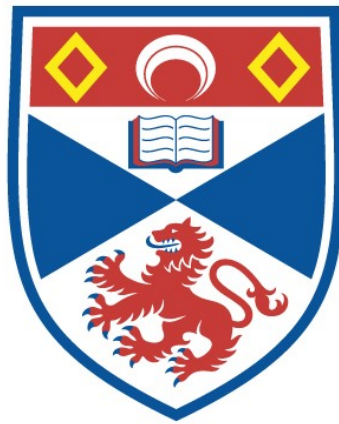


THE APPLICATION OF DATABASE TECHNOLOGIES TO THE
STUDY OF TERRORISM AND COUNTER-TERRORISM:
A POST 9/11 ANALYSIS

Neil Gordon Bowie

A Thesis Submitted for the Degree of PhD
at the
University of St Andrews



2012

Full metadata for this item is available in
St Andrews Research Repository
at:
<http://research-repository.st-andrews.ac.uk/>

Please use this identifier to cite or link to this item:
<http://hdl.handle.net/10023/3641>

This item is protected by original copyright

UNIVERSITY OF ST. ANDREWS

**THE APPLICATION OF DATABASE TECHNOLOGIES
TO THE STUDY OF TERRORISM AND COUNTER-
TERRORISM: A POST 9/11 ANALYSIS**

A thesis submitted in part-candidature

for the degree of

Doctor of Philosophy (Ph.D.)

Neil Gordon Bowie

School of International Relations

April 2011

DECLARATIONS

- (i) I, Neil Gordon Bowie, hereby certify that this thesis, which is approximately 80,000 words in length, has been written by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree.

Date: Signature of Candidate:

- (ii) I was admitted as a research student in October 2007, and as a candidate for the degree of Doctor of Philosophy (Ph.D.) in October 2007; the higher study for which this is a record was carried out in the University of St. Andrews between 2007 and 2011.

Date: Signature of Candidate:

- (iii) I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Doctor of Philosophy (Ph.D.) in the University of St. Andrews and that the candidate is qualified to submit this thesis in application for that degree.

Date: Signature of Supervisor:

- (iv) In submitting this thesis to the University of St. Andrews we understand that we are giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. We also understand that the title and abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker, that my thesis will be electronically accessible for personal or research use unless exempt by award of an embargo as requested below, and that the library has the right to migrate my thesis into new electronic forms as required to ensure continued access to the thesis. We have obtained third-party copyright permissions that may be required in order to allow such access and migration, or have requested the appropriate embargo below.

The following is an agreed request by candidate and supervisor regarding the electronic publication of this thesis:

Embargo on both [all] of printed copy and electronic copy for the same fixed period of five years on the following ground(s):

Publication would preclude future publication.

Date:

Signature of Candidate:

Signature of Supervisor:

ABSTRACT

THE APPLICATION OF DATABASE TECHNOLOGIES TO THE

STUDY OF TERRORISM AND COUNTER-TERRORISM:

A POST 9/11 ANALYSIS

Data and information of the highest quality are critical to understanding and countering acts of terrorism. As a tool, database technologies are becoming integral to the field of terrorism studies. The intelligence failings of September 11th 2001 illustrate the need for timely, relevant and accurate data, derived from a plethora of complex intelligence sources.

This thesis will argue that, at least until 9/11, the academic study of terrorism and counter-terrorism databases has been limited and that the subject lacks an overall coherency and direction. The thesis asks: what is the quality and practical value of database technologies in the field of terrorism and counter-terrorism post 9/11? The study will provide a cross-disciplinary approach, specifically from the disciplines of political science and computer science. It will present an understanding of the conceptual, design, operation, strengths and weaknesses of terrorism and counter-terrorism databases. The ramifications of post 9/11 and its impact upon the intelligence community, and the areas of security, privacy and emerging technologies in data mining and terrorism informatics are assessed.

This study will examine mainly open source information on terrorism and counter-terrorism databases. The research methodology will be carried out using a series of case studies, from the ITERATE, RAND/MIPT, WITS, and GTDB data sets. Primary sources, for example, codebooks, and secondary source materials such as Library of Congress and GAO reports are used. A comparative sampling of relational databases and terrorism data sets is undertaken.

