as he was identified again, due to the significant risk to public safety which his plans posed. A counter-terrorism officer noted that ”*It was always possible that Barot could have been alerted to what happened in Pakistan, and since we did not know how far advanced his attack plans actually were, the decision was made to arrest him as soon as he was next seen*” (The Guardian, 2006).

He was successfully identified by surveillance officers on 01 August and two days later he was arrested. His co-conspirators were also arrested in the UK in simultaneous Police raids (BBC, 2006a). Barot and others were also indicted in the U.S. on several counts of terrorism-related charges. These included plotting to attack targets within the US, and in Barot’s case, being a lead instructor at a jihadist training camp in Afghanistan around 1998 (U.S. District Court, 2007). Due to the custody laws in the UK, Barot could only be held for a maximum of 14 days, at which time he would either have to be charged, or released. The work required by the authorities to produce sufficient evidence to charge and convict Barot and his team was the most complex investigation which Scotland Yard had carried out to date (The Guardian, 2006). Almost 300 computers were seized and forensically examined, along with more than 1,800 items of removable media, all of which required forensic examination in addition to the computers. Over 4,000 individual garages and lock-ups were visited by Police in the course of the subsequent investigation, and more than 600 sets of physical keys had to be examined in conjunction with the garages and lock-ups (Metropolitan Police Service, 2006b). Despite these challenges, sufficient evidence was produced within the 14-day period that, when Barot was confronted with the charges against him, he pleaded guilty (CPS, 2006:1). He was sentenced in a UK court to 40 years imprisonment for conspiracy to murder, but this was subsequently reduced to 30 years on appeal. Six of Barot’s cell also received lengthy custodial sentences, ranging from 15 to 26 years, for conspiracy to murder (CPS, 2007b).

The decision to move in and arrest Barot highlights a point made previously, that there are occasions when the Police have no option but to arrest, even though they may lack sufficient evidence to bring a prosecution. The Intelligence cycle had been in action for some time when the advanced nature of Barot’s plans was revealed. As in the case of Operation CREVICE, the material collected would have increased the detailed understanding of the Intelligence agencies, regarding the nature of the threat and the movements of the key individuals. These updates would have been analysed and evaluated, and interim reporting issued, to provide an all-informed, “single version of the truth” for each of the partner agencies. Following on from dissemination, the collection plan would either continue or would be refined, to provide increasingly effective and targeted collection of raw material. The cases of Operation CREVICE, RHYME, PRALINE and others provide solid evidence that the Intelligence cycle works effectively, in theory, and in practice, to support counter-terrorism work in the UK. Like all models requiring the use of people, the cycle can, and does, suffer from human factors, but when used correctly, the model allows a terrorist target to be collected against in a systematic and effective way, resulting in a gradual construction of a more complete Intelligence picture.

4.4 PREPARE

The PREPARE strand of the CONTEST strategy concentrates on resiliency, mitigation and business continuity, while an attack is ongoing, and afterwards in the post-attack recovery phase. Once an attack is underway, the PREPARE strand aims to help the authorities to end the attack as safely and quickly as possible. A key requirement for this strand to function effectively is interoperability, especially among the groups of emergency services who are most likely to be in attendance at the scene. They must be able to communicate among themselves, have the ability to send situation reports up the chain of command and receive additional direction coming downwards. The ability of the Police to respond to a terrorist attack with the appropriate level of armed response is another key factor within the Prepare strand (Home Office, 2011:92–103). Earlier in this chapter, a summary of the UK's CNI was provided as part of the PROTECT strand. The UK's CNI estate includes many high-profile terrorist targets, some of which have wider public safety implications in the event of a terrorist attack against them. Examples of such facilities include nuclear power sites, utilities such as the water supply and the ability for the National Grid to deliver electricity as needed (CPNI, 2014).

4.4.1 The CBRN Threat

The government's ability to develop and maintain resilience includes Chemical, Biological, Radiological and Nuclear (CBRN) protective measures.

It is not only the physical sites of related installations which pose the potential for a terrorist attack. The actual attack itself could involve the use of weapons such as chemical or biological agents, radiological material or at the extreme end of the threat spectrum, a nuclear device. The threat of a CBRN attack is considered one of the four highest priority risks in the UK's National Security Strategy (Cameron 2010, pp.11,27–28).

Chemical weapons have been used before in terrorist attacks. The nerve gas attacks in Japan in 1994 and 1995 demonstrated how such an attack could rapidly overwhelm the abilities of the emergency services to respond to it. In the 1995 attack against the Tokyo subway system, 12 people were killed by the gas but more than 5,000 people required medical treatment, which the available medical staff and facilities simply could not cope with (Seto, 2001:1–4). The threat from radiological attack was also highlighted in the same year as the Tokyo gas attack. In 1995 and 1996, the Chechen Islamist rebel leader Shamil Basayev publicly threatened to use radiological dispersal devices (RDD) packed with explosives to target Russian facilities. Basayev's group showed containers of radioactive materials to journalists. The containers were assessed to contain either Cobalt-60, Cesium-137 or Strontium-90, the most likely candidate being Cesium-137 (Burke, 2006:39–41). Basayev's group also contacted Russian media in November 1995, describing the location in which they had hidden a canister of radiological material, buried in Izmailovskiy Park in Moscow. The TV station sent a film crew to locate the canister, after which they contacted the authorities and the material was removed. The canister contained around 33 pounds of Cesium-137, a material which is a by-product of nuclear fission. This incident was aimed at displaying that Basayev's group was serious in both their capability and their intent (Bale, 2004).[72] Al Qaeda has previously expressed its intention to construct an RDD. A declassified CIA report (2003:1-2) stated that:

[72] In Intelligence terms, capability and intent are separate characteristics. A useful definition of each is that provided by the U.S. Department of Defense (DoD), which defines capability as "*the ability to execute a specific course of action*" and intent as "*an aim or design to execute a specified course of action*" (Gortney, 2014).

> *"Al Qaeda is interested in radiological dispersal devices (RDDs) or "dirty bombs". Construction of an RDD is well within its capabilities as radiological materials are relatively easy to acquire from industrial or medical sources".*

Biological weapons have a long history of use, and were used at least as early as 2,500 years ago (Mayor, 2009:3–5). In 2001, less than two weeks after the Al Qa'eda attacks of 11 September, several letters containing anthrax spores were sent to U.S. politicians and media organisations. Five people died from anthrax poisoning contracted from the letters and a further 22 required medical treatment (Heinrich, 2003:1–3). The threat of a nuclear device being constructed and detonated by a terrorist group is clearly within the high impact but low likelihood quadrant of the risk spectrum, but it is a threat taken very seriously by the UK authorities, and is classed as a "Tier Two" risk (Cameron, 2010:27). The collection of Intelligence against the CBRN threat from Al Qa'eda and other groups remains a very high priority for the UK's intelligence agencies. The dangers of nuclear proliferation have been aptly demonstrated by the activities of the Pakistani scientists A.Q. Khan, who created an illicit supply chain for the clandestine programmes of Libya and other countries to design nuclear weapons (Butler, 2004:17–21;26–27). A former director of the FBI summarised the threat as follows:

> "*The economics of supply and demand dictate that someone, somewhere, will provide nuclear material to the highest bidder, and that material will end up in the hands of terrorists. Al Qaeda has demonstrated a clear intent to acquire weapons of mass destruction. In 1993, Osama bin Laden*

> *attempted to buy uranium from a source in the Sudan. He has stated that it is Al Qaeda's duty to acquire weapons of mass destruction. And he has made repeated recruiting pitches for experts in chemistry, physics, and explosives to join his terrorist movement*" (Mueller, 2007).

Thankfully the threat of a CBRN device remains a theoretical but possible threat for the UK authorities, but there is a clear intent by groups such as AQ to acquire this technology. It is difficult to assess the effectiveness of the Intelligence cycle in dealing with this threat, as the CBRN threat is a more highly classified topic than other terrorist threats such as the use of suicide bombers.[73] The fact that this is classed as a Tier 2 risk means that considerable Intelligence efforts will be targeted against this risk, and that any indication of an increase in likelihood of this threats being manifest would result in a major uplift of Intelligence effort, given the potential risk of mass casualties and environmental destruction.

4.4.2 Interoperability

A number of scenarios have also considerably influenced the PREPARE strand of the 2011 CONTEST strategy. Two of these were domestic incidents in the UK, and one was an overseas incident. The first was not a terrorist incident but a fire at King's Cross Underground station in London in 1985, which killed 31 people. The fire was accidentally started by a carelessly discarded match on a wooden escalator and it spread rapidly, killing 31 people. The inability of the emergency services to communicate among

[73] The Butler Report (2004) is probably the most informative document in this niche area, particularly the sections describing the A.Q. Khan network, and the WMD programmes of Iran, North Korea, Libya and Iraq, along with Usama bin Laden's efforts to acquire such technology for his organisation.

themselves and with other command elements was highlighted as a key factor in dealing with the incident. In the final report of the government's inquiry into the incident, the inquiry's Chairman, Desmond Fennell OBE QC (1989:137) noted in particular that:

> "*Staff at stations on London Underground have not been provided with radio equipment because current portable radios will only operate below ground if there is a continuous aerial system throughout the station. The only means of communication for staff at King's Cross on 18 November 1987 was the telephone or word of mouth. Members of the British Transport Police and the London Fire Brigade at the scene had their own personal radios, but they did not work between the surface and underground. Officers below ground within the station could not communicate by radio either unless within line of sight*". [74]

The concept of interoperability has always been firmly embraced by the UK's Armed Forces, and most operations nowadays are conducted in a fully tri-service framework. For this reason, training for joint operations is a staple of all UK military exercises and the ability for all elements to communicate among themselves is of paramount importance. The emergency services in the UK have not traditionally had the luxury of such dedicated training. They deal with real-time incidents on a daily basis, unlike the Armed Forces who are primarily training for war on a regular basis. Since 2001 the Armed Forces

[74] One of the most serious factors which impeded the rescue, evacuation and fire-fighting operation underground was the lack of a suitable communication system, enabling the emergency services to communicate with each other below ground, even if they were not in direct line of sight. Perhaps more importantly, this also prevented the fire-fighters and Police officers below ground to communicate with the command elements above ground, except by fixed landline telephone.

of the UK have been involved in almost continuous, large-scale, joint operations in Iraq and Afghanistan. One of the most important foundations of the UK's joint military training is the establishment and maintaining of communications. Without the ability to give and receive orders and situation reports, the Armed Forces cannot function effectively. The emergency services have traditionally lagged behind their military counterparts in this regard. A practitioner with experience in both the UK Police and the UK Armed Forces explained why this capability gap exists:

> "*In the military, we trained every day for a war that might never come. As a Police Officer, I was faced with real incidents every single day I walked the beat. I never knew what was coming next, from helping a lost tourist with directions, to attending a murder scene. That's the difference between the two jobs – one of them, you spend every day training for something you rarely have to do, and the other you do a fairly short training course, and then you're in the thick of it from then on*" (Source_14, 2011).

The PREPARE strand in the 2011 edition of the CONTEST strategy recognises this need and it paves the way for a four-year plan to enhance the government's response capabilities in four areas: building capabilities to respond to and recover from terrorist incidents and other emergencies; to improve general preparedness for highest-impact risks; to improve the ability of emergency services to collaborate when dealing with the aftermath of a terrorist attack; to the enhance communications capabilities and information-sharing capacity, when dealing with a terrorist attacks (Home Office, 2011:93–94).

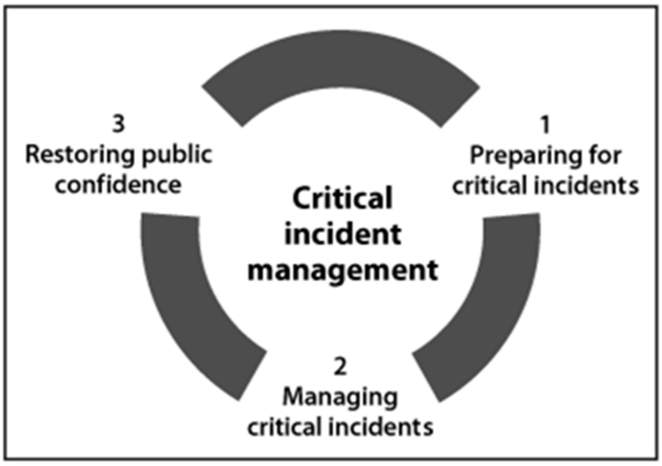
The second incident was the terrorist attacks against the London transport network in July 2005, and it was exactly the kind of incident that the PREPARE strand aims to deal with more effectively. It was a complex attack, using multiple assailants to hit different, geographically dispersed targets. The first three attacks were near-simultaneous, all causing multiple fatalities plus additional casualties. In a similar way to the communications issues encountered by the emergency services during the King's Cross fire the year before, there were communications issues which hampered the initial deployment of emergency services, and which compounded the problems they faced. These suicide attacks resulted in 52 fatalities and several hundred injured (Hallett, 2011:1).

In the first few minutes after the initial explosions took place, the overall picture was confusing for the authorities, which is to be expected in any similar incident. The Coroner's report highlighted the immediate need for answers to two questions: what had occurred, and where. It then explained the three main factors that caused difficulties in providing answers to these two questions. The first issue was that three of the explosions occurred inside the London Underground tunnels, so the explosions in such a confined space resulted in few eyewitnesses. The second issue was the lack of communications available. The third was that the available communications systems were overwhelmed by calls in the immediate aftermath of the explosions (Hallett, 2011:27–28).

Once again, communications had proved to be a weak link in the post-incident capabilities of the emergency services to respond accordingly. As the purpose of PREPARE is "*to mitigate the impact of a terrorist incident where it cannot be stopped*", it is understandable why this strand places such emphasis on the communications aspect of the response portfolio (May, 2011:94). The degree of collaboration and cooperation between agencies is also a central factor in ensuring that the PREPARE strand is as effective as possible. In this regard, the ISC were very clear in their perception of the role which inter-agency collaboration has to play. They voiced their desire to see this collaboration strengthen and improve, in the recommendations of their report which was placed in the context of international terrorism being countered (Murphy, 2006:44). This desire to see even stronger collaboration is addressed by the PREVENT strand (Home Office 2011, pp.100–101).

It is not only the following of procedures which is important in the immediate post-attack phase. For mitigation to be effective, it is vital that all those involved understand the procedures, that they are familiar with them, and that they are carried out properly. The testing and exercising of such SOPs is a component part of PREPARE. In real terms this translates into a range of exercises - from tactical training on the ground for the emergency services and associated departments to practice their responses to a terrorist incident, through to Cabinet Ministers being tested with table-top planning and simulation exercises.

Terrorist incidents such as the 2005 London bombings require the involvement of a large number of stakeholders and a significant number of actual staff deployed on the ground. The regular training of such staff, from a Police Constable to a Cabinet Minister, is essential in order to translate plans, SOPs and contingencies into actual behaviours that are carried out when an attack takes place. In addition to dealing with the actual incident, the Police (and by extension, the government of the day) also have to consider the impact of an incident upon the public's confidence. The Metropolitan Police Service's definition of a critical incident is "*any incident where the effectiveness of the police response is likely to have a significant impact on the confidence of the victim, their family and/or the community*" (NPIA, 2011:6). A simplified diagram of the critical incident model used by the UK Police is provided below (College of Policing, 2013).

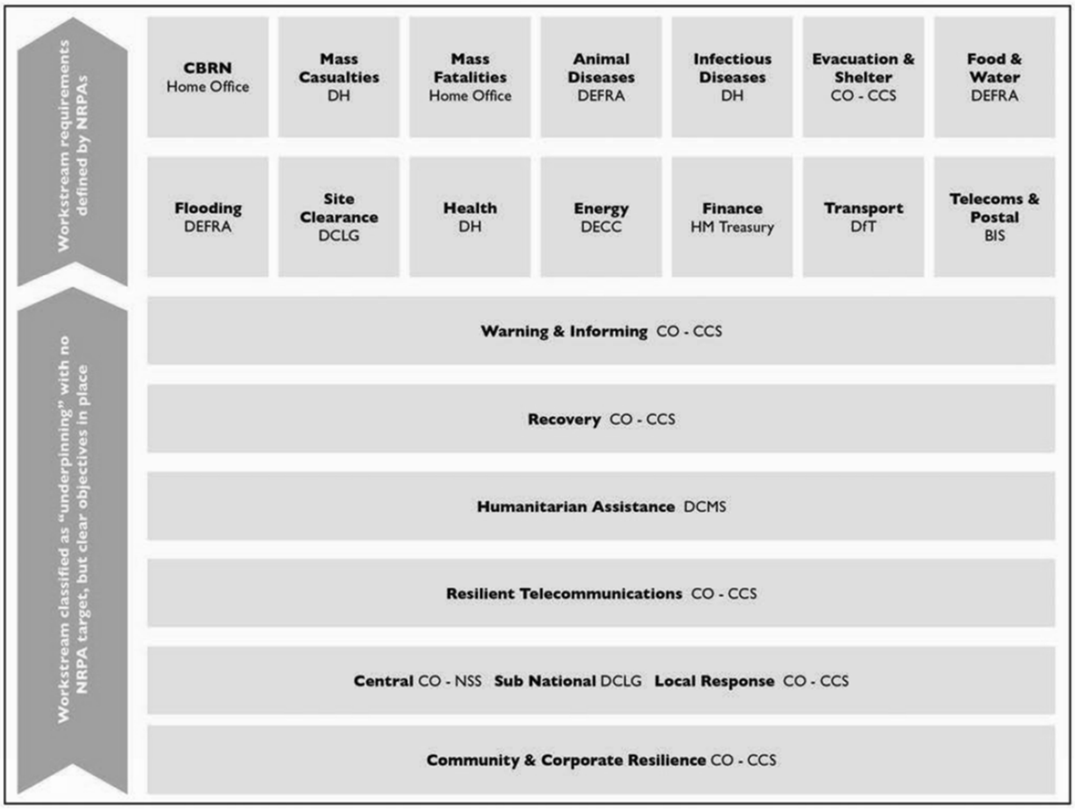

3
Restoring public confidence
Critical incident management
1
Preparing for critical incidents
2
Managing critical incidents

12 Three phases of Critical Incident Management (College of Policing, 2013)

The preparation phase includes several requirements. Staff must have had the appropriate training to deal with a critical incident and there must be sufficient resources available to manage the incident. Managing a critical incident includes the correct and early identification of an incident as being critical. It also requires that appropriately senior officers are informed of the incident as early as possible, to enable the command chain to respond with the appropriate level of authority, and to manage the incident effectively. The third phase is a very important one in terms of the relationship between the Police and the community. Restoring public confidence was a major requirement for the Police in the wake of the murder of Stephen Lawrence, and was identified as such by Lord Macpherson in his findings (1999:sec.45:12; 46:35; 58). Restoring public confidence involves regular Police engagement with the community and confidence-building measures. It may require victim support or victim care measures to be taken. The interaction with the media is also of key importance as this has a direct impact upon the public’s perception of a case or incident. When trust between the Police and the community breaks down, it can require a public inquiry such as the Macpherson enquiry to rebuild it (NPIA, 2011:69).

At the tactical and operational levels, drills and simulation exercises are crucial to mitigate the impact of an attack. At the strategic level, one of the most important aspects of the mitigation plan is the prior identification of responsibilities and roles for the various aspects of the Prepare strand. Within the UK's National Security Strategy, the UK Resilience Capabilities Programme has mapped out these responsibilities across 22 distinct work streams in a horizontal and vertical matrix, called the National Resilience Planning Assumptions (NRPA).

The NRPA provides roles and responsibilities for events such as a CBRN incident, in which the Home Office are assigned primacy, and a mass-evacuation event, in which the Cabinet Office's Civil Contingencies Secretariat (CCS) would take the lead (May, 2013:31). The prior identification of ministries and departments who would take the lead is a major step forward in reducing the duration of the initial paralysis which almost always occurs immediately after the start of a terrorist attack. The matrix of these workflows of the UK Resilience Capabilities is shown below (Home Office, 2011:95):



Workstream requirements defined by NRPAs

CBRN Home Office
Mass Casualties DH
Mass Fatalities Home Office
Animal Diseases DEFRA
Infectious Diseases DH
Evacuation & Shelter CO - CCS
Food & Water DEFRA

Flooding DEFRA
Site Clearance DCLG
Health DH
Energy DECC
Finance HM Treasury
Transport DfT
Telecoms & Postal BIS

Workstream classified as "underpinning" with no NRPA target, but clear objectives in place

Warning & Informing CO - CCS

Recovery CO - CCS

Humanitarian Assistance DCMS

Resilient Telecommunications CO - CCS

Central CO - NSS Sub National DCLG Local Response CO - CCS

Community & Corporate Resilience CO - CCS

NRPA: National Resilience Planning Assumptions

13 Workstreams of the UK Resilience Capabilities Programme

The third incident which played a major role in the thinking behind the PREPARE strand was the series of multiple terrorist attacks launched in Mumbai in 2008. A group of ten Lashkar-e Tayyiba (LeT) terrorists departed from Karachi on 22 November 2008 in a small boat, and around 30 minutes later, they were cross-decked to a larger vessel, the Al Husseini belonging to the LeT. An Indian fishing vessel, the MV Kuber, was captured by other LeT members and its crew was killed. The Captain was spared and the group boarded his vessel on 23 November. They forced the Indian captain to sail to Mumbai, arriving four miles from the coast at 1600 hours on 26 November. The captain of the vessel was then killed and the group boarded an inflatable dinghy to travel the remaining four miles to Mumbai, arriving in the vicinity of Badhwar Park.

The group split up into five attack teams and took taxis to their allocated targets: The CST Railway Station; the Leopold Café and Bar; the Taj Mahal hotel; the Oberoi-Trident hotel; Nariman House, a Jewish centre. A total of twelve separate attacks were launched and the attack span lasted for almost four days (Khetan et al., 2009:116–167). During the attacks, 163 people were killed and 308 were injured. The only surviving attacker, Ajmal Kasab, was subsequently convicted of 86 separate offences, sentenced to death by the Indian Supreme Court and executed on 21 November 2012 (Maryland Coordination and Analysis Center, 2012:1).

The scale and complexity of the attack indicated a very high degree of planning, training and probably rehearsals by the attackers. The attackers were equipped with handheld GPS satellite navigation units, GSM mobile phones and THURAYA satellite phones, which allowed them to employ robust command, control and communications, especially with their controllers while the attacks were in progress (Kronstadt, 2008:2). Some of their communications were encrypted using commercial, off-the-shelf encryption systems (Home Office, 2011:34). Previous attacks in India by LeT had been of a much lower order of complexity, mainly involving single IED attacks or isolated operations. The Mumbai attacks of 26 November provided a lethal illustration of the difficulties faced by the authorities when a complex attack is launched against multiple targets in different geographical areas.

The importance to the authorities of command, control and communications increases as a terrorist attack unfolds, as these factors are critical in enabling the authorities to develop an accurate picture of the incident. In the same way that Police Intelligence staff analyse a criminal's "routes to crime", so the travel and transport itineraries of the Mumbai attackers were analysed, to add to the picture of how the attack unfolded. By capturing an Indian vessel and using its Indian captain, the attackers evaded detection on their route into Mumbai. The terrorists accurately maintained a ship's log while on board the captured vessel, which helped the Indian authorities to plot the speed/time/distance vectors of the attackers. They even kept detailed logs of which terrorists were on deck watch, and at which times (Ministry of External Affairs, 2008:36).

In military terms, this ability to create a consolidated situational awareness is described as the “Recognised Picture of the Battlespace” (RPB). The inclusion of the word “recognised” was made in order to highlight that all stakeholders understand the need to work from the same picture, or Intelligence assessment. Initially this concept came from the Royal Navy, wanting to ensure that all RN vessels at sea had the same situational awareness of maritime traffic in their vicinity. This picture was produced and updated at a naval HQ in UK and was broadcast to all RN vessels on a secure communications link, to provide each vessel with the Recognised Maritime Picture (RMP) (Burke, 2006:77–78). This concept was adopted by the Royal Air Force to provide all aircraft and ground stations in the UK and overseas with a Recognised Air Picture (RAP).

As soon as the authorities are aware that an attack is underway, various procedures are initiated, such as a command room being stood up. Relevant stakeholders are immediately notified of the incident so they can begin to prepare response assets such as ambulances, fire engines, crowd control cordons and traffic management systems, which prevent traffic gridlock but also allow emergency services to access the incident areas. The Mumbai attacks lasted for four days. The dispersed nature of the attacks, coupled with incidents such as the fire which broke out at the Taj Mahal Palace and Tower Hotel, further strained the efforts of the Indian authorities to develop an accurate and timely overview of the situation across the city and to deliver a co-ordinated response to bring the attacks and the fire to an end (Khetan et al., 2009).

The 2011 PREPARE chapter identified several lessons learned from the Mumbai attacks, which had potential implications for the UK government’s ability to respond to a similar series of attacks. While London had to deal with multiple, near-simultaneous terrorist attacks against the bus and Underground travel infrastructure in 2005, there was one major difference. As the London attacks were solely suicide attacks, it meant that each of the four explosions were finished operations, in terms of them being self-contained incidents. In Mumbai, the attackers aimed to kill as many people as possible while they were still alive. The taking of hostages was the primary reason that the attacks lasted for four days and this resulted in extended publicity for the terrorists' cause. The CONTEST strategy aptly described these as "*marauding attacks*" and added that there have been significant changes to the equipment, tactics and resources of the UK Police, and also to the "*multi-agency response that such incidents would require*" (Home Office, 2011:14).

Several of the government's observations in CONTEST related to the use of firearms by the Police. The appropriateness of weapons and tactics deployed by the authorities against attacking terrorists is an important factor in how successful the government response is. One aspect is the calibre of the Police weapons, although the deployment and application of more powerful weapons do not necessarily bring a concomitant positive result. Weapons and calibres of ammunition must be carefully selected for the appropriateness of the task in which they are deployed.

An example of this is the deployment of armed Police officers at UK airports. Within any major UK airport terminal, it is common to see armed officers carrying Heckler and Koch MP5 sub-machineguns. This weapon fires a 9mm round, which has a considerably lower muzzle velocity and shorter range than the 5.56mm ammunition fired by traditional assault rifles found in NATO member states. In the crowded confines of an airport terminal, a low-velocity 9mm round is a safer option for the Police to use than a larger and/or high-velocity round.[75] By contrast an Armed Response Vehicle (ARV) of London's

[75] If a 9mm round is fired and misses the target, it will not travel as great a distance as a 5.56mm round. It will also have less velocity, and is less likely to ricochet if it hits a hard object. The 9mm round is also less likely to enter and fully exit a human body and continue on its path, potentially injuring additional people. For even more sensitive environments, such as the pressurised cabin of a passenger aircraft, 9mm ammunition can be adapted still further, for example the ammunition used by sky marshals. This kind of ammunition is less powerful, and can use frangible projectiles, which expand and flatten as they leave the barrel, allowing the bullet to still disable or kill an attacker,

Metropolitan Police may carry two assault rifles (Heckler and Koch G36) of 5.56mm calibre. It is unlikely that sufficient Police firepower (in terms of numbers of firearms and the appropriate calibres) could be deployed by ARVs alone, in the event of a Mumbai-style, multi-site, complex attack.

The 2011 CONTEST policy thus identified that armed Police officers would need access to more powerful and more appropriate weapons to deal with such an incident. It also identified the need to provide a faster response from the Armed Forces, at the request of the Police, to assist with the containment and neutralising of a complex attack (Home Office, 2011:97).[76] Another gap identified by the strategy was the firearms capacity of cities other than London. This regional capacity is being upgraded, as are the procedures for a city or Police force to request armed support from neighbouring regions (Home Office, 2011:97). An additional benefit of the UK hosting the 2012 Olympic Games was the enhanced training for firearms officers which was delivered early, as part of the CONTEST 2011 strategy (Home Office, 2011:6;97).

Assessing the effectiveness of the Intelligence cycle in the sphere of interoperability is made more difficult by the wide area of scope which this work strand covers. At one end of this scope are the London terrorist attacks of 07 July 2005, while at the other end is the accidental fire at Kings Cross station. The upgrading of the UK Police firearms capability was a direct result of the Intelligence gained about the planning and tactics used in the Mumbai attacks and in this case, the model was definitely of value as the provision of detailed reporting was used to effect a change in UK security policy. The Intelligence operation following the 07 July attacks, Operation THESEUS, was

while minimising the chance of the round accidentally puncturing the pressurised cabin wall, potentially leading to an explosive decompression.

[76] A previous example of such support from the Armed Forces was the intervention by the Special Air Service Regiment during the siege of the Iranian Embassy in London in 1980, in which the Police requested military support. In such a situation, the Police formally hand over control of the incident to the Armed Forces. The decision to assault the building was taken shortly after one of the hostages was executed by the terrorists, and the body dumped outside the Embassy steps. During the SAS assault, one hostage was killed and the remaining 19 were successfully rescued. Five of the six terrorists were killed during the rescue operation. For a full account of the siege and the assault, see Pearson, W., 2011. "*The Iranian Embassy Siege: The True Story*", (London: Weidenfeld & Nicholson).

primarily a reactive operation, although it obviously built upon existing Intelligence, including that collected as part of Operation CREVICE. There is no doubt that errors were made during CREVICE, the implications of which only surfaced after the 07 July attacks in 2005.[77] On the other hand, the Coroner's report stated that in order to have uncovered the link between Mohammed Qayam Khan (MQK), a suspected leader of an Al Qa'eda team in Luton, Mohammed Sidique Khan (MSK) and Omar Khyam, "*only an unjustified amount of intrusive investigative work would have led to the discovery of the link before that time*" (Hallett 2011, para.19).

4.5 Summary

This chapter has explained what the CONTEST strategy is, what it aims to achieve and how the Intelligence cycle works within it. The Intelligence cycle does not operate in a vacuum in the UK's counter-terrorism work. Within the Intelligence agencies it operates from the very top level, starting with the strategic requirements of the JIC, down to the lowest tactical level, such as the Intelligence briefings provided to armed Police officers before they forcibly enter a property to arrest a terrorist suspect. A JIC requirement such as "provide actionable Intelligence on the most serious, active terrorist plots within the UK" provides the direction from the Prime Minister's office, which is promulgated to the Intelligence agencies who initiate their own collection plans. Collation begins simultaneously, as does the inter-agency collaboration required to ensure that all available and relevant information is retrieved from the various data repositories. As collection begins to produce relevant information and pieces of Intelligence, analysis is conducted by the individual agencies, and the results shared at regular progress meetings. Evaluation

[77] See, for example, Section 18 of the Coroner's report into the 07 July 2005 bombings, which details the links between McDaid and Khan, and the fact that McDaid and Khan being in the same vehicle was not passed to the Security Service by West Yorkshire Police, even though the operation was jointly conducted by both of these organisations (Hallett 2011, para.18).

takes place throughout the process, providing the quality control aspects of the process, and ensuring that the Intelligence produced is subject to critical examination.

The dissemination of actionable Intelligence (as well as background Intelligence) can occur multiple times. It can require additional collection, deeper analysis or a secondary evaluation to compare what is known now to what was known previously. It can also require an assessment of whether or not the new picture is plausible and accurate. In the example given above, this could end with a Police firearms team being briefed on the contents of a target package which provides them with the tactical information needed before they launch an operation to arrest a terrorist suspect who they expect to respond with firearms. It could also end with a much softer takedown, where the suspect is arrested in a similar manner to Dhiren Barot, in Operation RHYME. Due to a leak, the U.S. media had published details identifying Muhammad Naeem Noor Khan as a suspected terrorist who was helping the U.S. authorities with their enquiries. Khan was in email contact with Barot and the Police in the UK knew that they had no choice but to quickly arrest Barot, instead of continuing the surveillance on him to collect more evidence and to covertly penetrate Barot's group. While under surveillance, Barot went for a haircut in Willesden. While he was sat in the barber's chair, two detectives in plain clothes entered the shop and conducted a very low-key arrest (Doward, 2006). This was a much more effective way to ensure public safety than an armed intervention.

All of this Intelligence work takes place within the framework of the CONTEST strategy. The PREVENT strand aims to negate the likelihood of an attack happening in the first place, by challenging the ideological landscape in which the terrorist groups operate; by identifying and working against the radicalisation of individuals to the terrorist cause, especially of vulnerable individuals such as minors, convicts, newly released prisoners and the mentally disabled; and by degrading the recruiting abilities of terrorist groups, which consequentially degrades their ability to operate with an effective and sustained support network.

The second strand, PROTECT, is closely tied to PREVENT. It aims to put the necessary measures in place to safeguard the elements of the national infrastructure deemed critical to the security of the UK. Two case studies were used as examples of the terrorist threat to the UK CNI and these demonstrated the considerable depth of planning which some groups have conducted in their attempts to destroy elements of this CNI. In addition to the CNI, the threat against crowded places was also outlined as this is considered a classic soft target by Al Qa'eda. The UK's transport sector has already been subjected to terrorist attack in 2005, with deadly results. The current PROTECT strand has taken the lessons identified in incidents such as the London bombings, as well as from non-terrorist incidents such as the King's Cross fire in 1985. It aims to strengthen the protective measures needed to secure these potential targets even further.

The six priorities of the PURSUE strand are all aimed at preventing attacks from happening, by interdicting the abilities of individuals and groups to participate in terrorist activity. Some of the work conducted under this strand is concentrated in the UK, such as domestic, Intelligence-led operations and when appropriate, prosecutions under the UK's legal framework. Other parts of this strand take place overseas, such as the mentoring of foreign officers and capacity-building programmes, particularly in developing nations. Liaison work and Intelligence-sharing with international partners spreads the workload and leads to a more effective division of labour for the countries involved in such agreements.

In the event that an attack does take place, the PREPARE strand is designed to ensure the rapid establishment and maintenance of effective command, control and communications. This helps the authorities gain an accurate picture of the nature of the incident. They decide what assets are needed to deal with it and send the necessary assistance to bring the attack under control. They can then deal with the aftermath so that normal business can be resumed as quickly as possible. Lessons from the London bombings and the Mumbai attacks have been used to make changes in key areas such as firearms tactics, weapons and ammunition, as well as in the areas of command, control and communication. This enables a more collaborative, multi-agency approach to be employed in dealing with the aftermath of a terrorist attack.

This chapter has clearly demonstrated the functioning of the Intelligence cycle across the four strands and the sixteen sub-strands of the CONTEST strategy, covering a very wide spectrum of operational focus. This includes the softer aspects of the strategy, such as engaging with vulnerable individuals at serious risk of radicalisation, through to identifying and implementing the measures necessary to protect the UK's CNI, and ending with disruptive, possibly lethal, action against active terrorist plots. The model, though simplistic in nature, is flexible enough to cover the majority of the CONTEST sub-strands, with the category of PREPARE being the only one which it is not specifically designed to support. That said, the model does still provide valuable inputs into this strand, especially in the areas of WMD and CBRN. The Intelligence cycle underpins the CONTEST strategy as without the continuous feed of Intelligence into the various sub-streams, the strategy would be almost impossible to implement. It can be said, then, that the CONTEST strategy is Intelligence-led, and that the Intelligence inputs resulting from the cycle drive the policy and action outputs. Having covered the CONTEST policy in detail, Chapter 5 next examines the 6-stage Intelligence cycle itself. The cycle has been refined several times and is taught within the Security Service, SIS, GCHQ, DI, the military Intelligence branches of the UK Armed Forces and as part of Police analysis training (National Policing Improvement Agency, 2008:11). Chapter 5 explains the six stages of the model, and how they work together. The explanations of the stages are illuminated with observations from a number of serving and retired practitioners with long experience in the counter-terrorism Intelligence field.

Their experiences provide a unique understanding of how the components of the model function in actual counter-terrorism work, allowing for a deeper examination of the Intelligence cycle in action.

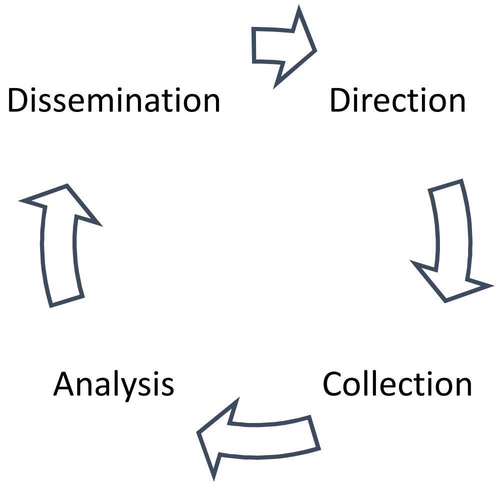
Chapter 5 The Intelligence Cycle

> "*You have trivialized our movement by your mundane analysis. May God have mercy on you*" - Ayman Al Zawahiri (Wright, 2002:29)

> "…*to be a good watchdog it is not sufficient to detect the approach of danger – you must bark at the right time: not too early, for then your master becomes dulled to danger by too much barking, nor too late, for he may then be overtaken by disaster; and you must not bark at false alarms*" (Jones, 1947:354)

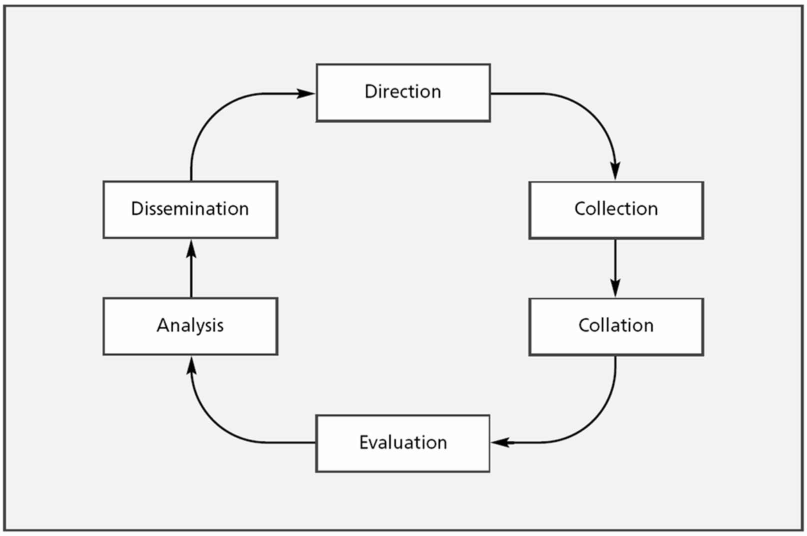
The previous chapter described the UK's counter-terrorism strategy (CONTEST), to illustrate the framework within which the Intelligence process takes place. This chapter focuses on the actual model of the Intelligence cycle itself, examining each of the 6 component stages in detail, and showing how these stages work in the field of counter-terrorism. Various academic and organisational contributions are provided to show how the cycle and its components can be viewed in different ways. Effective counter-terrorism is heavily dependent upon sound Intelligence, yet Intelligence work is more often described as an art rather than a science (Burke, 2013; Richards, 2010:97–144). The principal model used as the foundation of Intelligence collection for several decades has been the Intelligence cycle. In its earlier form in the 1980s, the Intelligence cycle was represented using just four components, and this model was the one taught in military Intelligence training in the UK during the 1980s.[78] It was represented thus:

[78] This version of the Intelligence cycle was taught by the British Army Intelligence Corps as early as 1984, and continued to be taught until at least early 1990.



14 British Army Intelligence Cycle, circa 1984

The model currently used by the UK Police and the Intelligence agencies is the 6-stage model shown below (National Policing Improvement Agency, 2008:11):



15 The 6-stage Intelligence Cycle

5.1 Direction

The Intelligence cycle notionally begins with direction, when Intelligence assets are provided with the collection requirements of the primary customer or customers. Within the Intelligence community this is also known as "tasking". Taking a government as an example, the national Intelligence assets may be tasked with providing detailed Intelligence on a terrorist target about which they have little or no current insight. This could be the sudden and unforeseen eruption of major unrest in a foreign country. Contemporary examples include the rise of Islamic State in Syria and in Iraq, or a significant terrorist action carried out by a previously unknown group, or the appearance of a new and advanced weapon system in a country which has traditionally been perceived as hostile.

The tasking of the UK Intelligence agencies has been subject to an extra layer of governmental authority since 2010, when it was announced that a National Security Council (NSC) would be established, as would a new post of National Security Adviser (NSA) (Prime Minister's Office, 2010). The post of NSA started on 12 May 2010, with the appointment of Sir Peter Ricketts who handed over to Sir Nigel "Kim" Darroch in January 2012 (Rifkind, 2011:36).The role of the NSC is a co-ordinating one, ensuring a joined-up approach across those agencies and departments which deal with threats to UK national security.[79] Such agencies and departments include Defence Intelligence, the FCO, the MOD and the Home Office among others.

Since its inception, the NSC meets weekly and is chaired by the Prime Minister. Permanent members of the NSC comprise the following: the Deputy Prime Minister, Chancellor of the Exchequer, Foreign, Home, Defence, Energy and Climate Change and International Development Secretaries, the Minister for Government Policy and Security, Chief Secretary to the

[79] Three Ministerial sub-committees were established under the NSC, which had specific remits: 1. Threats, Hazards, Resilience and Contingencies, which also includes a restricted group that examines Intelligence issues; 2. Nuclear Deterrence and Security; 3. Emerging Powers. A fourth, temporary sub-committee was established on 20 March 2011, which focused on co-ordinating the implementation of UN Security Council Resolution 1973.

Treasurer, Minister for Government Policy and with other Cabinet Ministers attending as required. The Chief of the Defence Staff (who also represents DI), Chairman of the JIC and Heads of the Intelligence and security Agencies also attend as required (Parliament, 2014:18). The NSC formulates and approves a National Security Strategy. This strategy details the 15 highest priority risks which the NSC perceives the UK to be facing. It lays out the strategic direction which the Intelligence community is expected to take, to produce Intelligence on these threats. Additional direction also flows from the following : Strategic Defence and Security Review (SDSR); the Strategic Priorities for Secret Intelligence Collection, coming from the Joint Intelligence Committee (JIC); and the Intelligence agencies' own Agency Strategic Objectives (ASOs). The importance of the National Security Strategy was underscored by the Chief of SIS, when he described it as "*the starting point for the requirements and priorities on the intelligence Agencies*" (Rifkind, 2011:38)

In the case of GCHQ and SIS, the Foreign Secretary confirmed to the ISC that he regularly tasks these two Intelligence agencies, saying:

> "*We task them all the time and I discuss with [the Chief of SIS] and with the director of GCHQ on an almost continuous basis their work. So I think, you know, how they allocate their resources is very much guided by us in the Foreign Office. I would say it's set by us predominantly, the overall oversight of these Agencies and their overall strategy is set by us*" (Rifkind, 2012:10).