The thesis will illustrate that with increased federal funding, new terrorism database technologies, post 9/11, operate under sophisticated schemata, requiring complex and systematic synthesis. In addition, issues of data sharing, fusion, interoperability and ethical concerns will be addressed.

Implications for future terrorism database technologies will be articulated. These require rigorous design methodologies be adopted, while safeguarding ethical and privacy concerns. The thesis provides a coherent systematic analysis of terrorism and counter-terrorism databases, from what to date has been a disaggregated subject field.

DEDICATION

To David

ACKNOWLEDGEMENTS

The journey is complete. I struggle to find the words of gratitude to express to my loving family, my supervisors, close friends and the many individuals and organisations that have helped me throughout the years.

To my late dad, Thomas Smith Bowie and my mum, Elizabeth Bowie, thank you from the very bottom of my heart. Through the most challenging of times they have always been there with their unconditional love, understanding and support; it will never be forgotten. Also, thanks indeed to my family, Graeme and Julie, David and Carol and Brian and Elaine for many years of continued support.

To Isa and Dave McLaren, and David - your unwavering love and support has been truly special. Thank you so much.

Although not with us today, I would like to say a special thanks to Aunty Buntly and Jimmy Bain, always supportive of my studies; I just know they would be delighted I made it!

One of the great privileges of my time at St. Andrews University was to have the highest standards of doctoral supervision. To Professor Ali Watson in the School of International Relations, my deepest thanks. Your on-going support, understanding and belief in me have touched me deeply. You helped me close the circle. To Dr. Alex P. Schmid, former Director of the Centre for the Study of Terrorism and Political Violence (CSTPV) at St. Andrews, I would like to convey my sincere and heartfelt thanks for the excellent supervision you gave to me both at St. Andrews and on your return to Vienna. Your patience, commitment, enthusiasm and willingness to give freely of your time has been remarkable. You entrusted me with opportunities in terrorism research that have been invaluable. I feel so truly privileged to have worked with you.

From the age of eighteen, as an undergraduate at the University of Aberdeen through to postgraduate studies at St. Andrews, to the late Professor Paul Wilkinson, I extend my most sincere gratitude. Professor Wilkinson inspired my interest in terrorism studies and for three decades gave generously of his time and support for my research. I will always treasure the phone call I made to let him know I had passed my Viva.

To my dear friends Susan, Jennifer, Alan, Gillian, Graham, Mooneen and Jan - always there for me, a massive thank you. To Frances McKee, what can I say? I'm lost for words. Your loving support from start to finish and beyond has been priceless. Thank you so much.

Many other people have shown much kindness over my years at St. Andrews University. I would particularly like to thank Professor Bruce Hoffmann and Donna Hoffmann, and also Gina Wilson. To Gillian Duncan and Julie Middleton of the CSTPV, you have been so very kind. Thank you for sharing so many special times. Finally, my thanks must also go to the many other people whose paths I've crossed in St. Andrews and beyond.

Neil G. Bowie
The University of St. Andrews
May 2012

TABLE OF CONTENTS

DECLARATIONS	ii
ABSTRACT	iv
DEDICATION	v
ACKNOWLEDGEMENTS	vi
TABLE OF CONTENTS	vii
LIST OF ILLUSTRATIONS	x
LIST OF TABLES	xii
LIST OF ABBREVIATIONS	xiii
CHAPTER I. THE NEED FOR KNOWLEDGE	
1.1 Introduction	1
1.2 Defining the problem	2
1.3 Scope and research design methodology	4
1.4 Data sets in historical context	6
1.5 Defining: data sets, chronologies and databases	12
1.6 Development of computerised terrorism data sets: The early years	13
1.7 Information technology and Terrorism Studies	18
1.8 Quantitative theory development	23
1.9 Conclusions	26
CHAPTER II. THE PRE-9/11 CONTEXT	
2.1 Introduction	28
2.2 Early Research – monographs	30
2.3 Early Research – journal articles and data sets	40
2.4 Early Research – technical literature	51
2.5 Conclusions	54
CHAPTER III. DESIGN AND DEVELOPMENT ISSUES IN TERRORISM AND COUNTER-TERRORISM DATABASES POST 9/11	
3.1 Introduction	55
3.2 Data definition: Defining Terrorism	57
3.3 Methodology	61
3.4 Sourcing data	70