The ISC explained how and why the Security Service is tasked differently. Operational control of the Security Service rests with the Director General (DG) of the Service, for two main reasons. First, the Security Service is mandated by the Security Service Act (Parliament, 1989:sec.1) to ensure:

> "*the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means*".

Second, it has traditionally been the case that each UK government continues to allow the Security Service to operate "*free from political direction*", a policy which is ideally suited to a liberal democracy (Rifkind, 2012:sec.10). Another key difference between the agencies is the Ministerial approval required for warrants to be obtained. Both GCHQ and SIS obtain their Ministerial authorisation from the Foreign Secretary, as the potential risks involved in conducting Intelligence operations overseas are considered much higher and the potential for political fallout is much greater, should an operation be compromised. At the more extreme end of the scale, diplomatic relations could be adversely affected. The Security Service obtains its Ministerial approval for intrusive surveillance warrants from the Home Secretary, but crucially the DG retains day-to-day decision-making powers, within the limits laid down in the legislation of the SSA. The Home Secretary explained how this affects tasking, and how he saw the oversight of the Security Service:

> "*I think it is important that there is an operational independence… but there is a process of discussion. I mean, the weekly discussions that I have with the Security Service are about where they are focusing their resources and particular operations that require that resource and questions I can ask about the issues that I see that need to be addressed and how they are doing them. So it's a different sort of accountability*" (Rifkind, 2012:sec.10).

Tasking not only provides the nature of the target, but it can also set priorities for Intelligence collection. Even the largest organisations have finite resources and Intelligence communities worldwide are no different in this respect. The prioritisation of tasking ensures that assets are devoted to targets in line with the requirements of the customers, and that agencies do not allocate resources unilaterally without clear direction. The priorities for Intelligence collection become Intelligence Requirements, or IRs.

The military Intelligence machinery in the UK uses a slightly different system for defining Intelligence requirements. Standard NATO procedures are used, which first determine Priority Intelligence Requirements (PIRs), usually strategic and therefore broad in nature. After this come Secondary Intelligence Requirements (SIRs) that continue at the lower levels of operational and tactical tasking. In NATO procedure, these PIRs and SIRs are the drivers for the process of an Intelligence collection plan. The PIRs and SIRs are just one part of the NATO system called Collection, Co-ordination and Intelligence Requirements Management (CCIRM). The CCIRM process was begun in earnest in the early 1990s, in an effort to ensure that Intelligence collection and analysis was not being unnecessarily duplicated.[80] The PIRs are further refined into Information Requirements, which rather confusingly uses the same abbreviation ("IR") as the other agencies use for "Intelligence Requirements" (Grebe, 2007).

At government level, PIRs provide the Intelligence community with the top-level questions to which the government requires answers. PIRs have been described as "*information that directly feeds the key decisions that will determine the success or failure of the mission*" (Gratch et al., 1999:2).[81] The

[80] When the CCIRM process was introduced, the author was working in a military Headquarters in an Intelligence function. The CCIRM process was met with a large amount of apathy and a small amount of resistance by the majority of the Intelligence division, who initially saw it as simply another layer of bureaucracy which had to be undertaken before requesting Intelligence collection against certain targets. Over time (approximately a year), the process became more streamlined and all elements involved in the CCIRM process became quicker and more efficient at carrying out the necessary procedures. The CCIRM process made a major contribution to minimising the duplication of effort.

[81] According to FM 34-8-2, good PIRs do the following: "Ask only one question; focus on a specific fact, event, or activity; provide the Intelligence required to support a single decision; are tied to key decisions that the commander has to make; and give a latest time of information of value (LTIOV)" (Department of the Army, 1998:sec.D–2).

U.S. Army defines PIRs as "*Intelligence requirements associated with a decision that will affect the overall success of the command's mission*" (Department of the Army, 1998:sec.D–1). PIRs at UK government level, although generally strategic in nature, can also be focused at the operational or even tactical level should the need arise. The JIC uses its own "JIC Requirements", while the NSC uses Strategic Requirements (SRs). Instances of government PIRs descending to the tactical level include the operation launched in the immediate aftermath of the 07 July 2005 suicide bombings in London (Operation THESEUS), and the unsuccessful attempted suicide attacks in London on 21 July 2005 (Operation VIVACE).

The unauthorised public release of almost a million classified reports from the U.S. and elsewhere, known as the "Wikileaks cables", have also resulted in an enormous quantity of primary source material being made available. The unauthorised release of highly classified information is a serious criminal offence, but there is no altering the fact that these documents are now so widespread in the public domain as to be uncontrollable, thus they lend themselves to serious academic study.

In the UK, direction for the Police comes ultimately from the Prime Minister via the Home Secretary, who sets the strategic priorities for policing. Each Police force, under the auspices of a Chief Constable, conducts a Strategic Tasking and Coordination (ST&C) process which enables the senior leadership of the Force to discuss, agree and set the strategic direction of the Force's activities, in line with the resources available to it. This is done through the mechanism of the Strategic Tasking and Coordination Group (ST&CG). The main outputs of this process (relevant to this study) are the Strategic Assessment, the Tactical Assessment and the Control Strategy. The Strategic Assessment considers a very wide vista of scanning, including items such as local and national policing issues, the public's perception of crime and social disorder, emerging criminal trends, the Force's own performance assessment measured against the relevant performance indicators, the sources of information used to create the assessment (including the classification of the assessment) and the priorities of the variously identified issues. The Strategic Assessment is a document which takes a long-term view of these issues,

The Tactical Assessment, on the other hand, aims to identify and describe the short-term issues which need to be analysed in the Tactical Tasking and Coordination Group (TT&CG). The Tactical Assessment aims to identify specific problems (e.g. the smashing of a series of car windows in a quiet street, to steal satellite navigation devices) and to identify specific individuals or groups of interest for their criminal activities. Like the Strategic Assessment, it also aims to identify emerging criminal trends, but at a more localised level. It also conducts performance reviews at the local level, and prioritises activities to be carried out in support of the pillars of prevention, intelligence, enforcement and reassurance.

The Control Strategy describes the operational priorities of the Force (or the Command area if below Force level), it sets the long-term plan for dealing with these priorities and enables the senior leadership team to better allocate resources to deal with the issues identified. The Control Strategy is set by the ST&CG and this is the only body which is empowered to review and to change the Control Strategy. An example of an IR is provided at Annex A.

5.2 Collection

Once tasked, the Intelligence assets will formulate a collection plan detailing specific subsets of the IRs. They will identify which assets are most capable of, and best suited to, collecting the necessary Intelligence. An example of an Intelligence Collection Plan is provided at Annex D. The collection of counter-terrorism Intelligence usually encompasses both overt and covert sources. The overt aspect encompasses a wide range of sources including technical journals, eyewitness reports, interviews, trade exhibitions, conferences and social media.[82] Covert sources can include Covert Human Intelligence Sources (CHIS), covert surveillance of individuals and premises (both directed and intrusive, including lawful interference with property and vehicles) and the interception of communications. Satellites provide a significant portion of the technical collection capabilities for the UK and U.S. Intelligence communities.[83] While most technical collection is automated to some degree, the collection of HUMINT remains largely non-automated.

Overt sources can reveal a key piece of information which, with the addition of analysis, can produce Intelligence results beyond expectations. One example was given in chapter 3.2, regarding the deployment of “bunker buster” bombs to Diego Garcia. Another example occurred in 1981, and led to the confirmation that Israel had a nuclear weapons manufacturing programme. On 07 June, Israeli fighter jets launched a strike on the Iraqi nuclear reactor at Osirak, to deny Saddam Hussein the capability of enriching fissile material to weapons-grade standard. The raid was a success in military terms, with the reactor being destroyed and no Israeli fighters being lost. On 09 June, the Israeli Prime Minister Menachim Begin gave a triumphant press conference where he described the raid, boasting to television reporters that the Israeli jets had also destroyed a covert facility which he said was located forty metres below ground, and was involved in the production of nuclear weapons.

There was no such facility forty metres beneath Osirak and the American Intelligence analysts knew this. What Begin had unwittingly described was Israel’s own, highly secret nuclear weapons construction facility located 40 metres below the supposed research reactor in Dimona. The clue gave American Intelligence analysts the necessary opening to look at Dimona more

[82] Some Intelligence academics, including former practitioners, (Omand et al. 2012) consider the field of social media as a standalone, additional category to the family of “-INT” branches, bestowing upon it the nomenclature of SOCMINT. In recent years, there have been other nomenclatures produced for the consideration of the Intelligence community, such as RESINT (Svendsen 2013). PROTINT (Omand 2010, p.32), PERSINT and others. There is a risk that such narrow distinctions dilute rather than reinforce the value of Intelligence categories when considering sources and methods as a family.

[83] Much open source material exists on the nature and capabilities of intercept. Many open-source reports contain varying degrees of inaccuracy. The lawful interception of communications is one of the most sensitive areas of Intelligence collection by the UK government, and it is only natural that technical details about this capability are protected from unauthorised public disclosure.

deeply, specifically for evidence of a nuclear weapons programme. The heads of the Israeli Defence Force and Mossad were both aware of the implications of Begin's mistake and the next day a press release stated that the facility had been four metres underground, not forty, but it was already too late. American Intelligence analysts were able to confirm the existence of the nuclear weapons facility as a result of the mistake. As a result, Israel was subjected to a prolonged and hostile media interest in its nuclear weapons programme (Claire, 2004:232–233; Turner, 1974; Clarke, 1980; Vanunu, 1987).

The NPIA (2011:sec.22) provides the following advice to Police Intelligence analysts and makes a further distinction between potential sources of information being "open" or "closed", stating:

> "*Closed sources of information are those with restricted access, for example, police crime recording systems and information available through sharing agreements with partners. Open sources of information are those that are widely available. They may require the user to pay a small fee, for example, online news, media, academic research and the electoral roll*".

According to a policy document released by Cumbria Police (2007:para.4.4), a sound Intelligence collection and management policy also assists with "*compliance with other information-related legislation*" such as the NIM, MoPI Code of Practice and Guidance (2005), the FIA, the DPA, the Criminal Procedure and Investigations Act (1996), and the HRA (1998). This is a major benefit for law enforcement and Intelligence agencies, as they constantly have to ensure that their operations and daily work remain within the confines of the legal boundaries established by the various instruments of legislation which governs them.

Some targets may only require single-source tasking, or indeed may only be open to single-source collection. Since the various UK governmental inquiries after the 2003 invasion of Iraq, a perception has persisted in the media that single-source Intelligence is inherently flawed and dangerous. This is not the case, and this misunderstanding has come about largely due to the revelations about the Intelligence derived from the source codenamed CURVEBALL, on the supposed 45-minute readiness capability of the Iraqi Armed Forces to lunch battlefield chemical munitions (Silberman & Robb, 2005:83).[84] The use of single source Intelligence requires greater care, and more solid analysis and evaluation. An organisation's culture and procedures can negatively affect the credibility of such Intelligence. An example from the CIA highlights this problem. After the 2003 invasion of Iraq, the then Deputy Director of Intelligence in the CIA discussed with a group of CIA staff members an internal CIA review on the decision to invade Iraq. He noted that the internal review had highlighted "*cases in which a single source has different source descriptions, increasing the potential for an analyst to believe they have a corroborating source*" (Miscik, cited in Russell 2007:192; Jehel, 2004). The Butler Report was very firm in its conclusion that single source reporting can be useful for operational purposes. It stated:

> "*It is incorrect to say, as some commentators have done, that 'single source' Intelligence is always suspect. A single photograph showing missiles on launchers, supporting a division deployed in the field, trumps any number of agent reports that missiles are not part of a division's order of battle. During the Second World War, innumerable Allied command decisions were taken on the basis of Intelligence reports from*

[84] The issue of single-source Intelligence and its influence on the UK and U.S. decision to invade Iraq in 2003 largely derives from the inclusion of Intelligence material obtained from a human Source codenamed CURVEBALL. He was an Iraqi national who defected to Germany and sought asylum there, initially in exchange for information about Saddam Hussein's WMD programme. Until the end of the invasion, CURVEBALL was only debriefed by his German handlers, and despite repeated requests for direct access to the Source, CIA Source Handlers were never allowed to debrief him (Drogin, 2007).

> *a single type of source (signals Intelligence, providing decrypts of high-level German and Japanese military plans and orders), and quite often (e.g. re-routing convoys in the middle of the Atlantic) important decisions had to be taken on the basis of a single report. As before, common sense and experience are the key*" (Butler, 2004:11).

Other terrorist targets may require all-source collection involving HUMINT, SIGINT, covert surveillance, OSINT and others. Such targets may be strategic ones, or targets involved in an active plot. When a terrorist cell moves from only talking about an attack, to actually planning an attack, it commensurately moves up the radar of the Intelligence agencies due to the overriding requirement to ensure public safety. The collection effort devoted to a cell involved in attack planning expands considerably, compared to a cell which is only involved in discussions. At this point, the full remit of the Intelligence collection apparatus will be directed at the cell. Solid and effective inter-agency co-operation is vital in such cases, to ensure that all collection agencies know their responsibilities in the collection plan. This co-operation is also necessary to ensure that inadvertent compromises are not made, due to one agency not knowing that another agency is involved in covert activity. For example, if an Intelligence agency recruits a CHIS in a terrorist cell, it requires very careful management of the operation to maintain the anonymity and security of that CHIS. The Intelligence agency not only has a need for the CHIS to produce actionable Intelligence from his covert role, but the agency also has a duty of care to ensure the physical safety of the CHIS. This is more than simply assisting the CHIS in maintaining a cover story. It is also of paramount importance that there should be no possibility of another agency taking intervention action which could unwittingly put the life of the CHIS in danger. One of the biggest risks with this kind of operation is that a "blue on blue" incident occurs, whereby government assets unwittingly engage in action against one of their own officers or covert Sources.[85]

When requesting Intelligence collection against a target, it is important that the capabilities and limitations of the various collection agencies are understood. For example, SIGINT assets can be rapidly directed against a new target but if there is no "cueing" or "triggering" (i.e. providing them with the technical information necessary to know where and what to collect) they cannot begin the collection process. HUMINT assets may also be able to begin Intelligence collection immediately, if the HUMINT agency already has a source in place with the appropriate access to begin fulfilling the tasking requirements. If there is no human source close to the information required, the HUMINT agency may need to start the HUMINT process from the beginning, identifying a potential source, recruiting and training them, shaping their path to enable them to gain the access required, before beginning to produce meaningful Intelligence. This can be a time-consuming process and this is usually at the more operational to strategic end of the scale. IMINT may be able to furnish satellite or aerial imagery almost immediately and fulfil the initial Intelligence requirement, but this depends on the detail of the requirement, and whether the relevant imagery has already been captured and is retrievable.

For example, in order to plan a covert surveillance deployment, detailed imagery of a terrorist target's residence and immediate surroundings may be required. For initial planning purposes, the imagery does not necessarily need to be the most current available. More important may be the target overview, showing whether the house is detached or not, how densely populated the adjoining properties are, whether there are any public places close by, such

[85] The term "blue on blue" originated in the Cold War period and was used by NATO forces to describe an engagement where NATO forces accidentally engaged their own troops, e.g. in a notional air strike on what were wrongly believed to be enemy troops.. On tactical maps, "friendly forces" (i.e. NATO) were always coloured in blue, while "enemy forces" (i.e. Warsaw Pact) were coloured in orange. In the early days of the Cold War, enemy forces were originally coloured in red. It was later changed from red to orange, to avoid tensions escalating between the U.S. and Soviet governments, as it was considered by the U.S. that it could be an unnecessary provocation to the Soviets, if enemy forces were always depicted in red.

as public houses or nightclubs, and even whether the immediate area is considered hostile to the Police. A detailed Community Risk Assessment would need to be conducted prior to any direct intervention taking place. When there is a direct intervention planned, such as an armed Police raid, then the imagery needs to be either near-real time" (NRT) or "real time" (RT). This may come from a variety of collection platforms, such as covert surveillance, intrusive surveillance probes and/or helicopter-borne cameras, to name but a few.

Intelligence collection management has now become a field in its own right and each agency has staff involved in single-source and all-source management. Allen (1995:37) goes so far as to describe it as "*the epitome of Intelligence professionalism*". Intelligence collection management can also impact upon what Intelligence material an analyst can and cannot see. Cases involving covert Intelligence collection can include major criminality, narcotics, national security issues or sensitive investigations such as child sexual abuse. Within UK Police forces, an analyst involved in a covert investigation is excluded from access to the raw Intelligence product to ensure that a "*sterile corridor*" is maintained, so that Intelligence does not unduly influence evidence (ACPO, 2006:42).

While some collection methods allow Intelligence to be collected remotely, such as intercept, other methods carry a high degree of risk, such as the use of a CHIS to penetrate a cell or a group. Terrorist cells are usually made up of a small core of people who will be directly involved in an operation, all of whom may be bonded by family or religious ties. Surrounding them are an outer circle of people who provide the necessary support functions to enable the attack planning, and the attack itself, to take place. This support can include the provision of communications (mobile phone handsets, SIM cards, email addresses, laptops, etc.), weapons, ammunition and explosives (usually the responsibility of a "Quartermaster"), vehicles (stolen, purchased or hired), documentation (genuine and forged) and safe houses, among others.

The covert penetration of a cell is one of the most dangerous tasks in CT work, regardless of whether an existing cell member is recruited as a CHIS, or an undercover officer is placed into a position from which they can be recruited into the cell. Extensive and thorough risk assessments need to be conducted before such operations are approved as there is a much higher degree of risk for the CHIS to be compromised, as well as for the cell to become aware that it has been penetrated. This awareness could result in a potential dispersal and relocation of the group, leaving the Intelligence agencies blind.

The collection of HUMINT is not exclusively derived from such high-risk, covert operations as the penetration of a cell. Telephone and internet hotlines also provide useful Intelligence and they have some advantages over the more covert methods. People who may not feel comfortable going to a Police station to provide information often have less resistance to providing information anonymously. The corollary that goes with this is that the flow of information can become a flood, requiring still more human resources to field calls, collate and analyse the information. In the case of the Washington Sniper crisis in 2002, more than 100,000 pieces of information were received as a result of the Police requesting information on the killers. Of these, around 40,000 were deemed worthy of further investigation (Hulnick, 2006:970). An additional hazard is that hotlines are often used to name individuals to the Police, for reasons such as personal revenge, or to cause difficulties for a competing business interest.

Interrogation also feeds into the collection part of the Intelligence cycle and it is a form of Human Intelligence. In the past decade, it has become increasingly controversial with globally recognised images such as those of abused Iraqi detainees in Abu Ghraib prison being broadcast around the world and causing violent protests in many countries. Interrogation frequently results in vital Intelligence being obtained on the identities and locations of terrorist figures and details of planned attacks. The divisiveness of the issue is mainly concerned with the techniques used and the line which separates interrogation from torture. Interrogation is a divisive topic and one which regularly appears in media stories, more so since the U.S. began the “Global War on Terror”, but it remains a tool in the arsenal of the Intelligence and Law Enforcement communities.

The conduct of interrogation is strictly legislated in the UK and it is carried out according to rules which dictate conditions, such as how long a suspect can be subjected to interrogation before being allowed to rest. Opinion is divided on whether techniques such as “water boarding” were a key enabler in the persuasion of Khalid Sheikh Mohammed to cooperate with his interrogators, and to provide material on Al Qaeda personalities and operations (Stelter, 2009; Senate Select Committee On Intelligence, 2014). While U.S. interrogation techniques such as “water boarding” have had extended coverage in media stories, the art of interrogation mainly depends on the psychological and social skills of the interrogator.[86]

5.3 Collation

The third stage of the cycle, collation, is omitted from some models of the cycle, while in others it is replaced with the term processing. Collation brings together all of the collected information and Intelligence to enable the analytical process to begin. Particularly if one or more of the sources is a HUMINT source, then a validation of both the source and the material will also be conducted. Collation is described by ACPO as:

> “*the organisation of material into a variety of formats that best facilitate analysis. Examples of these include:*

[86] A legal memo from the U.S. Attorney General’s office (Byebee, 2002) to the CIA, authorising water boarding and other techniques for use during Abu Zubaydah’s interrogation, demonstrates the depth of consideration which was undertaken before authorising the techniques. For a contemporary account of the use of interrogation techniques used after the 2003 invasion of Iraq, see Lagouranis’ account of working as an interrogator at Abu Ghraib prison (Lagouranis, 2008). The book also details the various interrogation approaches used by the U.S. Army, explaining what each one aims to achieve and how and why it can be effective.

> *• Charts;*
>
> *• Spreadsheets;*
>
> *• Tables;*
>
> *• Databases;*
>
> *• Maps;*
>
> *• Commodity flows including financial material;*
>
> *• Communication flow and frequency charts.*
>
> *It is essential that such products are not considered to be the final analytical product. The evaluation and subsequent interpretation of collated material are the key processes that change material into analysis*" (ACPO, 2006:66).

Collation often involves a high degree of manual manipulation of data by dedicated staff or, more usually nowadays, by analysts themselves. The employment of analytical tools such as i2 Analyst Notebook across the Intelligence community has blurred the lines between collation and analysis, as a considerable proportion of collation work could arguably be classed as preliminary analysis. Collation assumes high importance in counter-terrorism in the last two examples in the ACPO list above, as it is the analysis of this information which results in so much actionable Intelligence.

The tracking of terrorist financing is a key enabler in counter-terrorism work, but it is a specialist skill as the financial analyst needs a comprehensive understanding of how the international banking systems function, and how money is moved electronically between accounts and across borders and jurisdictions. The collation of financial transaction data can be time-consuming but it is a vital part in an investigation. Accurately depicting and labelling the paths of currency movements between accounts, individuals, banks and countries is all necessary to understand the money flow. Perri *et al* (2009:25) note that if the Police knew how terrorists were creating and obtaining their funding, they would gain the ability to penetrate or disrupt the group before any terrorist acts were committed. A sample i2 Analyst Notebook chart showing the analysis of an insider trading crime is shown at Annex E (Visual Analysis, n.d.).

The reading of all the available material may appear to be the *sine qua non* of the collation process but it is often overlooked. This omission has increased in line with the increase in the quantity of data now available for searching. The reading of collated material can serve as a coarse filter, showing the analyst which information gaps exist, which gaps could be filled quickly and simply, and which gaps may require more work in order to close them. In the early 1980s most of the British Army's information on the Warsaw Pact armed forces was extremely well organised, meticulously catalogued and usually available in printed form, but there was no easy way to search for information. Some Intelligence stations used 6" x 4" record cards for common queries but most searches involved a great deal of time spent in reading the various working aids. Some stations had full-time collators who knew their targets intimately and could quickly locate Intelligence almost on demand.

Since then, the situation has changed beyond recognition. We are now in the era of what the large technology companies call "big data", where there is a plethora of information available but one of the main difficulties encountered is in having the right tools, the access and the knowledge to be able to retrieve the required information (Duijvestijn et al., 2014). A key requirement in the counter-terrorism field is often described as "*blowing away the hay, to help reveal the needle*", which requires the ability to aggregate, sift and search huge quantities of electronic material held in a variety of repositories. As Gannon (2008:217) observes: "*The IC [Intelligence community] in one generation passed from an information-scarce environment to an information-glut environment. Major advances in technical collection provided more data than analysts could exploit.*"

Spreadsheets still have a very important role to play in collation and analysis and they remain a cornerstone of analytic product. Even the most basic spreadsheet allows data to be manipulated in ways which can reveal patterns, or can make more sense of a large amount of data. Users with a more advanced level of spreadsheet training can extract still more value by using tools such as pivot tables and modelling techniques. Spreadsheets are especially valuable in telephone call record analysis and they can be used to create timelines without the need for specialist charting software.

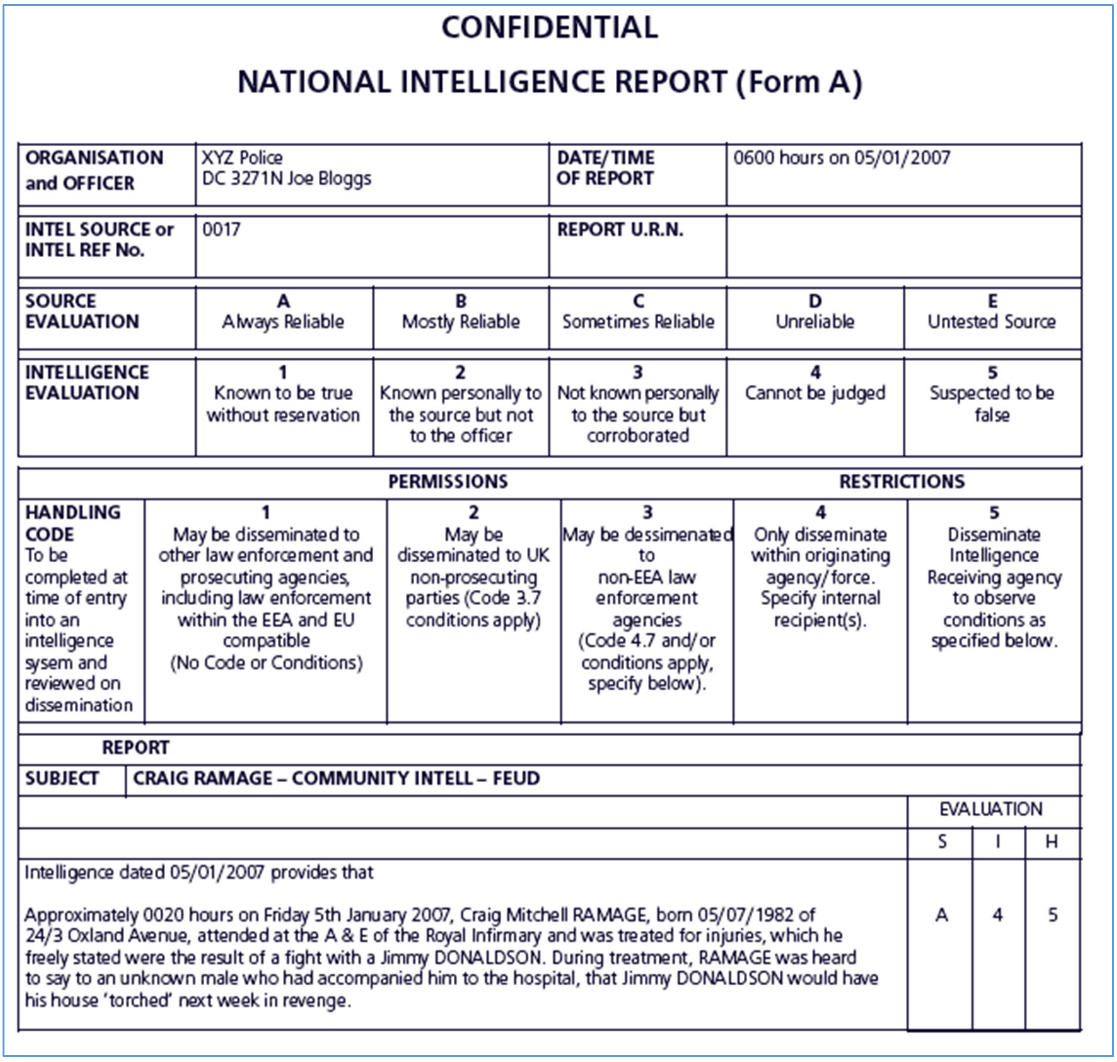
Databases are one of the most powerful tools available to the counter-terrorism analyst for collation purposes. The counter-terrorism collator or analyst will routinely access a multitude of closed databases accessible only to the Police and the Intelligence agencies. A sample of these databases and their potential uses is provided in the table below, but it should be noted that this is only a selection. Many more are used, especially in the areas of covert Intelligence.

Automatic Number Plate Reading (ANPR) Intelligence
Crimelink
Police National Computer
Child Protection Records
Telecommunications data (billing records, call records, etc.)
Custody data
National Method Index
Forensic Data
VODS/QUEST (Vehicle Online Descriptive Search), (Query Using Extended Search Techniques)
Prison Liaison
Sex Offenders Data
Special Branch
Central Ticket Office
Safety Camera Unit
Roads Policing Unit/Strategic Roads Unit
Aliens Department
Stop and Search database
BADMAN (Behavioural Analysis Data Management Auto-
Indexing Networking)
CATCHEM (Centralised Analytical Team Collating Homicide Expertise and Management).
Congestion Charge Database (Transport for London)
Benefits Agency Organised Fraud Investigation Data
DVAL (Driver Vehicle Licensing Authority)
Europol (European Law Enforcement Organisation) and INTERPOL
Forensic Intelligence Bureau (Part of the Forensic Science Service)
HMRC (Her Majesty’s Revenue and Customs)
IND (Immigration and Nationality Directorate)
HOLMES and HOLMES 2
Inland Revenue Data
Land Registry data
NFFID (National Firearms Forensic Intelligence Database)
VISOR (Violent and Sex Offenders Register)
UKPS (UK Passport Service)

Table 4 Sample of closed databases

5.4 Evaluation

Compared to other parts of the Intelligence cycle, evaluation has probably had the most negative press. This is mainly due to the criticisms levelled against the Intelligence which was used as a key factor in the UK government's decision to commit troops to the 2003 invasion of Iraq. The Butler Report (2004) provided the very detailed analysis of this Intelligence. The criticisms originated in the pre-invasion unease which was publicly debated by the Cabinet, the opposition, the media and the public, concerning the legal and moral justification for the UK going to war with Iraq in 2003. The UK's system used for the evaluation of information and Intelligence in the Police is commonly known as the "five by five by five" system (usually written as 5x5x5). The name comes from the construction of a Police National Intelligence Report, which has three separate evaluation criteria, each of which has five potential options. A sample report (The Scottish Government, 2012:, sec.4.14) is shown below:



CONFIDENTIAL

NATIONAL INTELLIGENCE REPORT (Form A)

ORGANISATION and OFFICER	XYZ Police DC 3271N Joe Bloggs	**DATE/TIME OF REPORT**	0600 hours on 05/01/2007
INTEL SOURCE or INTEL REF No.	0017	**REPORT U.R.N.**	

SOURCE EVALUATION	**A** Always Reliable	**B** Mostly Reliable	**C** Sometimes Reliable	**D** Unreliable	**E** Untested Source
INTELLIGENCE EVALUATION	**1** Known to be true without reservation	**2** Known personally to the source but not to the officer	**3** Not known personally to the source but corroborated	**4** Cannot be judged	**5** Suspected to be false

		PERMISSIONS			**RESTRICTIONS**
HANDLING CODE To be completed at time of entry into an intelligence sysem and reviewed on dissemination	**1** May be disseminated to other law enforcement and prosecuting agencies, including law enforcement within the EEA and EU compatible (No Code or Conditions)	**2** May be disseminated to UK non-prosecuting parties (Code 3.7 conditions apply)	**3** May be dessimenated to non-EEA law enforcement agencies (Code 4.7 and/or conditions apply, specify below).	**4** Only disseminate within originating agency/force. Specify internal recipient(s).	**5** Disseminate Intelligence Receiving agency to observe conditions as specified below.

REPORT			
SUBJECT **CRAIG RAMAGE – COMMUNITY INTELL – FEUD**			
	EVALUATION		
	S	I	H
Intelligence dated 05/01/2007 provides that Approximately 0020 hours on Friday 5th January 2007, Craig Mitchell RAMAGE, born 05/07/1982 of 24/3 Oxland Avenue, attended at the A & E of the Royal Infirmary and was treated for injuries, which he freely stated were the result of a fight with a Jimmy DONALDSON. During treatment, RAMAGE was heard to say to an unknown male who had accompanied him to the hospital, that Jimmy DONALDSON would have his house 'torched' next week in revenge.	A	4	5

16 Example of a National Intelligence Report (5x5x5)

Guidance from ACPO (NPIA, 2010:49) on information sharing provides a necessarily lengthy explanation of what ACPO considers evaluation to be, and why it is important:

> "*Police information will undergo a form of evaluation appropriate to the policing purpose for which the information was collected and recorded. All police information, particularly that which comes from Intelligence, is evaluated to determine*

> *its provenance, accuracy, continuing relevance to a policing purpose and any action to be taken. Provenance is the ability to determine the reliability and credibility of the source, and the value of the content of the information. The evaluation process determines the type of action that should be taken on the information. Action may include an immediate response, further development of the information, whether to share the information with others or deciding not to do anything with the information at that point in time, subject to review. Evaluation should be proportionate to the nature of the information*".

First to be evaluated is the source of the Intelligence. In HUMINT, this will reflect the evaluation of the actual Human Source providing the information, not the person or persons who the source obtained that information from. For example, CHIS A meets his Handler and tells him that one of his colleagues, B, wants to find a jihadist group in the UK, so he can "contribute something useful to the war". The information has come from a regular meeting which A has with a group of associates, some of whom talk with admiration about jihadist groups. When the Handler writes his report after the meeting, he must evaluate the source of the information, which is CHIS A, not colleague B. He must grade the information according to his previous experience in handling CHIS A, the previous reliability which A's information has shown, and the overall perceptions of the Handler (and Co-Handler if appropriate) regarding A's reliability as a source. The second criterion is where the content of the information or Intelligence itself is evaluated, and it is here where the Handler may use his own knowledge and experience, in addition to what the CHIS has told him, to grade the information. Finally, the third criterion is the handling and dissemination protocols which the originator of the report deems to be the most appropriate for the information (or in some cases it will be the protocol dictated by policies). Reports containing terrorism-related information or Intelligence are more tightly controlled than most other Intelligence reports, and dissemination is usually strictly limited. The originator of the report can keep the information ring-fenced within the originating agency by selecting number 4. For very sensitive information he can select number 5, which strictly limits dissemination to the original distribution list. The standard matrix used to select source evaluations by the UK Police is provided below (The Scottish Government, 2012):

A Always Reliable	B Mostly Reliable	C Sometimes Reliable	D Unreliable	E Untested Source
1 Known to be true	2 Known personally to source but not to officer	3 Not known personally to source but corroborated	4 Cannot be judged	5 Suspected to be false or malicious
1 May be disseminated to other law enforcement and prosecuting agencies	2 May be disseminated to UK non-prosecuting parties	3 May be disseminated to non EEA law enforcement agencies (special conditions apply)	4 Dissemination within originating agency only	5 No further dissemination

Table 5 Breakdown of the evaluation variables in the National Intelligence Report (5x5x5)

Harfield (2008:65) says of evaluation that it: "*asks simply, to what extent can we believe each different piece of information before us? The faith invested in each individual item of information determines the influence it exerts in the overall interpretation of all the information available*". His description is succinct and serves as a working definition of what should be contributed by the process of evaluation. Harfield neatly links the perceived provenance of information with the influence which it carries with it. SIS has long used an evaluation process in its HUMINT work and it was this evaluation of HUMINT material which would come under such close scrutiny in the post-invasion governmental inquiry chaired by Lord Butler. Initially using the term validation rather than evaluation, Butler set the scene in his opening chapter. He described the questions he expected an Intelligence agency to ask of itself, when evaluating the information it had gathered. Butler's view (2004:23) of this validation process, while longer than Harfield's, is one of the best summaries available:

> "*The validation of a reporting chain requires both care and time, and can generally only be conducted by the agency responsible for collection. The process is informed by the operational side of the agency, but must include a separate auditing element, which can consider cases objectively and quite apart from their apparent Intelligence value. Has the informant been properly quoted, all the way along the chain? Does he have credible access to the facts he claims to know? Does he have the right knowledge to understand what he claims to be reporting? Could he be under opposition control, or be being fed information? Is he fabricating? Can the bona fides, activities, movements or locations attributed to those involved in acquiring or transmitting a report be checked? Do we understand the motivations of those involved, their private agenda,*[87] *and hence the way in which their reports may be influenced by a desire to please or impress? How powerful is a wish for (in particular) financial reward? What, if any, distorting effect might such factors exert? Is there – at any stage – a deliberate intention to deceive? Generally speaking, the extent and depth of validation required will depend on the Counter-Intelligence sophistication of the target, although the complexity of the operational situation will affect the possibility of confusion, misrepresentation or deception*".

[87] This was particularly relevant in the case of Ahmed Chalabi, who had provided Intelligence on Iraq to the U.S. agencies for years, but whose political ambitions often meant that the information he provided was distorted, either deliberately or unwittingly (Jehel, 2004:2).

In a highly unusual and hitherto unprecedented public speech, the then Head of SIS mentioned Butler's concerns about the effectiveness of HUMINT evaluation and agreed with his criticism, saying that the report "…*was a clear reminder, to both agencies and the centre of Government, politicians and officials alike, of how Intelligence needs to be handled*" (Sawers, 2010). Butler's criticisms (2004:116) of SIS source evaluation procedures was measured and non-emotive. He wrote that he had been led to question SIS's standard procedures for checking on the validity of their human sources, the quality control procedures employed in their reporting, and whether these standard procedures were actually adhered to, in the production of the Iraq-based Intelligence. In his conclusions he identified two factors which were the main contributors to the doubts with which the SIS Intelligence on Iraq was viewed: the first was the actual implementation of the validation process, and the second was the inadequate resourcing of it (2004:152).

5.5 Analysis

The analysis stage can be as brief as examining a list of numbers called by a target, in order to scan for a known number, or it can be so lengthy as to require months or years of effort by teams of analysts working to identify and locate an individual or individuals.[88] The area of Intelligence analysis is one of the most widely written about areas in the Intelligence cycle. Examining the works of various writers on Intelligence provides an idea of why analysis appears to be such a divisive topic for practitioners and academics alike.

[88] An example of the latter would be the analytical effort devoted to positively identifying, locating and interdicting Abu Musab Al Zarqawi, a prolific terrorist who operated in Iraq between 2004 and 2006. In the two years in which Zarqawi was operationally active in Iraq, the UK and U.S. Intelligence agencies (among others) dedicated several entire teams to the task of locating and capturing or killing him. Following Intelligence provided by an informant, coalition forces were able to locate his spiritual adviser, Sheikh Abd-al-Rahman, who was placed under surveillance and who was eventually tracked to a safe-house on the outskirts of Baqubah, where he held a personal meeting with Zarqawi. Once Zarqawi was positively identified, an airstrike was conducted on the building, using two air-launched 500-lb bombs. Zarqawi was pulled out alive, but died almost immediately afterwards, not surviving the airlift to hospital. The U.S. government stated that the operation to locate him "*did not occur in a 24-hour period. It truly was a very long, painstaking, deliberate exploitation of intelligence, information- gathering, human sources, electronic, signal intelligence that was done over a period of time - many, many weeks - that led us last night to that target*" (Caldwell, 2006). The Intelligence effort to locate Osama bin Laden took even longer than that to locate Zarqawi.

Lowenthal, a former Assistant Director of Central Intelligence for Analysis and Production (IAFIE, 2014), considers the literature on Intelligence analysis to be rich (2003:96). Gentry (1993:207) on the other hand, considered it to be a much smaller realm some 22 years ago, "*filled with judgments and assertions at variance with ...reality*", illustrating how far the literature has advanced in this area. Definitions of Intelligence analysis have covered a wide area and have been crafted with reference to "*the sources and classifications of information, processes, purposes, individual and organizational efforts, and consumers*" (Mangio & Wilkinson, 2008:3). LeFebvre (2004:11) provides a detailed definition of Intelligence analysis, of his own crafting, which he describes thus:

> "*Intelligence analysis is the process of evaluating and transforming raw data acquired covertly into descriptions, explanations, and judgments for policy consumers. It involves assessing the reliability and credibility of the data and comparing it to the knowledge base available to the analyst to separate fact from error and uncover deception. Each collected item is then examined to determine its nature, proportion, function, relevancy, and interrelationships. Related items will be grouped together and the extent to which they confirm, supplement, or contradict each other will be determined. Once done, the relevant information will be synthesized in order for the analyst to make predictions, gain insight, identify information gaps, or explain a complex set of facts and relationships*".

His definition captures much of the analytical process, particularly the transforming of raw product into something which can assist the decision-making processes of those whom he considers "*policy consumers*" (Lefebvre, 2004:11). Another key item in his definition is that outputs should somehow have a transformative effect, such as providing a better understanding of relationships, or a clearer picture of a timeline. LeFebvre's definition is one of the most useful definitions of Intelligence analysis available in the current academic literature of Intelligence studies. He continues with another theory, that most analysis is predictive and therefore follows a simple pattern, namely that it "*describes what is known…it highlights the interrelationships that form the basis for the judgments…it offers a forecast*" (Lefebvre, 2004:112).

The relationship between what Intelligence reports, and the subsequent decisions to take action based upon it, is complex and frequently misunderstood. This is especially the case with civil servants who often receive Intelligence product for the first time, when they are more advanced in their career. A number of them will only remain in such a role for one tour before moving on to another role. During the delivery of Intelligence training overseas, a foreign Intelligence officer asked why the Intelligence being produced did not include a course of action, or a recommendation for interdiction. This simple question resulted in around 20 hours of classroom discussion about the collection, the analysis and the dissemination of counter-terrorism reporting. It was a useful reminder about the importance of Intelligence speaking truth unto power, yet not making the decision for the policymaker.[89]

Two analytical processes have entered the academic discussion of analysis since at least the mid-1980s. These are generally defined as "bottom-up" and

[89] The quotation "*speak truth unto power*" is widely used in the UK Intelligence community. Its exact origins are uncertain, and it is often attributed to Sir Winston Churchill, but the most probable source of the original quote is from the Quaker movement in the 18th Century. An expanded extract explains this as follows (Cary et al., 1955:1): "*Our title, Speak Truth to Power, taken from a charge given to Eighteenth Century Friends, suggests the effort that is made to speak from the deepest insight of the Quaker faith, as this faith understood by those who prepared this study. We speak to power in three senses: To those who hold high places in our national life and bear the terrible responsibility of making decisions for war or peace. To the American people who are the final reservoir of power in this country and whose values and expectations set the limits for those who exercise authority. To the idea of Power itself, and its impact on Twentieth Century life. Our truth is an ancient one: that love endures and overcomes; that hatred destroys; that what is obtained by love is retained, but what is obtained by hatred proves a burden. This truth, fundamental to the position which rejects reliance on the method of war, is ultimately a religious perception, a belief that stands outside of history. Because of this we could not end this study without discussing the relationship between the politics of time with which men are daily concerned and the politics of eternity which they too easily ignore*". It remains one of the most compelling instructions to an Intelligence community. A more detailed explanation can be found on http://www.quaker.org/sttp.html accessed on 01 August 2012.