3.5	Data Validity	72
3.6	The Codebook	86
3.7	Error Rates	87
3.8	Other Data Collection Methods	88
3.9	User Manuals	91
3.10	Database Management Systems (D.B.M.S)	98
3.11	Alternative approaches to terrorism data set design	100
3.12	Database Organisation and Structure	101
3.13	Advantages and Disadvantages of Database Management Systems	105
3.14	Conclusions	117

CHAPTER IV. POST 9/11: AN ANALYSIS OF TERRORISM AND COUNTER-TERRORISM DATABASES: THE PUBLIC, THE PRIVATE AND THE IN-BETWEEN

4.1	Introduction	119
4.2	Examining Terrorism Data Sets	120
4.3	The Public Profile	123
4.4	The Private: Government and Commercial	215
4.5	Government (Restricted and Unclassified) Terrorism Data Sets	220
4.6	Academic Terrorism Data Sets	254
	Case Study: South Africa	269
4.7	Conclusions	274

CHAPTER V. TERRORISM AND COUNTER-TERRORISM DATABASES POST-9/11: A COMPLEX MATRIX WITH FUTURE CHALLENGES

5.1	Introduction	276
5.2	The 9/11 Commission	280
5.3	U.S. Border Screening	290
5.4	Information Sharing	300
5.5	The Markle Foundation	304
5.6	Legislation Post 9/11	309
5.7	Conclusions	311

CHAPTER VI. SUMMARY AND CONCLUSIONS

6.1	Introduction	315
6.2	Summary	316
6.3	Conclusions	320

APPENDICES:	1
	7
Appendix A - List of Publicly Accessible Terrorism Databases for Chapter 4	328 1
Appendix B - Field Visits undertaken pre and during Thesis research	329
Appendix C - Poster Presentation – IEEE 2010, Vancouver, Canada	330
BIBLIOGRAPHY	331

LIST OF ILLUSTRATIONS

Figures	Page No.
Figure 1: Number of Incidents of Terrorism Worldwide, 1970-2007 (GTD)	130
Figure 2: Number of Terrorist Incidents Worldwide, 1992-2008, attributed to Al-Qaeda, according to GTD	131
Figure 3: Number of Incidents of Terrorism in Western Europe, Eastern Europe, former USSR & the Newly Independent States (NIS) 1997-2007 (GTD)	131
Figure 4: Trends in Person-borne Improvised Explosive Device (PBIED) vs. Suicide Vehicle-borne Improvised Explosive Device (SVBIED) attacks for Pakistan (NCTC 2008 Report on Terrorism)	139
Figure 5: Trends in Person-borne Improvised Explosive Device (PBIED) vs. Suicide Vehicle-borne Improvised Explosive Device (SVBIED) attacks for Rest of World. (NCTC 2008 Report on Terrorism)	140
Figure 6: Comparison of Terrorism Fatalities and Incidents by Region (NCTC 2008 Report on Terrorism)	141
Figure 7: Comparison of High-Fatality Sunni Attacks in Iraq (IZ) and Afghanistan (AF) versus Rest of World (RoW), 2004-2008 (NCTC 2008 Report on Terrorism)	142
Figure 8: Comparison of Terrorist Attacks and Victims by Region (NCTC 2008 Report on Terrorism)	143
Figure 9: International Terrorism Casualties, 1968-2007 (ITERATE)	149
Figure 10: International Terrorist Activity of Three Major Terrorist Groups, 1968-2007 (ITERATE)	150
Figure 11: Worldwide Terrorist Incidents by Year, 1999 - 2005 (MIPT)	156
Table 12: Top Twenty Countries in terms of Terrorist Fatalities per Million People 1968-2006 (MIPT)	156
Figure 13: Terrorist Incidents by Weapon, RAND-MIPT Terrorism Incident Database, 1 Jan. 2005 - 31 Dec. 2005 (MIPT Terrorism Annual 2006)	161
Figure 14: Terrorist Incidents by Target, RAND-MIPT Terrorism Incident Database, 1 Jan. 2005 - 31 Dec. 2005 (MIPT Terrorism Annual 2006)	162
Figure 15: Domestic Incidents of Terrorism by Region, RAND-MIPT Terrorism Incident Database, 1 Jan. 2005 - 31 Dec. 2005 (MIPT Terrorism Annual 2006)	163
Figure 16: Total International Terrorist Attacks, 1982-2003 (Patterns of Global Terrorism 2003)	168
Figure 17: Incidents of Terrorism Worldwide (Country Reports on Terrorism 2008: National Counterterrorism Center: Annex of Statistical Information)	169
Figure 18: Internal Terrorism in Western Europe, 1950-2004 (TWEED at http://folk.uib.no/sspje/tweed.htm)	172
Figure 19: Weekly Fatalities: Major Conflicts in South Asia, 9 -15 March, 2009 (SATP, <i>Weekly Assessments & Briefings</i> , Vol. 7, No. 36, 16 March 2009)	176
Figure 20: All Israeli Fatalities, Monthly, Palestinian – Israeli Conflict, 2000-2003 (www.ict.org.il)	180
Figure 21: All Palestinian Fatalities, Monthly, Palestinian – Israeli Conflict, 2000-2003 (www.ict.org.il)	181
Figure 22: Increasing Human Insecurity, 1976-2008 (Median Scores) (www.politicalterroryscale.org http://www.ict.org.il).	182
Figure 23: Decreasing Human Insecurity 1976-2008 (Median Scores) (www.politicalterroryscale.org http://www.ict.org.il).	185
Figure 25: Number of failed, foiled or successful attacks and number of arrested suspects for separatist terrorism in member states 2006-2008 (TE-SAT Report 2009).	191