"top down" analysis. The most authoritative writing on this is by Schum and others, whose work encompasses a wide area which includes Intelligence analysis, hypotheses and legal argument. Schum (1988:52) describes the bottom-up model as one in which "*reasoning proceeds from observable evidence to possible conclusions*" and describes the top-down model as one in which "*a possible conclusion allows us to generate a chain or hierarchy of events leading to one or more potentially observable events whose occurrence or non-occurrence would be evidence bearing upon our possible conclusion*". The focus of each model is also different, with the bottom-up model being data driven, and the top-down model being inference driven.[90] The bottom-up model is much more common within the UK Intelligence community, particularly in counter-terrorism, although these terms are rarely used in the UK community. The data-driven emphasis of the "bottom-up" approach concentrates on the information collected, highlighting any gaps to drive additional collection, and including a critical evaluation of the data made.

The critical evaluation should ideally lead to a subsequent hypothesis (or hypotheses) which can be tested. Naturally, hypotheses can also appear during the collection phase, or during the initial reading of the material, in the collation phase. They do not necessarily fit into the neatness of an academic plan for their creation. This is how the majority of the UK's Intelligence machinery functions and it appears to be effective. The top-down method has been criticised by some Intelligence academics, such as Ryan (2006) and Johnson (2005), as it takes a hypothesis as a starting point and tests the data against the hypothesis. Johnson (2005:22–23) takes issue with the top-down approach, saying:

> *"What tends to occur is that the analyst looks for current data that confirms the existing organizational opinion or the opinion that seems most probable and, consequently, is easiest to support.... This*

[90] Schum (1988:20) also writes on the differences between deductive, inductive, and abductive reasoning, all of which have direct relevance to the field of Intelligence analysis, especially regarding the way in which an analyst might approach a given problem.

> *tendency to search for confirmatory data is not necessarily a conscious choice; rather, it is the result of accepting an existing set of hypotheses, developing a mental model based on previous corporate products, and then trying to augment that model with current data in order to support the existing hypotheses*".

In academic terms, this in itself may not necessarily be a negative factor, and it has clear uses in social science research. In the field of counter-terrorism Intelligence, however, this method leaves analysts open to two particularly dangerous pitfalls. Firstly, it can encourage an analyst to "make the facts fit the story", a common media criticism. If one starts with a hypothesis, and initial analysis appears to confirm the analysis, it can have a blinding effect on the analytical process. That process could then suffer from impediments such as linkage blindness, groupthink and bias.[91] Secondly, such an approach can actually facilitate analysts being given one particular hypothesis for investigation, which at the extreme end of the scale paves the way for accusations of the politicisation of Intelligence.

In the post-2003 period following the UK governmental inquiries into the Intelligence process and the Iraq war, accusations of encouraging the politicisation of Intelligence are something which no agency wants to find itself on the receiving end of. Ryan (2006:309) believes that credibility problems could be reduced by the avoidance of this hypothesis-based analysis which she considers "*lends itself well to extreme politicization of Intelligence".* Her critical examination of this hypotheses-based analysis cites the example of

[91] Linkage blindness is generally considered to have been identified as a pathology of Intelligence by Professor Steven Egger (Egger 1984; Egger 1999; Egger 1992). Janis (1972), a Yale University psychologist, detailed the concept of "groupthink" in 1972, after studying the abortive "Bay of Pigs" operation to overthrow Fidel Castro's regime in Cuba. In his paper, Janis described how it was possible for a group of individuals, working collectively on a problem, to actually decide upon the worst possible outcome, as their combined decision. In brief, Janis postulated that loyalty to the group often becomes the highest motive for the members of the group, and this in turn acts as a powerful disincentive for an individual to speak out against the direction the rest of the group is taking. Professor Heuer (1999) published an internal paper for the CIA in 1999, originally classified as SECRET, which analysed the psychological processes which affect the work of Intelligence analysts. A declassified version of this work was later released to other agencies. This author referred to Heuer's work extensively while working on counter-terrorism cases. Heuer's work is widely considered to be the definitive work on how psychological processes impact upon our ability to process and analyse information in the Intelligence field. His chapters on bias (Chapters 9-13) cover all the various types which analysts experience.

the US-produced National Intelligence Estimate (NIE) on Iraqi Weapons of Mass Destruction (Walpole, 2002), which played a fundamental role in the U.S. decision to invade Iraq in 2003. Describing the period immediately preceding the 2003 invasion of Iraq, Ryan (2006:287) states:

> "*Rather than constructing a 'fact-based hypothesis', the Pentagon's Office of Special Plans (OSP), followed to a significant degree by the CIA particularly in the pivotal National Intelligence Estimate (NIE) of October 2002, designed an (sic) 'hypothesis-based analysis', which started with a preferred scenario and then found data that might support that. In effect, it was a worst-case scenario presented as a probability.*"

Johnson (2005:22) agrees with Ryan, tackling the subject directly and pointing out this tendency for an analyst to look for facts which fit a theory, rather than looking at facts and deducing meaning from them:

> "*What tends to occur is that the analyst looks for current data that confirms the existing organizational opinion or the opinion that seems most probable and, consequently, is easiest to support.... This tendency to search for confirmatory data is not necessarily a conscious choice; rather, it is the result of accepting an existing set of hypotheses, developing a mental model based on previous corporate products, and then trying to augment that model with current data in order to support the existing hypotheses.*"

Analysis is sometimes shown as "Analysis/Processing". This is due to the amount of electronic processing which now takes place in order to turn a large proportion of information collected into a format that is understandable and useable by analytical staff. The term “processing” can be ascribed to a variety of both automated and manual workings which can include decryption, translation of material from the original language, as well as the conversion or enhancement of audio-visual files, among others. The importance of processing in the Intelligence cycle can be gauged by a comment from a former Director of NSA. When asked by Loch K. Johnson what were the three biggest problems facing his agency, he replied; “*processing, processing, processing*” (Johnson, 2006:120). Due to the highly sensitive nature of this topic, processing is not covered in further detail in this paper.

5.6 Dissemination

The dissemination of product is the final stage of the Intelligence cycle and usually consists of some kind of report being issued to the customers. At the tactical end of the scale, this can be as brief as a formatted “tipper” consisting of a single paragraph to alert customers to time-sensitive material. At the opposite end of the scale, a strategic report can stretch to several thousand pages of dense material, such as a classified, all-source country profile.[92] Some reports are single-source, an example of which would be a HUMINT report describing a meeting of Intelligence interest, attended by the source. Other reports are all-source, such as a terrorist profile which could contain relevant Intelligence information from a variety of collectors, including HUMINT and surveillance.

Since at least 1990, the “Intelligence support to the war fighter” initiative has aimed to push actionable, sanitised Intelligence down to the lowest possible levels which require it. This initiative was important as it was the real starting

[92] The author has worked on such strategic papers, some of which were built up over many years. It is not uncommon for an Intelligence specialist to spend several years covering one or several countries, mainly updating and expanding such country profiles.

point of the move towards sanitising an Intelligence product to the lowest level for use, instead of the classification of the Intelligence report being immovably applied.[93] Today this has been refined into the “tear line report”, a system which enables a finished Intelligence report to be written at two or more levels of classification. A section below the tear line is produced at the lowest suitable level, and enables the Intelligence staff to simply detach the lower part of the report and to hand it to tactical assets for operational use. This system is now widely used in NATO, and the same system is also used among the coalition nations contributing forces and assets to the International Security Assistance Force (ISAF) in Afghanistan.

Nowadays, UK Intelligence reports usually include some kind of feedback mechanism, to provide customers with a vehicle for stating whether a particular report met their requirements, and if not, why this was the case. Some models of the Intelligence cycle include feedback as a component part, while others either leave it as an implied factor, or include it as a dotted “feedback loop” between some or all of the components of the cycle. Among the elements of the UK Intelligence community, there exist both formal and informal feedback mechanisms. Formal feedback is often an integral part of a report, most often placed at the end of the content. This format usually asks readers a set of questions, requesting customers to grade topics such as relevance and timeliness, whether or not they found it useful and if they would be interested in further reports on this or similar topics.

Alongside the formal mechanism for customer comments, an informal mechanism also takes place and this is just as important as the formal system. In the decade from 2000-2010 in particular, inter-agency liaison and inter-departmental co-operation increased significantly among the UK’s secret Intelligence agencies. Individual analysts, case officers and other specialists are continuously building their own personal networks with their colleagues in

[93] To the Author’s knowledge, this was the first occasion on which this “Intelligence support to the war fighter” was actively embraced by the Intelligence elements of the UK’s Armed Forces.

other agencies, and discussing cases, Intelligence access, best practice, problems and opportunities.

Customer comments have become invaluable in helping collectors, analysts and reporters to refine their understanding of customers' requirements. This commentary mechanism assists an agency with its internal auditing, allowing it to streamline the degree of fit between tasking, collection, analysis and reporting. At the same time, it allows valuable feedback from other agencies. While these feedback mechanisms are important on a daily basis, another tool introduced by the Intelligence agencies during the past decade was score carding. Similar to the process used within corporate companies, score carding allows representatives from one Agency to meet formally with representatives from another agency or agencies, to discuss the Intelligence reports it has issued. Usually carried out on a monthly basis, this process encourages a frank assessment of all the issued product of a department or a team. The score carding results in a percentage score for the agency producing the Intelligence reports. The results are then fed back to the team or department, providing a detailed critique of the accuracy, usefulness and timeliness of the Intelligence. When working in a team providing direct support to another Intelligence agency, this score carding mechanism was invaluable in helping the team to ensure that their collection and reporting was aligned with the needs of the external customer.

Within the UK Intelligence community, dissemination has traditionally been conducted using the "need to know" principle. Until April 2014, this was defined by the Cabinet Office (2011) in Her Majesty's Government Security Policy, through the framework of the Government Protective Marking System, as the principle that "*access must only be granted to those who have a business need and the appropriate personnel security control (BPSS or National Security Vetting)*". The principle of need to know is at the heart of Intelligence sharing and is fundamental to the security of all protectively marked Government assets, as the allowing of casual access to government protectively marked assets is never permitted.

This principle underwent some revisions during the decade of the 2000s, and although these do not appear to have been formally codified, the expanded version being communicated downwards to become "*need to know – need to share – need to hold*". This expands the principle to include a check on whether someone who has this classified knowledge also needs to share it with others, or whether distribution should remain only to the original recipients. Need to hold was added as an aid to document security, partly to ensure that hoarding of highly classified documents does not take place and partly to ensure that no more copies of a highly classified document were in existence than were necessary. As the Commander of the United States Marine Corps said in 2005, "*It's not a technical issue any more. It's really more about culture and the "need to share" rather than the "need to know*" (Joint Chiefs of Staff, 2013:chap.V–2).

The GPMS system was replaced in April 2014 by a new system called the Government Security Classifications Policy (GSCP) (Cabinet Office, 2014) which replaced the previous five categories (TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, UNCLASSIFIED) with 3 main categories (TOP SECRET, SECRET, OFFICIAL) although the classification of OFFICIAL now has a sub-set of OFFICIAL-SENSITIVE. This sub-set is defined as covering information which "*could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media which can be applied*" (Cabinet Office, 2014:8). The principle of access, mentioned previously, was re-written as "Principle Three", which stated: "*access to sensitive information must ONLY be granted on the basis of a genuine "need to know" and an appropriate personnel security control*" (Cabinet Office, 2014:5).

Additional measures, such as special handling caveats, descriptors and codewords, can also be applied to further restrict dissemination of sensitive Intelligence. Special handling caveats cover especially sensitive areas such as some collection methods. Descriptors cover restrictions such as

“COMMERCIAL”, “LOCSEN” and “PERSONAL” (Cabinet Office, 2014:11).[94] Codewords add an additional layer of “need to know” protection, which further restrict access to, and dissemination of, an Intelligence product.[95] The new policy was introduced in the aftermath of a number of massive leaks of highly classified information which has had wide-scale implications for UK policy.[96]

The dissemination of Intelligence product is a perennial topic among Intelligence staff. The Australian government’s “Report of the Inquiry into Australia’s Intelligence Agencies” (known as the “Flood report”) (2004:7) provided a concise and useful summary of what the committee expected the dissemination of Intelligence to provide:

- “*Warning, notably of terrorist plans, but also of potential conflicts, uprisings and coups*
- *Understanding of the regional and international environment with which decision makers will need to grapple*
- *Knowledge of the military capabilities and intentions of potential adversaries, a vital ingredient in defence procurement and preparedness*

[94] The Cabinet Office (2014:para.21) defines the use of a descriptor as “…*to identify certain categories of sensitive information and indicate the need for common sense precautions to limit access…descriptors should be used in conjunction with a security classification and applied in the format: “OFFICIAL-SENSITIVE [DESCRIPTOR]*”. Three core descriptors are maintained by the Cabinet Office, and these are defined as follows: “*COMMERCIAL”: Commercial- or market-sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed. “LOCSEN”: Sensitive information that locally engaged staff overseas cannot access. “PERSONAL”: Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations, vulnerable individuals, or the personal / medical records of people in sensitive posts (e.g. military, SIA)*. The new policy from the Cabinet Office (2014:para.23) further dictates that information covered by descriptors cannot be sent to international partners, due to the potential for confusion.

[95] The Cabinet Office (2014:para.24) defines a handling codeword as “…*a single word expressed in CAPITAL letters that follows the security classification to providing security cover for a particular asset or event. They are usually only applied to SECRET and TOP SECRET assets*”.

[96] One of the most damaging Intelligence leaks in the USA’s modern history was the series of “Wikileaks” revelations entitled “The Afghan War Logs” and the “Iraq War Logs”. These consisted of more than 500,000 classified reports from the U.S. Military Intelligence network SIPRNET, and they were leaked along with a further 250,000 classified U.S. diplomatic cables. At the time of writing, the legal case against Specialist Bradley Manning, now legally known as Chelsea Elizabeth Manning, was concluded with Manning being sentenced to 5 years' confinement, reduction in rank to Private, forfeiture of all pay and allowances, and a dishonourable discharge. Manning will be eligible for parole after serving one-third of the sentence imposed. Many of the diplomatic cables covered topics and regions about which Manning had no “need to know”, in his Iraq-based role as a Military Intelligence Analyst. Had the correct systems been in place, his access would have been markedly more limited.

- *Support for military operations, minimising casualties and improving the environment for operational success*
- *Support for an active and ambitious foreign, trade and defence policy*
- *And beyond these vital roles of Intelligence in providing information, modern Intelligence can be a more active tool of government – disrupting the plans of adversaries, influencing the policies of key foreign actors and contributing to modern electronic warfare*."

The U.S. Armed Forces also produce finely detailed documentation on almost every area of the operational spectrum including military Intelligence. A U.S. Joint Publication by the Joint Chiefs of Staff (JCS) describes eight factors which are assessed as important for disseminated Intelligence products. They broadly follow the UK military principles, a fact not surprising given the high degree of joint working between the UK and U.S. Armed Forces in the period since the Second World War. These factors provide a sound checklist for Intelligence managers, prior to releasing an Intelligence report or product to consumers and customers. The JCS (2013:chap.II–7) list eight "attributes of Intelligence excellence".[97] This is an updated version of their previous concept of "five tenets of Intelligence". They consider that, in order to achieve the standards of excellence required, an Intelligence report should be:

1. Anticipatory (allowing commanders to
2. Timely
3. Accurate

[97] The full definitions of these eight attributes of Intelligence excellence, as considered by the JCS, can be found at Annex I

4. Usable

5. Complete

6. Relevant

7. Objective

8. Available

5.7 Summary

In its current form, the Intelligence cycle used by the UK Intelligence community is a simple, 6-stage process. This chapter conducted a detailed examination of these stages, describing what each stage means, how it is conducted and how it relates to, and functions in, the work of counter-terrorism. The chapter started with direction, or “tasking”, examining the UK’s political process and its role in Intelligence direction. This included the changes imposed in 2010, such as the establishment of a new coordinating body (the NSC) and a new Adviser position (the NSA), to better coordinate the work of the various agencies and departments involved. The throughput of this additional body and additional post, in the form of the National Security Strategy, were also covered. An explanation was provided, of how this dovetails with other strategies and other bodies, such as the Strategic Priorities for Secret Intelligence Collection which are promulgated by the JIC. Commentary from former politicians was provided, showing how individuals such as a former Home Secretary considered the nature of tasking and how the resources of the UK’s secret Intelligence agencies are then deployed in accordance with this. The method of categorising this direction into Intelligence Requirements was next described, showing how primary and secondary requirements are developed from the initial direction.

The next stage, collection, began with an expansion of some of the overt and covert sources and methods which can be deployed in this phase. A UK Police definition of “open” and “closed” Intelligence sources was provided, and the topic of single-source Intelligence was expanded upon, to explain some of the reasons why this is such a perennial topic, especially in the media. This section outlined why single-source Intelligence is not always a negative concept, using commentary from the Butler Report to reinforce this principle. Some of the limitations of the various sources and methods were also detailed, using examples to highlight how the various sources and methods work together in close collaboration in a counter-terrorism operation, such as the “cueing” by one source (e.g. covert surveillance) to notify another source or method to begin collection. The use of covert sources carries a high risk in counter-terrorism operations. Some of these risks were described in detail, such as the compromising of the source, or the target group dismantling their operation and relocating, thus forcing the Intelligence agencies to expend extra efforts just locate the group again.

Collation is often ignored or misunderstood, even by Intelligence professionals. As this section explained, it is a necessary part of the model. Beginning with a definition of collation by ACPO, this section provided a sample of some of the databases available to the UK Police, emphasising just how large the scale and scope of a simple query of available data sources could be. Unless all available data is gathered together at the initial stage prior to analysis commencing, there is a risk that the omission of a key facts could inadvertently skew the initial direction of an investigation. The importance of collation in military Intelligence was also covered, showing just how far technology has advanced in the last 30 years. It has moved from wooden trays of 6” x 4” record cards to 3-dimensional databases accessed by charting technology such as i2 Analyst Notebook, which can identify relationships between people/bank accounts/mobile phones and other entities and display this graphically.

The automation of tasks in the Intelligence process increases all the time, partly due to the vast volumes of information being searched through and partly due to the development and introduction of new techniques to speed up parts of the process. There is much debate within the Intelligence community about how far such automation can, and should, go. Despite the improvements brought about by technological developments, the human factor remains paramount and the Intelligence analyst, particularly in counter-terrorism, is unlikely to be replaced by machines in the near future. Goodman confirms this view, stating that "…*while the target may change, and the means by which Intelligence is procured will alter, the analyst will remain crucial*" (Goodman, 2011:275).

The process of evaluation was described in considerable detail, partly due to the very public debate which raged about this, following the UK's participation in the 2003 invasion of Iraq. The importance of the provenance of information was covered, explaining why the source of the information, as well as the information itself, must be evaluated in order for the cycle to function as accurately as possible. Butler's thoughts were provided, on the types of questions which he considered should be asked during the evaluation process. Some of the criticisms of the evaluation process carried out before the 2003 invasion were also described. Samples were provided of the current UK Confidential Intelligence Report and of the grading and evaluating system currently in use by the Police, the Armed Forces and the Intelligence agencies of the UK. This section finished with a quote from the Chief of SIS at the time, clearly indicating that he fully accepted the need for a robust evaluation process, in order to avoid the mistakes made prior to the 2003 invasion of Iraq.

The description of the sixth and final stage of the cycle, Dissemination, began with a brief comparison of the differences in a tactical report and a strategic report, before going on to explain how the dissemination of Intelligence has progressed in the last 30 years. It has advanced from the principle of need to know, through to the concerted push in 1990-91 for classified Intelligence to be sanitised so that it could be fed down to the lowest levels required, where action could still be taken on it. This section then covered the advance of Intelligence reporting to include the tear line report, which allows highly classified Intelligence to be sanitised to a much lower level, removing any reference or indicator to the source of the Intelligence, yet still providing the salient points of actionable Intelligence. The principle of customer feedback was also covered, and the section concluded with a comparative list from a U.S. Manual on Intelligence, containing the eight attributes of Intelligence excellence which the U.S. Joint Forces are expected to abide by in their Intelligence reporting.

The language used in a report can be a key factor in determining whether the disseminated report is misunderstood or not. Intelligence customers and consumers need to clearly understand that absence of evidence does not necessarily equate to evidence of absence. The Nicoll report (1981:para.58 cited in Goodman, 2007:20) identified this more than thirty years ago, noting:

> *"The Chairman of the JIC has made the point that readers of JIC reports may sometimes read more than is intended into a JIC report of 'no evidence'. In this field of indicator and warning intelligence, where aggressors will do their best to conceal their preparations, it is especially important for the JIC to make it clear how far we would expect to receive evidence, and how far 'no evidence' simply means an absence of information*".

No model is infallible and the next chapter considers the relative strengths and weaknesses of the Intelligence cycle, complete with the addition of primary source material. The opinions of more than a dozen serving or retired Intelligence practitioners are used in the following chapter to add a unique perspective on how the cycle functions in actual counter-terrorism work, and how these practitioners view the model in their various roles.

Chapter 6 Strengths and Weaknesses of the Intelligence Cycle

> "*If we are to think seriously about the world, and act effectively in it, some sort of simplified map of reality, some theory, concept, model, paradigm, is necessary*" (Huntington, 2011:29).

This chapter builds upon the theoretical framework, the detailed analysis of the Intelligence cycle and the policy framework of the CONTEST strategy. It considers the relative strengths and weaknesses of the model, using another author's critical paper (Hulnick, 2006) as a framework, and overlaying these criticisms onto the UK's 6-stage model. Various challenges and vulnerabilities are then detailed, as perceived by a number of prominent authors in this field. The ground-breaking work of Sheptycki's classification of Intelligence pathologies (Sheptycki, 2004) is described, to provide a comprehensive overview of some of the perceived weaknesses within the Intelligence process. Redressing the balance of analysis, the strengths of the model are then discussed.

6.1 Weaknesses of the Intelligence Cycle

Identifying and analysing weaknesses in the Intelligence cycle is not a simple task as many factors identified as vulnerabilities of the model are not actually components of the model itself, rather they are often behaviours which directly influence the model. A former U.S. Intelligence officer, Hulnick is now a Professor of Intelligence studies (Boston University, 2014). He authored a paper which criticised the concept of the Intelligence cycle and is therefore the most appropriate paper to use for an analysis of some arguments against the Intelligence cycle. In his opening abstract (Hulnick, 2006:959) he presents the following arguments against the model:

> "*In the modern era, almost all intelligence professionals will study the Intelligence Cycle as a kind of gospel of how intelligence functions. Yet it is not a particularly good model, since the cyclical pattern does not describe what really happens. Policy officials rarely give collection guidance. Collection and analysis, which are supposed to work in tandem, in fact work more properly in parallel. Finally, the idea that decision makers wait for the delivery of intelligence before making policy decisions is equally incorrect. In the modern era, policy officials seem to want intelligence to support policy rather than to inform it. The Intelligence Cycle also fails to consider either counter-intelligence or covert action. Taken as a whole, the cycle concept is a flawed model, but nevertheless continues to be taught in the U.S. and around the world*".

Hulnick's approach to this paper is understandably a US-centric one, but his paper has importance not least because some of his criticisms of the model are echoed elsewhere (Davies et al., 2014; Davies, 2002; Richards, 2014). It is worth examining the individual components of Hulnick's abstract with a UK-centric lens to ascertain how accurately, if at all, these components map to the UK experience of the model as used within the counter-terrorism sphere. Within the context of UK counter-terrorism, the Intelligence cycle is an accurate descriptor of the processes which take place within it. As chapter 5 covered in detail, the classic depiction of the cycle only shows the progressive movement from one stage to the next. The feedback loops are traditionally explained as sub-processes which can happen at any stage of the cycle, and do not necessarily have to revert to the preceding stage.

A feedback loop can take the process back to any stage as far as the start and this happens frequently in the actual work carried out by the agencies. For example, direction may be given to collect Intelligence on a named individual who is suspected of material involvement in terrorist activities. The collection process begins and while this is ongoing, the collation process would also be carried out. The combined data resulting from the collection and collation would be analysed and evaluated, possibly as part of a wider, ongoing investigation. As the picture on the individual is built up, it may become apparent to the analyst that the named individual is unlikely to be involved in the suspected activities because of the pattern of life, movements and other evidence of the individual's daily activities. The case would be discussed internally, and could possibly require a multi-agency discussion involving other partner agencies. A decision may be taken to remove the individual from the collection plan. This decision would be communicated to the originator of the direction, whereupon new instructions may be given to target a different individual. Conversely, no new individuals may be added to the collection plan, but an instruction may be provided to continue with the ongoing investigation.

Hulnick's next criticism is that policy officials rarely give collection guidance. This comment muddies the waters somewhat, when considering this from the UK perspective, as Hulnick has used the second phase of the UK cycle (collection) instead of the first phase (direction). In the case of the UK if we assume that by "policy officials" Hulnick would mean the senior political leadership, both elected (such as the Prime Minister) and non-elected (such as the Permanent Under-Secretary of State (PUS)), his point would be correct. Policy officials such as these do not usually provide detailed collection guidance, as this is not their function. This would then flow down to the Directors of the Intelligence agencies and onto their staff. This guidance would come as a result of the process of the JIC, as the Chairman of the JIC reports directly to the Prime Minister for the overall supervision of the JIC's output.[98] The JIC produces its list of priority collection requirements, and the agencies collect against these requirements. Moving Hulnick's criticism back one stage to "direction" (which is where it was most likely aimed), it is an inaccurate criticism when applied to the UK cycle as the UK model does receive direction from policy makers, which is then translated into a collection strategy within the agencies. Chapter one of this paper described the UK's Intelligence machinery in detail and it is clear from this that the task of collection, unlike direction, is not one which sits under UK policy officials within government.

His next point states that "collection and analysis, which are supposed to work in tandem, in fact work more properly in parallel". Both parts of this statement can be said to be true in the UK model. It can be argued that this is a necessary function of the cycle, and that this is a common misunderstanding of the model often criticised by opponents of the concept of Intelligence work being carried out according to a cyclical model. Yet the model was designed to be a simple, functional and easily memorised process primarily aimed at military Intelligence staff. The current, 6-stage cycle still adheres to this principle.

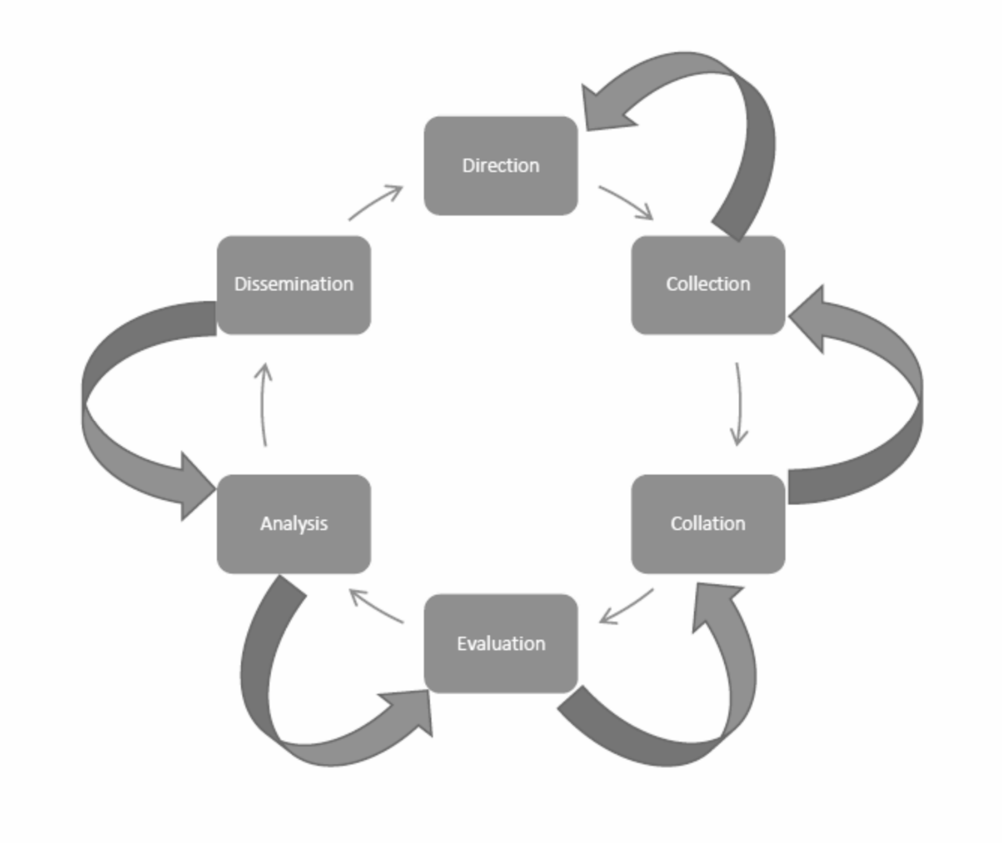
Where a common misunderstanding frequently occurs is that, in depicting the cycle as a circular process with 6 stages, it can be interpreted as meaning that one stage cannot start until the preceding stage has finished, and at the point when the cycle moves on to a new stage, the preceding stage must, by definition, have ceased completely. This is not the case. Intelligence staff who undergo formal training in Intelligence, which necessarily includes the cycle, are not simply provided with a 6-stage, cyclical model and told to follow each stage in isolation, ending one stage completely before moving onto the next stage. The cycle is usually depicted in its current form for simplicity,

[98] See Chapter 1.4

particularly when students new to the field of Intelligence work are being instructed.[99]

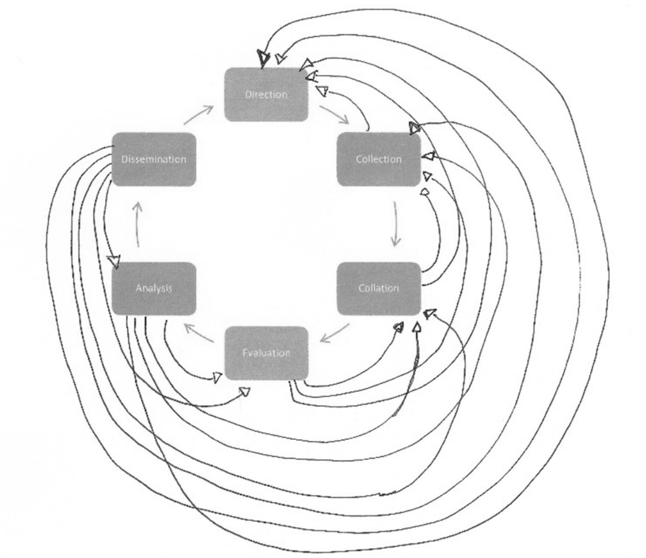
The detailed descriptions of the cycle, however, include a considerable amount of time devoted to the explanation of the feedback mechanisms upon which the model relies upon in real life. The instructor usually draws these by hand, to explain how the cycle can move back to any preceding stage, including all the way back to the start, as discussed in the above paragraph. The lines are added by hand to allow the core model to remain as simple as possible, and are erased afterwards to return the model to its natural, 6-stage state. Adding just one feedback loop to each stage results in the model looking much clumsier and less clear, as can be seen below:

[99] This is an area which requires additional, specialist research in collaboration with the UK Intelligence community. The Author is currently discussing this possibility with various officials.



17 Intelligence cycle with single-stage feedback loops

Once all of the possible permutations for feedback loops have been added in, the model becomes very messy indeed, as can be seen below on a diagram annotated by hand and used by the author in a training course for foreign students:



18 Intelligence cycle with hand-drawn, multiple-stage feedback loops

The next issue raised by Hulnick is that "*in the modern era, policy officials seem to want intelligence to support policy rather than to inform it*". Phythian states that "*the Intelligence-policymaker interface has long been viewed as the most frequent location of Intelligence failure*" (Phythian 2011, p.115).The professionals in the UK Intelligence community are acutely aware of the debate on whether the UK has Intelligence-led policy or policy-led Intelligence. An oft-raised criticism of the period immediately prior to the allied invasion of Iraq in 2003 was that Intelligence was being moulded to fit a desired policy outcome, i.e. a legally acceptable (and possibly more importantly, a legally defensible) provision of a *casus belli* for a ground invasion of Iraq to be joined by UK troops.[100] One of Butler's (2004:155) conclusions on the use of Intelligence by policy-makers stated that:

[100] See the text of the U.S. State Department's press release (2002) detailing the casus belli used by the U.S. President for the invasion of Iraq in 2003. For the detailed summery of the UK's decision to go to war, see The Butler Report (2004:93–97). Butler (2004:96) considered that the UK's decision was based partly on UNSCR 1441 (UNSC, 2002), but also based on the advice from the Attorney General that UNSCR 687 (UNSC, 1991) provided sufficient *casus belli*, as it "……*suspended, but did not terminate, the authority to use force under Resolution 678*".

> "….*if intelligence is to be used more widely by governments in public debate in future, those doing so must be careful to explain its uses and limitations. It will be essential, too, that clearer and more effective dividing lines between assessment and advocacy are established when doing so*".

Yet one of the underpinning principles of secret Intelligence lies in the descriptor, *viz*. that the end product of the process is almost always classified. As discussed previously, the maxim of "need to know" was expanded to include "need to hold" and "need to share".[101] It is this "need to share" which will require intensive consideration by the appropriate elements of the government of the day including the Prime Minister, should they contemplate a similar, sanitised release of classified material for public consumption in the future, in order to explain a given situation to the general public.

Gannon (2008:221-222) considers politicisation to be just one of two distinct types of what he calls the distortion of analysis and he defines politicisation as "*the wilful distortion of analysis to satisfy the demands of Intelligence bosses or policymakers*". The other form is one he calls "*analytical bias*", defining it as "*a subtle but pervasive influence based on the unconscious exertion of pressure*". Ott (2003:69-94) concurs with Gannon, adding that: "*the value of Intelligence to senior policymakers and to the nation rests to a critical degree on the confidence that the process is not corrupt – that Intelligence collectors and analysts speak truth to power, however unpalatable that might be at any one time*". Writing from a more UK-centric viewpoint, Phythian believes that as far as the Intelligence and Security Committee is concerned, a more important question needs to be asked: "…*to whom are the oversight committee accountable?..appointed by the executive, reporting to the executive and*

[101] See Chapter 5.6, Dissemination.

holding membership at the pleasure of the executive…" (Phythian, 2006:conclusion).

Treverton (2008:93) identifies five distinct form of politicisation of Intelligence, which are shown in the following table, together with his descriptors and the ways in which he believes these forms can potentially be mitigated:

Type	Description	Ways to Mitigate
Direct pressure from policy	Policy officials intervene directly to affect analytic conclusion	Rare but can be subtle - logic is to insulate Intelligence
"House" view	Analytic office has developed strong view over time, heresy discouraged	Changed nature of target helps, along with need for wide variety of methods and alternative analyses. NIE-like process can also help across agencies
"Cherry Picking"	Policy officials see a range of assessments and pick their favourite.	Better vetting of sources, NIE-like process to confront views
Question asking	How the question is framed, but Intelligence or policy, affects the answer	Logic is closer relations between Intelligence and policy to define question, along with contrarian question-asking by Intelligence
Shared "mindset"	Intelligence and policy share strong presumptions	Very hard - requires new evidence or alternative arguments

19 Treverton's forms of politicisation

The dividing line between groupthink and "shared mindset" can be a thin one at times. This is less common in the counter-terrorism field than it is in more strategic areas, such as the specific focus on one particular country or regime. This is possibly due to the faster-moving scenarios in counter-terrorism, and the fact that a large part of counter-terrorist Intelligence work dwells mainly in the tactical and operational areas, but it is difficult to accurately identify the reasons with any certainty. Treverton, discussing the Cold War analysis of Soviet capabilities, sees a distinction between this more strategic, long-term work, and the international terrorism landscape of the current era. He notes that "*the terrorist target, however, is utterly different. It is the ultimate "asymmetric threat", shaping its threat to our vulnerabilities*" (Treverton, 2008:97).

An enemy which conducts asymmetric warfare is a very difficult opponent to fight and this is precisely why asymmetric warfare is so popular with the groups which engage in it. It is almost as difficult to define as terrorism, with academic papers devoted entirely to the debate on how to define it. Buffaloe (2006:2) highlights some of the variations which may or may not be considered the same as asymmetric warfare, such as "*low-intensity conflict, military operations other than war, asymmetric warfare, fourth-generation warfare, irregular warfare*". Former U.S. President John F. Kennedy encapsulated the spirit of asymmetric warfare in 1962, describing it as

> "*another type of war, new in its intensity, ancient in its origin—war by guerrillas, subversives, insurgents, assassins, war by ambush instead of by combat; by infiltration, instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him. . . . It preys on economic unrest and ethnic conflicts. It requires in those situations where we must counter it, and these are the kinds of challenges that will be before us in the next decade if freedom is to be saved, a whole new kind of strategy, a wholly different kind of force, and therefore a new and wholly different kind of military training*".[102]

[102] President John F. Kennedy, Remarks to the Graduating Class of the U.S. Military Academy, West Point, on 06 June 1962, cited by Buffaloe (2006:1–2) in "*Defining Asymmetric Warfare*".

Perhaps the most apt description of it comes from Taber (1965:27–28) who wrote: "*The guerrilla fights the war of the flea, and his military enemy suffers the dog's disadvantages: too much to defend; too small, ubiquitous and agile an enemy to come to grips with*". The current spectrum of the UK's Intelligence collection for counter-terrorism purposes takes place in the environment of opponents who engage in asymmetric warfare. The importance of Intelligence-led operations is paramount in this fight. Politicisation of Intelligence in the UK is not something which any of the interviewees mentioned having observed or having been part of. In the author's opinion it is a rarity, but that is not to say that it does not occur.

Of Treverton's five forms, "cherry picking" and direct pressure from policy are probably more likely than the other three forms, with regard to the political landscape of the UK. An inherent danger of "cherry picking" is that in the majority of cases, it would be invisible to, and thus remain undetectable by, the Intelligence community if it were done at the highest levels of policymaking in Whitehall. As for direct pressure, in the period preceding the decision to go to war in Iraq in 2003 the declassification of material graded top secret, and the subsequent publication of it for the consumption of the general public in the UK was unprecedented. Direct pressure from policy certainly had a part to play in the solidifying of cross-party support for a ground invasion. Butler (2004:150–151) commented on this in his conclusions, stating:

> "*When the Government concluded that action going beyond the previous policy of containment needed to be taken, there were many grounds for concern arising from Iraq's past record and behaviour. There was a clear view that, to be successful, any new action to enforce Iraqi compliance with its disarmament obligations would need to be backed with the credible threat of force. But there was no recent intelligence that would itself have given rise to a conclusion that Iraq was*

> *of more immediate concern than the activities of some other countries. Intelligence on Iraqi nuclear, biological, chemical and ballistic missile programmes was used in support of the execution of this policy to inform planning for a military campaign; to inform domestic and international opinion, in support of the Government's advocacy of its changing policy towards Iraq; and to obtain and provide information to United Nations inspectors*".

From the narrative in what has become known as "The Secret Downing Street Memo", it is clear that the Director of SIS recognised the politicisation of Intelligence which was occurring within the inner circle of the U.S. President's closest advisers. The memo contains the following statement" "*C reported on his recent talks in Washington. There was a perceptible shift in attitude. Military action was now seen as inevitable. Bush wanted to remove Saddam, through military action, justified by the conjunction of terrorism and WMD. But the intelligence and facts were being fixed around the policy.*" (Rycroft, 2002:1).

Butler also identified the customers of Intelligence as being part of the problem, noting how important it is for the end users of Intelligence product to be aware of the material they receive, the provenance of it and in particular, the pros and cons of such material. He wrote (Butler, 2004:14-15):

> "*JIC judgements have to cover both secrets and mysteries. Judgement must still be informed by the best available information, which often means a contribution from intelligence. But it cannot import certainty. These limitations are best offset by ensuring that the ultimate users of intelligence, the decision-makers at all levels, properly understand its strengths and limitations and have the opportunity to acquire experience in handling it. It is not easy to do this while preserving the security*

> *of sensitive sources and methods. But unless intelligence is properly handled at this final stage, all preceding effort and expenditure is wasted*".

Thus the actual risk of politicisation is omnipresent, although academics seem to disagree on the severity of it compared to other issues. Betts (2004:7), for example, takes a slightly divergent stance, noting that "*the typical problem at the highest levels of government is less often the misuse of Intelligence than the non-use*". Interestingly, Phythian (2009:353) seems to accept the inevitability of *some* degree of politicisation in the oversight of UK Intelligence, commenting that "*Oversight of Intelligence, whoever carries it out, is inescapably political and those conducting it must remember that they are engaged in contests of power in which the stakes are high*".

Returning to Hulnick's criticisms about the Intelligence cycle, he next cites the absence of covert action and counter-Intelligence as a flaw in the cycle. It should be noted that the model was designed for the Intelligence process, and was not designed to encompass specific, operational aspects. The cyclical model, as far as can be determined, had its inception in the military world which to this day maintains a clear distinction between two disciplines: that of Intelligence, designated as J2, and that of Operations, designated as J3.[103] Within the contemporary concept of Intelligence-led operations, it is the Intelligence itself which usually dictates which operations can and cannot take place, thus the Intelligence is the key driver for the operation. Previously, this concept was inverted and operations were conceived, then planned. Intelligence was requested as required, to support the operational planning and execution. The aspect of covert action is the implementation or execution of policy and should not be included in the Intelligence cycle.

[103] When considered as a joint or all-arms function, the designator letter is "J"; otherwise the designator letter reflects the single-service designation, i.e. N2 for Navy, G2 for Army, A2 for Air Force.

Much hard work has been done in the past three decades to dismantle the physical and psychological barriers between the disciplines of operations and Intelligence.[104] On the battlefield the two are unequivocally intertwined, to the extent that they are usually co-located, from as low down as a Company-level HQ to as high up as a Corps HQ. In permanent locations such as Permanent Joint Headquarters (PJHQ) both J2 and J3 staffs work in joint teams, often with the addition of J5 staff who focus on contingency planning. In a purely military context it is possible for the military Intelligence machinery to own the entire Intelligence cycle, with no input from external sources. As the military also own the operational actors, such as the "teeth Arms" (usually classed as the infantry, artillery, armour and engineers), joint working is essential for battlefield success. In the less-clearly defined sphere of counter-terrorism, the same co-operation exists between the Intelligence arm and the assets tasked with operational response, the difference being that the operational actors are not owned by the Intelligence chain. The UK Police ensure that a so-called "sterile corridor" is maintained, between the Intelligence collection/analysis/production elements and any "evidential functions", to ensure that officers working on the investigation are not exposed to raw Intelligence which is not evidence.(Harfield 2013, p.365) It also excludes, as far as possible, an officer inadvertently disclosing sensitive Intelligence, for example, during a Police interview with a suspect. The sterile corridor enables the Intelligence to drive the investigation or the operation, and this is aided by the Intelligence cycle. Instead of a system wherein the investigation or operation is launched, and Intelligence is requested to support it (which was more usual in the 1970s and 1980s), the cycle now aids the symbiosis between the Intelligence and the operation, resulting in a continuous refinement of the available information and of the processed product.

[104] In the 1980s, the divide between Intelligence (J2) and Operations (J3) was very often physical. When the author worked in a military Intelligence role overseas, the analysis function was in a different part of the building to the operational planning function. The physical divide encouraged the separation of the two elements. By the early 1990s, the experiences of the Gulf War in Iraq had contributed much to the realisation that Operations and Intelligence needed to occupy the same office space. By the time that the second Gulf War started, there was a firm belief that J2 and J3 needed to be enmeshed, so that intelligence could actually steer operations in real time.

For domestic counter-terrorism work in the UK, this function is usually carried out by Counter-Terrorism Command (SO 15) officers, who may be supported by other assets such as Specialist Crime and Operations Specialist Firearms Command (SC&O 19).[105] For counter-terrorism operations overseas, the operational responsibility for this has traditionally fallen to the UK's Special Forces (Urban, 2010). The cycle exists to produce Intelligence which should ideally be "actionable", informing a policy- or decision-maker to enhance their ability to select a course of action as a result of the Intelligence received. Not all Intelligence is actionable, and much of it fleshes out the bigger picture without adding anything significant, Actionable Intelligence remains the "gold standard" sought by Intelligence professionals. Hulnick's desire to see covert action and counter-Intelligence added to the cycle would result in a much larger, more hybrid model as it would, by necessity, become an "Intelligence-Operations Cycle".

Returning to a previous comment, a fundamental principle of Intelligence is to "speak truth unto power".[106] The provision of accurate and timely Intelligence to policy-makers is a desired output of the cycle. A range of options will be available to the policy-makers and these options will change with every case. These options can be considered as a tactical menu (Burke, 2014). As an example, an individual may be under surveillance as he is suspected of being involved with a terrorist group operating within the UK. As the collection phase contributes more data regarding his pattern of life, analysis reveals that he is the main "Quartermaster" for the group. He is responsible for the provision of material support (which could include money, vehicles, safe houses, mobile phones, computers and even weapons and explosives). Once the individual is confirmed as the Quartermaster, the options on the tactical menu may be as follows:

1. Cease surveillance on the target

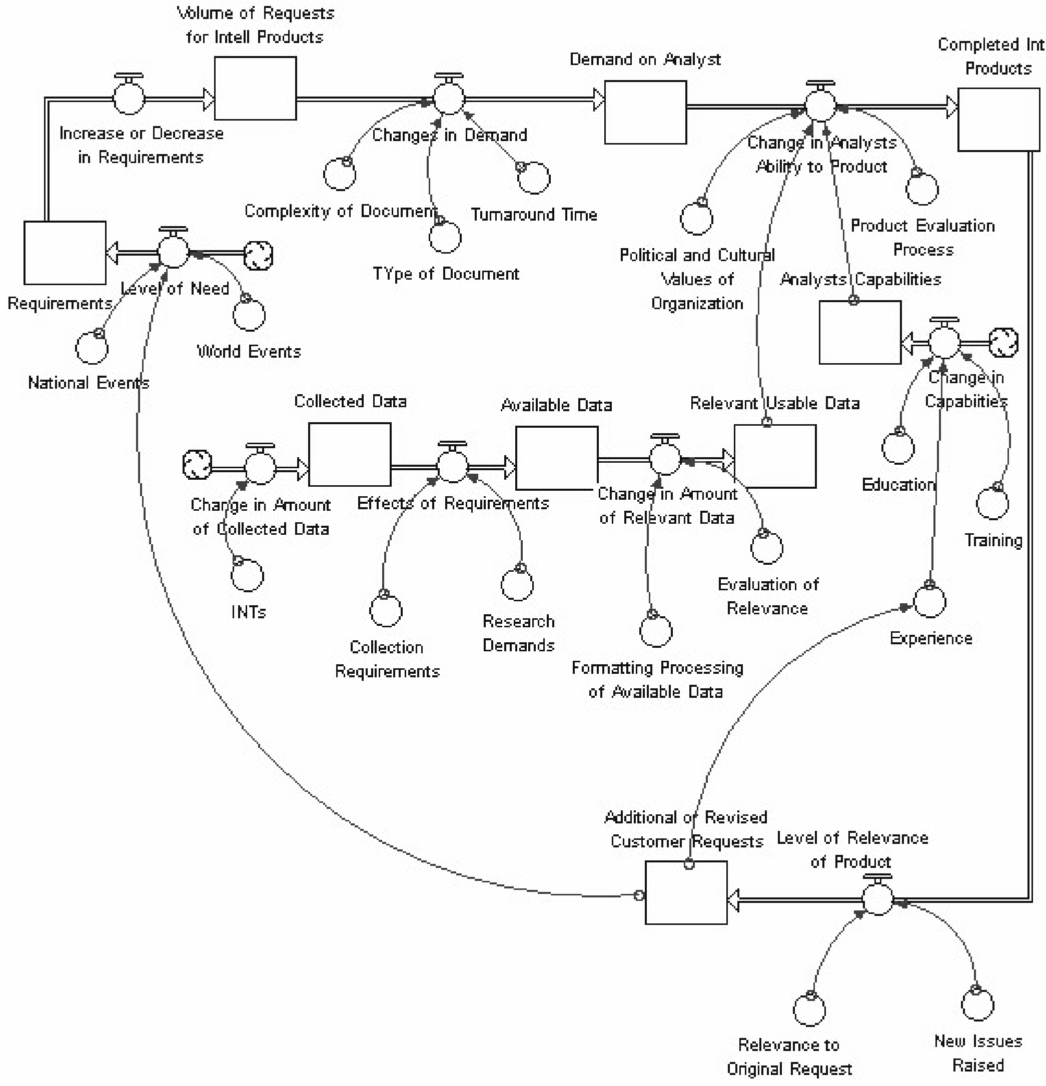
[105] Counter-Terrorism Command was formed in 2006 from an amalgamation of the Special Branch and the Anti-Terrorism Branch (ATB).

[106] See Chapter 5.5

2. Continue surveillance (directed / intrusive)
3. Conduct covert penetration of the target group
4. Overtly warn the target
5. Disrupt the group
6. Arrest and interview
7. Prosecution and conviction
8. Hard arrest (if suspected that the individual or group will use weapons or explosives to resist arrest)

There are several potential courses of action and the planning required to carry out an operational response can require sizeable teams from multiple agencies and departments. It is difficult to see how the Intelligence cycle could be modified to include the potential operational actions (such as covert action or counter-Intelligence,) which may follow from the dissemination of actionable Intelligence to policy-makers. The workflow for such a model would need to include not only the potential feedback loops inherent (but traditionally not shown) within the model, but would also need to include the expanded processes, from dissemination through to eventual operational action. Would such a model also need to include additional process loops for the possibility of an operational action being unsuccessful and needing either an additional iteration, or a return to the Intelligence-producing aspects of the model? If so, it would rapidly become very large and unwieldy.

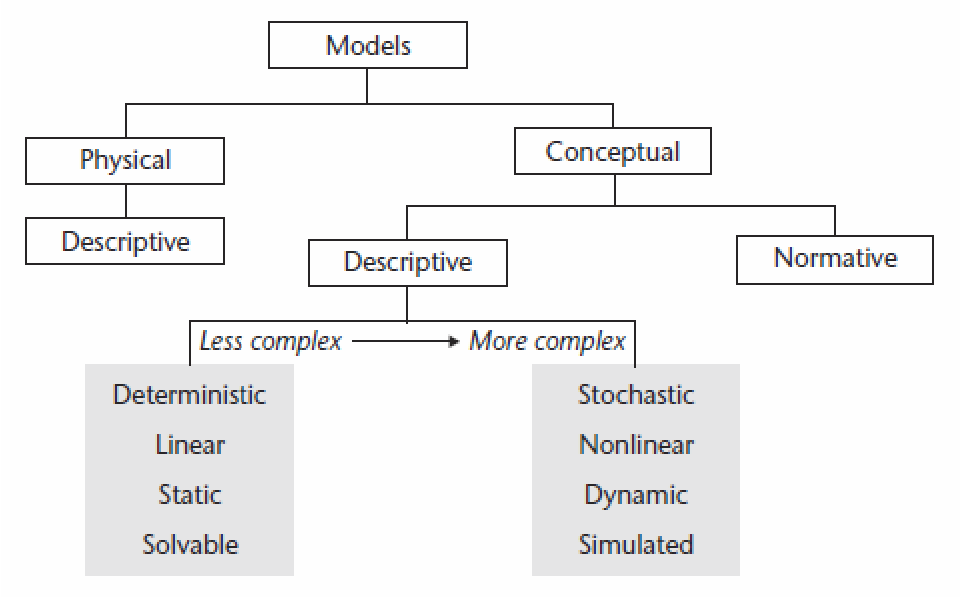
The following diagram shows a different approach taken to the Intelligence cycle, this time using a “systems approach” (Johnston, 2005). The model has four representation described as stocks, flows, converters, and connectors and these purport to show the various relationships (e.g. systemic, process flow) between the four components. The difficulties in explaining this model’s processes to new recruits into an Intelligence function would be considerable. It would be unrealistic to expect a student to learn a diagram such as this one, and to subsequently apply it in operational Intelligence work. This diagram constitutes more of a workflow than an actual model.


Volume of Requests for Intell Products
Demand on Analyst
Completed Intell Products
Increase or Decrease in Requirements
Changes in Demand
Change in Analysts Ability to Product
Complexity of Document
Turnaround Time
TYpe of Document
Political and Cultural Values of Organization
Product Evaluation Process
Analysts Capabilities
Requirements
Level of Need
World Events
National Events
Change in Capabiities
Collected Data
Available Data
Relevant Usable Data
Change in Amount of Collected Data
Effects of Requirements
Change in Amount of Relevant Data
Education
Training
INTs
Collection Requirements
Research Demands
Formatting Processing of Available Data
Evaluation of Relevance
Experience
Additional or Revised Customer Requests
Level of Relevance of Product
Relevance to Original Request
New Issues Raised

20 A systems approach to the Intelligence cycle

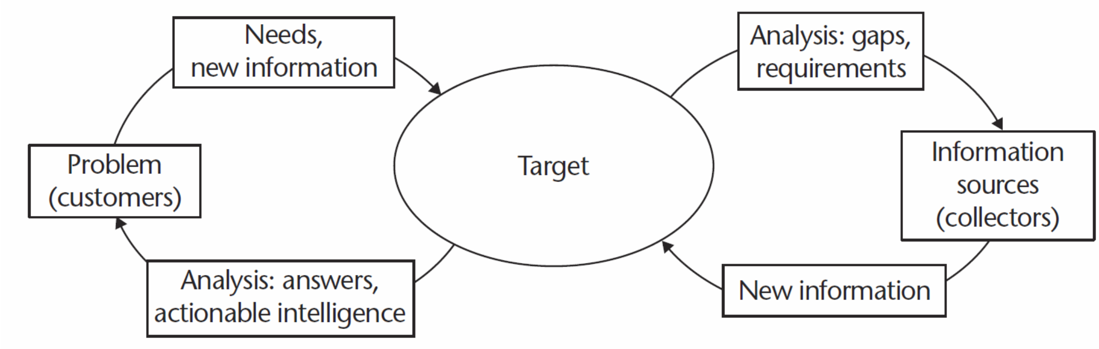
At this point we have moved from the original Intelligence cycle of 1948, containing just four components, to a systems model produced in 2007, containing more than 30 components and a large number of interactive processes and dependencies. The previous paragraph mentioned the complexities involved in trying to include the various operational options of the tactical menu within an intelligence cycle model and it would be useful here to state a consideration which is often ignored by critics of the Intelligence cycle. The cycle was designed as a model, largely for the purposes of instruction; it was not designed as an all-encompassing workflow, against which could be mapped all the inherent processes, sub-stages, feedback mechanisms and potential outcomes. A common criticism of the Intelligence cycle is that it does not fully represent the interactions which take place within the process. In order to map all the interactions which take place, any model would be much larger in scope and complexity than the system-focused model shown previously.

Management experts at Gartner, one of the world's largest research and advisory companies, define a workflow as "….*a form of flow management technology that coordinates interactions between people and software systems*", and further clarify that a workflow "*coordinates the flow, the interaction patterns across manual and systemetized (sic) tasks*" (Hill, 2010:1). Some models of the Intelligence cycle clearly display these characteristics, such as the systems model above. Clark is a former U.S. Air Force Intelligence officer and is now a Professor of intelligence studies (Sage Publications, 2014). His work is particularly relevant as he writes extensively on models, their classification and their application within the Intelligence world. Clark (2012:37) defines a model as: "*a replica, or representation, of an idea, an object, or an actual system. It often describes how a system behaves*". He considers that conceptual/descriptive models are the most useful model types within the Intelligence sphere and he posits that instead of a cyclical model, or a linear model, the most appropriate type of model for the contemporary Intelligence community would be what he describes as a "*network process*" (Clark, 2012:37). Where Clark's approach has merit is the focus on the target, as opposed to the process. His work builds on that of Cebrowski and Garstka (1988:28-35) which examined the concept of a "*network-centric collaboration process*" used by commercial entities such as General Electric and Wal-Mart, and the pair then applied it to the military sphere. Clark (2012:35) provides a useful, diagrammatical representation of a hierarchy of models, reproduced below.



21 Clark's Hierarchy of Models

Clark (2013:8) also provides a model of his own version of the Intelligence cycle, which he calls "*the target-centred view of the Intelligence process*", and considers this new approach necessary in order that this process can take fully exploit the current information systems, and can ably tackle complex challenges. His model is shown below (Clark, 2012:8):

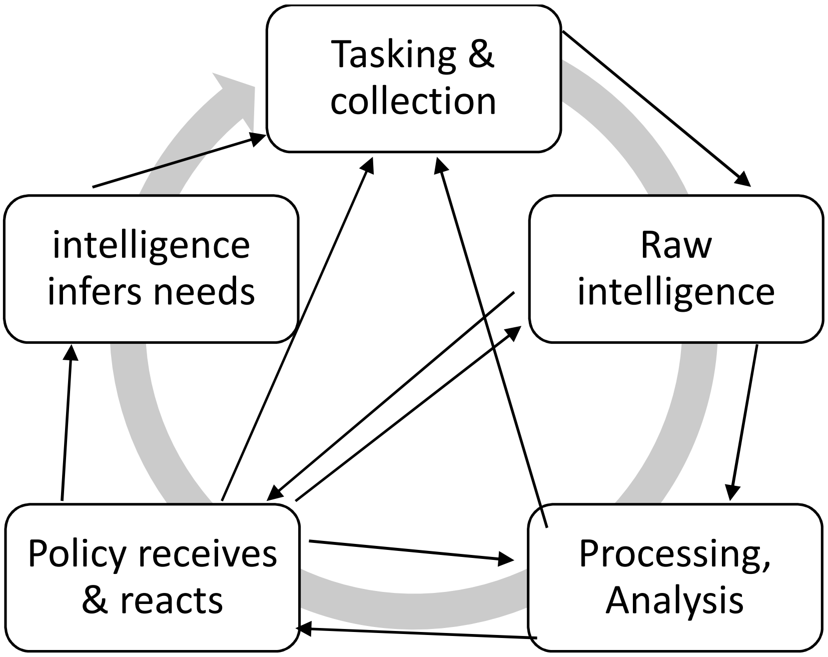

Needs, new information
Analysis: gaps, requirements
Problem (customers)
Target
Information sources (collectors)
Analysis: answers, actionable intelligence
New information

22 Clark's target-centred view of the Intelligence Process

In Clark's process, the customers identify what they want to know and communicate this to the analysts, who then produce requirements from this stated need. Working together with collectors, the analysts build up a picture of the target which at some point is provided to the customer. Apart from the fact that there is no evaluation in this model, it does not refine the process further, by bringing anything new or more efficient to that described in detail in Chapter 5. The customer provides direction on what Intelligence is required; analysts and collectors collaborate on the collection and collation work; as material is collected, it undergoes analysis (having almost certainly have been evaluated in addition); when necessary, an Intelligence product is provided to the customer(s), who may ask additional questions requiring the process to continue. Or they may ask for deeper clarification or refinement, requiring the process to be entered at a later stage, such as analysis, and thus requiring another iteration from that point forwards.

In describing the actual functioning of the target-centric process, however, Clark does bring added value with his consideration that the work inside the process is more of a networked, or meshed, model. By placing the target at the centre of the model, he emphasises that the target (and the need to build up a picture of it) is central to the process, and that the process exists to carry out this function. It is a useful reminder that the aim of the cycle is to produce actionable Intelligence. Yet the model does not suffice as a standalone description of the process, as far as the UK's machinery and concepts are concerned. Taking a contemporary example, concern is growing within the Security Service about the number of British citizens or residents travelling, or planning to travel, to Syria in order to actively support groups such as Islamic State, or Al Nusra Front. In 2014, the Metropolitan Police estimated the number of British citizens fighting for the Islamist groups in Syria to be in the mid-hundreds, which they saw as a substantial increase from the previous year (Whitehead, 2014; BBC, 2014b). At a strategic level, this issue may be passed to the JIC with an instruction to produce a JIC paper for the Prime Minister and others. Or it may already come under an existing JIC priority, such as “prevent harm to the UK and prevent harm to other nations from individuals travelling from the UK”. The need to collect against this target cannot simply be passed directly to analysts, as this would omit the collection management function which exists to ensure that: there is no duplication of collection; that priorities are set correctly and realistically against the JIC requirements; that sufficient assets are allocated to the collection work; and that the question has not already been answered previously, or is already undergoing collection. The target-centred process of Clark’s is therefore more a depiction of the inner functioning of the cycle once it is underway.

Treverton (2001:49) took the complexity formed from combining the Intelligence cycle with the feedback process, and attempted to clarify it, depicting it thus:[107]



23 Treverton's "Real Intelligence Cycle"

[107] Cited by Johnston (2005:49)

He combines processing and analyses, which is a sensible amalgamation, and the cycle moves thence to policy, receiving and reacting with the received output. Once policy has received the product, which we assume to be a finished, disseminated product, an examination of Intelligence needs is conducted. This then feeds the tasking and collection component. In this model, once Intelligence is processed and analysed it is disseminated to the customer, in this case to policy makers. As with other models, however, there is no explicit evaluation function in this model, which leaves a functional gap in the overall process. The use of the term "raw Intelligence" is more opaque than enlightening, as this would usually be classed as "information", as it has not been subjected at this stage to an analytical process.[108]

Keagan (2004:3–5) does not describe an Intelligence cycle *per se*, but lists "*five fundamental stages*" of Intelligence, which he considers to be essential, if Intelligence is to be of use. The first stage is acquisition, noting that Intelligence has to be found. Next we have delivery, and Keegan notes that the Intelligence must be sent to what he describes as the "potential user". The third stage is one unseen in other models – acceptance, i.e. the Intelligence must be believed. Fourth is interpretation, which involves the assembly of the various pieces of Intelligence and information into as whole a picture as possible. The final stage is implementation, which Keagan interprets differently than what one might expect from the use of the term. He sees implementation as the task of Intelligence officers being content with the accuracy of their raw material, in order to convince their superiors that the finished Intelligence product is also accurate.

Keagan's stages are interesting for their very different take on the process of Intelligence. His first stage of acquisition equates to collection, but misses out any direction or tasking. He considers that Intelligence has to be found, but in most cases the Intelligence only comes towards the end of the process. At that stage, much of what is collected or acquired is only raw information. The

[108] See Chapter 3 for a fuller explanation.

third stage moves straight to the credibility of the Intelligence, considering that it has to be believed. There is no mention of any evaluation or validation aspect, only whether the material is believable or not. This is not the same as evaluation and chapter 5.5 of this paper explained why this stage is so crucial in the process. His fourth stage of interpretation corresponds to analysis (which could possibly be said to implicitly include processing). This puts the pieces of the jigsaw together to form a clearer picture. His final stage is difficult to map against other models, but it emphasises the importance of the product's recipients being convinced of its reliability. Keagan's five stages are an interesting aspect of study and they provide some good points for thought, but they are unsuitable for practical use as a model or a process.

6.1.1 Challenges and vulnerabilities in Intelligence

Considerable academic research has been conducted into the problems encountered in the Intelligence process, with the foremost research in this field coming from the likes of Sheptycki (2004), Heuer (Heuer & Pherson, 2011), Krizan (1999), Trent (Trent et al., 2007) and Hutchins (Hutchins, S. G., Pirolli, P., and Card, 2007).[109] The majority of this research has focused on the analysis of Intelligence, as this is one of the more subjective functions in the process. The subject of Intelligence analysis is vast and many specialist works are devoted just to this one part of the process. As mentioned previously, the basic Intelligence analysis course for the British Army's Intelligence Corps lasts 14 weeks, but the subject of analysis is truly immense, with a very substantial written corpus of both practical and academic theory (Martenson & Horndahl, 2005; Bar-Joseph, 2011; Gannon, 2008; Betts, 1978; Marrin, 2007; Marrin, n.d.; Richards, 2010). The following table (Zelik et al., 2007) provides just a sample of some of the perceived vulnerabilities and challenges in the field of Intelligence analysis, identified by

[109] Also see Stanier (2012) for more contemporary research on Sheptycki's pathologies.

Krizan (1999), Heuer (1999), Trent (Trent et al., 2007), Hutchins (Hutchins et al., 2007) and Johnson (2005):

Intelligence Analysis Challenges and Vulnerabilities				
Krizan	**Heuer**	**Trent, et al.**	**Hutchins, et al.**	**Johnson**
Prematurely Formed Views	The Vividness Criterion	Inappropriate Mental Set	High Cognitive Workload	Secrecy versus Efficacy Trade-off
Wilful Disregard of New Evidence	Absence of Evidence	Environmental Pressure	Potential for Error	Focus on Current Production
Lack of Empathy	Base-Rate Fallacy	Fixation	Time Pressure	Time Constraints
Ethnocentrism & Mirror- Imaging	Oversensitivity to Consistency	Recognition of Relevant Data	Coping with Uncertainty	Confirmation Bias, Norms, and Taboos
Ignorance	Anchoring	Trust	Data Overload	Analytic Identity
Rational-Actor Hypothesis or Denial of Rationality	Assessing Probability of a Scenario	Experience viewed as Expertise	Synthesizing Multiple Sources of Information	Production-based Rewards and Incentives
Proportionality Bias	Availability Rule	Learning	Insufficient Tools	Analytic Training
Defensive Avoidance & Wishful Thinking	Similarity of Cause and Effect	Tool Understanding	Organizational Context	Perception of “Tradecraft” Versus Scientific Methodology
Conservatism in Probability Estimation	Internal vs. External Causes of Behaviour	Sustained Attention	Complex Human Judgments	
Presumption that Support for One Hypothesis Disconfirms Others	Persistence of Impressions Based on Discredited Evidence			
Best-Case Analysis or Worst-Case Analysis	Overestimating Our Own Importance			
Image and Self-Image	Illusory Correlation			
Overconfidence in Subjective Estimates	Expression of Uncertainty			
Inappropriate Analogies & Superficial	Bias Favouring Perception of Centralized Direction			

Lessons from History				
Evoked-Set Reasoning	Coping with Evidence			
Excessive Secrecy	of Uncertain Accuracy			
Presumption of Unitary Action by Organizations & Organizational Parochialism	Bias in Favour of Causal Explanations			

Table 6 Intelligence Analysis Challenges and Vulnerabilities

At first glance, it may seem that the Intelligence process is beset by pathologies. Yet the problems which are often cited as examples of weaknesses within the Intelligence cycle are not strictly problems of the model’s architecture *per se*. The majority could be more accurately classed as human failings, with a smaller number classed as system failings or cultural failings. Although these factors can certainly have a direct impact upon the processes and outputs of the model, there is a strong argument which posits that such factors should not be considered as *de facto* weaknesses of the model. Other factors, also suggested as weaknesses of the model, could be labelled as cultural factors, such as time constraints, which may be decreed by senior managers, or which may be self-imposed by the analyst. Still other factors could be labelled as systemic factors. One such example is data overload, which can occur as a result of inefficient filtering of raw data when querying against a database, thus returning too many results to allow the analyst to find a start point for his work. It can also result from a temporary inundation of crucial information, which frequently happens in the immediate aftermath of a major incident. An example of this was the sheer volume of calls to emergency services in the period immediately following the first explosions on 07 July in the London terrorist attacks.[110]

[110] Another example occurred while the Author was working in an Intelligence role covering the Middle East and Africa region. During the Allied bombing campaign designated OPERATION DESERT FOX against Iraqi targets in December 1998, many analysts and managers were swamped with tactical and strategic reporting in the first few hours of the CRUISE missile strikes, resulting in a delay in the ability to provide an overall situational report to

Reconstructing this list to show the challenges and vulnerabilities listed taxonomically as human/systems/cultural factors shows a different picture, as seen below, though it should be noted that some factors, e.g. analytic training, can arguably lie in more than one taxonomical class:

customers. A number of factors caused this data tsunami, including insufficient filtering of reporting, reports being repeated by various elements which resulted in needless duplication, as well as frequent interruptions from customers and internal staff wanting real-time updates.

Human Factors	System Factors	Cultural Factors
Confirmation bias Recognition of relevant data Norms & Taboos Ability to sustain concentration Fusing of sources Illusory correlation Experience viewed as expertise Fixation Organisational parochialism Overconfident estimates Similarity of cause & effect Anchoring Analytic training Mindset Language of Probability Language of uncertainty groupthink cognitive bias assessment of probability	Data overload system limitations insufficient tools or training time constraints of IT	Time constraints Secrecy Vs. Utilisation Production-based rewards Organisational parochialism

Table 7 Intelligence challenges and vulnerabilities listed by taxonomy

Some issues such as groupthink and mind-set have been discussed previously, and it would be incorrect to consider many of these challenges and vulnerabilities as constituting weaknesses in the model itself. The model describes the top-level processes which should happen in order to facilitate the Intelligence process taking place. If individuals involved in various stages of the process are unwittingly engaged in groupthink, or have a particularly trenchant mind-set supporting one belief system or another, the fault does not lie within the model itself. The fault then lies with how the model is being used, either by people (human factors), the organisational culture (cultural factors) or by the systems within it (system processes). In the same way, a model depicting how to construct an item of flat-pack furniture could not be held to be flawed if an individual decided to use a hammer instead of the recommended screwdriver to assemble the item.

One of the vulnerabilities, bias, is of particular note as it can take various forms. Cognitive bias is a frequently mentioned problem amongst analysts. Davis (2008:160) summarises cognitive biases as "…*essentially unmotivated (i.e. psychologically based) distortions in information processing)*, which he differentiates from what he calls *"Motivational biases",* describing these as *"distortions in information processing driven by worldview, ideology or political preferences*". The most influential work in this area is without doubt that done by Heuer (1999) who wrote a seminal work for the CIA in 1999 entitled "*The Psychology of Intelligence Analysis*". Heuer studied the impact of bias upon the various processes involved in Intelligence analysis and produced a book which was originally classified SECRET and was authorised solely for internal distribution within the CIA. It has since been sanitised and released as a declassified book, allowing for even wider distribution. It remains the foremost work on this topic within the UK Intelligence community.[111] Heuer (1999:111) defines cognitive bias in the following way:

> "*Cognitive biases are mental errors caused by our simplified information processing strategies. It is important to distinguish*

[111] During several years of working in a UK agency, with frequent interaction with colleagues from the U.S.A, no other work on bias and the psychological processes involved in Intelligence analysis had the impact which this book has had. Analysts from the U.S. agencies appear to be considerably more familiar with Heuer's concepts, such as cognitive bias, and the analysis of competing hypotheses (ACH), than their counterparts in the UK.

> *cognitive biases from other forms of bias, such as cultural bias, organizational bias, or bias that results from one's own self-interest. In other words, a cognitive bias does not result from any emotional or intellectual predisposition toward a certain judgment, but rather from subconscious mental procedures for processing information. A cognitive bias is a mental error that is consistent and predictable*".[112]

It is unavoidable that bias, both cognitive and personal, has a direct influence on the tasking process and this is closely linked to the problem of "groupthink".[113] The individual and group perceptions play an important part in the whole process. An analyst's own individual perceptions are intrinsic to how s/he carries out the analytical process, and being provided with relevant training goes a long way to ensuring that the analysis is as rigorous as possible. Teamwork is not something which is often covered in analytical training, but it is of great importance in helping to negate the effects of individual bias. The opinions of other analysts can encourage groupthink, but they can also help to force new thinking about an issue or to propose new hypotheses for the Intelligence already held.

A senior GCHQ official (Source_12, 2011) lamented that "*there is never enough time to analyse everything that we'd like to, or ought to*" which he believed led to "*not enough long-term Intelligence*" being produced. This particular problem seemed to resonate more with the SIGINT community than with the HUMINT community, possibly due to the sheer volume of raw data now being processed in the SIGINT world. The GCHQ official also considered that evaluation should be done by more experienced and properly trained staff, to ensure the quality control of the whole process (Source_12, 2011).

[112] In his extensive book, Heuer gives credit to Tversky and Kahneman (1974:1124-1131) specifically recommending their work "*Judgment under Uncertainty: Heuristics and Biases*".

[113] See chapter 5.5

This was echoed by a military Intelligence expert (Source_10 2011), who stated that “*evaluation should really be a specialisation in its own right. When you think of the importance it has, we should be selecting and training our best people to provide the evaluation, in the reporting phase, and definitely in the QC (Quality Control) phase before release*”.

6.1.2 Pathologies of Intelligence Sharing

Sheptycki (2004) published a detailed study of the problems “*manifest in Police Intelligence systems*”, and this study has become a core work on the problems encountered in the field of Intelligence sharing. His work took the results of a 2003 UK study and compared these findings to the issues noted among the Police forces of the Netherlands, Canada and Sweden. He found that the majority of problems in Intelligence sharing were also encountered in the overseas Police forces, not just in the UK (Sheptycki, 2004:307-332). He identified eleven distinct pathologies which a decade later, remain just as current as when the paper was published. The following brief summary of these pathologies will illustrate how they still have a negative impact in the field of Intelligence.

The “digital divide” manifests itself in two ways. The first is in the number of disparate databases which may contain similar or even identical data, resulting in difficulties experienced when database searches are necessary. Sheptycki illustrates this with an anecdote from one UK Police force which had two separate databases for firearms, weapons and ammunition data, which resided on different, standalone machines. Another database of firearms incidents was housed in a Force-wide system which was not linked to the two firearms databases. The second type of divide manifests itself through the medium of communication. Sheptycki’s example describes an actual case wherein two young boys were reported missing, and a 12-hour search ensued, involving assets such as police dogs and a helicopter. It was eventually discovered that the boys had been found one hour after they were reported missing, and had actually been at a neighbouring Police station for the duration of the search. Counter-terrorism work in the UK relies on databases held by SIS, Security Service, GCHQ, NCA and Special Branch, to name but a few. Each of these agencies has a multitude of databases, with varying degrees of ease of access by partner agencies. The creation of JTAC in 2003 was a major step in combating the "digital divide" in UK counter-terrorism, by bringing together in one location a number of officers from each of the main agencies, together with access to their own databases and tools, with the aim of the collective power being greater than the sum of its composite parts.[114] A GCHQ official did not consider the digital divide to be an issue of significance within that agency (Source_11, 2011).

Linkage blindness results from a paucity of data, rather than analysts having to contend with multiple databases. It differs from the digital divide in that the failure is a systems one, not a technical one. The sharing of Intelligence between agencies is never a simple process, requiring formal agreements as well as informal support. Sheptycki (2004:315) makes a prescient point about the passage of information within an organisation, saying that "*horizontal flow in information hierarchies is often poor because most effort is directed at ensuring vertical flow*". The degree to which the UK's Intelligence agencies now co-operate is unprecedented, and nowhere is this clearer than in the area of counter-terrorism. Specialists from all the agencies are seconded to other agencies, to learn their processes and to understand the organisational culture of the hosting agency in which they are embedded. A military Intelligence specialist held the opinion that this issue is of considerably more importance in deployed theatres of operations, such as Iraq and Afghanistan.

[114] The author visited JTAC on various occasions and was a recipient of JTAC product on a regular basis. Its establishment was one of the most significant steps forward for UK counter-terrorism work in the last twenty years. As Intelligence officers from the various agencies were all equipped with desktop computers connected to their own Agencies' databases, the speed of all-source access was vastly increased compared with previously. In addition, they were embedded in geographical or themed teams, with the result that a report released by an agency could be reviewed, discussed and formally assessed from a truly all-source perspective, with discussion being enhanced by the immediate access to all of the various agencies' repositories. As the remit of JTAC was clearly aimed at assessing and analysing existing reporting, it was able to quickly establish itself in the Intelligence community as a real "value-add" partner. The impact of JTAC's work on the Intelligence cycle itself is difficult to assess from an outsider's perspective, but in the stages of evaluation and analysis, the author considers this area to have been markedly improved by the input and reporting commentary of JTAC staff.

He observed that, in the military Intelligence community, "*we can feel like the poor relation a lot of times, especially when we're in the sand*" (Source_10, 2011).

Although he does not define noise, Sheptycki points to the concept which he has borrowed from the idea of "signal to noise" ratio, or threshold, familiar to SIGINT analysts. The concept can best be described using the analogy of the chaff being sorted from the wheat. As in the analogy, the real Intelligence can be missed due to the quantity or volume of the noise. The noise can render analysts unable to correctly discern the importance of a piece or pieces of important information which could be transformed into useful Intelligence. Sheptycki (2004:316) also highlights the problem with the quantity of raw data, stating that "*the larger the volume of bytes gathered for interpretation, the greater the capacity to produce noise*".

Intelligence overload refers more to a problem of analytical capacity than anything else and this can be especially acute during periods such as a build-up in tension (e.g. the period before the decision was announced to deploy UK troops to support the allied invasion of Iraq in 2003), or once a terrorist incident is underway (e.g. the immediate aftermath of the 07 July bombings in central London). If the overload is extreme, it can result in analytical paralysis and/or decision paralysis.[115] Several comments from interviewees confirmed this problem, especially when in the middle of an ongoing operation or incident, or while deployed in overseas theatres. An SIS officer (Source_06, 2011) remembered "*this feeling that you just can't write your report fast enough, because as you do, more and more info is hitting you*". A GCHQ official (Source_11, 2011) concurred, saying "*You have your team, and they're all working flat out to produce.....and the other departments are adding to the picture, which all takes more analysis, and more evaluation......and you might need to discuss it all with colleagues in another agency, but just when*

[115] An example of such an overload was at the start of the allied invasion of Iraq during the first Gulf War of 1991, sheer volume of reporting coming into analytical centres paralysed some of them and they were rendered temporarily non-functional.

you're about to, your boss asks you for a SITREP [situation report] *and you just know you're at max capacity*".

The highly dynamic environment described by the SIS and GCHQ officers above mirrors the situation described in Chapter 6.1.1 concerning the sudden and overwhelming overload of sensor data and spot reporting which occurred in the first couple of hours of Operation Desert Fox. The Intelligence cycle is a resilient tool but the Intelligence staff who employ it have a finite limit of capacity, both mental and physical, a fact often overlooked in crisis planning and in real-time crisis management. These physical and mental limitations have had an additional factor overlaid across them in recent years, especially the past decade – the massive quantities of data now available, which result in analytical searches returning much greater volumes of semi-processed information than previously. Professional tools such as i2 Analyst Notebook have brought an increasingly accurate search capability to the assistance of Intelligence analysts but when collection sources such as telephone billing data are involved, the results can still take days or weeks to refine, before something is produced which can be worked on effectively. Modern collection methods can be a victim of their own success, as a bottleneck is easily created in the collection stage, which then cripples the analysis or evaluation stages.

Two or three decades ago, one of the biggest problems facing the Intelligence agencies was a paucity of information. This problem has become inverted in the last decade, to the point where the agencies now have more data than they can easily process. New techniques have had to be employed and new tools developed to conduct faster, more accurate, more semantically-capable searches of vast data repositories, to try to draw linkages and relationships from an increasingly larger pool of raw information. Information produced by IBM in 2012 showed that in one average minute, users of the video-sharing platform YouTube uploaded around 50 hours of video content; 200 million email messages were transmitted; the Google search engine received 2 million queries for information and Facebook users uploaded around 600,000 distinct pieces of content.[116] The processing and storage capabilities of the Intelligence agencies have had to expand to keep pace with this increase, but the work of the analyst has become more difficult as a result of this data explosion.

Non-reporting and non-recording of information deprives the wider system of being able to include the missing data in any search results, and can result in an Intelligence failure, where the key information was actually known, but was either not reported or it was not satisfactorily recorded. Sheptycki (2004:318) provides a clear example of this in the firearms area, stating that "*there may be separate data-banks relating to the ammunition, the weapon and/or the incident that generated the report. Further, each separate report could necessitate double (or even treble) keying the same information*".

Intelligence gaps can occur for many reasons, and they are an occupational hazard for professional Intelligence staff.[117] Sheptycki's example concentrates on criminal who are assessed to lie somewhere between level 2 and level 3 targets, according to the National Intelligence Model, although this primarily relates to criminal targets.[118] Analysts often experience gaps in collecting and analysing Intelligence pertaining to terrorist targets. Due to the interest in terrorist trials in the UK, mainstream media reporting has gradually increased the level of technical detail which is reported on such cases. Revelations of the presence of listening devices in the cars and houses of terrorist (and major criminal) suspects (Court of Appeal, 2013; Cobain, 2006; BBC, 2007d) have contributed to a growing awareness by the terrorist-criminal-narcotics community, regarding the technical capabilities of the law enforcement and Intelligence agencies.

[116] From IBM internal documentation dated 2013, on information dated 2012.

[117] See chapter 3.1.1

[118] For a fuller examination of recommendations for closing Intelligence, information and capacity gaps in UK policing, see "*Closing the Gap - A Review of 'Fitness for Purpose' of the Current Structure of Policing in England & Wales*" (HMIC, 2005). Level 2 targets are those whose activities cross Force boundaries, such as narcotics supplies moving from Liverpool to Manchester. Level 3 targets are those who activities are national, or international, such as the narcotics "kingpins" who bring in shipments from the Balkans through the Netherlands, into the UK, in large quantities.

An Intelligence gap can occur, for example, because the agencies have no access to a source of information which could provide Intelligence on a certain target. Hypothetical examples might include the targeting of elements of the North Korean political and military leadership, or the inner workings of Albanian organised crime groups in London. Both groups may be considered as “difficult to target” and/or “difficult to penetrate” for various reasons. Identifying Intelligence gaps is an integral part of the PIR process.[119]

The issue of duplication is multifaceted. Sheptycki only discusses the duplication of targeting, wherein two or more agencies may be looking at the same target, yet each of the agencies may be unaware of the other’s involvement in the same case. At the extreme end of the scale, this could result in what the Police and military term a “blue on blue” incident, in which officers open fire on other officers, mistaking them for criminals or terrorists. Sheptycki cites Marx (1988) and Fijnaut and Marx (1995) for deeper examinations of these issues.

This problem has been somewhat mitigated by allocations of primacy to one agency or another in certain areas. For example, Sheptycki (2004:319) cites Customs officials having the lead in investigations into overseas importations of narcotics into the UK. Another fact of duplication is that of the same data being entered more than once in the same data repository, usually with differing details. Sometimes detailed are entered into multiple repositories, again with differing details. The implications of this can be severe. One UK Intelligence repository had 28 different spellings of the name “Mohammed”, resulting in many individuals being missed out of search records, if a user were simply to enter a casual search against the name “Muhamed” (Source_10, 2011).

The problem of institutional friction between SIS and the Security Service is well-known historically, and it has been extensively written about, particularly

[119] See chapter 5.

during the height of the Cold War.[120] The levels of rivalry which existed in the 1960s have greatly diminished and the threat of international terrorism now receives an impressive level of multi-agency co-operation in the UK. Friction can occur not just between agencies but at all levels, from inter-departmental through to simple animosity between two individuals. Institutional friction presents a bigger headache as it is often the by-product of an organisational culture which unofficially encourages it.