FIGURES	Page No.
Figure 26: Left-wing and Anarchist Terrorist Attacks by Target, 2006-2008 (TE-SAT Report 2009)	192
Figure 27: Sample ISVG Omniscope Dataplayer – Incidents by Tactics, Philippines 30/12/00 – 13/6/09 (www.isvg.org)	196
Figure 28: Sample ISVG Omniscope Dataplayer – Incidents by Targets, Jemaah Islamiya 01/08/00 – 22/07/08 (www.isvg.org)	196
Figure 29: Sample Algeria from Armed Conflict Database – The International Institute for Strategic Studies (www.iiss.org)	201
Figure 30: Sample Myanmar from Armed Conflict Database – The International Institute for Strategic Studies (www.iiss.org).	202
Figure 31: Deaths from non-state forces' bombings and those killed fifty or more (Iraq Body Count)	205
Figure 32: Confirmed incidents involving unauthorized possession and related criminal activities, 1993-2008 (www.ns-iaea.org)	207
Figure 33: Incidents reported to the ITDB involving theft or loss, 1993-2008 (www.ns-iaea.org)	208
Figure 34: Conflicts by Region 1946-2007 (UCDP website)	213
Figure 35: Peace Agreements in Armed Conflicts 1989-2007 (UCDP website)	213
Figure 36: Post-Conflict Countries that revert to Conflict 1960-2007 (www.cidcm.umd.edu)	215

LIST OF TABLES

Tables	Page No.
3.1 Working Definition of Terrorism in Five Terrorism Databases	60
3.2 Events excluded from the WITS database	63
3.3 Terrorism Definitional Criteria – Global Terrorism Database (GTD)	67
3.4 Codesheet Model for IDC International Standard	113
4.1 Simple Functional Description of Data Sets, Chronologies and Databases	122
4.2 Classification of Public Profile Data Sets, Chronologies and Databases	123
4.3 Classification of Private, Government and Commercial data sets, chronologies and databases.	216

LIST OF ABBREVIATIONS

ATS	The American Terrorism Study
CRS	Congressional Research Service
CSTPV	The Centre for the Study of Terrorism and Political Violence
GAO	General Accounting Office
GTD	Global Terrorism Database
IBC	Iraq Body Count
ISVG	The Institute for the Study of Violent Groups
ITDB	Illicit Trafficking Database
ITERATE	International Terrorism: Attributes of Terrorist Events
MIR	Minorities at Risk Project
MIPT	Memorial Institute for the Prevention of Terrorism
NCTC	National Counterterrorism Center
PTS	Political Terror Scale
RAND	The RAND Corporation
SATP	South Asia Terrorism Portal
TE-SAT	Europol Terrorism Situation and Trend Report
TWEED	Terrorism in Western Europe: Events Data
UCPD	Uppsala Conflict Data Program
WITS	Worldwide Incidents Tracking System
WMD	Monterey Weapons of Mass Destruction Terrorism Database