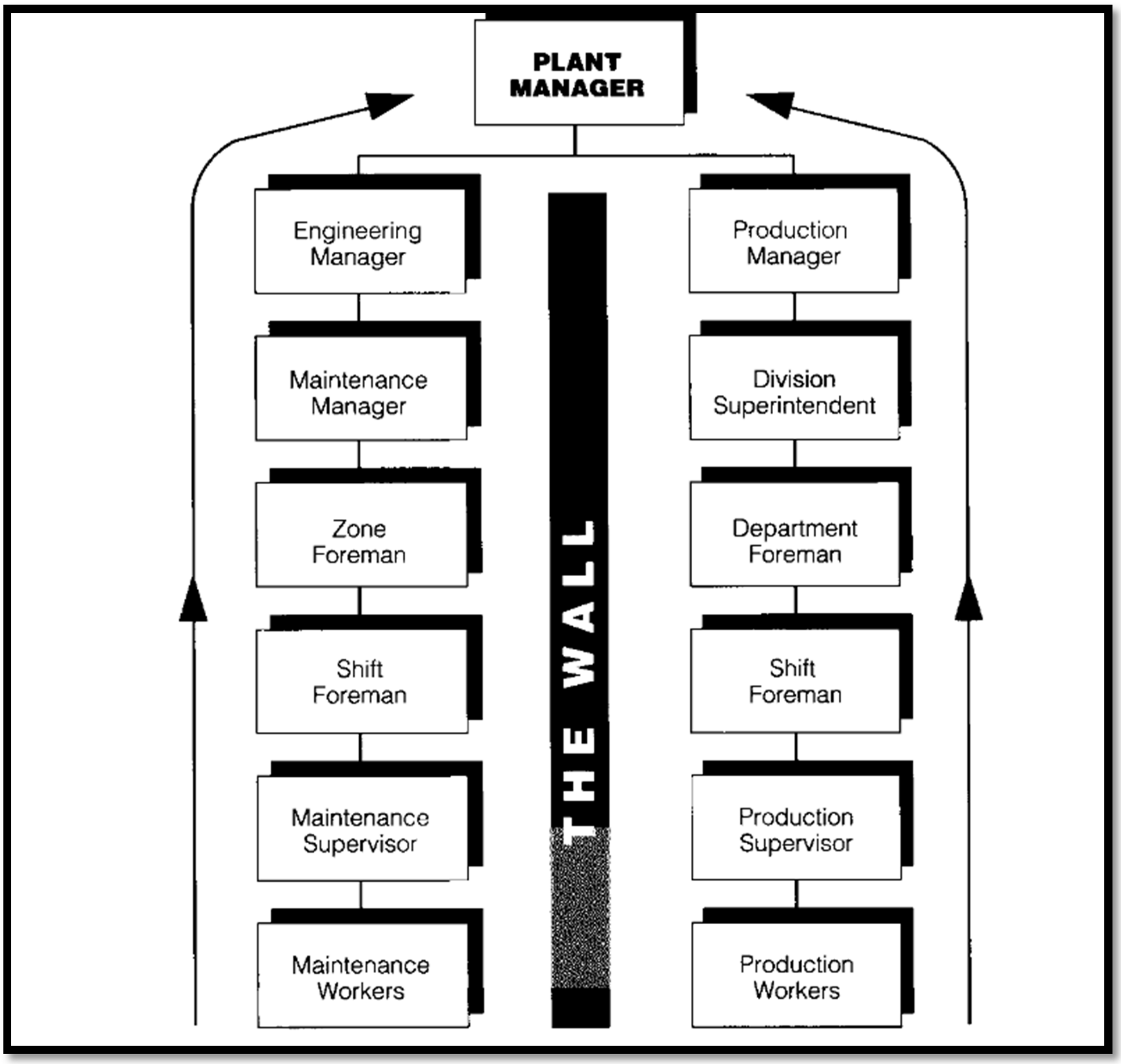
The build-up to the first Gulf War in 1991 saw a rapid push to break down the traditional Intelligence-hoarding culture which had been prevalent for the previous decades, especially in the UK and U.S. military Intelligence communities. Along with this organisational push came a sustained effort to reduce the debilitating effect of information silos. It was made clear that this desire for an end to information hoarding was coming from the very top of the U.S. military command chain and was supported by the most senior levels of the UK military and civilian Intelligence functions. A frequent culprit for the existence of hoarding is the age-old maxim that knowledge is power. The possession of more knowledge on a very topical issue can be perceived as endowing the possessor of such information with a cachet unavailable to others. In addition, the concept of “need to know” has been applied over-zealously in many branches of the Intelligence community. This has resulted in valuable Intelligence not being sanitised and/or released to the operational elements which could have acted upon it. In counter-terrorism, this philosophy is no longer the culturally entrenched and regularly occurring phenomenon which it used to be.

Information silos can be created deliberately or unwittingly. The ability to map the desired flow of information and Intelligence within and between departments and agencies is vital if the cycle is to function effectively. The introduction of customer feedback tear-off slips has been very useful use in helping departments and agencies to establish whether the dissemination of a

[120] See Corera (2012) and Thomas (2009) for more background on this rivalry.

product is being received by the correct customer base. They also show whether the information is timely, accurate and of use, providing a mechanism for customers to give quick opinions on such product. Nevertheless, silos still exist and sometimes are only noticed during a crisis or emergency, when there is little time to analyse why such a silo came into being. A senior Police officer (Source_04, 2011) commented that information silos have now become more complex due to the terrorist threat, saying that "*they are now very specialised…..which can lead to the problem of self-tasking*".

Another negative function of silos is the inhibition of information and Intelligence flowing horizontally across and between teams, departments and agencies, because the flow has been optimised for vertical transmission. The concept of an information silo was identified by an organisational development consultant named Ensor, who used the term "*functional silo*" in a report while working for the Goodyear Tire and Rubber Company (1988:16). Ensor noticed that the vertical hierarchies in several large companies led to problems with the flow of information in any other direction other than strictly vertical, with the majority of the flow only travelling upwards. He produced the following diagram (Ensor, 1988a:09-11) from a case study carried out at a Goodyear factory. It is easy to extrapolate from Esnor's diagram, replacing the industrial components with those of an Intelligence agency, to visualise the same problem which silos can produce in the Intelligence world.



24 Engineering and production functions isolated in their own separate functional silos

The issue of defensive data concentration appears to be similar to that of data duplication at first glance, but Sheptycki provides it with its own taxonomical class. Defensive data concentration constitutes the creation of separate data repositories for single-issue analysis, or for specialist analytical topics. His examples include firearms incidents, tobacco smuggling, sex crimes and other such single-issue topics. This problem was also witnessed in Iraq, where a specialised data repository was established in one Intelligence team, to focus on nominals of interest. Within a short period of time, almost all the information produced on any individual was only being logged in the nominal database. The result of this was that analysts conducting queries against multiple terms were unwittingly missing out on a large amount of primary data, due to this defensive data concentration.

Occupational subcultures are broken down by Sheptycki into two categories: intra-agency and inter-agency subcultures. The intra-agency issues are often reinforced by the prevalent culture within one agency or Force. This has been a particular issue within the Police, as Sheptycki highlights, citing Reiner (2000:115-137) who describes the animosity between Police officers and Intelligence analysts. Much of this came about because Police officers initially saw the introduction of a civilianised Intelligence cadre as posing a threat to the cadre of detectives who had traditionally done their own research and analysis. As mentioned previously, there was also a traditional rivalry between SIS and the Security Service, most notably during the decades of the Cold War, but this has now largely waned.[121]

Within counter-terrorism work the problem of inter-agency subcultures also has the potential for a negative impact. The lack of operational awareness within one team or department can result in missed leads, duplication of effort, analytic blindness and elitism. The impact of organisational culture is a very important factor in the Intelligence process but it is often overlooked during internal reviews and workshops. The cross-pollenisation of staff moving between specialisations makes a positive contribution to the understanding of other organisational cultures, in the same way that foreign travel helps to raise one's personal awareness of other cultures. This cross-pollonisation contributes equally to building mutual understanding at inter-agency as well as intra-agency level.

[121] See Andrew (2010) for a detailed history.

6.2 Strengths of the Intelligence Cycle

> "*Pursuit of a perfectly correct model is, as a result, only relative to the purpose of the model and the audience that uses that model.*"[122]

A model can be described as a human construct which provides a simplified depiction of a system. The system is often considerably more complex than the model which represents it. Returning to the primary purpose of the Davidson and Glass Intelligence cycle (1948), it was designed as an instructional aid to help teeth-arm commanders (i.e. those in the infantry, tanks, engineers and artillery) to understand the importance of Intelligence on the battlefield. It was also designed to educate them in the provenance of the Intelligence they received. As the authors clearly state in their introduction:

> "*Intelligence is not an academic exercise, nor is it an end in itself. Its prime purpose is to help the commander make a decision, and thereby to proceed more accurately and more confidently with the accomplishment of his mission*" (Glass & Davidson,1948:f.1)."[123]

[122] Comments by Prof. Paul Cook, American Military University, in critical response to an article entitled "*Let's kill the Intelligence Cycle*" by Kristan J. Wheaton, Associate Professor of Intelligence Studies at Mercyhurst University (Wheaton, 2011).

[123] From the book's flyleaf.

As a high-level construct, the 6-stage Intelligence cycle presents the neophyte with a simplified yet comprehensible overview of the entire Intelligence process in terms which s/he can understand. It does not overwhelm the beginner with the various collection mechanisms (e.g. SIGINT, HUMINT and IMINT) or by the intricacies which take place within the cycle, in order to produce a finished product (e.g. decryption, geospatial analysis, pattern of life mapping). This is a particular strength when it is used for the instruction and training of *ab initio* students, as it helps them to gain a simplified impression of this foundational precept. A basic course of instruction in techniques of Intelligence analysis, as used by some elements of the UK Intelligence community, lasts for 14 weeks of full-time study. The Intelligence cycle is one of the very first topics covered, and the importance of the model is emphasised in the first week, as students are instructed in how the model underpins everything that they will learn on the course. The position of analyst is a key one in the various government departments which deal with Intelligence, either as collectors, producers or consumers. It is often the first position which an individual fills, in an Intelligence-focused career. The importance, quality and relevance of the training which they receive will be an important foundation for future roles and training courses, so it is vital that new staff are able to conceptualise the Intelligence domain quickly and accurately. This is where the Intelligence cycle adds real value as a model.

As the course progresses the students learn how the parts of the model function in the real world, through the medium of exercises based closely on actual scenarios. The six-stage model can thus be considered as an expository tool which helps to lay the foundations for any formal course of instruction in Intelligence work. Johnson confirmed this concept of simplicity in his authoritative book on the analytical culture in the U.S. intelligence agencies, which is still used by the CIA and FBI today. He wrote that the Intelligence cycle is "…*represented visually to provide an easy-to-grasp and easy-to-remember representation of a complex process*" (Johnson, 2005:47).

This was confirmed by a senior Police officer, stating: "*the thing about the cycle is that it's not standalone. People draw it as a circle but the reality is that it's active and it's receiving and disseminating Intelligence at all levels. Its disseminating internally and externally, and collection is also being done internally and externally*" (Source_02, 2011). Sims (Sims & Gerber 2005:40–41), a former CIA officer and now Professor of Intelligence Studies, confirms the benefits of the model's simplicity, stating:

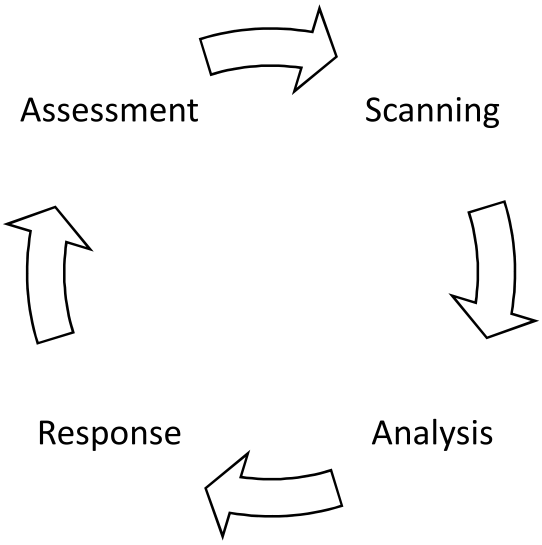
> "*The theoretically ideal intelligence process is a simple intelligence cycle…What makes this model useful is not that it is an accurate depiction of the American intelligence system, or even of most systems, but that it allows us to develop simple metrics for performance and to compare the Intelligence system in any government to what is perhaps ideal*".

The simplicity of the model is a key strength when looking at the workflow of a particular Intelligence department, in order to assess or evaluate the flow of information and Intelligence within it. As discussed previously, other models of the Intelligence cycle can be considerably more detailed and have been designed to encompass more of the systemic elements within the complete workflow. This inherent simplicity provides one of the model's core strengths. Phythian (2013:15) goes so far as to point out that a strength of the model is its wide-ranging utility:

> "*The traditional Intelligence Cycle is essentially a process-oriented model, whose four or five (or sometimes more) boxes describe the set of processes that are under-taken between actors in the intelligence business. The actors themselves are implied rather than specified in the model and this is one of its*

> *strengths as a conceptual process model, since it allows it to be applied to any number of organisations and situations. Indeed, other sectors have developed similar process models, such as Microsoft's four-box Business Intelligence cycle which comprises Analysis, Insight, Action and Measurement. That the commercial world has adopted a similar notional model attests to its simplicity and validity*".

A Police Intelligence analyst might use the SARA (Scanning-Analysis-Response-Assessment) model as a foundational structure with which to approach their daily workload. A representation of the model is provided below.



25 The SARA model

It is unreasonable to assume that the SARA model would incorporate all aspects of the analytical tasks performed during a typical day. Such a model, as described previously, would more accurately be classed as a workflow. It would need to encompass actions such as interrogating data repositories, liaising with other departments/forces/agencies, conducting deep analysis of linkages and relationships using specialised tools such as i2 Analyst Notebook and others. In much the same way as the SARA model is deployed in community policing, the Intelligence cycle enables users to ensure that the processes which they carry out to produce Intelligence are mapped against a model which ensures that the most important aspects of the Intelligence process have been taken into account. As one Police Intelligence specialist notes: "*the semantic purists might say that it's got to be done THIS way or THAT way, but it doesn't really - it's broadly telling you what the process is*" (Source_02, 2011).

The 6-part UK model has functioned equally effectively in some of the largest counter-terrorism investigations in the UK, as well as in foreign Intelligence departments comprised exclusively of *ab initio* recruits with no previous training in Intelligence or investigative work. Much of the reason for this success is down to the speed with which the model can be deployed, being a simple, 6-part process. A military Intelligence specialist (Source_10, 2011) noted that:

> "…*when we're sent to the back of beyond, and told that elements such as the Special Forces and RAF Aircrew will be dependent on the Intelligence we will produce, it focuses the mind that we have to start quickly, that others are relying on us, and that if we screw it up, people can get killed. That's the reality of what we deal with. So if I'm asked if the Intelligence cycle works for us, the answer is yes. It's simple, it's effective and we all understand it. Do I want to see it replaced with something that looks like a circuit diagram? No. It isn't just Intelligence specialists that are involved nowadays.*

> *Everybody collects, so it needs to be understandable by the lowest common denominator*".

This statement resonates strongly with the concept introduced by the U.S. Armed Forces during the aftermath of the invasion of Afghanistan, which stated with elegant simplicity "*every solider a sensor*" (Magnuson, 2007; U.S. Army, 2013). The idea behind this philosophy is that, while out on patrol, each member of the sub-Unit has the potential to collect and produce raw information, partly based on what they observe and partly based on what they are told by the local populace. At the end of a patrol, it is now standard practice for the patrol leader to submit a patrol report, which is a collective effort, based on the experiences of the patrol members. This is entered into a database and analysed, sometimes by professional Intelligence staff and on other occasions by infantry soldiers trained in Intelligence work, who then work in a Battalion or Brigade Intelligence cell. The analysts can request further details from the patrol members, should their information require further analysis.[124]

The 6-stage model is also useful when it is provided to a person with little or no formal Intelligence training. It allows them to assimilate the concepts of the cycle and to extrapolate the deeper linkages from it such as the feedback loops, allowing the model to portray a sufficiently clear representation of the reality in which it functions. Thus the model provides a valuable construct which is equally useful, both in training and in operational deployment. This has a direct impact upon the collection stage of the model, as newly trained Intelligence staff can begin to collect effectively, because they understand where their work fits into the wider picture. The Australian Attorney General's office wrote a paper (McDowell, 1997) to encourage the development of

[124] The U.S. Army (2013:sec.9.1) calls the concept ES2, and defines it thus: "ES2 ensures that Soldiers are trained to actively observe for details for the commander's critical information requirement (CCIR) while in an AO. It also ensures they can provide concise, accurate reports. Leaders will know how to collect, process, and disseminate information in their unit to generate timely intelligence".

strategic Intelligence in the Australian Federal and State Police. The paper strongly supports the importance and validity of the Intelligence cycle as: "*… the basis for the development of all forms of intelligence, principally because it is such a logical sequence of processes that lends itself to flexible application depending upon the particular requirements of the intelligence task*" (McDowell, 1997:14).

During the mentoring of an Intelligence department in a foreign agency, it was this 6-stage version of the Intelligence cycle which the author selected to be taught during the initial training for the analysts, as well as to explain the strategic processes to the senior management of the department.[125] The same model was then used by the senior leadership team as a continual checklist of the processes ongoing within the department. Within one year, the 6-stage model became the standard Intelligence cycle for this foreign Intelligence department. It was codified still further when the Minister of the Interior for that country formally enshrined a local variant of the National Intelligence Model as the standard to be followed by all the security forces in that country.[126]

Within the modern Intelligence community of the UK, there is a very wide range of roles which contain "analyst" in their job description, and it follows that the duties and responsibilities of these analysts will have an equally wide spectrum, even when they work within the same Intelligence discipline. One COMINT analyst may typically spend his working day looking at the actual content of messages, extracting information to build up the knowledge about a particular subject such as a new weapon system. Another analyst in the same department may concentrate solely on network analysis, examining the

[125] The author was responsible for mentoring this department and its senior leadership team. The selection of the 6-stage model was made in preference to the U.S. model, partly because of the inclusion of evaluation as a component, and partly because the author had seen this model deployed in various theatres of operations, against a variety of targets and it was considered to be the most appropriate tool for this assignment.

[126] The initial draft of the local National Intelligence Model was written by a colleague of the author, who wishes to remain anonymous. It was subsequently enlarged and made more suitable for local consumption by the author. Essentially a cut-down version of the UK NIM, it helped to provide a structure and a framework for the eventual improvement of the department from a purely tactical focus, to the eventual production of more strategic Intelligence.

relationships, identities, locations and relative importance of component parts of that network. This could include individuals, modes of communication, geospatial details, responsibilities, etc.

One HUMINT analyst may focus primarily on a single individual's pattern of life, possibly to collect enough Intelligence on that person to enable the agency to approach them with a view to recruiting them as an Intelligence source. Another analyst in the same department could be conducting analysis on an individual who is involved in terrorist activities. The primary aim of the analyst's work could be to develop sufficient Intelligence to create a target folder which can be used to locate and arrest the individual, or to disrupt his activities. The range of tasks and the variations within the different roles of analysts renders it impossible to construct a model which would serve every use case. Hence the requirement for a generic and holistic tool which can be applied to all instances of the Intelligence domain. As one practitioner in SIGINT states:

> "*In my career, I've covered different countries, languages, threats and targets but everything I've worked on has been based on the Intelligence cycle. Now that I manage a team, I'm more involved in the cycle as a whole, not just the analysis and reporting. I get more involved in the tasking process, I ask questions about why certain things are tasked, and how they fit in to what I know is going on elsewhere, from colleagues in other teams. I also QC* [quality control] *reports now, so I'm big on evaluating the reports which we send out. It's so important……. because other agencies will come back and ask "why did you say X in this report?", but then again, we do the same. If it's relevant, I discuss their reports and ours with my opposite numbers in the other agencies*" (Source_12, 2011).

Omand (2010:248-249) states that the analyst is being asked to "*generate in the mind of the policy maker the equivalent of a virtual reality model of a possible future to which the policy-maker needs to respond*". The application of the 6-stage model is the precursor to the analyst being able to provide the policy-maker with Omand's virtual reality model of the future. He goes on to question the inevitability of the Intelligence cycle being a zero-sum game, accepting that this was arguably more the case during the Cold War. He posits that in more contemporary times, both sides can be seen to gain. He uses the example of the UK-U.S. revelations about the A. Q. Khan network which illicitly supplied the Libyan government with WMD technology. In this case, the Libyan government benefited from dismantling its WMD programme, and the UK and U.S. governments benefiting from the effective neutralisation of this serious threat to peace (Omand, 2010:134-35).

The Intelligence cycle was used effectively in the UK during several decades of the Cold War. At its highest point it operated on the grand strategic level, aimed at providing long-term policy guidance to senior, political decision-makers including the Prime Minister. It also functioned right down to the tactical level, providing Unit-level military commanders with detailed Intelligence on the capabilities of the Soviet elements which opposed them.[127] In the last two decades, as the threat of international terrorism has increased substantially, the cycle has been deployed against large groups, whether organised or semi-organised, as well as against small cells of active plotters numbering only three or four individuals. It has also been deployed effectively against "lone actors", one of the most difficult Intelligence targets to collect against.[128] The problem of the "lone actor" in terrorism is a relatively new field

[127] In the Armed Forces of the UK, a Unit is classed as a Regiment/Battalion or above. Elements below a Regiment/Battalion, such as a Company or a Platoon, are classified as sub-Units/

[128] One of the prime difficulties in targeting a "lone actor" is the absence of a known start point from which to begin an Intelligence collection effort. Gill, Horgan and Deckert (Gill et al., 2013) identified seven major findings: there was no uniform profile of lone-actor terrorists; In the time leading up to most lone-actor terrorist events, evidence suggests that other people generally knew about the offender's grievance, extremist ideology, views and/or intent to engage in violence; A wide range of activities and experiences preceded lone actors' plots or events; Many but not all lone-actor

of study, and recent research of interest is by Gill (Gill et al., 2013) and Borum (Borum et al., 2012).

In certain circumstances, Intelligence professionals are required to establish a new team or department at very short notice. In such a situation, they may have little or no prior knowledge of the target(s) which they will be tasked with collecting and reporting on. One such instance could be the deployment of British troops being sent to a small African nation which has descended into violent, internecine conflict such as the deployment of elements of the British Army to Sierra Leone as part of Operation PALLISER in 2000. Another such instance could be the establishing of a new team to conduct multi-agency cooperation within the Intelligence community. Intelligence professionals are often required to begin their operations from a blank sheet of paper. The pressure for the team or department to become fully operational as soon as possible can be very intense, especially if the operation receives Ministerial interest or if it takes place in the midst of constant media interest. In these circumstances it is imperative that the Intelligence collection plan can be transformed from theory into action, quickly and effectively. The Intelligence cycle has been deployed in numerous examples such as the ones described above, and has enabled targeted, actionable Intelligence to be collected within hours of the team being deployed.[129]

A key strength found within the UK Intelligence community is that the same, simple model of the cycle is widely understood across the agencies, which allows for a shorter timescale from the standing-up of a new, multi-agency team or department to the start of productivity. As one SIS officer commented:

terrorists were socially isolated; Lone-actor terrorists regularly engaged in a detectable and observable range of behaviours and activities with a wider pressure group, social movement or terrorist organization; Lone-actor terrorist events were rarely sudden and impulsive; Despite the diversity of lone-actor terrorists, there were distinguishable differences between ideological subgroups. Due to the sensitivity, it is not possible to discuss this particular “lone actor” case.

[129] The Author has been personally involved in a number of similar operations, working in a variety of roles including collector, analyst, and reporter and later directing the Intelligence operation.

> , "*…it helps that we are all on the same page as far as the basics go. When we work with the other agencies, everyone knows what needs to happen and, in general, we just get on with it. Don't get me wrong, we don't all sit in a meeting and discuss the intelligence cycle, or ask who does what. We've been working together for a long time now, and we all know what the others can bring to the table. I'd say that below the age of fifty, everyone is going to be familiar with it in our place. I can't speak for the other agencies in terms of numbers, but personally I'm used to working with people who understand the Intelligence cycle*" (Source_05, 2011).

Within the military Intelligence community of the UK, the use of "cross-pollenisation" (also known as cross-fertilisation in the Policing community) has constantly grown over the past 20 years. This principle is based on the recognition that there is much benefit to be gained by taking Intelligence staff from one specialisation, or agency, or even country, and embedding them with a different specialisation, agency or country. In the British Army's Intelligence Corps, this has long been a formalised process, wherein a language specialist, for example, could apply to train as a HUMINT source handler. The language specialist could then spend two or three years working in their new discipline before returning to their core specialisation.

As all specialist Intelligence operators are trained in the same model of the Intelligence cycle, they understand from the outset how different disciplines fit into the wider panorama of the Intelligence landscape. The linguist brings to the HUMINT Unit a different perspective, usually involving deeper and longer-term analysis which adds greater benefit to the targeting and recruitment team in particular. Conversely, the HUMINT Unit's work shows the linguist that the evaluation of a HUMINT source, in particular, is usually a more time-consuming process than it can be in SIGINT, particularly if the linguist is more used to working against a military target than a terrorist one. Once the linguist returns from the HUMINT world and resumes work in the SIGINT sphere, s/he will have gained a wider appreciation of the Intelligence collection effort and will have learned additional skills which can be employed in their daily Intelligence work.

This cross-pollenisation pays the largest dividends in the area of all-source fusion and this is especially strong in counter-terrorism, where multi-agency collaboration is essential. At the collection stage of the cycle, Intelligence specialists often work in uni-disciplinary teams or units, especially in the early years of their careers. This can result in an unintentionally blinkered *weltanschauung* of the collection field, as less experienced staff only see the collection, collation and analysis within their own field. Direction may be invisible to them, as they may simply receive their daily workload in their electronic in-box, which instructs them what to work on. Evaluation may also be invisible to them, as it may be conducted as a distinct, yet detached, process which takes place outside of their involvement or even awareness. While this may appear to be an ineffective, or even an elitist process, this is not necessarily the case. Some collectors may only be cleared for CONFIDENTIAL access and the output of their work moves up the chain to an area in which the staff may be cleared for access to SECRET or TOP SECRET material. The collected and processed material which left the analyst as a CONFIDENTIAL output would then be evaluated and analysed, and possibly reported on by staff with access to more than one source of Intelligence, or in some cases, to all-source Intelligence.

Examples of this in the UK include the Permanent Joint Headquarters (PJHQ), and the Joint Terrorism Analysis Centre (JTAC). In organisations such as these, Intelligence staff witness the complete cycle in action. At the highest level of security clearance, an analyst or manager would have access to the relevant JIC priorities, established in conjunction with the Prime

Minister. Collection of Intelligence would be conducted by the multiplicity of sources and methods, which could include SIGINT, HUMINT, IMINT, MASINT, OSINT and GEOINT among others. Collation would be done within PJHQ, accessing a vast array of data repositories using powerful aggregators and analytics engines designed to cope with “big data”. This helps produce detailed insights and reveal linkages and patterns which would otherwise remain invisible to the human eye.

Evaluation would be conducted as an on-going process by a multi-agency collection of staff, both military and civilian. They would look at all of the collection material from all of the providing sources, allowing for comparative analysis to be carried out across a wide range of incoming Intelligence. Analysis would also be done by a mixture of staff from different backgrounds and specialisations, which provides for a robust system of checks and balances. The intelligence is examined from multiple viewpoints and is comparatively assessed on a source by source basis.

The reporting work is sometimes done by the same team of analysts. At other times it is done by a dedicated team of reporters, and this can vary from section to section. The finished product which leaves PJHQ can be disseminated downwards and upwards. It can be sent to deployed Units in operational theatres, and it can equally be sent to the 4-star General holding the appointment of Commander Joint Operations. This could be the case for a strategically important report on a particular hot topic, such as the impending evacuation of UK nationals from a country in crisis, or a major change in the disposition of enemy forces in a theatre in which UK troops are engaged on the ground.

The cycle runs continuously in all-source establishments such as PJHQ and JTAC, covering foci such as geographical (e.g. Middle East and Africa), thematic (e.g. WMD proliferation), targeted (e.g. Al Qaeda in the Arabian Peninsula (AQAP)), or even single-person (e.g. the previous hunt for Abu Musab Al Zarqawi). All Intelligence staff, regardless of which areas of the cycle their work covers, are familiar with the cycle. They understand where their work fits into it and are able to deploy the cycle from scratch when a new Intelligence tasking is received, which has little or no existing information against it.

This requirement, for a team to be able to produce Intelligence as soon as possible after deploying, is commonplace for military Intelligence staff. The requirement brings with it the pressure to deliver accurate results in a potentially short time. At a strategic or operational level, there are generally not the same pressures on the staff. At the tactical level, the self-perceived responsibility can generate increased stress on the Intelligence staff, especially if operational action will be undertaken as a direct result of the Intelligence produced. As one Special Forces operator noted, "*when we go through the door, we want to know that it's the right door, and we want to know what opposition we're expecting. Going into the wrong building is a nightmare, but going into the right building and being out-gunned is a whole different kind of nightmare*" (Source_07, 2011).

Several practitioners highlighted the importance of evaluation in the cycle. Talking about the process of evaluation, an experienced senior analyst in GCHQ (Source_11, 2011) stated:

> "*…it starts immediately after direction. We usually know why we are collecting on the various targets, and without going into detail, there are many ways to skin a cat, so even before collection begins, there may be discussions about the suitability of this method versus that method, as the best way to provide what we are looking for. As an analyst, I'm involved in that process when it has a direct bearing on my work. I'll also routinely evaluate the collection, and when I'm engaged in the actual analysis, of course I'm evaluating what I'm*

> *analysing at the same time. Sometimes it's a subconscious process that I'm doing while I work, and I'm not really aware of it until I reach a natural break, or the end of the working day, when I look back over what I've been working on, and I can see my own evaluation process running through the day's work"*.

This comment raises an important point in the composition of the cycle. The placing of evaluation as a discrete component of the cycle carries with it a number of implications: that the evaluation process does not start until midway through the cycle; that the evaluation itself is carried out *en bloc*; and that once it is complete, the part of evaluation in the complete process has finished. An SIS officer (Source_06, 2011) agreed, adding that:

> "…*in HUMINT, evaluation is one of the most important things we do. When you're dealing with people, and what they tell you, it's crucial for us to evaluate not only the source, but also what they tell us. So while they're talking, I'm not just listening to what they are saying, and taking notes on the content. I'm also evaluating their words, their body language, how it fits with what I actually know already, whether it makes any alarm bells ring. I'm constantly evaluating, during the meeting and then afterwards, when I do the write-up. Because when I press the send button, you know, I have to be able to justify what I've written. I mean, internally, to my own people, and …… more and more now, externally, to customers outside my own organisation*".

This is underscored by a comment by Butler (2004:09), stating: "*for imagery and signals intelligence this is not usually an issue, although even here the danger of deception must be considered. But for human intelligence the validation process is vital.*" Towards the end of the 1990s, SIS had realised that their evaluation processes should be strengthened. As the former Controller of SIS, Sir Richard Dearlove, testified to the Butler commission:

> "*The Service has a very tough source evaluation process which was completely revised in the period late 1999 to 2001. It was a long exercise and we introduced new processes and systems. Now they, for resource reasons, obviously couldn't be immediately applied, because they are heavy duty, to every case but . . . it's something that we take incredibly seriously, where we have a highly developed process*" (Butler, 2004:103).

What Butler (2004:09) described in his overview of the validation process provides a succinct summary of the kinds of questions which analysts should ask themselves when evaluating information and Intelligence.[130] The *raison d'être* for the Butler report specifically included the evaluation of Intelligence, as Butler (2004:01) clearly pointed out in his introduction:

> "*to investigate the intelligence coverage available in respect of WMD programmes in countries of concern and on the global trade in WMD, taking into account what is now known about these programmes; as part of this work, to investigate the accuracy of intelligence on Iraqi WMD up to March 2003,and*

[130] See chapter 5.4

> *to examine any discrepancies between the intelligence gathered, evaluated and used by the Government before the conflict, and between that intelligence and what has been discovered by the Iraq survey group since the end of the conflict; and to make recommendations to the Prime Minister for the future on the gathering, evaluation and use of intelligence on WMD, in the light of the difficulties of operating in countries of concern*".

In the aftermath of the allied invasion of Iraq, the issue of evaluation came under very public scrutiny by large segments of the international media. A military Intelligence analyst agreed with the focus of attention, saying that:

> "*if we got it wrong about something as important as the invasion of another country, then it stands to reason that the decision-making should be examined. We all do evaluation as part of our jobs. You can't work as an analyst and not do it. But that's half the problem, isn't it? Who's to say if my evaluation is on target? I'm experienced enough, and sufficiently long in the tooth, that my bosses trust my judgement. I've been doing this a long time, and I learned from some of the best in the business. So when I put my name against a report, I'm also putting my professional reputation on the line, in a way. Below me, I'm a lot harder on my juniors, because what they tell me will have a major influence on what I report. That's the way it works. It probably doesn't sound very fool-proof, but all I can say is that you don't usually get put in a position of such responsibility until the system sees that you're the right fit, that you mainly "get it*

> *right" and that you're experienced enough to know what's what*" (Source_10 2011).

6.3 Summary

As with any model which attempts to show a high-level view of a process, the 6-stage Intelligence cycle has strengths and weaknesses. Certainly one of the most highlighted weaknesses from the range of interviews conducted with Intelligence practitioners was the fact that the evaluation component needed strengthening, and also that evaluation was not a single stage in the process. The pathologies identified by Sheptycki are rightly well-known within the academic study of Intelligence, as they created the first concrete contributions to the lexicon of such problems. It is often easier to tackle a problem when it can be identified and bounded. Some of these pathologies are almost so close to one another that there is an argument for some combinations being classed as a single pathology, but the work that Sheptycki did was unique. He led the way in classifying some of the more common problems which can be seen to afflict Police forces (and Intelligence agencies) in various parts of the world.

As with Hulnick's observations, though, it cannot be said that all of the problems, issues, vulnerabilities and challenges considered in this chapter are failures of the Intelligence cycle. The model describes the high-level processes which should ideally occur for the Intelligence process to take place. The large majority of the vulnerabilities identified by a number of academics are more human factors than anything, and while the model depends on the human input throughout its life-cycle, the mental processes undertaken by people, along with all of the resultant impedances such as bias, groupthink, etc., cannot be taken as flaws within the actual model.

One of the biggest strengths of the model is its simplicity, which allows it to be assimilated more quickly than, for example, the systems model described in this chapter. Another of its strengths is its ubiquity across the UK Intelligence community. This facilitates joint working in the counter-terrorism area, as there is a common understanding of the top-level processes which need to happen for the collection, production and dissemination of Intelligence to take place successfully. The description of how the cycle runs continuously in PJHQ illustrates how the entire model can run within one organisation. It collects and produces at tactical, operational and strategic levels if necessary, to support operations.

Chapter 7 Conclusions

The aim of this research was to examine the Intelligence cycle, specifically to assess whether it is still a suitable model for use in UK counter-terrorism. The Intelligence cycle would benefit from some restructuring and consolidation, resulting in an updated model called the “Intelligence triosphere”.

More so than Intelligence, the concept of terrorism is especially contentious. Defining a concept is never an easy task as any definition is inherently subjective in nature. The concept of terrorism holds an additional problem: chapter 3.1 demonstrated that there is a fundamental disagreement among the academic and legal community about whether the idea of defining terrorism can even be considered as a sound premise. The use of one or another definition to demonise and de-legitimise the opposition was also described, and within this issue resides one of the particular difficulties of creating a definition of terrorism which is seen as fair, inclusive, accurate, non-politicised and legally enforceable in accordance with UK, EU and UN concepts of rights. Indeed, the employment of a particular definition to delegitimise opposing views, groups or ideologies has been described as the weaponisation of terrorism definitions (Burke, 2013). Various definitions of terrorism were examined, which were created by international bodies, instruments of legislation, think-tanks, academics, legal scholars and others. One only needs to look at the decades of conflict between Palestinians and Israelis to see how the application of the terrorist label can be used as a political weapon, and how the labelling of various acts as terrorist acts can be amorphous. Even the United Nations has been incapable of formulating an organisation-wide definition for this problem. The academic discourse on defining terrorism is considerable and the many definitions of terrorism testify to the amount of study directed at this problem. Regarding the UK, however, the definition of terrorism which has the most relevance is that enshrined in the Terrorism Act 2000, as it is this definition against which acts are deemed to be, or not to be, terrorist acts.

The work of the Intelligence cycle in UK counter-terrorism takes place within the context of the CONTEST strategy, with its four constituent components: PURSUE, PREVENT, PROTECT and PREPARE. The CONTEST strategy is currently in its second revision, with a third revision due sometime in 2016. It has been shown that CONTEST is a broad yet deep strategy. It aims to stop terrorist attacks from taking place, to prevent individuals from being radicalised, to ensure that the critical national infrastructure is protected, and to allow post-attack recovery to take place as quickly and efficiently as possible.

CONTEST has not been without its critics, who raise concerns such as state surveillance, the ethics of detention and interrogation, and the delicate balance between free speech and glorifying or condoning terrorism. Nevertheless, the strategy is well constructed and its component parts have strong linkages between them, providing a cohesive national strategy. Some enhancements to CONTEST have come about as a result of non-terrorist action. One example is the realisation after the Kings Cross Underground fire, that robust and effective communications networks are essential for managing a major incident, and for implementing the post-incident/attack recovery phase.

The 6-stage Intelligence cycle was described in detail and each of the six stages were examined within the context of counter-terrorism work. Direction is set at the top level, by bodies such as the JIC and the NSC. This direction flows down to agency level and a collection plan is formulated for specified requirements. The collection process begins and it can involve one or more agencies, including those that do not collect Intelligence as a primary function. As the collection process gets underway, collation happens simultaneously. Complex searches are carried out against an array of data repositories, to retrieve existing data relevant to the target. Evaluation takes place at multiple layers and at all stages. In HUMINT and SIGINT, the source is evaluated separately from the Intelligence it provides. The importance of evaluation in the UK Intelligence cycle was underscored by Lord Butler's review following the 2003 invasion of Iraq

Analysis is often the most complex stage in the cycle. Despite the automation of some elements of the process, the human factors are still critical to the process. Nuances of language are still beyond the abilities of machine translation for any kind of fully automated process and are likely to remain so for some years. Various challenges have been identified in the field of analysis, and it remains the component most vulnerable to the vagaries of human behaviour.

The desired aim of an Intelligence product is usually to inform the decision-making process. This is the final stage of the model, dissemination, which produces the end product and distributes it to the relevant audience. Dissemination is controlled by caveats, such as security clearance, functional role and nationality. This final stage has undergone several changes in the past 30 years. The principle of "need to know" enshrined in Cold War policies underwent a dramatic change to "Intelligence support to the war fighter" in an effort to sanitise Intelligence and push it down to the lowest possible level at which it could be used, but could still be protected. The tear-line report provided a mechanism for this, allowing a report to be written at TOP SECRET above the dashed tear-line, and a highly sanitised version to be produced at a lower classification, below the tear-line.

Finally, the strengths and weaknesses of the Intelligence cycle were reviewed, drawing heavily on the experience of long-serving Intelligence professionals from across the UK Intelligence community. The various challenges of the analytical process were mapped against a range of common identifiers such as human factors, system factors and cultural factors.

Challenges within the analysis phase are often labelled as weaknesses of the Intelligence process itself. As chapter 6 explained, however, many of these challenges exist because of the human factors involved in analysing information. These can include an array of various biases, the conscious or unconscious pressures of peers that can result in groupthink, and the politicisation of Intelligence by policy makers or influencers.

Evaluation was identified as a weakness by Butler and others and the importance of this component to a valid and effective Intelligence process cannot be understated. This is an aspect that has had to be strengthened in the UK community during the decade following the 2003 invasion of Iraq. The politicisation of Intelligence poses particularly difficult problems for those engaged in collecting, analysing and reporting. The higher up the politicisation occurs, the greater the potential ramifications can be. The example of the Downing Street Memo was used as an example of this, showing how Sir Richard Dearlove believed the US administration were moulding their Intelligence to fit a desired political aim or outcome, an inversion of the concept of Intelligence-led policy.

A large number of challenges and vulnerabilities were detailed, which have been identified by a number of academics. The large number of challenges listed in the table gives an insight into some of the reasons why things can and do go wrong in the Intelligence process. These factors were mapped onto a separate landscape of human, system and cultural factors. The sheer number classified as human factors testifies to the pervasive roles which personality, mind-set, bias and previous experience play in the whole process of Intelligence production. Criticism has been levelled at the Intelligence cycle for being too simplistic, or for not reflecting the actual processes of real life. As chapter 6 explained, however, the simplicity of the model is also a key strength.

The importance was made of distinguishing between a model and a workflow. While a model is a simplified depiction of a process, a workflow can be expected to encompass a much greater level of detail. Some models put forward in recent years are highly detailed breakdowns of inputs, decision junctions and outputs, yet these are less suitable for the purposes of instruction, and for rapid deployment, due to their level of complexity. One of the main advantages of the 6-stage model is its simplicity. The ability to take a simple yet functional model and employ it in inter-agency work is a key strength. Likewise is the ability to use the model as an easy-to-understand tool when training Intelligence officers in developing nations. Attempting to teach a very detailed Intelligence workflow in such situations would be counter-productive, whereas even trainees with no prior Intelligence experience are able to grasp the components of the cycle. They can understand how the components interact with each other, and how feedback can loop back from any stage to any preceding stage.

This thesis has examined the Intelligence cycle in detail, not only insofar as its composition and components, but also within the wider context of the UK's counter-terrorism policy landscape. The contours of this policy landscape, like geographical contours, are not impervious to change and this policy landscape demonstrates displays evidence of change. The 6-stage cycle fulfils a necessary role within the counter-terrorism community and it has been used in many different conflicts and operational theatres with high success. There are some changes that could be made, however, that would make the model yet more effective.

While some US models have started with a joint component of planning and direction, the UK model has traditionally omitted the function of planning. In US models, this is widely perceived to take place at the policy level, and before direction is promulgated. Accepting that the model of the Intelligence cycle cannot encompass every aspect of the process from political decision-making through to covert action, it is suggested that the revised model still begins with direction, yet adds planning as the next function. Direction thus remains as the first step, when the Intelligence agencies are formally tasked with a target or a topic of interest. This direction is typically set at the national level by the JIC and its list of priority topics, and/or by the NSC. Chapter 1.5 explained how the JIC process functions and how the JIC priorities are derived. It is this strategic direction that arguably starts the planning process.

Planning becomes the second stage in the revised model, but in a slightly different capacity to that implied in US models. Here, the planning is more the designing of the Intelligence collection plan that outlines which assets, sources and methods will be used to conduct the collection. In temporal terms, this function sits between the formal tasking of the agencies and the start of the collection and collation process. It is an oft-unconsidered but vitally important function. Not only does it allocate resources but it also ensures that deconfliction is properly planned as a key part of the process.

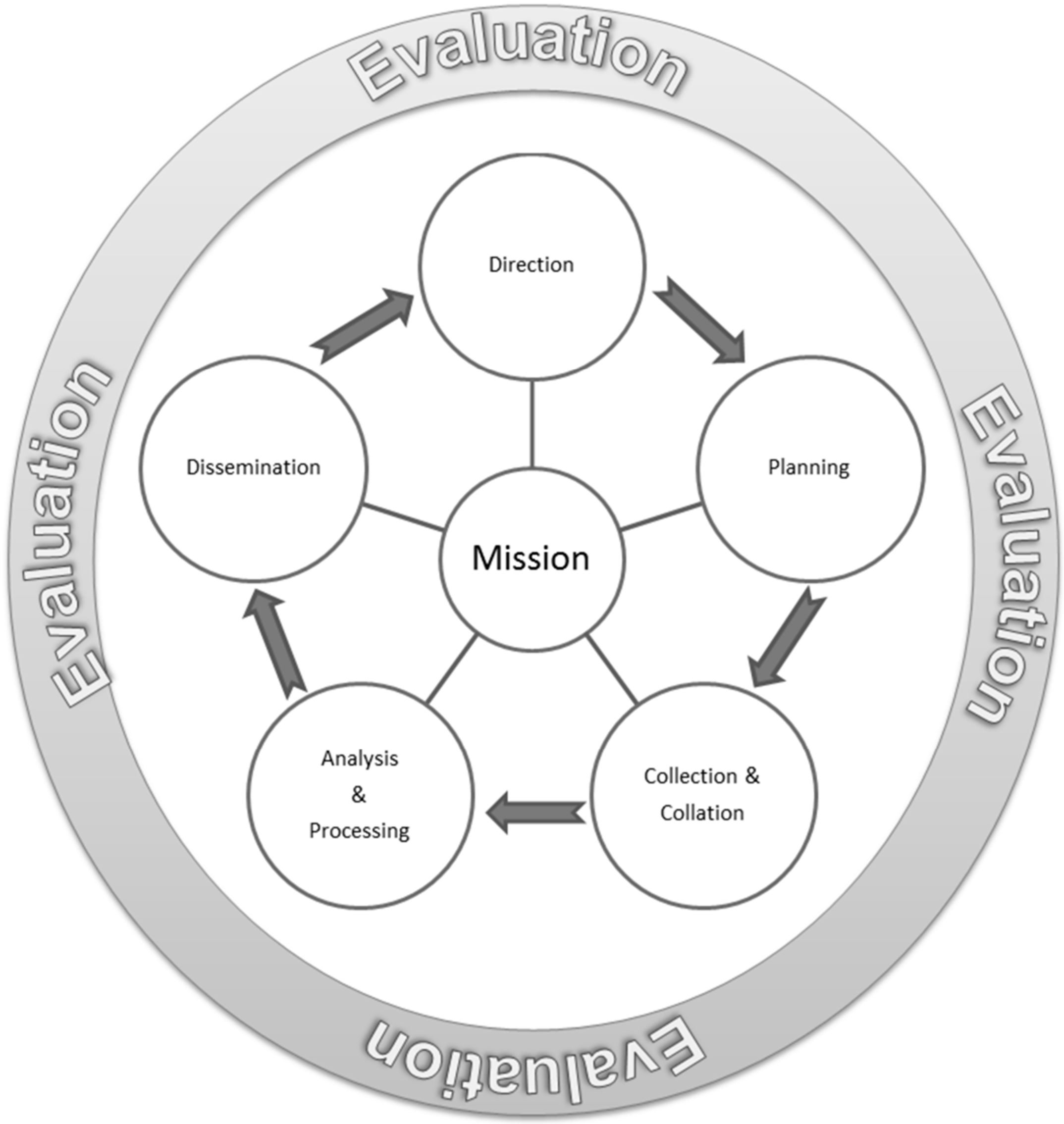
The importance of collation in the Intelligence process was explained, and the point was made that collation and collection often take place simultaneously. Both processes are not just conducted once in the cycle. When agencies are collecting against a high-value target (HVT) for example, collection can be instigated and continue for days, with no dissemination taking place during that time. Separating the two processes implies firstly that one process naturally follows the other. It also implies that one process cannot begin until the previous process has ended. In the case of collation and collection, this is not strictly true. Combining the processes into one component is a more accurate reflection of reality, and also ensures that collation is not dispensed with as a valuable and necessary process.

Analysis has traditionally been an individual component in the UK model, whereas in US models it is often combined with processing. Chapter five touched on this point, mentioning some of these processing tools such as decryption, translation, conversion, enhancement, etc. As so much raw information currently collected needs to undergo some kind of processing, it is beneficial to include it in the cycle. The natural bedfellow of processing is still analysis and the two components are better suited when combined in one stage.

Placing evaluation before analysis implies that no further evaluation takes place once the analysis begins. This is not the case, and evaluation plays a very important role in the analytical process. A good analyst will constantly be evaluating the material and its potential meaning or significance. Placing evaluation after analysis implies that everything which happens in the cycle until that point has taken place with no evaluation being done at all. Again, this is not an accurate reflection of the reality of the model in action. It is clear that the evaluation of Intelligence is less of an independent component in a cyclical model, and more of an intrinsic and omnipresent aspect that must be considered at every stage in the cycle. These considerations did not require a *tabula rasa* re-design from the ground upwards, but resulted in a revised model of the Intelligence cycle which is evolutionary, not revolutionary.

The revised model is the "Intelligence triosphere". It has a single composition, but with three distinct yet mutually connected spheres. Evaluation is placed within the outer, encompassing sphere, to more accurately reflect that the Intelligence cycle actually takes place *within* the environment of evaluation. Chapter 5.4 was devoted to the importance of evaluation and this importance is reflected in the new model. The triosphere model strengthens the concept that every part of the cycle, from planning to dissemination, must be subject to continuous evaluation to ensure that the necessary rigour of quality control takes place. .

Inside the middle sphere is the model itself, now consisting of the five components mentioned above, but presenting a more realistic depiction of the key processes. Finally, at the core of the model lies the mission. It is the mission that drives the cycle and without the mission, or an aim, the cycle is redundant. The mission is central to each component. At every stage of the process, Intelligence staff should be asking themselves whether their work is supporting the mission, and if not, what needs to change to ensure that it does. The updated model, the Intelligence triosphere, is depicted below:



26 The Intelligence Triosphere

The Intelligence domain has undergone major changes over the past 30 years. In 1984, much of the existing body of knowledge existed in printed form. Analysts commonly maintained individual “databases” in card index systems. Often these would be unique, meaning that it was difficult or even impossible to query the data within, unless one was physically located in the same place as the card index, or if there were secure communications with that location. Information was hard to come by, and there was generally a shortage of it, as a raw material for the Intelligence process. Nowadays the opposite is true. Intelligence officers are often engulfed in a “data tsunami”, and it can be a very time-consuming process to instigate a query and then have to pare down the results to a meaningful quantity, before any real analysis or evaluation can begin.

New skills have been added to the analyst’s profession, such as the ability to calculate geo-locational positions of various entities through highly technical means, such as the analysis of mobile phone metadata. Newer data sources can provide real-time Intelligence, especially in investigations into high-value targets.[131] Modern technology such as i2 Analyst Notebook has given analysts the ability to identify connections and relationships invisible to the naked eye, due to the complexity and size of the data sets involved. These include linkages between people and the things that they interact with, such as cars, international flights, mobile phones and email accounts.

Yet the fact remains that the work of Intelligence officers in UK counter-terrorism still follows a recognisable process that is best depicted as a cyclical model. The Intelligence triosphere proposed in this paper comes as a result of a thorough investigation into the functioning of the 6-stage cycle. This analysis has been enhanced through the personal experiences of a range of Intelligence officers familiar with its use in counter-terrorism. It has also been aided by the analysis of a substantial corpus of written material, primarily

[131] One example of this is the ability for Automatic Number Plate Recognition (ANPR) to generate a real-time alert when a target vehicle passes an ANPR sensor, providing genuinely real-time Intelligence to Investigators and analysts.

academic in nature, regarding the wider ecosystem within which the Intelligence process takes place. The enhancements made to the model are subtle refinements rather than ground-breaking alterations, as this paper has shown that the 6-stage cycle was not in need of major surgery, only a “nip and tuck”. Presenting this updated and refined model to Intelligence practitioners in governmental bodies would not involve any major re-think of the way in which their core business is conducted. Neither would it require much additional work in explaining this model to *ab initio* students encountering Intelligence theory and practice for the first time.

While the cycle itself benefits from this research, there is still work to be done. Defining terrorism is beset with an array of issues that strongly polarise the topic. As far as UK legislation is concerned, the definition enshrined in law continues to be that laid down in section one of the Terrorism Act 2000. Even if we accept that defining terrorism may be close to impossible, the debate itself generates useful material and ensures that the subject remains high on domestic and foreign agendas. The attempts to define Intelligence also encounter problems, but in this field the mix of academics and practitioners will hopefully ensure that research in this area continues to expand. Both of these areas of study can have a direct impact upon Intelligence work and the various models employed by agencies.

There will be criticism of any model of the Intelligence cycle, as anyone involved in the study, whether academic or practitioner, brings to the debate his or her own particular perception of the process. This can result in differences regarding a definition’s scope (e.g. broad and inclusive, or narrow and specific), or its focus (e.g. the process, or the outputs), or its targets (e.g. primarily foreign, or covering a wider spectrum of potential threats). There will also be criticism of the need to even have an Intelligence cycle, especially from those academics who see the model as an anachronism. Without a process, the collection and use of Intelligence cannot function effectively and the Intelligence triosphere is a simple yet robust model. The 6-stage cycle worked effectively, this much is evident from the comments from experienced practitioners as well as from the research detailed in this thesis. The main enhancements it required was that of evaluation being changed into a continuous aspect, rather than a distinct component, and the mission being placed at the core of the process. The updated Intelligence triosphere model proposed in this thesis refines the 6-stage Intelligence cycle but retains its core principles.

Counter-terrorism work in the UK will continue to be Intelligence-led for the foreseeable future, this much is certain. The employment of a simple, robust and effective model such as the Intelligence triosphere can only help to ensure that the Intelligence process is carried out effectively.

Annex A - Example of a Priority Intelligence Requirement

PIR	Intelligence Required	OSINT	SIGINT	HUMINT	IMINT	MILO	DIP	UN / NGOs
1.0.0	**How significant is ASEAN area as a generator of terrorism, internally and externally?**							
1.1.0	What is the Terrorism threat in each country?							
1.2.0	What is the Terrorist threat between the ASEAN states?							
1.3.0	How significant is the area, as an exporter of terrorism?							
2.0.0	**Does ASEAN have effective CT structures and measures in place? Are they effectively supported or implemented by ASEAN members?**							
2.1.0	What CT structures, if any, does ASEAN have in place?							
2.2.0	What CT structures ***should*** ASEAN have in place?							
2.3.0	What CT measures, if any, does ASEAN have in place?							
2.4.0	What CT measures, if any, ***should*** ASEAN have in place?							
2.5.0	How effectively are these CT strategies and measures supported by ASEAN states?							
2.6.0	How effectively are these CT strategies and measures implemented by ASEAN states?							
2.7.0	Are there any external factors which influence ASEAN CT strategies and their implementation?							
2.8.0	What are the effective capabilities of ASEAN							

	states to counter the terrorist threat?							
2.9.0	Is ASEAN efficient/effective in influencing CT in the SE Asian region?							
2.10.0	What counter-subversion capabilities does ASEAN have?							
	How important a factor is corruption of officials, in the overall CT issue?							
3.0.0	**What are the particular strengths/weaknesses of main ASEAN states in fight against terrorism, and what influence can the UK bring to bear to improve their performance?**							
3.1.0	Which are the main ASEAN states, and why?							
3.2.0	Has Thailand been successful in countering the terrorist threat? If so, why? If not, do they have a different terrorist threat to other ASEAN states?							
3.3.0	Could the FPDA be used as a model for inter-State cooperation?							
3.4.0	what did Australia do, post-Bali attack, in order to increase co-operation and effectiveness on CT strategies							
3.5.0	What does/could the UK do in the region to better stabilise the region?							
3.6.0	Can/should ASEAN countries deal/talk with terrorist organisations?							
	What opportunities and threats does the UK face, in any CT cooperation with ASEAN?							

Annex B - Participant Consent Form

INFORMED CONSENT FOR PARTICIPATION IN DOCTORAL THESIS EXAMINING THE INTELLIGENCE CYCLE

Research Project:

FIT TO FIGHT OR UNFIT FOR PURPOSE? THE EFFECTIVENESS OF THE INTELLIGENCE CYCLE IN UK COUNTER-TERRORISM SINCE 2003.

.

Researcher

Paul Burke

Dear Participant,

My name is Paul Burke and I am a former Intelligence professional who has spent his career working in this area. I am studying for a Professional Doctorate in Policing, Security and Community Safety at London Metropolitan University (LMU) in the United Kingdom. I am examining the effectiveness of the Intelligence cycle in UK counter-terrorism since 2003, as part of the requirement for the completion of this Doctorate. My credentials and affiliation as a student at the LMU can be established by contacting Dr. Nicholas Ridley, senior lecturer for the Department of Applied Social Sciences (DASS) at the LMU. He can be reached at:

email: (removed only in thesis copy)
tel: (removed only in thesis copy)This document constitutes an agreement to participate in my research project, the objective of which is to establish whether or not the Intelligence cycle is fit for purpose as a tool for UK counter-terrorism.

This portion of my research project consists of a participant's interview consisting of several open ended questions regarding your views and opinions in this particular area. Your involvement in this process is foreseen to last no more than 90 minutes.

Information will be recorded in hand-written format and/or will be captured by computer data entry or audio recorded for future transcription. Any information you disclose will be coded, analyzed, and compared to data obtained from other research participants. Where appropriate, information will be summarized in an anonymous format in the body of the final report. At no time will any specific comments be attributed to any individual unless specific agreement has been obtained beforehand. Audio recordings will not be disseminated publicly. Raw data including notes and tapes obtained from interviews will not be retained beyond the following durations. Audio recordings will be transcribed as soon as possible after the interview, following which the audio recording will be securely shredded beyond U.S. Department of Defense recommended standards (seven complex overwrites). Written notes will only be retained until the doctoral thesis has been accepted as submitted by London Metropolitan University, and until the oral defence of the thesis (the Viva) has been successfully conducted. Once these stages have been passed, the written notes will also be deleted. Until that time, all written and audio records of interviews will be encrypted using strong, commercial encryption.

In addition to submitting my final report to the LMU in partial fulfilment for a Doctorate of Policing and Community Safety Degree, I may discuss my research findings in general terms with UK government officials, but this will not involve any discussions on sources, roles, identities or other potentially identifying details. I may use the final paper for personal reasons and may include all or portions of it in future presentations, workshops or seminars. In the future, I may also use my findings and completed report for a journal submission or to be included in a book.

A copy of the final report will be offered by the Author to all respondents who provided an interview. It is planned that public access to the final paper through London Metropolitan University will be restricted at the Author's request, but this cannot be guaranteed.

If you choose to provide an interview, you are free to withdraw your consent at any time without prejudice. Any research data obtained from you will not be included in the research and will be destroyed as detailed above. If you would prefer to decline the audio recording of your interview, in preference for a written record only, this can be arranged. At any point in the interview, if you wish the audio recording to be stopped, and/or the written notes to cease, this will be complied with immediately.

If you have any further questions, I will be pleased to answer them prior to beginning this interview process.

By signing this letter, you give free and informed consent to participate in this project.

Name (Please Print)____

Signed:____

Date: ________________________________

Further to the above, if you do not wish to review the audio recording or transcribed version of your interview, please complete the below portion:

Name (Please
Print):____

Signed____

Date_____________________________________

Annex C – UN Conventions

The relevant UN conventions and instruments relating to terrorism are:

1. Convention on the High Seas, Apr. 29, 1958, 13 U.S.T. 2312;
2. United Nations Convention on Law of the Sea, Dec. 10, 1982, 21 I.L.M. l261;
3. Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, 27 I.L.M. 668;
4. Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, IMO. Doc. Sua/Con/l6/ Rev.1; 27 I.L.M. 685 (l0 Mar. l988);
5. Convention on Offences and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, 2 I.L.M. l042;
6. Convention for the Suppression of Unlawful Seizure of Aircrafts (Hijacking Convention), Dec. 16, 1970, l8 I.L.M. 1419;
7. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC Convention], Jan. 13, 1993, 32 I.L.M. 800;
8. Convention for the Suppression of the Financing of Terrorism [Terrorism Financing Convention];
9. U.N. Doc. a/54/l09 (9 Dec. l999) l33 (l6 Dec. l970);
10. Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Jan. 26, 1973, l0 I.L.M. 1151;
11. Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving Civil Aviation [Montreal Protocol], Jan. 12, 1988, 27 I.L.M. 627;

12. Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents [Diplomats Convention], Dec. 14, 1973, 13 I.L.M. 41;

13. Convention Against the Taking of Hostages [Hostage-Taking Convention], Dec. 17, 1979, l8 I.L.M. 1456;

14. Convention on the Safety of United Nations and Associated Personnel [U.N. Personnel Convention], available at http://www.un.org/law/cod/safety.htm (last visited Feb. 1, 2003);

15. Convention on the Marking of Plastic Explosives for the Purpose of Detection, Mar. 1, 1991, 30 I.L.M. 721;

16. Convention for the Suppression of Terrorist Bombings [Terrorist Bombing Convention], U.N. Doc. A/Res/52/164 (9 Jan. 1998);

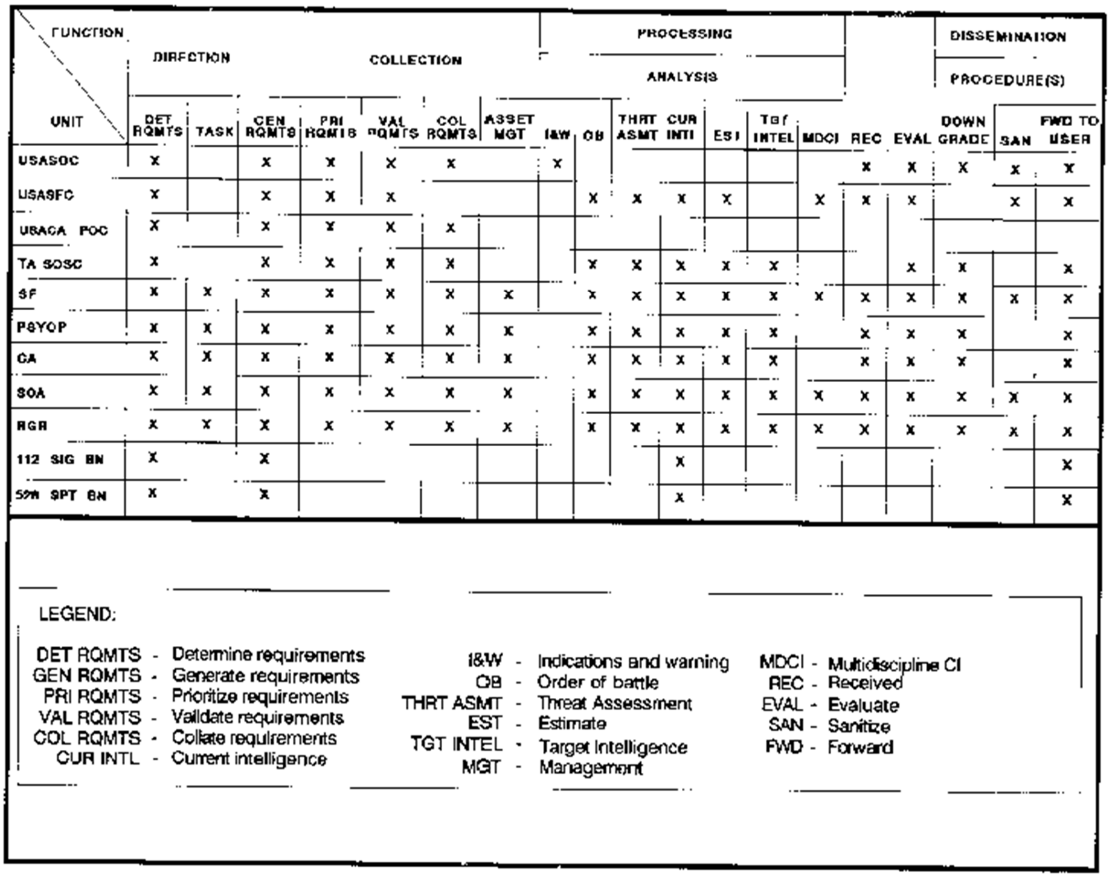
17. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction [BWC Convention], Apr. 10, 1972, 11 I.L.M. 309;

18. Convention on the Physical Protection of Nuclear Material, IAEA Doc. C/225;1456 U.N.T.S. 101; l8 I.L.M. 1419 (3 Mar. l980)

19. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC Convention], U.N. Doc. A/Res/47/39; l974 U.N.T.S. 3; 32 I.L.M. 800 (l3 Jan. l993)

Annex D – Example Intelligence Collection Plan

The following shows an actual sample of a U.S. Intelligence Collection Plan. Across the top are the requirements, broken down by the components of the Intelligence cycle. On the left side, are the collection assets.[132]



FUNCTION	DIRECTION				COLLECTION					PROCESSING							DISSEMINATION		
										ANALYSIS							PROCEDURE(S)		
UNIT	DET RQMTS	TASK	GEN RQMTS	PRI RQMTS	VAL RQMTS	COL RQMTS	ASSET MGT	I&W	OB	THRT ASMT	CUR INTL	EST	TGT INTEL	MDCI	REC	EVAL	DOWN GRADE	SAN	FWD TO USER
USASOC	X		X	X	X	X		X							X	X	X	X	X
USASFC	X		X	X	X				X	X	X	X		X	X	X		X	X
USACA POC	X		X	X	X	X													
TA SOSC	X		X	X	X	X			X	X	X	X	X			X	X		X
SF	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
PSYOP	X	X	X	X	X	X	X		X	X	X	X	X		X	X	X		X
CA	X	X	X	X	X	X	X		X	X	X	X	X		X	X	X		X
SOA	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
RGR	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
112 SIG BN	X		X								X								X
528 SPT BN	X		X								X								X

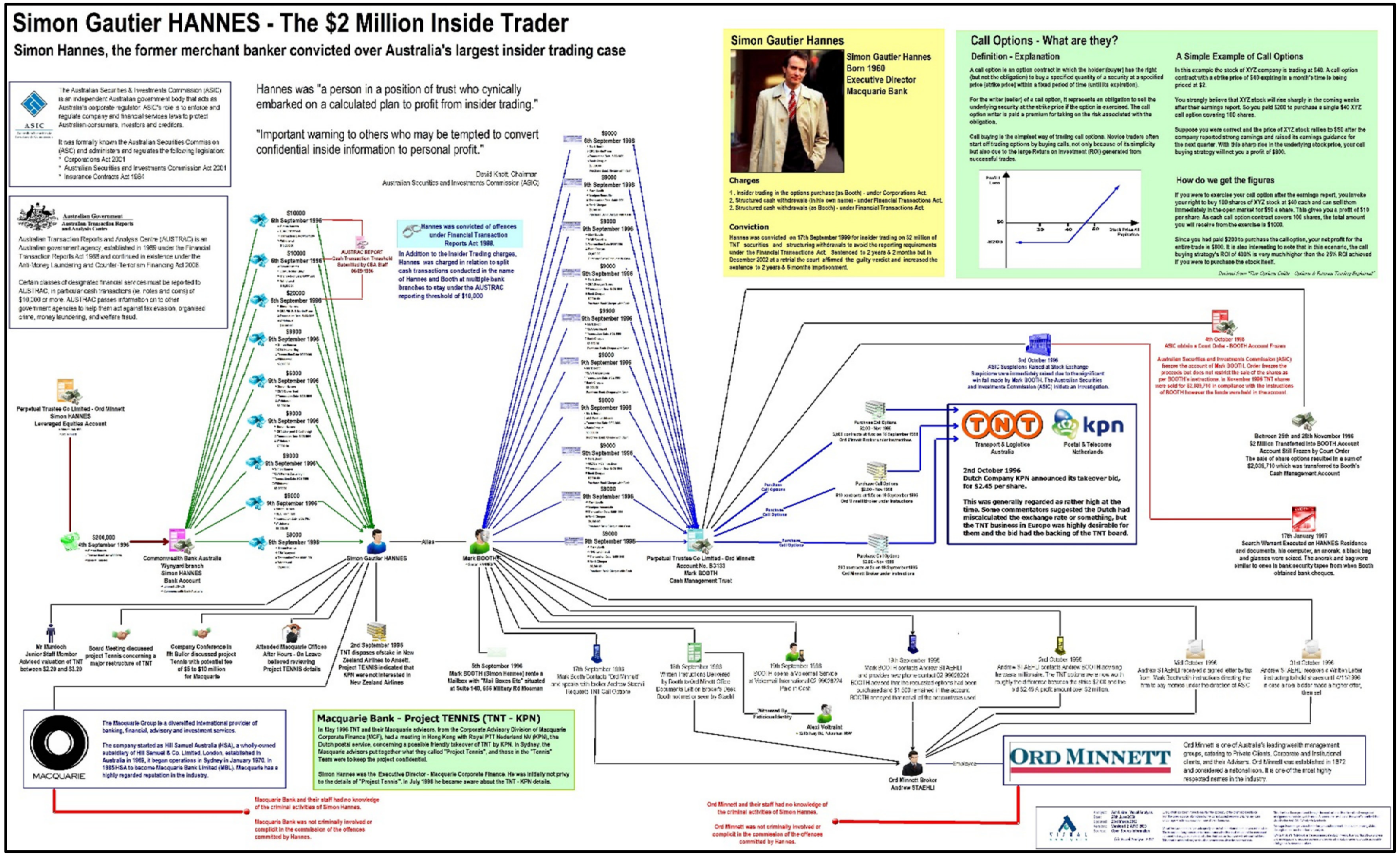
LEGEND:

DET RQMTS	Determine requirements	I&W	Indications and warning	MDCI	Multidiscipline CI		
GEN RQMTS	Generate requirements	OB	Order of battle	REC	Received		
PRI RQMTS	Prioritize requirements	THRT ASMT	Threat Assessment	EVAL	Evaluate		
VAL RQMTS	Validate requirements	EST	Estimate	SAN	Sanitize		
COL RQMTS	Collate requirements	TGT INTEL	Target Intelligence	FWD	Forward		
CUR INTL	Current intelligence	MGT	Management				

Figure 2-2. Intelligence cycle functional responsibilities.

[132] From the author's collection

Annex E –Financial investigation infographic



Simon Gautier HANNES - The $2 Million Inside Trader

Simon Hannes, the former merchant banker convicted over Australia's largest insider trading case

The Australian Securities & Investments Commission (ASIC) is an independent Australian government body that acts as Australia's corporate regulator. ASIC's role is to enforce and regulate company and financial services laws to protect Australian consumers, investors and creditors.

It was formally known the Australian Securities Commission (ASC) and administers and regulates the following legislation:
* Corporations Act 2001
* Australian Securities and Investments Commission Act 2001
* Insurance Contracts Act 1984

Australian Government Australian Transaction Reports and Analysis Centre

Australian Transaction Reports and Analysis Centre (AUSTRAC) is an Australian government agency, established in 1989 under the Financial Transaction Reports Act 1988 and continued in existence under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

Certain classes of designated financial services must be reported to AUSTRAC, in particular cash transactions (ie. notes and coins) of $10,000 or more. AUSTRAC passes information on to other government agencies to help them act against tax evasion, organised crime, money laundering, and welfare fraud.

Hannes was "a person in a position of trust who cynically embarked on a calculated plan to profit from insider trading."

"Important warning to others who may be tempted to convert confidential inside information to personal profit."

David Knott, Chairman
Australian Securities and Investments Commission (ASIC)

Hannes was convicted of offences under Financial Transaction Reports Act 1988.

In Addition to the Insider Trading charges, Hannes was charged in relation to split cash transactions conducted in the name of Hannes and Booth at multiple bank branches to stay under the AUSTRAC reporting threshold of $10,000

Simon Gautier Hannes

Simon Gautier Hannes
Born 1960
Executive Director
Macquarie Bank

Charges

1. Insider trading in the options purchase (as Booth) - under Corporations Act.
2. Structured cash withdrawals (in his own name) - under Financial Transactions Act.
2. Structured cash withdrawals (as Booth) - under Financial Transactions Act.

Conviction

Hannes was convicted on 17th September 1999 for insider trading on $2 million of TNT securities and structuring withdrawals to avoid the reporting requirements under the Financial Transactions Act. Sentenced to 2 years & 2 months but in December 2002 at a retrial the court affirmed the guilty verdict and increased the sentence to 2 years & 5 months imprisonment.

Call Options - What are they?

Definition - Explanation

A call option is an option contract in which the holder (buyer) has the right (but not the obligation) to buy a specified quantity of a security at a specified price (strike price) within a fixed period of time (until its expiration).

For the writer (seller) of a call option, it represents an obligation to sell the underlying security at the strike price if the option is exercised. The call option writer is paid a premium for taking on the risk associated with the obligation.

Call buying is the simplest way of trading call options. Novice traders often start off trading options by buying calls, not only because of its simplicity but also due to the large Return on Investment (ROI) generated from successful trades.

A Simple Example of Call Options

In this example the stock of XYZ company is trading at $40. A call option contract with a strike price of $40 expiring in a month's time is being priced at $2.

You strongly believe that XYZ stock will rise sharply in the coming weeks after their earnings report. So you paid $200 to purchase a single $40 XYZ call option covering 100 shares.

Suppose you were correct and the price of XYZ stock rallies to $50 after the company reported strong earnings and raised its earnings guidance for the next quarter. With this sharp rise in the underlying stock price, your call buying strategy will net you a profit of $800.

How do we get the figures

If you were to exercise your call option after the earnings report, you invoke your right to buy 100 shares of XYZ stock at $40 each and can sell them immediately in the open market for $50 a share. This gives you a profit of $10 per share. As each call option contract covers 100 shares, the total amount you will receive from the exercise is $1000.

Since you had paid $200 to purchase the call option, your net profit for the entire trade is $800. It is also interesting to note that in this scenario, the call buying strategy's ROI of 400% is very much higher than the 25% ROI achieved if you were to purchase the stock itself.

Derived from "The Options Guide - Options & Futures Trading Explained"

Mr Murdoch
Junior Staff Member
Advised valuation of TNT between $2.20 and $3.20

Board Meeting discussed project Tennis concerning a major restructure of TNT

Company Conference in Mt Buller discussed project Tennis with potential fee of $5 to $10 million for Macquarie

Attended Macquarie Offices After Hours - On Leave believed reviewing Project TENNIS details

2nd September 1996
TNT disposes of stake in New Zealand Airlines to Ansett. Project TENNIS indicated that KPN were not interested in New Zealand Airlines

5th September 1996
Mark BOOTH (Simon Hannes) rents a Mailbox with "Mail Boxes Etc" situated at Suite 140, 656 Military Rd Mosman

17th September 1996
Mark Booth Contacts "Ord Minnett" and speaks with broker Andrew Staehli Requests TNT Call Options

18th September 1996
Written Instructions Delivered by Booth to Ord Minnett Office Documents Left on Broker's Desk Booth not met or seen by Staehli

19th September 1996
BOOTH opens a Voicemail Service at Voicemail International 02 99028224 Paid in Cash

19th September 1996
Mark BOOTH contacts Andrew STAEHLI and provides new phone contact 02 99028224 BOOTH advised that the requested options had been purchased and $1 500 remained in the account. BOOTH annoyed that not all of the account was used

2nd October 1996
Andrew STAEHLI contacts Andrew BOOTH advising he was a millionaire. The TNT options were now worth roughly the difference between the strike $2.00 and the bid $2.45 A profit amount over $2 million.

Mid October 1996
Andrew STAEHLI received a signed letter by fax from Mark Booth with instructions directing the firm to pay monies under the direction of ASIC

31st October 1996
Andrew STAEHLI receives a Written Letter instructing to hold shares until 4/11/1996 in case a rival bidder made a higher offer, then sell

3rd October 1996
ASIC Suspicions Raised at Stock Exchange
Suspicions were immediately raised due to the significant windfall made by Mark BOOTH. The Australian Securities and Investments Commission (ASIC) initiate an investigation.

4th October 1996
ASIC obtain a Court Order - BOOTH Account Frozen

Australian Securities and Investments Commission (ASIC) freeze the account of Mark BOOTH. Order freezes the proceeds but does not restrict the sale of the shares as per BOOTH's instructions. In November 1996 TNT shares were sold for $2,039,710 in compliance with the instructions of BOOTH however the funds were held in the account.

TNT Transport & Logistics Australia

kpn Postal & Telecome Netherlands

2nd October 1996
Dutch Company KPN announced its takeover bid, for $2.45 per share.

This was generally regarded as rather high at the time. Some commentators suggested the Dutch had miscalculated the exchange rate or something, but the TNT business in Europe was highly desirable for them and the bid had the backing of the TNT board.

Between 25th and 28th November 1996
$2 Million Transferred into BOOTH Account
Account Still Frozen by Court Order
The sale of share options resulted in a sum of $2,039,710 which was transferred to Booth's Cash Management Account

17th January 1997
Search Warrant Executed on HANNES Residence and documents, his computer, an anorak, a black bag and glasses were seized. The anorak and bag were similar to ones in bank security tapes from when Booth obtained bank cheques.

MACQUARIE

The Macquarie Group is a diversified international provider of banking, financial, advisory and investment services.

The company started as Hill Samuel Australia (HSA), a wholly-owned subsidiary of Hill Samuel & Co. Limited, London, established in Australia in 1969, it began operations in Sydney in January 1970. In 1985 HSA to become Macquarie Bank Limited (MBL). Macquarie has a highly regarded reputation in the industry.

Macquarie Bank - Project TENNIS (TNT - KPN)

In May 1996 TNT and their Macquarie advisors, from the Corporate Advisory Division of Macquarie Corporate Finance (MCF), had a meeting in Hong Kong with Royal PTT Nederland NV (KPN), the Dutch postal service, concerning a possible friendly takeover of TNT by KPN. In Sydney, the Macquarie advisors put together what they called "Project Tennis", and those in the "Tennis" Team were to keep the project confidential.

Simon Hannes was the Executive Director - Macquarie Corporate Finance. He was initially not privy to the details of "Project Tennis". In July 1996 he became aware about the TNT - KPN details.

Macquarie Bank and their staff had no knowledge of the criminal activities of Simon Hannes.

Macquarie Bank was not criminally involved or complicit in the commission of the offences committed by Hannes.

ORD MINNETT

Ord Minnett is one of Australia's leading wealth management groups, catering to Private Clients, Corporate and Institutional clients, and their Advisers. Ord Minnett was established in 1872 and considered a national icon. It is one of the most highly respected names in the industry.

Ord Minnett and their staff had no knowledge of the criminal activities of Simon Hannes.

Ord Minnett was not criminally involved or complicit in the commission of the offences committed by Hannes.

Annex F – Example Tear Line Report

SIMULATION SECRET

Report Serial: 6V92PQR-001

Flags: TERRORISM/CIGARISTAN LIBERATION ARMY/WEAPONS/MONEY-LAUNDERING

Title: JOHN SMITH IDENTIFIED AS SENIOR UK-BASED PLANNER FOR CIGARISTAN LIBERATION ARMY. CONFIRMED INVOLVEMENT IN ORGANISING MOVEMENT OF FUNDS TO FACILITATE PURCHASE OF AUTOMATIC WEAPONS AND EXPLOSIVES FOR ONWARD SHIPMENT TO CIGARISTAN

Source Evaluation: A-3-4

Source Description: A previously reliable source with indirect access to SMITH. Confirmed by Agency X.

John SMITH has been confirmed as the senior, UK-based operational planner for the Cigaristan Liberation Army (CLA). Smith is believed to have held the role for at least two years and is responsible for all financial operations (including the laundering of criminally obtained funds) and the purchasing and transfer of weapons and explosives.

SMITH is the director of a small logistics company which is used to facilitate the transfer of weapons and explosives and is also used to move other…..

SIMULATION SECRET

------Detach below this line for SIMULATION CONFIDENTIAL report---------

SIMULATION CONFIDENTIAL

John Smith has been identified as a senior member of the Cigaristan Liberation Army.

------------------------------------ CONFIDENTIAL ----------------------------------

Annex G - Community Engagement to Counter-Terrorism

(Metropolitan Police Authority 2007, sec.G)

3. What is the main purpose or aims of the policy, strategy or project?

- Sustain and widen informed, factual debate on how our society should respond to the terrorist threat
- Provide an opportunity for the police to explain what they do in this field, and why, and to dispel any misconceptions or misinformation
- Heighten public understanding of the national and international dimensions of MPS counter-terrorism functions and roles
- Enable the community to inform the police of their issues, considerations and tensions, leading to better-informed police decision-making
- Seek policy direction and strategic steer on counter-terrorism for the police from the public
- Challenge unproductive stereotyping of communities and polarisation of arguments with regard to terrorism and counter-terrorism
- Enable the MPA better to scrutinise MPS expenditure on counter-terrorism policing and better to oversee the community engagement aspects of this expenditure
- Enable the MPA to make a more informed assessment of the corporacy of the MPS approach to counter-terrorism
- Elicit from members of the community new ideas for new ways of working
- Foster a sense of public ownership of the problems, and their solutions
- Increase the likelihood of generating future community intelligence
- Increase public understanding of and confidence in the role of the MPA
- Demonstrate the MPA as guarantor of police transparency and accountability
- Build social capital – and therefore resilience – in London
- Assist other organisations to appreciate the impact their activity has on London's communities with regard to counter-terrorism

Annex H – Relevant Public Authorities – RIPA 2000

The following bodies are authorised to conduct covert surveillance under the auspices of the Regulation of Investigatory Powers Act 2000 (RIPA).

Regulation of Investigatory Powers Act 2000 c. **23** 95

SCHEDULES

SCHEDULE 1 Section 30.

Relevant Public Authorities

Part I

Relevant authorities for the purposes of ss. 28 and 29

Police forces etc.

1. Any police force.
2. The National Criminal Intelligence Service.
3. The National Crime Squad.
4. The Serious Fraud Office.

The intelligence services

5. Any of the intelligence services.

The armed forces

6. Any of Her Majesty's forces.

The revenue departments

7. The Commissioners of Customs and Excise.
8. The Commissioners of Inland Revenue.

Government departments

9. The Ministry of Agriculture, Fisheries and Food.
10. The Ministry of Defence.

11. The Department of the Environment, Transport and the Regions.

12. The Department of Health.

13. The Home Office.

14. The Department of Social Security.

15. The Department of Trade and Industry.

The National Assembly for Wales

16. The National Assembly for Wales.

Local authorities

17. Any local authority (within the meaning of section 1 of the Local 1999 c. 27.

Government Act 1999).

Sch. 1

Other bodies

18. The Environment Agency.

19. The Financial Services Authority.

20. The Food Standards Agency.

21. The Intervention Board for Agricultural Produce.

22. The Personal Investment Authority.

23. The Post Office.

Part II

Relevant authorities for the purposes only of s. 28

The Health and Safety Executive

24. The Health and Safety Executive.

NHS bodies in England and Wales

1977 c. 49. 25. A Health Authority established under section 8 of the National Health
Service Act 1977.
26. A Special Health Authority established under section 11 of the National Health Service Act 1977.
1990 c. 19. 27. A National Health Service trust established under section 5 of the National
Health Service and Community Care Act 1990.