CHAPTER I

THE NEED FOR KNOWLEDGE

1.1. Introduction

At the dawn of the 21st century, the issue of terrorism and political violence remains high on the agenda of governments, security agencies and those individuals concerned with maintaining democracy and the rule of law. The analysis of terrorism events data by policy makers, analysts and academics requires information of the highest quality if sound judgements are to be made. Their diverse need for information has produced a plethora of databases on terrorism. Sophisticated computerised database systems to record and interrogate the accumulated body of knowledge on terrorist data have been available for several years. Unfortunately the technical potential of these has not always been translated into practical reality. Whilst traditional terrorist tactics e.g. bombings, kidnappings and hijackings, have largely remained unchanged, the methods by which information on acts of terrorism can be stored on computer have been revolutionised in the past twenty years. As a result, the advent of widely available, relatively cheap, but highly advanced computer technology, permits storage and a much more sophisticated level of interrogation and retrieval of information.

The subject of information technology within the terrorism field has been poorly defined. Classification of the topic under the headings of 'Information Terrorism', 'Technology and Terrorism', 'Computers and Terrorism', and latterly 'Cyber Terrorism' has left the subject area in a somewhat confused state. The use of

terrorism events data sets¹ for the analysis of terrorism incidents has been used widely in the research field in recent years.² Unfortunately, however, our understanding of the application of computerised data sets to the study of terrorism has remained somewhat limited. To date there exists an array of computerised data sets on terrorism, all of which vary in size and quality. The development of the data sets has been somewhat haphazard. Moreover, no overall body provides guidelines for the establishment of computerised databases on terrorism. As a result there is little consistency or continuity in their development. This has major repercussions for quantitative and empirical research in the terrorism field. Apart from seminal research undertaken by Fowler in 1981,³ and Schmid and Jungman's compilation of databases on terrorism in 1988,⁴ no comprehensive inventory of terrorism databases post 9/11 exists. It is the aim of this thesis to undertake such an analysis with particular reference to databases post 9/11.

1.2. Defining the Problem

This thesis sets out to answer the following questions: first, what is the quality, practical value and impact of database technologies in the field of terrorism and counter-terrorism post 9/11?; and second, how can the application of database

¹ Data sets on terrorism events data are usually held within databases systems. They can, however, also be used within spreadsheets and word-processors, with more limited functionality.

² The literature using terrorism events data sets for quantitative analysis is wide and varied. A key U.S. Government publication is the National Counterterrorism Center's (NCTC) annual *Report on Terrorism*. See: http://www.nctc.gov/witsbanner/docs/2009_report_on_terrorism.pdf Earlier pre 9/11 data sets included the United States Department of State's *Patterns of Global Terrorism* and Edward Mickolus's *ITERATE* (New York: Greenwood Press, 1988).

³ Fowler, William Warner. *Terrorism Data Bases: A Comparison of Missions, Methods, and Systems*. RAND Corporation. Santa Monica 1981. N-1503-RC. See: <http://www.rand.org/pubs/notes/N1503.html> [Accessed 13/06/10]

⁴ Schmid, Alex P. and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*. (New Brunswick, USA: Transaction Books, 2nd. Ed, 1988.)

systems improve the quality of terrorism and counter-terrorism research? The principal advantage of new technology is in its ability to absorb massive quantities of raw data, complete an almost infinite array of manipulations, finally synthesising and producing data that is meaningful in terms of the questions being asked. Impressive as this may sound, further questions relating specifically to the application of database systems to terrorism research need to be asked. For example, what is the present state of the art with regard to the development of computerised data sets?; what are the major conceptual, definitional, theoretical and practical problems faced in the design of computerised data sets on terrorism?; do these have any major repercussions for terrorism data sets?; can the subject of computerised terrorism data sets be clearly defined within the information technology area of terrorism studies?; what are the strengths and weaknesses of existing open source terrorism data sets, and can the quality of these data sets be improved?; can some form of minimum standards be agreed upon in the practical design of terrorism data sets?; and, indeed, why is this study crucial to the study of terrorism?

With these questions in mind, the main hypotheses of this thesis are:

1. That the study of computerised terrorism databases has had very little direction.
The subject area needs to be drawn together under the classification of 'Terrorism Informatics' if its full potential is to be realised.
2. That despite the fact that computerising terrorism data sets has allowed for more sophisticated levels of interrogation, this still does not deal with the issues surrounding the problem of soft qualitative data.

3. The application of computerised databases to terrorism research requires a high level of inter-disciplinarity. This includes the disciplines of international relations, computer science and other techniques (empirical, quantitative, content analysis, link analysis etc.) derived from a variety of social science disciplines, e.g. economics and psychology. The task of integrating such an eclectic array of subjects requires a systems approach to the fusion of computers and the study of terrorism.
4. The inevitable shift towards a more technologically based response to countering acts of terrorism requires the field of Terrorism Informatics to be more formally recognised for the full potential of technology to be realised.

1.3. Scope and Research Design Methodology

The thesis is particularly concerned with the information aspects of terrorism and counter-terrorism in general, and database management systems specifically. The scope of databases used in this thesis is mainly limited to publicly available data sets, databases and chronologies on terrorism. The thesis will draw upon a wide range of publicly accessible sources of information. These include opens source material, as well as a number of case studies. In addition, through a variety of field visits, the opinions of those people currently working in the field of terrorism research, as to the efficacy of particular data sets has been considered. These will be highlighted throughout the thesis.

Open Source Material

The thesis will use various research methods to build a comprehensive evidence base to answer the above research questions. This study will examine mainly open source material and both primary and secondary source material is used. Primary source material will include terrorism database codebooks, whilst secondary source material will include academic literature, commercial literature, Library of Congress material, U.S. Government Accounting Office (GAO) publications and various relevant websites. The open source material will cover two distinct time periods: early terrorism database literature pre-9/11 and post 9/11 literature on terrorism and counter-terrorism databases. The early pre-9/11 literature will be used in Chapter 1 and part of Chapter 2 to provide the historical context and foundation from which one can analyse the seismic changes that have occurred in the field of terrorism and counter-terrorism database technologies, as a consequence of the events of September 11th 2001. This contextual foundation will provide a point of reference from which an analysis of database technologies and their application to terrorism and counter-terrorism post-9/11 can be undertaken.

Case Studies

In addition to primary and secondary source material, the thesis will use a selection of case studies to illustrate key arguments and to advance understanding. The case studies will focus on three terrorism databases in particular: The Worldwide Incidents Tracking System (WITS), The Global Terrorism Database (GTD) and the RAND Worldwide Terrorism Incident Database (RWTID). These three databases have been chosen for several reasons. First, they represent a mixture of both new and

established open source terrorism databases that all have legacy, and reflect the use of state of the art database technologies. In addition to these principle databases, the thesis will refer to many other terrorism and counter-terrorism databases where relevant, sometimes in some detail, to allow for a cross-comparison of terrorism events data to be undertaken. There is a plethora of terrorism and counter-terrorism databases within Government, academia and the private sector. The temptation to spread the analysis over dozens of databases would be at the cost of the quality of analysis. Thus the three principle databases chosen provide the opportunity for both in-depth analysis whilst at the same time reflecting the many generic issues involved in the development and operation of mainstream terrorism and counter-terrorism databases. Importantly, a key element of Chapter Four of the thesis will be the development of an Inventory of Terrorism Databases. The inventory will be used to provide a comprehensive set of data and narrative commentary on some of the world's principle open-source terrorism databases. The following section provides a brief historical context to the early development of data sets in international relations and their subsequent use in terrorism studies.

1.4. Data sets in historical context

The use of social science data sets as a measurement tool for understanding violent social phenomena dates back to the early 1930's. Pioneers in this field include the significant body of work carried out by researchers such as Lewis F. Richardson, Quincy Wright⁵ and Pitirim A. Sorokin.⁶ Their analysis of conflict by means of

⁵ Early efforts in this field were carried out by Lewis Fry Richardson, Quincy Wright and Pitirim Sorokin. Their use of quantitative and empirical techniques for events data analysis was ground-breaking at the time. See:

quantitative and empirical techniques for the numeric recording of events was a move away from traditional historical, normative and purely theoretical methods of international relations analysis. The main pioneers of events data⁷ research carried out their work in Universities in the United States and Europe. Among some of the earliest empirical data sets developed were Stanford's Crisis project (1914), the Correlates of War Project (COW) at the University of Michigan and the International Crisis Behaviour project conducted by the University of Maryland. Pioneering empirical work carried out by Lewis Fry Richardson⁸ on the mathematical measurement and analysis of international conflict and the arms race broke the mould of traditional theoretical analysis of international relations and set the scene for contemporary quantitative techniques. Thus, although in its infancy, this diversification from the descriptive, historical analysis of international relations to more quantitative techniques, provided an early basis for future empirical research.