The Royal Pharmaceutical Society of Great Britain

28. The Royal Pharmaceutical Society of Great Britain.

Annex I – The Eight Attributes of Intelligence Excellence, as considered by the U.S. Joint Chiefs of Staff

In their Joint Publication 2-0 (Joint Intelligence) of 2013, the JCS (Joint Chiefs of Staff 2013, pp.II–6 to II–8) define eight attributes of Intelligence excellence. Their definitions of these attributes are provided below.

a. **Anticipatory.** Intelligence must anticipate the informational needs of the commander and joint force staff in order to provide a solid foundation for operational planning and decision-making. Anticipating the joint force's intelligence needs requires the intelligence staff to identify and fully understand the command's current and potential missions, the commander's intent, all relevant aspects of the OE (operational environment), and all possible friendly and adversary COAs (courses of action). Most important, anticipation requires the aggressive involvement of intelligence in operation planning at the earliest time possible.

b. **Timely.** Intelligence must be available when the commander requires it. Timely intelligence enables the commander to anticipate events in the operational area. In turn, this enables the commander to time operations for maximum effectiveness and to avoid being surprised. Usually, the need to balance timeliness and completeness should favor timeliness, and if incomplete should be stated in the product, and followed up later. Recognizing and balancing the subtle differences relative to timeliness and completeness is one of the critical art forms for good intelligence.

c. **Accurate.** Intelligence must be factually correct, relay the situation as it actually exists, and provide an understanding of the OE based on the rational judgment of available information. This judgment should evaluate the possibility of an adversary's denial and deception effort. The accuracy of intelligence products may be enhanced by placing proportionally greater emphasis on information reported by the most reliable sources. Evaluate source reliability through a feedback process in which past data received from a source is compared with the "ground truth" (for example, when subsequent events or information confirm the source's accuracy).

d. **Usable.** Intelligence must be tailored to the commander's specific needs, and provided in forms suitable for immediate comprehension. Providing useful intelligence requires its producers to understand the decisions facing the commander, the relevance and impact of intelligence on those decisions, and how to deliver the intelligence to the commander in context so that it balances efficiency and effectiveness. Commanders operate under mission, operational, and time constraints that shape their intelligence requirements and determine how much time they have to study the intelligence provided. They must be able to quickly apply intelligence to the task, and may not have sufficient time to analyze complex intelligence reports. Therefore the "bottom line" must be up front used to effectively convey intelligence.

e. **Complete.** Complete intelligence answers the commander's questions about the adversary and other aspects of the OE to the extent possible, and informs the commander of significant intelligence gaps. To be complete, intelligence must identify relevant aspects of the OE that may impact mission accomplishment or the joint operation execution and offer alternative analysis. Complete intelligence informs the commander of all major COAs that are available to the adversary, and identifies those assessed as most likely and most dangerous. While providing available intelligence to those who need it when they need it, the intelligence staff must give priority to the commander's unsatisfied critical requirements. Intelligence organizations must anticipate and respond to the commander's existing and contingent intelligence requirements by evaluating the intelligence process input and output surrounding the mission.

f. **Relevant.** Intelligence must be relevant to the planning and execution of the operation at hand, and aid the commander in the accomplishment of the mission. It must contribute to the commander's understanding of the adversary and other significant aspects of the OE, but not burden the commander with intelligence that is of minimal or no importance to the current mission. To produce relevant intelligence, the J-2 staff must remain cognizant of the commander’s intent and understanding of how the operational concept inflicts desired effects upon the adversary to achieve the military objectives and secure the end state. The J-2 staff must also update requirements as the friendly mission or the adversary situation changes.

g. **Objective.** Due to the decisive and consequential impact of intelligence on operations and reliance of planning and operations decisions on intelligence, it is important for the J-2 to maintain objectivity and independence in developing assessments. When informing the commander, joint intelligence must be vigilant in guarding against biases that shade, slant, or frame assessments to favor the commander’s chosen COA or to fit the commander’s preconceived notions. In particular, intelligence should recognize each adversary as unique, and avoid mirror imaging while realizing the possible bias involved in their assessment type. For example, current intelligence and warning intelligence estimates may assess the same indicators differently. Red teams can be used to check analytical judgments by ensuring assumptions about the adversary are sound and intelligence assessments help minimize mirror imaging and cultural bias.

h. **Available**. Intelligence must be readily accessible to the commander. Availability is a function of not only timeliness and usability, but also appropriate security classification, interoperability, and connectivity. Intelligence producers must strive to provide information at the most appropriate level of classification and least restrictive releasability caveats, thereby maximizing the consumers’ access, while protecting sources of information and methods of collection.

Index

analysis, 18, 19, 20, 22, 24, 29, 32, 33, 41, 43, 45, 46, 47, 48, 58, 61, 62, 65, 69, 71, 73, 75, 76, 78, 80, 82, 111, 127, 130, 139, 186, 187, 189, 191, 196, 199, 201, 206, 207, 208, 211, 217, 218, 219, 220, 221, 222, 225, 230, 234, 235, 237, 241, 242, 247, 248, 253, 256, 262, 263, 266, 272, 273, 275, 278, 279, 280, 281, 284, 285, 286, 287, 295, 298, 301

AS, 31

Assessments Staff, 31

CBRN

Chemical, Biological, Radiological, Nuclear, 171

CDRP, 113

CESG, 28

Chomsky, 17

Chomsky, Noam, 17

CIA, 15

Central Intelligence Agency, 49, 68, 69, 82, 124, 172, 201, 206, 221, 222, 262, 275

CNI, 74, 156, 171, 188

Critical National Infrastructure, 27

collation, 24, 78, 115, 139, 206, 207, 208, 209, 220, 230, 236, 253, 285, 294, 298

collection, xi, 15, 18, 20, 24, 25, 26, 27, 29, 41, 46, 49, 62, 63, 68, 69, 71, 73, 75, 82, 84, 111, 124, 136, 139, 173, 186, 187, 191, 193, 196, 198, 199, 200, 201, 202, 203, 204, 205, 208, 216, 219, 220, 225, 226, 230, 235, 236, 237, 244, 248, 253, 254, 255, 275, 276, 279, 282, 283, 285, 286, 287, 292, 294, 298, 302, 312

CONTEST, xi, 23, 62, 111, 112, 113, 114, 127, 137, 160, 171, 174, 176, 184, 185, 187, 189, 191, 234, 294

Critical National Infrastructure, 27, 74, 112, 156

Current Intelligence Groups, 31

Davidson-Glass, 15

Davies, 16

Defence Advisory Notice 5

D Notice, 26

DI, 25, 26, 29, 138, 189

direction, 15, 24, 30, 48, 60, 91, 115, 130, 139, 171, 186, 193, 194, 195, 196, 221, 229, 230, 236, 253, 255, 271, 287, 294, 297, 315

DIS, 26, 29

dissemination, 20, 47, 73, 80, 115, 187, 213, 215, 219, 223, 225, 226, 227, 231, 249, 270, 292, 295, 298

evaluation, 24, 64, 75, 76, 80, 113, 115, 139, 187, 201, 207, 211, 212, 213, 215, 217, 220, 231, 253, 255, 256, 263, 266, 280, 285, 287, 288, 289, 290, 291, 295, 298, 299, 301, 303

FBI, 15

Federal Bureau of Investigation, 75, 157, 165, 173, 275

Feedback, 224

GCHQ, 26, 28, 30, 31, 36, 57, 58, 64, 115, 126, 139, 189, 194, 195, 263, 265, 266, 287
Glass, 14

high-value target
    HVT, 133, 298
HUMINT, 26, 46, 199, 202, 203, 205, 206, 213, 215, 217, 223, 263, 275, 281, 284, 286, 288

IA
    Information Assurance, 28
Intelligence cycle, 191
Intelligence failure. *Also See* Intelligence gap
Intelligence gap. *Also See* Intelligence Failure
Intelligence Services Act 1994, 27, 28, 36
Intelligence triosphere, 293, 299, 301, 302, 303
Interoperability, 174

JIC, 22, 30, 31, 32, 33, 66, 115, 139, 186, 194, 197, 229, 236, 245, 253, 285
JIO, 31
Joint Intelligence Committee, 30, 33, 194
Joint Intelligence Organisation, 31
JTAC, 25, 28, 29, 265, 285, 286

MAPPA, 113

pathology
    pathologies, 221, 291
Permanent Joint Headquarters (PJHQ), 285
PHIA, 31, 32, 33
politicisation, 16, 18, 20, 33, 83, 85, 109, 221, 241, 242, 245, 246, 296
PREPARE, 23, 111, 112, 113, 171, 174, 176, 177, 178, 181, 183, 188, 294
PREVENT, 23, 69, 111, 112, 113, 115, 125, 126, 131, 141, 142, 143, 144, 145, 146, 147, 152, 154, 178, 187, 188, 294
Priority Intelligence Requirements. *See* PIRs
processing, 15, 60, 68, 75, 206, 222, 255, 256, 262, 268, 298
PROTECT, 23, 111, 112, 156, 159, 171, 188, 294
PURSUE, 23, 111, 113, 114, 115, 116, 125, 128, 133, 136, 188, 294

Regulation of Investigatory Powers Act, 28
RIPA, 28, 116, 117, 122, 123, 316

Security Services Act 1989, 27
SIGINT, 28
silos. *Also See* stovepipes
stovepipes. *Also see* silos

Tasking, 193

validation. *See* evaluation

Warner, 16

Zarqawi, Abu Musab Al, 217

Bibliography

Abass, A., 2011. *Assessing NATO's involvement in Libya*, Available at: http://unu.edu/publications/articles/assessing-nato-s-involvement-in-libya.html.

Aburish, S.K., 1999. *Arafat: From Defender to Dictator*, London: Bloomsbury Publishing.

ACPO, 2006. *Major Incident Analysis Manual (Revised Edition 2006)*, Wyboston.

ACPO, 2014. National CHANNEL Referral Figures. *ACPO Website*. Available at: http://www.acpo.police.uk/ACPOBusinessAreas/PREVENT/NationalChannelReferralFigures.aspx [Accessed October 2, 2014].

ACPO, 2015. What PREVENT means to you. *ACPO Website*. Available at: http://www.acpo.police.uk/ACPOBusinessAreas/PREVENT/WhatPreventmeanstoyou.aspx [Accessed January 26, 2015].

ACPO PREVENT Delivery Unit, 2009. *Channel – A Partnership Approach to Support Individuals Vulnerable to Recruitment by Violent Extremists*, London.

ACPO TAM, 2008. *ACPO (TAM) Police PREVENT Strategy - Partners Briefing*,

Aid, M., 2009. All glory is fleeting: SIGINT and the fight against international terrorism. In C. Andrew, R. J. Aldrich, & W. K. Wark, eds. *Secret Intelligence: A Reader*. Oxford: Routledge (Taylor and Francis), p. 552.

Aldrich, R.J., 2009. Intelligence and Iraq. In *Secret Intelligence: A Reader*. Oxford: Routledge (Taylor and Francis), pp. 229–244.

Aldrich, R.J., 2005. Whitehall and the Iraq War on UK's Four Intelligence Enquiries. *Irish Studies in International Affairs*, 16, pp.73–88.

Allen, G., 1995. The Professionalization of Intelligence. In D. H. Dearth & T. R. Goodden, eds. *Strategic Intelligence: Theory and Application*. Washington, D.C.: Joint Military Intelligence Training Center (JMITC).

Andrew, C., 2004. *Intelligence analysis needs to look backwards before looking forward Christopher Andrew*, Cambridge. Available at: http://www.historyandpolicy.org/policy-papers/papers/intelligence-analysis-needs-to-look-backwards-before-looking-forward.

Andrew, C., 2010. *The Defence of the Realm: The Authorized History of MI5* 1st ed., London: Penguin.

Andrew, C., Aldrich, R.J. & Wark, W.K., 2009. *Secret Intelligence: A Reader* 1st ed. Richard J. Aldrich, C. Andrew, & W. K. W. Wesley Wark, eds., Oxford: Routledge (Taylor and Francis).

Anon, 2008. HC Deb 06 February 2008 c959. Available at: http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080206/debtext/80206-0004.htm.

Anon, 1994. HC Deb 22 February 1994 vol 238 cc153-244. Available at: http://hansard.millbanksystems.com/commons/1994/feb/22/intelligence-services-bill-lords.

Australian Law Reform Commission, 2002. *Report 95*, Sydney. Available at: http://www.alrc.gov.au/report-95.

Baker-Beall, C., 2015. *Counter-radicalisation: critical perspectives* C. Heath-Kelly, L. Jarvis, & C. Baker-Beall, eds., Abingdon, Oxon ; New York, NY: Routledge.

Bale, J., 2004. *The Chechen Resistance and Radiological Terrorism Introduction * The Transformation of the Chechen Resistance Movement in the Mid-*, Available at: http://www.nti.org/analysis/articles/chechen-resistance-radiological-terror/.

Bar-Joseph, U., 2011. The Professional Ethics of Intelligence Analysis. *International Journal of Intelligence and CounterIntelligence*, 24(1), pp.22–43. Available at: http://www.informaworld.com/openurl?genre=article&doi=10.1080/08850607.2011.519222&magic=crossref||D404A21C5BB053405B1A640AFFD44AE3.

Barot, D., *Hazards*,

Barot, D., *Rough Presentation for Gas Limos Project*, Available at: http://www.nefafoundation.org/miscellaneous/Barot/NYSE.pdf.

Baxter, R.R., 1974. A Skeptical Look at the Concept of Terrorism. *Akron Law Review*, 7, pp.380–385. Available at: http://www.uakron.edu/dotAsset/39d8547c-745e-4b5d-8a6c-c4bef76a7bcf.pdf.

Bayley, D.H., 1999. Policing: the world stage. In R. I. Mawby, ed. *Policing across the World: Issues for the Twenty-First Century*. London: University College London Press, pp. 3–12.

BBC, 2007a. 21 July investigation (photo 6). *BBC News*. Available at: http://news.bbc.co.uk/2/hi/in_pictures/6237594.stm [Accessed August 5, 2014].

BBC, 2004. Blair urges new era in crime fight. *BBC News*. Available at: BBC News http://news.bbc.co.uk/2/hi/uk_news/politics/3905547.stm [Accessed July 20, 2012].

BBC, 2013. David Miranda row -Seized files endanger agents' lives. , (August 2013). Available at: http://www.bbc.com/news/uk-23898580 [Accessed October 4, 2013].

BBC, 2007b. Dhiren Barot's co-conspirators. *BBC News*. Available at:

http://news.bbc.co.uk/2/hi/uk_news/6756685.stm [Accessed January 31, 2015].

BBC, 2005. Do prisons radicalise inmates? *BBC News*. Available at: http://news.bbc.co.uk/2/hi/uk_news/4727723.stm [Accessed January 1, 2015].

BBC, 2007c. Fertiliser bomb trial: Bugged talk. *BBC News*. Available at: http://news.bbc.co.uk/2/hi/uk_news/6466817.stm [Accessed January 31, 2015].

BBC, 2014a. Germany expels CIA official in US spy row. *BBC News*, p.1. Available at: http://www.bbc.com/news/world-europe-28243933 [Accessed October 27, 2014].

BBC, 2014b. Help identify "aspiring terrorists" - Scotland Yard. *BBC News*, (26 August 2014). Available at: http://www.bbc.com/news/uk-28935613 [Accessed January 25, 2015].

BBC, 2010. Parcel bomb plotters "used dry run" say US officials. *BBC News*. Available at: http://www.bbc.co.uk/news/world-us-canada-11671377 [Accessed August 11, 2014].

BBC, 2006a. Police terror probe of vast scale. *BBC News*. Available at: http://news.bbc.co.uk/2/hi/uk_news/6125338.stm [Accessed January 31, 2015].

BBC, 2007d. Revealed: Bomber transcript. *BBC News*. Available at: http://news.bbc.co.uk/2/hi/uk_news/6611803.stm.

BBC, 2006b. Ryanair issues security ultimatum. *BBC News*. Available at: http://news.bbc.co.uk/2/hi/uk_news/5261908.stm [Accessed August 12, 2014].

BBC, 2003. Soham trial: "Crucial" phone evidence. *BBC News*. Available at: http://news.bbc.co.uk/2/hi/uk_news/england/cambridgeshire/3246111.stm [Accessed July 2, 2012].

BBC, 2007e. Support team "aided terror plot." *BBC News*. Available at: http://news.bbc.co.uk/2/hi/uk_news/6615717.stm [Accessed January 31, 2015].

BBC, 2006c. UN appalled by Beirut devastation. *BBC News*. Available at: http://news.bbc.co.uk/2/hi/middle_east/5207478.stm.

BBC, 2001. Who is Richard Reid? *BBC News*. Available at: http://news.bbc.co.uk/1/hi/uk/1731568.stm [Accessed September 28, 2011].

Berger, C., 2014. *Countering Terrorism: An Institution-Building Approach for Yemen*, Georgetown. Available at: http://www.cfr.org/terrorism/countering-terrorism-institution-building-approach-yemen/p32345.

Betts, R.K., 1978. Analysis, War, and Decision: Why Intelligence Failures Are inevitable. *World Politics*, 31(1), pp.61–89.

Betts, R.K., 2004. The new politics of intelligence: Will reforms work this time? *Foreign Affairs*, 83, pp.2–8.

Bhayani, G., 2013. *Reclaiming a National Icon*. London Metropolitan University.

Billingsley, R. ed., 2009. *Covert Human Intelligence Sources: The "Unlovely" Face of Police Work*, Hampshire: Waterside Press.

Borum, R., Fein, R. & Vossekuil, B., 2012. Dimensions of Lone Offender Terrorism. *Aggression & Violent Behavior: A Review Journal*. Available at: http://extremisproject.org/2012/11/moving-away-from-a-lone-wolf-mindset/.

Boston University, 2014. Arthur Hulnick, Boston University. *Boston University Public Relations webpage*, p.1. Available at: http://www.bu.edu/experts/profiles/arthur-hulnick/ [Accessed December 10, 2014].

Bowden, M., 2000. *Black Hawk Down*, London: Corgi.

Brandon, J., 2009. *Unlocking Al-Qaeda - Islamist Extremism in British Prisons"*,

Brown & Aspin, 1996. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence (the "Brown-Aspin" report)*, Washington, D.C. Available at: http://www.gpo.gov/fdsys/pkg/GPO-INTELLIGENCE/content-detail.html.

Brune, L.H., 1998. *THE UNITED STATES AND POST-COLD WAR INTERVENTIONS*, Claremont, CA: Regina Books.

Bryant, C., 2010. HC Deb 21 Jan 2010 c443 Echange Rate Movements (FCO). Available at: http://www.publications.parliament.uk/pa/cm200910/cmhansrd/cm100121/debtext/100121-0004.htm.

BSU, 2008. *Behavioural Science Unit Operational Briefing Note - Understanding radicalisation and violent extremism in the UK*, London. Available at: http://www.theguardian.com/uk/2008/aug/20/uksecurity.terrorism1/print.

Buckley, J., 2009. Managing Information from the Public. In R. Billingsley, ed. *Covert Human Intelligence Sources: The "Unlovely" Face of Police Work*. Hampshire: Waterside Press, pp. 97–108.

Buffaloe, D., 2006. *Defining asymmetric warfare*, Available at: http://www.ausa.org/SiteCollectionDocuments/ILW Web-ExclusivePubs/Land Warfare Papers/LWP_58.pdf [Accessed January 2, 2015].

Bures, O., 2011. *EU Counterterrorism Policy: A Paper Tiger?*, Farnham, Surrey: Ashgate Publishing Limited.

Burke, J., 2004. *Al Qaeda: The True Story of Radical Islam*, London: Penguin books.

Burke, P., 2013. *Intelligence: Art, Science or Both?*, Dubai.

Burke, P., 2015. Problem shared, problem halved? Towards a common national security policy for the Baltic States. *Journal on Baltic Security*, 1(2).

Burke, P., 2014. The double-edged sword: How terrorists collect and use Intelligence in their attack planning. In *Transport Security Conference 2014*. London, p. 25. Available at: http://www.transec.com/programmes/conference-timetable.

Burke, P., 2006. *The Growing Terrorist Threat to UK Maritime Security: An Analysis*. Brunel University.

Burke, P., 2011. *The Terrorist Threat to the Maritime Security of the UAE* 1st ed. F. Field, ed., Abu Dhabi: Emirates Center for Strategic Studies and Research.

Burnett, J. & Whyte, D., 2005. Embedded expertise and the new terrorism. *Journal for Crime, Conflict and the Media*, 1(4), pp.1–18. Available at: http://www.diplomatie.gouv.fr/fr/IMG/pdf/expertise_terrorisme.pdf [Accessed May 16, 2014].

Burns, L., 2001. Toward a Contemporary Definition of Terrorism. *Forum of Public Policy*, (September 2001), pp.1–29.

Butler, R., 2004. *Review of intelligence on weapons of mass destruction* 1st ed., London: The Stationery Office.

Byebee, J.S., 2002. *Memorandum for John Rizzo. Acting General Counsel of the Central Intelligence Agency. Interrogation of al Qaeda Operative*, Washington, D.C. Available at: http://www.fas.org/irp/agency/doj/olc/zubaydah.pdf.

Cabinet Office, 2010a. *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*, London.

Cabinet Office, 2014a. *Draft Protection Of Charities Bill*, London: Parliament. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/365715/43820_Cm_8954_draft_protection_of_charities_bill.pdf [Accessed February 10, 2015].

Cabinet Office, 2014b. *Government Security Classifications Version 1.0 October 2013*, London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf.

Cabinet Office, 2011. HMG Security Policy. *Official Guidelines*, p.35. Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/hmg-security-policy_0_0.pdf on 01 August 2012.

Cabinet Office, 2010b. *National Intelligence Machinery 2010*, London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf.

Cabinet Office, 2005. *REVIEW OF INTELLIGENCE ON WEAPONS OF MASS DESTRUCTION: IMPLEMENTATION OF ITS CONCLUSIONS*, London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61171/wmdreview.pdf.

Cabinet Office, 2013. *Tackling Extermism in the UK: Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism*, London.

Caldwell, W., 2006. Major General William Caldwell Remarks on the Killing of. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/06/08/AR2006060800961.html.

Cameron, D., 2010. *A Strong Britain in an Age of Uncertainty : The National Security Strategy*,

Carl, L.D., 1990. *International Dictionary of Intelligence*, McLean, PA: Maven books.

Carlile, A., 2011. *Report to the Home Secretary of Independent Oversight of Prevent Review and Strategy*,

Cary, S.G. et al., 1955. *Speak Truth to Power: A Quaker Search for an Alternative to Violence*, Philadelphia, PA. Available at: http://www.quaker.org/sttp.html [Accessed August 1, 2012].

Casciani, D., 2007. 21/7: Was it linked to 7/7? *BBC News*. Available at: http://news.bbc.co.uk/2/hi/uk_news/6249118.stm.

Casciani, D., 2009. Liquid bomb plot: What happened. *BBC News*, (07 September 2009). Available at: http://news.bbc.co.uk/1/hi/uk/8242479.stm [Accessed September 3, 2012].

Cavendish-Bentinck, V. & Capel-Dunn, D., 1945. *The Intelligence Machine: Report to the Joint Intelligence Sub-Committee*, lond.

Cebrowski, A.K. & Garstka, J.J., 1988. Network-Centric Warfare: Its Origin and Future. *Proceedings of the Naval Institute*, 124(1), pp.28–35. Available at: http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future [Accessed January 10, 2015].

CFR, About CFR. Available at: www.cfr.org/about.

Charity Commission, 2008. *Charity Commission Counter-terrorism Strategy 2008*, London.

Charity Commission, 2012. *Charity Commission Counter-Terrorism Strategy 2012 (revised)*, London. Available at: http://forms.charitycommission.gov.uk/media/89498/ctstext.pdf.

Chilcot, J. et al., 2008. *Privy Council Review of Intercept as Evidence: Report to the Prime Minister and the Home Secretary, 30 January 2008*, London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228513/7324.pdf.

Chomsky, N., 2003. On Israel, the US and Turkey. *Unidentified Kurdish newspaper*. Available at: http://www.chomsky.info/interviews/200309--.htm.

Christmann, K., 2012. *Preventing Religious Radicalisation and Violent Extremism*,

CIA, 1993. *A Consumer's Guide to Intelligence* 1st ed., Washington, D.C.: Central Intelligence Agency.

CIA, 2003. *Terrorist CBRN : Materials and Effects*, Langley, VA.

Claire, R.W., 2004. *Raid on the Sun: Inside Israel's Secret Campaign that Denied Saddam the Bomb* 1st ed., New York City: Broadway Books.

Clark, M., 1955. *Intelligence Activities*, Washington, D.C.

Clark, R.M., 2012. *Intelligence Analysis - A Target-Centric Approach* 4th ed., London: CQ press.

Clarke, B.C., 1980. *Interagency Intelligence Memorandum - The 22 September 1979 Event*, Langley, VA. Available at: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB190/03.pdf.

Clarke, P., 2007. Operation Crevice: MPS statement by DAC Peter Clarke. *MPS Website*, (30 April 2007), pp.1–3. Available at: http://content.met.police.uk/News/Operation-Crevice-MPS-statement/1260267589317/1257246745756 [Accessed November 27, 2014].

Clausewitz, C., 1976. *On War* 1st ed. M. E. Howard & P. Paret, eds., Princeton, NJ: Princeton University Press.

Cobain, I., 2006. Feared clan who made themselves at home in Britain. *The Guardian*, p.1. Available at: http://www.theguardian.com/uk/2006/mar/28/drugsandalcohol.ukcrime.

Coll, S. & Glasser, S.B., 2005. Terrorists Turn to the Web as Base of Operations. *Washington Post*, p.1. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html [Accessed

September 11, 2008].

College of Policing, 2013. Introduction and types of critical incidents. *College of Policing Website*. Available at: http://www.app.college.police.uk/app-content/critical-incident-management/types-of-critical-incident/ [Accessed January 3, 2014].

Collins, J., 2002. Terrorism. In J. Collins & R. Glover, eds. *COLLATERAL LANGUAGE: A USER'S GUIDE TO AMERICA'S NEW WAR*. N: New York University Press, p. 230.

Corera, G., 2012. *MI6: Life and Death in the British Secret Service*, London: Weidenfeld & Nicholson.

Court of Appeal, 2013. *R v Baybasin*, Liverpool. Available at: https://www.crimeline.info/uploads/cases/2013/2013ewcacrim2357.rtf.

CPNI, 2010. *PROTECTING AGAINST TERRORISM - Third Edition*, London.

CPNI, 2014. The national infrastructure. *CPNI Website*. Available at: http://www.cpni.gov.uk/about/cni/ [Accessed January 11, 2014].

CPS, 2010. CPS Summary: "The Airline Bomb Plot. *CPS Website*. Available at: http://www.cps.gov.uk/publications/prosecution/ctd_2010.html#a09 [Accessed August 11, 2014].

CPS, 2007a. Four 21/7 terrorists guilty of murder conspiracy. *CPS Website*. Available at: http://www.cps.gov.uk/news/latest_news/143_07/ [Accessed July 11, 2009].

CPS, 2005. *R v Omar Khyam et al: Prosecution Response to the Skeleton Argument on Behalf of Omar Khyam in the Central Criminal Court*,

CPS, 2006. Terrorist sentenced for conspiracy to murder. *CPS Website*, p.1. Available at: http://www.cps.gov.uk/news/latest_news/161_06/ [Accessed January 31, 2015].

CPS, 2007b. The Counter-Terrorism Division of the Crown Prosecution Service: Barot and others. *CPS Website*. Available at: http://www.cps.gov.uk/publications/prosecution/ctd_2007.html#a02 [Accessed August 5, 2014].

CPS, 2007c. The Fertiliser Plot. *CPS Website*, p.1. Available at: http://www.cps.gov.uk/publications/prosecution/ctd_2007.html#a01 [Accessed September 12, 2013].

Cumbria Constabulary, 2007. *Management of Intelligence Policy - Doc Ref: MDI 139*, Penrith. Available at: http://www.cumbria.police.uk/Admin/uploads/attachment/files/MoPI_Management-Intelligence-Policy.pdf.

Cummings, A. & Masse, T., 2004. *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress*, Washington, D.C. Available at: http://fas.org/irp/crs/RL32336.html [Accessed March 22, 2012].

Davies, P.H.J., 2009. Ideas of Intelligence. In C. Andrew, R. J. Aldrich, & W. K. Wark, eds. *Secret Intelligence: A Reader*. Oxford: Routledge (Taylor and Francis), p. 552.

Davies, P.H.J., 2002. Ideas of Intelligence: Divergent National Concepts and Institutions. *Harvard International Review*, 24(3), p.62.

Davies, P.H.J., 2012a. *Intelligence and Government in Britain and the United States, A Comparative Perspective, Volume 1: Evolution of the U.S. Intelligence Community*, Praeger.

Davies, P.H.J., 2012b. *Intelligence and Government in Britain and the United States, A Comparative Perspective, Volume 2: Evolution of the U.K. Intelligence Community* 1st ed., London: Praeger.

Davies, P.H.J., 2005. Lecture on Definitions of Intelligence.

Davies, P.H.J., Gustafson, K. & Rigden, I., 2014. The Intelligence Cycle is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine,. In *Understanding the Intelligence Cycle2*.

Davis, D. & Lewis, I., 2009. HC Deb 07 July 2009 c940: Government Policy (Torture Overseas). Available at: http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm090707/debtext/90707-0020.htm.

Davis, J., 2008. Why Bad Things Happen To Good Analysts. In R. George, ed. *Analyzing Intelligence*. Georgetown University Press. Available at: http://press.georgetown.edu/book/georgetown/analyzing-intelligence [Accessed December 27, 2014].

Defence, S. of S. for, 2008. Defence Advisory Notices. Available at: http://www.dnotice.org.uk/danotices/danotice_05.htm.

Deffains, B. & Fluet, C., 2014. *Social Norms and Legal Design : Fault-Based vs Strict Liability Offences*,

Denzin, N.K., Maanen, J. Van & Manning, P.K., 1989. *Interpretive Biography (Qualitative Research Methods)* 1st ed., Newbury Park, CA: Sage Publications.

Department of the Army, 1998. *FM 34-8-2: Intelligence Officer's Handbook* 1st ed., Washington, D.C.: Department of the Army.

Disley, E. et al., 2012. *Individual Disengagement from Al Qa'ida-Influenced Terrorist Groups: A Rapid Evidence Assessment to inform policy and practice in preventing terrorism*,

Dobson, N., 2013. Public law ultra vires. *Law Gazette*, pp.49–50. Available at: http://www.lawgazette.co.uk/law/public-law-ultra-vires/69307.fullarticle [Accessed January 1, 2015].

Doward, J., 2006. How a barbershop arrest led to heart of al-Qaeda's web.

The Guardian. Available at: http://www.theguardian.com/uk/2006/nov/12/alqaida.terrorism [Accessed January 15, 2015].

Drogin, B., 2007. *CURVEBALL - Spies, Lies and the Man Behind Them: The Real Reason America Went to War in Iraq* 1st ed., London: Ebury Press.

Duijvestijn, L.M., Stahl, E. & Plach, A., 2014. *Performance and Capacity Implications for Big Data*, Armonk, NY. Available at: http://www.redbooks.ibm.com/redpapers/pdfs/redp5070.pdf.

Durant, M.J., 2004. *In The Company Of Heroes*, London: Corgi.

ECHR, 1993. *HEWITT AND HARMAN v. THE UNITED KINGDOM*, Available at: http://echr.ketse.com/doc/20317.92-en-19930901/view/ [Accessed September 18, 2013].

Egger, S., 1984. A Working Definition of Serial Murder and the Reduction of Linkage Blindness. *Journal of Police Science and Administration*, 12(3), pp.348–357.

Egger, S., 1999. Linkage Blindness and Crime Analysis. *International Association of Crime Analysts*, (November).

Egger, S., 1992. Linkage Blindness and Multiple Murder Investigations. *Contemporary Issues in Criminal Justice: Serial Murder*, (April).

EHRC, 2012. England and Wales High Court (Administrative Court) Decisions (EHRC v Prime Minister & Ors 2011). *EHRC*, pp.1–24. Available at: http://www.bailii.org/ew/cases/EWHC/Admin/2011/2401.html.

EHRC, 2011. Equality and Human Rights Commission (EHRC) Commission to argue that Government torture guidance violates the law. *wired.gov*. Available at: http://www.wired-gov.net/wg/wg-news-1.nsf/0/E40FE7D71C035C66802578BD00435794?OpenDocument [Accessed August 7, 2014].

Elliott, M., 2002. The Shoe Bomber's World. *TIME Magazine*, pp.1–6.

English, R., 2003. *Armed Struggle: The History of the IRA*, Pan books.

Ensor, P., 1988a. Tearing Down the Functional Silos. , pp.4–14.

Ensor, P., 1988b. The Functional Silo Syndrome. *AME Target, Spring*. Available at: http://www.ame.org/sites/default/files/target_articles/88q1a3.pdf [Accessed January 5, 2015].

European Council, 2002. *EU Council Framework Decision 2002/475 on Combating Terrorism , 13 June 2002*, Available at: http://www.refworld.org/docid/3f5342994.html.

European Court of Human Rights, 2010. *European Convention on Human Rights*, Available at:

http://www.echr.coe.int/Documents/Convention_ENG.pdf.

European Court of Human Rights, 1985. Malone v The United Kingdom. Available at: http://caselaw.echr.globe24h.com/0/0/united-kingdom/1985/04/26/case-of-malone-v-the-united-kingdom-article-50-57532-8691-79.shtml.

Evans, J., 2007. Address to the Society of Editors by the Director General of the Security Service, Jonathan Evans.

Ezzarqui, L., 2010. *De-radicalization and Rehabilitation Program: The Case Study of Saudi Arabia Leila*. Georgetown University. Available at: https://repository.library.georgetown.edu/bitstream/handle/10822/553485/ezzarquiLeila.pdf?sequence=1&isAllowed=y [Accessed January 26, 2015].

FBI, 2010. Chicago Man Charged with Providing Material Support to al Qaeda by Attempting to Send Funds Overseas. *FBI Website*. Available at: http://www.fbi.gov/chicago/press-releases/2010/cg032610-1.htm [Accessed November 18, 2013].

FBI, 1995. Terror Hits Home: Oklahoma City Bombing. *FBI Website*. Available at: http://www.fbi.gov/about-us/history/famous-cases/oklahoma-city-bombing [Accessed January 1, 2015].

FEMA, 1993. *The World Trade Center Bombing : Report and Analysis*, New York City.

Fennell, D., 1989. Investigation into the King's Cross Underground Fire. *Fire Safety Journal*, 15(1), pp.107–109. Available at: http://linkinghub.elsevier.com/retrieve/pii/0379711289900519.

Fijnaut, C. & Marx, G.T., 1995. *Undercover. Police surveillance in international perspective*, The Hague: Kluwer.

Flood, P., 2004. *Report of the inquiry into Australian intelligence agencies (Flood report)*, Government of Australia. Available at: http://apo.org.au/report-inquiry-australian-intelligence-agencies-flood-report [Accessed February 6, 2015].

Foreign Affairs Committee, 2003. *Ninth Report of the Foreign Affairs Committee Session 2002-03 - The Decision to go to War in Iraq*, London. Available at: http://www.publications.parliament.uk/pa/cm200203/cmselect/cmfaff/813/81302.htm.

Gabbard, C. & Treverton, G.F., 2008. *Assessing the Tradecraft of Intelligence Analysis*, Santa Monica CA: RAND Corporation.

Gannon, J.C., 2008. Managing Analysis in the Information Age. In *Analyzing Intelligence: Origins, Obstacles and Innovations*. Jamestown.

Ganor, B., 2002. Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? *Police Practice and Research*, 3(4), pp.287–304.

Available at: http://www.tandfonline.com/doi/abs/10.1080/1561426022000032060 [Accessed September 3, 2014].

GCHQ, 2011. GCHQ: About US. *GCHQ official website*. Available at: http://www.gchq.gov.uk/about_us/index.html [Accessed August 5, 2011].

Gedeon, G., 2003. Building Terrorism Mitigation - Blast and CBR Measures. In M. D. Brown & S. Lowe, Anthony, eds. *FEMA 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (2003)*. Diane Publishing COmpany, p. 395.

Geertz, C., 1973. *The Interpretation of Cultures (Basic Books Classics):*, New York: Basic Books.

Gentry, J.A., 1993. *Lost Promise: How CIA Analysis Misserves the Nation: Amazon.co.uk: John A. Gentry: 9780819189516* 1st ed., Washington, D.C.: University Press of America.

Gill, P., 2011. A Formidable Power to Cause Trouble for the Government? Intelligence Oversight and the Creation of the UK Intelligence and Security Committee. In M. S. Goodman & R. Dover, eds. *Learning from the Secret Past: Cases in British Intelligence History*. Georgetown: Georgetown University Press.

Gill, P., 2009. “Kowing the self, knowing the other”: the comparative analysis of security Intelligence. In L. K. Johnson, ed. *The Handbook of INtelligence Studies*. Oxford: Routledge (Taylor and Francis), pp. 82–90.

Gill, P., 2000. *Rounding Up the Usual Suspects? Developments in Contemporary Law Enforcement Intelligence* 1st ed., Farhnam, Surrey: Ashgate Publishing Limited.

Gill, P., Horgan, J. & Deckert, P., 2013. *Tracing the Motivations and Antecedent Behaviors of Lone Actor Terrorism*, Available at: http://sites.psu.edu/icst/2013/02/06/seven-findings-on-lone-actor-terrorists/.

Gillespie, A., 2009. Juvenile Informers. In R. Billingsley, ed. *Covert Human Intelligence Sources: The “Unlovely” Face of Police Work*. Hampshire: Waterside Press, pp. 109–122.

Glass, D., 2006. *IPCC Independent Investigation into the Shooting of Muhammad Abdulkahar in 46 Lansdown Road, Forest Gate on Friday 2 June 2006*, London. Available at: http://www.ipcc.gov.uk/sites/default/files/Documents/investigation_commissioner_reports/report.pdf [Accessed February 8, 2015].

Glass, R. & Davidson, P., 1948. *Intelligence is for commanders,* Harrisburg Pa.: Military Service Pub. Co.

Goodman, M.S., 2011. Avoiding Surprise: The Nicoll Report and Intelligence Analysis. In R. Dover & M. S. Goodman, eds. *Learning from the Secret*

Past: Cases in British Intelligence History. Georgetown: Georgetown University Press.

Goodman, M.S., 2007. The Dog That Didn't Bark: The Joint Intelligence Committee and Warning of Aggression. *Cold War History*, 7(4), pp.529–551.

Gormley, D.M., 2004. The Limits of Intelligence: Iraq's Lessons. *Survival*, 46(3), pp.7–28.

Gortney, W.E., 2014. *JP 1-02 Department of Defense Dictionary of Military and Associated Terms*, Available at: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf [Accessed December 18, 2014].

Gratch, J. et al., 1999. Deriving Priority Intelligence Requirements for Synthetic Command Entities. In *8th Conference on Computer Generated Forces and Behavioral Representation, Orlando, FL, May 1999*. Orlando, FL, p. 7.

Grebe, C., 2007. *ARRC (Allied Rapid Response Corps) Intelligence Collection Management Process*,

Green, P.S., 2001. Democratic Gains Falter With Tighter Security in Central Europe. *New York Times*. Available at: http://www.nytimes.com/2001/10/04/world/democratic-gains-falter-with-tighter-security-in-central-europe.html [Accessed March 14, 2011].

Grieve, J., 2004. Developments in UK Criminal Intelligence. In J. H. Ratcliffe, ed. *Stretegic Thinking in Criminal Intelligence*. Sydney: Federation Press, pp. 25–36.

Griffith, J., 1987. Reviews: The Second Oldest Profession by Phillip Knightley; Spycatcher by Peter Wright. *The Modern Law Review*, 50(7), pp.982–989. Available at: http://www.jstor.org/stable/1096337.

Güngör, U. & Akgul, F., 2013. After NATO's Libya Intervention: Any Implication for International Law? *errorism: An Electronic Journal and Knowledge Base*, II(1).

Gupta, D., 2010. *Channel: Supporting individuals vulnerable to recruitment by violent extremists - A guide for local partnerships*, London.

Haas, R., 1996. *Making Intelligence Smarter*, New York.

Hague, W., 2013. Countering terrorism overseas. In *Terrorism and the UK*. London: GOV.UK. Available at: https://www.gov.uk/government/speeches/countering-terrorism-overseas [Accessed January 28, 2015].

Hallett, H., 2011. *Coroner's Inquests into the London Bombings of 7 July 2005*, London.

Hannah, G., O'Brien, K.A. & Rathmell, A., 2005. *Intelligence and Security*

Legislation for Security Sector Reform, Cambridge.

Hardy, T., 2014. Keeping the public safe: The use of Advance Passenger Data to strengthen Border security. In *World BORDERPOL Congress 9-11 December 2014 - Budapest*. Budapest: UK Border Force, p. 12.

Harfield, C. ed., 2013. *Blackstone's Police Operational Handbook: Practice And Procedure* 2nd ed., Oxford: Oxford University Press.

Harfield, C., 2009. The Regulation of CHIS. In R. Billinglsey, ed. *Covert Human Intelligence Sources: The "Unlovely" Face of Police Work*. Hampshire: Waterside Press, pp. 43–56.

Harfield, C. & Harfield, K., 2008. *Intelligence: Investigation, Community and Partnership* 1st ed., Oxford: Oxford University Press.

Harfield, K. & Harfield, C., 2012. *Covert Investigation* 3rd ed., Oxford: Oxford University Press.

Harrison, E., 2012. *The Young Kim Philby: Soviet Spy and British Intelligence Officer* 1st ed., Exeter: Liverpool University Press.

Heathrow Airport, 2006. Heathrow Airport Security New Rules. *Heathrow Airport website*. Available at: http://www.heathrowairport.com/heathrow-airport-guide/heathrow-security/faqs#newrules [Accessed January 28, 2015].

Heinrich, J., 2003. *BIOTERRORISM - Public Health Response to Anthrax Incidents of 2001*, Washington, D.C. Available at: http://www.gao.gov/assets/250/240162.pdf.

Herman, M., 2001. *Intelligence Services in the Information Age*, London: Frank Cass.

Herman, M., 2011. The Postwar Organization of Intelligence: The January 1945 Report to the Joint Intelligence Committee on "The Intelligence Machine." In M. S. Goodman & R. Dover, eds. *Learning from the Secret Past: Cases in British Intelligence History*. Georgetown: Georgetown University Press.

Heuer, R.J., 1999. *Psychology of intelligence analysis*, Central Intelligence Agency.

Heuer, R.J. & Pherson, R.H., 2011. Structured Analytic Techniques. In *Structured Analytic Techniques for Intelligence Analysis*. p. 25.

Higgins, R., 1997. The General International Law of Terrorism. In *Terrorism and International Law*. Routledge (Taylor and Francis), p. 396.

Hill, J.B., 2010. Do You Understand the Difference Between Workflow and BPM? *Gartner official website*, pp.1–8. Available at: http://blogs.gartner.com/janelle-hill/2010/04/22/do-you-understand-the-difference-between-workflow-and-bpm/ [Accessed September 25, 2014].

Hindi, E. al, 1999. *The Army of Medinah in Kashmir* 1st ed., Birmingham:

Maktabah Al Ansar. Available at: http://www.streetdawah.com/books/Kashmir.pdf [Accessed January 1, 2009].

HMIC, 2005. *Closing the Gap - A Review of "Fitness for Purpose" of the Current Structure of Policing in England & Wales.*, London.

Hoffman, B., 1986. Defining Terrorism. *Social Science Record*, pp.1–183. Available at: http://eric.ed.gov/?id=EJ343115 [Accessed September 24, 2014].

Holmes, K.R., 2001. America Strikes Back : Looking Ahead. *The Heritage Foundation*, pp.8–11. Available at: http://www.heritage.org/research/reports/2001/10/america-strikes-back [Accessed March 14, 2011].

Home Affairs Committee, 2012. *The work of the UK Border Agency July-September 2012 - Home Affairs Committee - Final*, London. Available at: http://www.parliament.uk/documents/commons-committees/home-affairs/HC792-UKBA-Q3-Report-FINAL.pdf.

Home Office, 2011. *Contest: The United Kingdom's Strategy Countering Terrorism 2011*,

Home Office, 2010. *Covert Surveillance and Property Interference: Revised Code of Practice (Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000)*,

Home Office, 2005. *e-Borders: Creating an integrated, secure border for the 21st century*, London. Available at: http://www.dematerialisedid.com/PDFs/whatiseborders.pdf.

Home Office, 2013. *Regulation of Investigatory Powers Act (RIPA) 2000 guidance*, London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/270617/ripa.pdf.

Honderich, T., 1984. *Punishment, the Supposed Justifications*, London: Penguin books.

Howells, K., 2009. *Intelligence and Security Committee annual report 2008-2009* 1st ed., London: HMSO.

Hulnick, A., 2006. What's wrong with the Intelligence Cycle. *Intelligence and national Security*, 21:6(August 2011), pp.959–979.

Huntington, S.P., 2011. *The Clash of Civilizations and the Remaking of World Order* 1st ed., Simon & Schuster.

Hutchins, S.G., Pirolli, P. & Card, S.K., 2007. What Makes Intelligence Analysis Difficult?: A Cognitive Task Analysis of Intelligence Analysts. In Robert R. Hoffman (Ed.), ed. *Naturalistic Decision-Making, Vol. 6, Expertise Out of Context.*

Hutton, B., 2004. *Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly C . M . G . by Lord Hutton*, London.

IAFIE, 2014. International Association for Intelligence Education - Mark Lowenthal - Executive Director. *IAFIE Website*. Available at: http://www.iafie.org/?Board_ExecDirector [Accessed March 12, 2014].

ICEP, 2012. Islam & Citizenship Education: Developing A Citizenship Curriculum Through An Islamic Perspective. *Islam & Citizenship Education*. Available at: http://www.theiceproject.sdsa.net/welcome [Accessed August 3, 2011].

ICG, 2007. *" DERADICALISATION " AND INDONESIAN PRISONS: Asia Report No. 142*,

Ilston, G., 2014. Primary school children among those at risk of radicalisation - . *POLICEPROFESSIONAL website*. Available at: http://www.policeprofessional.com/news.aspx?id=9719 [Accessed August 6, 2014].

INTERPOL, 2010. Interpol Orange Notice PR091-2010. *INTERPOL website*. Available at: http://www.interpol.int/en/Media/Files/Notices/Public-Orange-Notices-PDF/PR091-2010-orange-notice [Accessed August 9, 2012].

Jackson, R., 2007. the Core Commitments of Critical Terrorism Studies. *European Political Science*, 6(3), pp.244–251. Available at: http://www.palgrave-journals.com/doifinder/10.1057/palgrave.eps.2210141 [Accessed September 23, 2014].

Jackson, R., 2009. Knowledge, Power and Politics in the Study of Political Terrorism. In R. Jackson, M. Smyth, & J. Gunning, eds. *Critical Terrorism Studies. A new research agenda*. London: Routledge, p. 274.

Janis, I.L., 1972. *Victims of groupthink: a psychological study of foreign-policy decisions and fiascoes*, Boston: Houghton.

Jehel, D., 2004. THE STRUGGLE FOR IRAQ: INTELLIGENCE; Stung by Exiles' Role, CIA Orders a Shift in Procedures. *New York Times*. Available at: http://www.nytimes.com/2004/02/13/world/struggle-for-iraq-intelligence-stung-exiles-role-cia-orders-shift-procedures.html?pagewanted=print.

Jenkins, B., 1980. *The Study of Terrorism: Definitional Problems*, Santa Monica, CA.

Jentleson, B.W., Paterson, T.G. & Rizopoulos, N.X. eds., 1997. *Encyclopedia of U.S. Foreign Relations, Volume 2*, Oxford: Oxford University Press.

Jervis, R., 2006. Reports, politics, and intelligence failures: The case of Iraq. In *Journal of Strategic Studies*. pp. 3–52.

Johnson, A., 2010. *Pursue Prevent Protect Prepare The United Kingdom's*

Strategy for Countering International Terrorism, London: The Stationery Office. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228907/7833.pdf.

Johnson, L.K., 2006. A Framework for Strengthening U.S. Intelligence. *Yale Journal of International Affairs*, Winter-Spr, pp.116–131.

Johnston, R., 2005. Analytic Culture in the US Intelligence Community: An Ethnographic Study. *The Center for the Study of Intelligence*, 160, p.72.

Joint Chiefs of Staff, 2013. *JP 2-0 Joint Intelligence*, Available at: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf [Accessed December 18, 2014].

Jones, A., 2007. *Terrorism studies: theoretically under-developed ?*,

Jones, G., 2008. Charity Commission reveals revised counter-terrorism strategy. *Civil Society website*, p.1. Available at: http://www.civilsociety.co.uk/finance/news/content/3508/charity_commission_reveals_revised_counter-terrorism_strategy [Accessed January 1, 2015].

Jones, R.V., 1947. Scientific Intelligence. *Journal of the Royal United Services Institution*, XCII, pp.352–360.

KAPLAN, S., 2003. A TYPOLOGY OF TERRORISM SHAWN KAPLAN ADELPHI UNIVERSITY. , pp.47–66.

Karam, Z., 2006. Munich mastermind has no regrets. *Seattle Post Intelligencer*. Available at: http://www.seattlepi.com/olympics/260723_mastermind24.html.

Keagan, J., 2004. *Intelligence In War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, London: Pimlico.

Kent, S., 1949. *Strategic Intelligence for American world policy*, Princeton, NJ: Princeton University Press.

Khetan, A. et al., 2009. *26/11: Mumbai attacked* 1st ed. H. Baweja, ed., New Delhi: Lotus.

King, T., 1995. *Intelligence and security committee annual report 1995*, London: HMSO. Available at: http://isc.independent.gov.uk/files/1995_ISC_AR.pdf.

Krizan, L., 1999. *Intelligence essentials for everyone*, Washington, D.C. Available at: http://www.lib.miamioh.edu/multifacet/record/mu3ugb4151695 [Accessed December 24, 2014].

Kronstadt, K.A., 2008. *Terrorist attacks in Mumbai, India, and implications for U.S. interests*, Washington, D.C. Available at: http://fas.org/sgp/crs/terror/R40087.pdf.

Kundnani, A., 2009. *Spooked! How not to prevent violent extremism*, London: Institute of Race Relations. Available at: http://www.irr.org.uk/pdf2/spooked.pdf.

Kushner, H.W., 2002. *Encyclopedia of Terrorism*, Brooklyn, New York: Long Island University.

Lagouranis, T., 2008. *FEAR UP HARSH: AN ARMY INTERROGATOR'S DARK JOURNEY THROUGH IRAQ*, Berkeley: New American Library.

Lalor, B. ed., 2003. *The Encyclopaedia of Ireland.*, Dublin, Ireland: Gill & Macmillan.

Laqueur, W., 1985. *World of Secrets: The Uses and Limits of Intelligence:*, Basic Books.

League of Nations, 1937. *League of Nations Convention for the prevention and punishment of Terrorism 1937*, Geneva: League of Nations. Available at: http://dl.wdl.org/11579/service/11579.pdf.

Lefebvre, S., 2004. A look at intelligence analysis. *International Journal of Intelligence and …*, 2003, pp.1–43. Available at: http://www.tandfonline.com/doi/full/10.1080/08850600490274908 [Accessed September 24, 2014].

London Law School, 2013. London Law School - CONFIDENTIALITY. , p.2. Available at: http://www.londonschooloflaw.co.uk/Policies/CONFIDENTIALITY_POLICY.pdf [Accessed August 2, 2013].

Lowenthal, M., 2003. *Intelligence: From secrets to policy* 3rd ed., Washington, D.C.: CQ Press.

Macartney, J., 1995. How Do You Define Intelligence? *Intelligencer: Journal of U.S. Intelligence Studies*, 6(1), pp.3–4.

Macintyre, B., 2014. *A Spy Among Friends: Kim Philby and the Great Betrayal*, London: Bloomsbury Publishing.

Macpherson, W., 1999. *Report of the Stephen Lawrence inquiry*, London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/277111/4262.pdf [Accessed February 1, 2015].

Magnuson, S., 2007. Army wants to make "every soldier a sensor." *National Defense Magazine*. Available at: http://www.nationaldefensemagazine.org/ARCHIVE/2007/MAY/Pages/ArmyWantSensor2650.aspx [Accessed February 11, 2015].

Mandela, N., 2004. *Long Walk to Freedom Volume II*, London: Time Warner Books.

Mangio, C.A.C. & Wilkinson, B.J.B., 2008. *Intelligence analysis: Once again*, San Francisco, CA. Available at:

http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA520278 [Accessed September 24, 2014].

Manningham-Buller, E., 2011. BBC REITH LECTURES 2011: SECURING FREEDOM; Lecture Two: Security. , (13 September 2011), pp.1–31.

Manningham-Buller, E., 2006. Speech By The Director General Of The Security Service Dame Eliza Manningham-Buller At Queen Marys College London 09 November 2006. *Security Service official website*. Available at: https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-international-terrorist-threat-to-the-uk.html.

Marrin, S., Intelligence Analysis : Turning a Craft Into a Profession. , pp.1–5.

Marrin, S., 2007. Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities. *Intelligence and National Security*, 22, pp.821–846.

Martenson, C. & Horndahl, A., 2005. Using semantic technology in intelligence analysis. In *Proceedings of the Skövde Workshop on Information Fusion Topics*.

Martin, G.T., 2014. *NSA Spying , Secrecy , and the Totalitarian Threat*, Available at: http://www.radford.edu/~gmartin/NSA Spying and the Totalitarian Threat.pdf.

Marx, G.T., 1988. *Undercover. Police surveillance in America*, Berkeley: University of California Press.

Maryland Coordination and Analysis Center, 2012. Mumbai Terror Attacks: Surviving Gunman Hanged in India. *Maryland Coordination and Analysis Center Website*, p.1. Available at: http://www.mcac.maryland.gov/newsroom/TerrorismNews/20121121_Mumbai_Terror_Attacks_Surviving_Gunman_Hanged_in_India_UK_Guardian [Accessed February 1, 2015].

Mattar, P. ed., 2005. *Encyclopedia of the Palestinians*, Facts on File Inc.

May, T., 2013. *CONTEST: The United Kingdom's Strategy for Countering Terrorism - Annual Report 2013*,

May, T., 2014a. Oral statement to Parliament: Communications data and interception, 10 July 2014. *GOV.UK*, pp.1–5. Available at: https://www.gov.uk/government/speeches/communications-data-and-interception.

May, T., 2011. *Prevent Strategy*,

May, T., 2014b. Theresa May MP 1. *HANSARD*, pp.1–6.

Mayor, A., 2009. *Greek Fire, Poison Arrows and Scorpion Bombs: Biological Warfare in the Ancient World*, London: Gerald Duckworth & Co Ltd.

McDowell, D.D., 1997. *STRATEGIC INTELLIGENCE & ANALYSIS -*

Guidelines on Methodology & Application by Don McDowell, Available at: http://www.intstudycen.com/docs/strat_meth_guide.pdf [Accessed December 18, 2014].

Mehra, B., 2002. Bias in Qualitative Research: Voices from an Online Classroom. *The Qualitative Report*, 7(1), pp.1–14. Available at: http://www.nova.edu/ssss/QR/QR7-1/mehra.html [Accessed February 7, 2015].

Metropolitan Police Authority, 2007. *Counter-Terrorism: The London Debate*,

Metropolitan Police Service, 2007. *Five convicted of charges under the Terrorism Act*, London. Available at: http://content.met.police.uk/News/Five-convicted-of-charges-under-the-Terrorism-Act/1260267589429/1257246745756#.

Metropolitan Police Service, 2014. Metropolitan Police Service - Counter Terrorism Security Advisers. *MPS Website*. Available at: http://content.met.police.uk/Article/Counter-Terrorism-Security-Advisers/1400006571857/1400006571857 [Accessed August 11, 2014].

Metropolitan Police Service, 2006a. Operation Rhyme. *MPS Website*. Available at: http://www.met.police.uk/pressbureau/rhyme/index.htm [Accessed February 1, 2010].

Metropolitan Police Service, 2006b. Terrorist jailed for life for conspiracy to murder in the UK and US. *MPS Website*. Available at: http://content.met.police.uk/News/Terrorist-jailed-for-life-for-conspiracy-to-murder-in-the-UK-and-US/1260267887712/1257246745756 [Accessed August 5, 2014].

Middle East Security Ltd, 2011. Bunker Busters moved to Diego Garcia, possibly for use against Iranian targets. *Middle East Security website*, p.4. Available at: http://www.mideastsecurity.co.uk/?p=377 [Accessed September 15, 2011].

Ministry of External Affairs, 2008. *Mumbai Terrorist Attacks (Nov. 26-29, 2008)*, New Delhi.

MOD, 2015. How Defence Intelligence does its work. *MOD official website*, p.1. Available at: https://www.gov.uk/defence-intelligence#how-defence-intelligence-does-its-work [Accessed January 8, 2015].

Moloney, E., 2002. *A Secret History of the IRA*, London: Penguin books.

Moore, C. & Whitehead, T., 2014. Edward Snowden leaks mean GCHQ takes three times as long to track terrorists. *The Daily Telegraph*. Available at: http://www.telegraph.co.uk/news/11155355/Edward-Snowden-leaks-mean-GCHQ-takes-three-times-as-long-to-track-terrorists.html [Accessed January 1, 2015].

Mostyn, T., 2010. Mohammed Oudeh (Abu Daoud) obituary - Mastermind behind the attack on Israeli athletes at the 1972 Munich Olympics. *The*

Guardian. Available at: http://www.theguardian.com/world/2010/jul/04/mohammed-oudeh-abu-daoud-obituary.

Mueller, R.S., 2007. Nuclear Terrorism: Prevention Is Our Endgame. In *Global Initiative Nuclear Terrorism Conference*. Miami. Available at: http://www.fbi.gov/news/speeches/nuclear-terrorism-prevention-is-our-endgame [Accessed June 29, 2014].

Murphy, P., 2006. *Intelligence and security committee report into the London terrorist attacks on 7 July 2005*, London.

Muskingum University, What is Intelligence? *Intelligence literature*. Available at: http://intellit.muskingum.edu/whatis_folder/whatisintelintro.html [Accessed March 17, 2013].

National Policing Improvement Agency, 2008. *Practice Advice on Analysis*, Wyboston. Available at: http://library.college.police.uk/docs/npia/practice_advice_on_analysis_interactive.pdf.

NCIS, 2000. *The National Intelligence Model*, London: NCIS Corporate Communications.

Neumann, P.R., 2010. *Prisons and Terrorism Radicalisation and De-radicalisation in 15 Countries*,

Nicoll, D., 1981. *The JIC and Warning of Aggression*, London.

Nobel Prize, The Nobel Peace Prize 1994. Available at: http://www.nobelprize.org/nobel_prizes/peace/laureates/1978/ [Accessed October 28, 2011].

Norton-Taylor, R., 1995. Tories block inquiries into spying past. *The Guardian*.

NPIA, 2010. *Guidance on The Management of Police Information Second Edition*, Wyboston. Available at: http://www.acpo.police.uk/documents/information/2010/201004INFMOPI01.pdf.

NPIA, 2011. *Practice Advice on Critical Incident Management: (Second Edition) July 2011*, Wyboston.

Nye, J.S., 1994. Peering into the Future. *Foreign Affairs*, 73(4), pp.82–93.

O'Conner, T., *Intelligence Failures - Homeland Security Class*,

O'Connor, T., *Intelligence Failures - Homeland Security Class*, Available at: http://www.ics.uci.edu/~ucrec/intranet/miscdocs/HSclassnotes/class5.html.

Office of the Attorney General, 2015. Umar Farouk Abdulmutallab Sentenced to Life in Prison for Attempted Bombing of Flight 253 on Christmas Day 2009. *Department of Justice website*, (August 2009). Available at: http://www.justice.gov/opa/pr/2012/February/12-ag-227.html [Accessed

August 8, 2014].

Omand, D., 2005. Reflections on secret intelligence. *Gresham College Transcript (London 20 Oct. 2005).*

Omand, S.D., 2010. *Securing the State* 1st ed., london: hurst & company.

Omand, S.D., 2013. The Cycle of Intelligence. In M. S. Goodman, R. Dover, & C. Hillebrand, eds. *Routledge Companion to Intelligence Studies*. London: Routledge, pp. 59–70.

Omand, S.D., Bartlett, J. & Miller, C., 2012. Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, 27(6), pp.801–823.

OSCT, 2011a. Protecting the UK against terrorism. *Home Office website*. Available at: http://www.homeoffice.gov.uk/counter-terrorism/OSCT/ [Accessed June 17, 2011].

OSCT, 2011b. *The United Kingdom's Science and Technology Strategy for Countering International Terrorism*, London. Available at: www.homeoffice.gov.uk/publications/counter-terrorism/science-and-technology/science-and-technology-strategy%3fview=Binary.

OTT, M., 2003. Partisanship and the Decline of Intelligence Oversight. *International Journal of Intelligence and CounterIntelligence*, 16(1), pp.69–94. Available at: http://www.ingentaconnect.com/content/routledg/ujic/2003/00000016/00000001/art00005 [Accessed December 31, 2014].

Parliament, 2014. *Cabinet Committee Membership Lists 2014*, London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/391889/CabinetCommitteeMembershipLists_Tables.pdf.

Parliament, 2008. *Counter Terrorism Act 2008*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/2008/28/pdfs/ukpga_20080028_en.pdf.

Parliament, 1996. *Criminal Procedures and Investigations Act 1996*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/1996/25/introduction.

Parliament, 1998a. *Data Protection Act 1998*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/1998/29/introduction.

Parliament, 2000a. *Freedom of Information Act 2000*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/2000/36/contents.

Parliament, 1679. *Habeus Corpus Act 1679*, United Kingdom. Available at: http://www.legislation.gov.uk/aep/Cha2/31/2/.

Parliament, 1998b. *Human Rights Act 1998*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/1998/42/contents.

Parliament, 2005. *Prevention of Terrorism Act 2005*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/2005/2/pdfs/ukpga_20050002_en.pdf.

Parliament, 2000b. *Regulation of Investigatory Powers Act (RIPA) 2000*,

Parliament, 2006a. *Report of the Official Account of the Bombings in London on 7th July 2005*, London.

Parliament, 1989. *Security Service Act (1989)*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/1989/5/pdfs/ukpga_19890005_en.pdf.

Parliament, 2000c. *Terrorism Act 2000*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/2000/11/pdfs/ukpga_20000011_en.pdf.

Parliament, 2006b. *Terrorism Act 2006*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/2006/11/introduction.

Parliament, 2011. *Terrorism Prevention and Investigation Measures Act 2011*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/2011/23/pdfs/ukpga_20110023_en.pdf.

Parliament, 2010. *Terrorist Asset-Freezing Act 2010*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/2010/38/pdfs/ukpga_20100038_en.pdf.

Parliament, 2006c. *The Al-Qaida and Taliban United Nations Measures Order 2006*, Available at: http://www.legislation.gov.uk/uksi/2006/2952/pdfs/uksi_20062952_en.pdf.

Parliament, 1994. *The Intelligence Services Act 1994*, UK. Available at: http://www.legislation.gov.uk/ukpga/1994/13/introduction.

Parliament, 2000d. *The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000*, United Kingdom: Home Secretary. Available at: http://www.legislation.gov.uk/uksi/2000/2417/pdfs/uksi_20002417_en.pdf [Accessed June 20, 2012].

Parliament, 2006d. *The Terrorism (United Nations Measures) Order 2006*, United Kingdom. Available at: http://www.legislation.gov.uk/uksi/2006/2657/pdfs/uksi_20062657_en.pdf.

Parliament, 1946. *United Nations Act 1946*, United Kingdom. Available at: http://www.legislation.gov.uk/ukpga/1946/45/pdfs/ukpga_19460045_en.pdf.

Perri, F.S., Lichtenwald, Terrance, G. & MacKenzie, P.M., 2009. THE CRIME-TERROR NEXUS. *The Forensic Examiner*.

Peters, S., 2012. *Channel: Protecting vulnerable people from being drawn into terrorism - A guide for local partnerships - October 2012*, Lon. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118194/channel-guidance.pdf.

Phythian, M., 2008. *Intelligence Theory: Key Questions and Debates*, Taylor & Francis.

Phythian, M., 2011. Political Interference in the Intelligence Process: The Case of Iraqi WMD. In M. S. Goodman & R. Dover, eds. *Learning from the Secret Past: Cases in British Intelligence History*. Georgetown: Georgetown University Press.

Phythian, M., 2009. The British Experience with Intelligence Accountability. In C. Andrews, R. J. Aldrich, & W. K. Wark, eds. *Secret Intelligence: A Reader*. Oxfordshire: Routledge, pp. 337–357.

Phythian, M., 2013. *Understanding the Intelligence Cycle (Studies in Intelligence)* 1st ed. M. Pythian, ed., London: Routledge.

Pistole, J.S., 2013. Oral Statement of TSA Administrator John S. Pistole Before the United States House of Representatives Committee on Homeland Security Subcommittee on Transportation Security - 14 March 2013. , pp.1–6. Available at: http://www.tsa.gov/sites/default/files/publications/pdf/testimony/13_0314_jsp_testimony.pdf.

Pond, E., 2013. *Rebalancing Security and Freedom in the 21 st Century*, Berlin. Available at: http://transatlantic.sais-jhu.edu/Rebalancing Security and Freedom in the 21st Century.pdf.

Porges, M.L., 2010. Deradicalisation, the Yemeni Way. *Survival*, 52, pp.27–33.

Prime Minister's Office, 2010. Establishment of a National Security Council. *Prime Minister's Office*. Available at: http://webarchive.nationalarchives.gov.uk/20130109092234/http://number10.gov.uk/news/establishment-of-a-national-security-council/ [Accessed January 15, 2015].

RAND, RAND's Institutional Principles. Available at: http://www.rand.org/about/principles.html.

Ratcliffe, J.H., 2008. *Intelligence-led Policing* 1st ed., Cullompton, Devon: Willan.

Ratcliffe, J.H., 2003. Intelligence-led policing. *Trends & Issues in Crime and Criminal Justice*, (248), pp.1–6. Available at: http://aic.gov.au/media_library/publications/tandi/ti248.pdf [Accessed January 12, 2015].

Rayment, S. & Blomfield, A., 2010. Detroit terror attack : Britain sends counter-terrorist forces to Yemen. *Daily Telegraph*, pp.1–4. Available at: http://www.telegraph.co.uk/news/worldnews/middleeast/yemen/6924502/Detroit-terror-attack-Britain-sends-counter-terrorist-forces-to-Yemen.html [Accessed April 4, 2011].

Reiner, R., 2010. *The Politics of the Police* 4th ed., Oxford: Oxford University Press.

Rice, C., 2010. US embassy cables: Washington requests personal data on Hamas. *The Guardian*. Available at: http://www.theguardian.com/world/us-embassy-cables-documents/176247 [Accessed July 20, 2012].

Richards, J., 2014. Peddling Hard: Further Questions about the Intelligence Cycle in the Contemporary Era. In *Understanding the Intelligence Cycle*.

Richards, J., 2010. *The Art and Science of Intelligence Analysis*, Oxford: Oxford University Press.

Rifkind, M., 2011. *Intelligence and Security Committee Annual Report 2010 – 2011*,

Rifkind, M., 2012. *Intelligence and Security Committee Annual Report 2011 – 2012*,

Rifkind, M., 2013. *Intelligence and Security Committee Annual Report 2012 – 2013*, London: TSO.

Rogers, P., 2008. Contesting and Preventing Terrorism: On the Development of UK Strategic Policy on Radicalisation and Community Resilience. *Journal of Policing, Intelligence and Counter Terrorism*, 3(2), pp.38–61.

Rose, C., 2014. *The Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers 2013-2014*, London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229219/0498.pdf.

Rose, C., 2012. *The Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers, 2011-2012*, London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229219/0498.pdf.

Roy, A., 2002. *The algebra of infinite justice* 5th ed., Bronx, NY: Flamingo.

Russell, R.L., 2007. Achieving All-Source Fusion. In *Handbook of Intelligence Stuidies*. London: Routledge (Taylor and Francis), pp. 189–198.

Ryan, M., 2006. Filling in the “unknowns”: hypothesis-based intelligence and the Rumsfeld Commission. *Intelligence & National Security*, 21(2), pp.286–315.

Rycroft, M., 2002. *The Secret Downing Street Memo*, London.

Sage Publications, 2014. Author - Robert M. Clark. *SAGE Publications website*. Available at: http://www.uk.sagepub.com/authorDetails.nav?contribId=659076 [Accessed February 10, 2015].

Saul, B., 2008a. *" Terrorism " in International Law*, Sydney.

Saul, B., 2006. *Defining Terrorism in International Law*, New York: Oxford University Press.

Saul, B., 2007. Defining "Terrorism" to Protect Human Rights. In D. Staines, ed. *INTERROGATING THE WAR ON TERROR: INTERDISCIPLINARY PERSPECTIVE*. Cambridge: Cambridge Scholars Publishing, pp. 190–210.

Saul, B., 2008b. *Definition of "Terrorism" in the UN Security Council*, Sydney.

Saul, B., 2008c. Sydney Law School. , (08), pp.1985–2004.

Saul, B., 2008d. *The Curious Element of Motive in Definitions of Terrorism: Essential Ingredient - Or Criminalising Thought?*, Sydney: Federation Press. Available at: http://papers.ssrn.com/abstract=1291571.

Sawers, J., 2010. The Chief's speech, 28th October 2010: Britain's Secret Frontline. , (October 2010), pp.1–9. Available at: https://www.sis.gov.uk/about-us/the-chief/the-chief%27s-speech-28th-october-2010.html.

Schbley, A., 2003. Defining Religious Terrorism: A Causal and Anthological Profile. *Studies in Conflict & Terrorism*, 26(2), pp.105–134. Available at: http://www.tandfonline.com/doi/abs/10.1080/10576100390145198 [Accessed September 24, 2014].

Schindler, J.R., 2009. Intelligence and Strategy in the war on Islamsit terrorism. In C. Andrew, R. J. Aldrich, & W. K. Wark, eds. *Secret Intelligence: A Reader*. Oxford: Routledge (Taylor and Francis), pp. 245–258.

Schmemann, S., 2001. A NATION CHALLENGED: U.S. REALIGNMENT; A Growing List of Foes Now Suddenly Friends. *New York Times*, p.4. Available at: http://www.nytimes.com/2001/10/05/world/a-nation-challenged-us-realignment-a-growing-list-of-foes-now-suddenly-friends.html [Accessed July 1, 2011].

Schmid, A.P., 2004. Terrorism: The Definitional Problem. *Journal of International Law*, 36, pp.375–395.

Schmid, A.P. & Alex, P.S., 2004. FRAMEWORKS FOR CONCEPTUALISING TERRORISM. *Terrorism and Political Violence*, 16(2), pp.197–221. Available at: http://www.tandfonline.com/doi/abs/10.1080/09546550490483134 [Accessed June 2, 2014].

Schmid, A.P. & Jongman, A.J., 2005. *Political terrorism: A new guide to* *actors, authors, concepts, data bases, theories, and literature*, New Jersey: Transaction Publishers.

Schulsky, A. & Schmitt, G., 2002. *Silent Warfare: Understanding the World of Intelligence*, Washington, D.C.

Schum, D.A., 1988. *Evidence and inference for the intelligence analyst*, London: University Press of America. Available at: https://openlibrary.org/books/OL22471516M/Evidence_and_inference_for_the_intelligence_analyst [Accessed February 5, 2015].

Security Service, 2015. Joint Terrorism Analysis Centre - The Security Service. *Security Service official website*, p.1. Available at: https://www.mi5.gov.uk/home/about-us/who-we-are/organisation/joint-terrorism-analysis-centre.html [Accessed January 15, 2015].

Security Service, *Security Service Memo SYS00011080-001: OP CREVICE SUMMARY*,

Security Service, 2011. Security Service: What We Do. *Security Service website*, p.1. Available at: https://www.mi5.gov.uk/home/about-us/what-we-do.html [Accessed June 15, 2011].

Senate, 1947. *National Security Act 1947*, USA. Available at: http://www.intelligence.senate.gov/nsaact1947.pdf.

Senate Select Committee On Intelligence, 2014. *Senate Select Committee On Intelligence: Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*, Washington, D.C. Available at: http://www.intelligence.senate.gov/study2014/sscistudy1.pdf [Accessed February 3, 2015].

Seto, Y., 2001. The Sarin Gas Attack in Japan and the Related Forensic Investigation. *Synthesis*.

Sheptycki, J., 2004. Organizational Pathologies in Police Intelligence Systems: Some Contributions to the Lexicon of Intelligence-Led Policing. *European Journal of Criminology*, 1(3), pp.307–332. Available at: http://euc.sagepub.com/cgi/doi/10.1177/1477370804044005 [Accessed September 24, 2014].

Silberman, L.H. & Robb, C.S., 2005. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Washington, D.C. Available at: http://www.gpo.gov/fdsys/pkg/GPO-WMD/pdf/GPO-WMD.pdf.

Sims, J.E. & Gerber, B., 2005. *Transforming U.S. Intelligence* J. E. Sims, ed., Georgetown: Georgetown University Press.

SIS, 2011. SIS: Strategy & Values. *SIS Website*, p.1. Available at: https://www.sis.gov.uk/about-us/sis-strategy-and-values.html [Accessed July 30, 2011].

Source_02, 2011. *Interview 02*,

Source_04, 2011. *Interview 04*,

Source_05, 2011. *Interview 05*,

Source_06, 2011. *Interview 06*,

Source_07, 2011. *Interview 07*,

Source_08, 2011. *Interview 08*,

Source_10, 2011. *Interview 10*,

Source_11, 2011. *Interview 11*,

Source_12, 2011. *Interview 12*,

Source_14, 2011. *Interview 14*,

Stanier, I., 2012. *Contemporary organisational pathologies in police information sharing : new contributions to Sheptycki 's lexicon of intelligence led policing*. London Metropolitan University.

Stein, kenneth, 1999. *Heroic Diplomacy: Sadat, Kissinger, Carter, Begin, and the Quest for Arab-Israeli Peace*, London: Routledge.

Stelter, B., 2009. How '07 ABC Interview Tilted a Torture Debate. *New York Times*, pp.2–5. Available at: http://www.nytimes.com/2009/04/28/business/media/28abc.html?_r=0&ref=business&pagewanted=all.

Stern, J., 2000. *The Ultimate Terrorists*, Harvard: Harvard University Press.

Stewart, R.W., 2003. *The United States Army in Somalia, 1992-1994*, Claitors.

Straw, J., 2010. *PREVENTION AND SUPPRESSION OF TERRORISM: The Proscribed Organisations (Name Changes) Order 2010*, United Kingdom. Available at: http://www.legislation.gov.uk/uksi/2010/34/pdfs/uksi_20100034_en.pdf.

Sturcke, J., 2006. Man gets life sentence for terror plot. *The Guardian*. Available at: http://www.theguardian.com/world/2006/nov/07/terrorism.uk [Accessed January 17, 2015].

Summers, C., 2012. Mobile phones - the new fingerprints. *Synergy Forensics*. Available at: http://news.bbc.co.uk/1/hi/uk/3303637.stm [Accessed January 1, 2015].

Summers, C. & Casciani, D., 2007. Fertiliser bomb plot: The story. *BBC News*. Available at: http://news.bbc.co.uk/2/hi/uk_news/6153884.stm [Accessed January 1, 2015].

Supreme Court, 2010. Judgement: HM Treasury v Ahmed. Available at: http://www.bailii.org/uk/cases/UKSC/2010/2.html.

Svendsen, A.D.M., 2013. Introducing RESINT: A Missing and Undervalued "INT" in All-Source Intelligence Efforts. *International Journal of*

Intelligence and CounterIntelligence, 26(March 2015), pp.777–794. Available at: http://www.tandfonline.com/doi/abs/10.1080/08850607.2013.807196.

SWARB, 2014. Malone v The United Kingdom; ECtHR 02 Aug 1984. *SWARB website*. Available at: http://swarb.co.uk/malone-v-the-united-kingdom-echr-2-aug-1984/ [Accessed January 15, 2015].

Taber, R., 1965. *War of the Flea: Guerilla Warfare in Theory and Practice* 1st ed., New York: Lyle Stuart.

Taylor, A., 2003. *Intelligence and Security Committee Iraqi Weapons of Mass Destruction – Intelligence and Assessments*, London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/224708/Iraq_WMD.pdf.

Taylor, P., 1997. *Provos, The IRA and Sinn Fein*, London: Bloomsbury Publishing.

The Guardian, 2006. Barot operation posed complex challenge. *The Guardian*. Available at: http://www.theguardian.com/uk/2006/nov/07/usa.terrorism [Accessed October 4, 2013].

The Scottish Government, 2012. *Common Knowledge: Thematic Inspection of Information and Intelligence Sharing - Chapter 4.14 Intelligence Grading System*, Edinburgh. Available at: http://www.scotland.gov.uk/Publications/2007/03/13161000/8.

Thomas, G., 2009. *Secret Wars*, London: St. Martins Press.

Tiefenbrun, S., 2003. A SEMIOTIC APPROACH TO A LEGAL DEFINITION OF TERRORISM. *ILSA Journal of International and Comparative Law*.

Travis, A., 2011. Official review finds scant evidence of state funds going to extremists. *The Guardian*, pp.1–3. Available at: http://www.theguardian.com/uk/2011/jun/07/review-state-funding-extremism/print [Accessed March 23, 2014].

Trent, S., Patterson, E. & Woods, D., 2007. Challenges for Cognition in Intelligence Analysis. *Journal of Cognitive Engineering and Decision Making*, 1, pp.75 – 97.

Treverton, G.F., 2008. Inteligence Analysis: Between “Politicization” and Irrelevance. In R. Z. George & J. B. Bruce, eds. *Analyzing Intelligence: Origins, Obstacles and Innovations*. Washington, D.C.: Georgetown University Press, pp. 91–104.

Treverton, G.F., 2009. *Intelligence for an Age of Terror* 1st ed., Cambridge: Cambridge University Press.

Treverton, G.F., 2001. *Reshaping National Intelligence for an Age of Information*, Cambridge University Press.

Treverton, G.F. et al., 2006. Toward a Theory of Intelligence. Workshop Report G. F. Treverton et al., eds. Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA449313 [Accessed September 23, 2014].

TTRSL, 2008. *TTSRL Policy Brief Number 2*, The Hague. Available at: http://www.transnationalterrorism.eu/tekst/newsletters/TTSRL Policy Brief 3.4.pdf [Accessed January 12, 2015].

Turner, S., 1974. *Special National Intelligence Estimate SNIE 4-1-74: Prospects for Further Proliferation of Nuclear Weapons*, Langle. Available at: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB240/snie.pdf.

Tversky, A. & Kahneman, D., 1974. Judgment under Uncertainty: Heuristics and Biases. *Science1*, 185, pp.1124–1131.

U.S. Army, 2013. Every Soldier a Sensor. In *U.S. Army FM 3-21.75: The Warrior Ethos and Soldier Combat Skills*. CreateSpace Independent Publishing Platform, p. 316.

U.S. Attorney, 2010. *Babar 5k letter: United States v Mohammed Junaid Babar*, New York.

U.S. District Court, 2004. *Abu Hamza Al Masri indictment in US Court*, New York. Available at: http://www.justice.gov/usao/nys/pressreleases/October12/ChargingDocs/Mustafa, Mustafa Indictment.pdf.

U.S. District Court, 2007. Dhiren Barot indictment. *U.S. District Court, Southern District of New York*. Available at: http://www.washingtonpost.com/wp-srv/articles/hindi.pdf [Accessed March 28, 2013].

U.S. District Court, 2002. *Richard Reid Indictement*, Massachusetts. Available at: http://www.fas.org/irp/news/2002/01/reidindictment.pdf.

U.S. District Court, 2006. *United States v. Zacarias Moussaou, Criminal No. 01-455-A*, Virginia. Available at: http://www.vaed.uscourts.gov/notablecases/moussaoui/exhibits/.

U.S. State Department, 2002. *Joint Resolution to Authorize the Use of United States Armed Forces Against Iraq*, Washington, D.C. Available at: http://georgewbush-whitehouse.archives.gov/news/releases/2002/10/20021002-2.html.

UK Government, 2015. Director, Chief of the Assessments Staff - Role Description. *www.reference.data.gov.uk*. Available at: http://reference.data.gov.uk/2011-09-30/doc/department/co/post/52 [Accessed October 23, 2015].

UK Government, 1998. *The Agreement: Agreement reached in the multi-party negotiations*, UK.

UKBA, 2011. UK Border Agency: About us. *UKBA Website*. Available at:

http://www.ukbaguide.co.uk/aboutus.htm [Accessed August 12, 2012].

UN, Somalia - UNOSOM II Background. Available at: www.un.org/en/peacekeeping/missions/past/unosom2backgr1.html.

UNGA, 2002. *United Nations General Assembly Report of the Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996, Sixth session (28 January-1 February 2002)*, Available at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N02/248/17/PDF/N0224817.pdf.

UNHRC, 2006. *Report of the Commission of Inquiry on Lebanon pursuant to Human Rights Council resolution S-2/1*, Available at: http://web.archive.org/web/20070630133336/http:/www.ohchr.org/english/bodies/hrcouncil/docs/specialsession/A.HRC.3.2.pdf.

United Nations, 1945. *Charter of the United Nations*, United Nations website. Available at: http://www.un.org/en/documents/charter/index.shtml.

UNSC, 2005. *UN Security Council 1624 Threats to International Peace and Security (Security Council Summit 2005)*, UN Security Council. Available at: http://unscr.com/en/resolutions/1624.

UNSC, 2009. *UN Security Council Resolution 1904*, Available at: http://www.un.org/press/en/2009/sc9825.doc.htm.

UNSC, 2004. *United Nations Security Council Resolution 1566*, UN Security Council. Available at: http://unscr.com/en/resolutions/1566.

UNSC, 2011. *UNited Nations Security Council Resolution 1973*, UN Security Council. Available at: http://unscr.com/en/resolutions/1973.

UNSC, 1993. *United Nations Security Resolution 814*,

UNSC, 2002. *UNSCR 1441*, Available at: http://www.un.org/Depts/unmovic/documents/1441.pdf [Accessed January 1, 2015].

UNSC, 1991. *UNSCR 687*, Available at: http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/596/23/IMG/NR059623.pdf?OpenElement [Accessed January 1, 2015].

Urban, M., 1993. *Big Boys' Rules: SAS and the Secret Struggle Against the IRA*, London: Faber and Faber.

Urban, M., 2010. *Task Force Black* 1st ed., London: Little, Brown.

Vanunu, M., 1987. Dimona and Vanunu. *Journal of Palestine Studies*, 16(2), pp.171–181.

Visual Analysis, *Simon HANNES - the $2 Million Insider Trader*, Canberra. Available at: https://www.visualanalysis.com/Images/ANB/CHARTS/Simon HANNES - the $2 Million Insider Trader.jpg [Accessed February 3, 2015].

Walpole, R.D., 2002. *National Intelligence Estimate: Iraq's continuing programs for Weapons of Mass Destruction, October 2002*,

Walters, V., 1978. *Silent Missions*, Garden City, NY: Doubleday.

Warner, M., 2002. Wanted: a definition of intelligence. *Studies in Intelligence (declassified or unclassified articles from the CIA's internal journal)*, 46, pp.15–23.

Weiss, P., 2002. International Law Related to Terrorism. In *Institute of Energy and Environmental Research Conference: Nuclear Dangers and the State of Security Treaties*. New York, pp. 1–5. Available at: http://www.tni.org/archives/archives_weiss_ieer [Accessed June 11, 2011].

Wheaton, K.J., 2011. Let's Kill the Intelligence Cycle. *Sources and Methods website*. Available at: http://sourcesandmethods.blogspot.nl/2011/05/lets-kill-intelligence-cycle-original.html [Accessed September 22, 2013].

Whitehead, T., 2014. Up to 700 Britons feared to be in Syria. *Daily Telegraph*, p.1. Available at: http://www.telegraph.co.uk/news/uknews/law-and-order/10785316/Up-to-700-Britons-feared-to-be-in-Syria.html [Accessed December 22, 2014].

Wintour, P., 2012. UK special forces will stay in Afghanistan in anti-terror role. *The Observer*. Available at: http://www.guardian.co.uk/world/2012/may/20/special-forces-stay-in-afghanistan on 20 July 2012 [Accessed July 20, 2012].

Wright, L., 2002. The Man Behind Bin Laden: How an Egyptian doctor became a master of terror. *The New Yorker*. Available at: http://www.newyorker.com/magazine/2002/09/16/the-man-behind-bin-laden [Accessed January 15, 2015].

Zeldin, W., 2012. Anti-Terror Law Ruled Constitutional (R. v. Khawaja, supra, § 126.). Available at: http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403436_text [Accessed January 31, 2015].

Zelik, D., Patterson, E.S. & Woods, D.D., 2007. *When is Analysis Sufficient: A Study of How Professional Analysts Judge Rigor*,

Zunes, S., 1988. International terrorism. *Foreign Policy in Focus*, 3(38), pp.335–337.

Zeldin, W., 2012. Anti-Terror Law Ruled Constitutional (R. v. Khawaja, supra, § 126.). Available at: http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403436_text [Accessed January 31, 2015].

Zelik, D., Patterson, E.S. & Woods, D.D., 2007. *When is Analysis Sufficient: A*

Study of How Professional Analysts Judge Rigor,

Zunes, S., 1988. International terrorism. *Foreign Policy in Focus*, 3(38), pp.335–337.

VITA

Paul Burke is a career Intelligence professional with over thirty years of experience working in Intelligence, counter-terrorism and national security.