Data sets on political conflict, wars, political violence, terrorism and other social phenomena have by their very nature involved the use of multiple variables⁹. At the most basic level this will involve the use of numbers and text.¹⁰ The use of such data sets in quantitative and empirical research on terrorism often requires the application of techniques from the simple aggregation of terrorism incidents to more

Dougherty, James E. and Robert L. Pfaltzgraff, Jr. *Contending Theories of International Relations*. (New York: Harper & Row, 1990.) p.36-41.

⁶ Sorikin, Pitrim A. *Social and Cultural Dynamics* (New York: American Book, 1937), vol. 3, *Fluctuation of Social Relationships, War and Revolution*.

⁷ Events data is defined by Dougherty and Pfaltzgraff as a "single action events of nonroutine, extraordinary, or newsworthy character that in some clear sense are directed across national boundaries and have in most instances a specific foreign target." Dougherty, James E. and Robert L. Pfaltzgraff, Jr. *Contending Theories of International Relations*. (New York: Harper & Row, 1990.) p.152

⁸ Ibid.

⁹ Some of the most common variables used in terrorism events data sets include: incident number, incident description, date, location, type of incident (e.g. bombing, IED, hi-jacking) fatalities, injured, and perpetrator.

¹⁰ Numerical variables can include numbers injured, numbers killed, estimated damage (financial). Text within terrorism data sets often provides a narrative on a particular incident, information about the perpetrator (terrorist group and group members) and any relevant contextual political background.

sophisticated methods of analysis such as Markovian and Poisson probability models.¹¹ Whilst the increasing use of computers to carry out such quantitative measurement has now become a standard tool amongst social science researchers, this has not always been the case. The rapid development of computers from basic calculating and scientific machines to highly sophisticated research tools has changed the face of social science research to almost unrecognisable proportions. However, without accurate and reliable techniques to carry out such statistical analysis of terrorism events, all data would be rendered invalid. Moreover, issues of accuracy and reliability are not confined solely to the statistical analysis of terrorism data sets held on computer. Of increasing importance is an understanding of how the terrorism data set sits within the overall database schema.¹² In other words, the validity of codification and mapping of terrorist variables into a computerised data set requires considerable thought and bears on-going responsibilities for terrorism researchers. Formal design procedures and documentation in the codification of terrorism data sets vary enormously.¹³ This is due partly to the sensitive subject of terrorism itself, the respective organisations developing the data set, (for example The National Counterterrorism Center, the RAND Corporation and The Federal Bureau of Intelligence (FBI))¹⁴ and the security implications that follow. While such documentation in the terrorism field remains limited,¹⁵ it is not without precedent¹⁶

¹¹ For further discussion on these models of analysis see Gurr, Ted Robert. "Empirical Research on Political Terrorism: The State of the Art and How it Might be Improved.", in Robert O. Slater and Michael Stohl (eds.), *Current Perspectives on International Terrorism* (London: Macmillan, 1988), pp.115-154.

¹² The *description* of the database is called the Database Schema; this is distinguished from the actual database.

¹³ These issues are further expanded upon in Chapter 3 of the thesis.

¹⁴ The National Counterterrorism Center (<http://www.nctc.gov>), RAND (<http://www.rand.org>) and F.B.I <http://www.fbi.gov/news/testimony/the-terrorist-screening-database-and-watchlisting-process> [accessed 29/03/11] all produce a series of data sets on terrorism related issues. For further details see Chapter 3.

¹⁵ The analogy of formal documentation in the area of conflict data sets is useful to a point. On the specific topic of terrorism data sets, the very sensitive nature of terrorism incidents or group activities deem that

as there is a recognised methodology in cognate areas of study, e.g. low-intensity conflict and irregular warfare.¹⁷

Many such data sets are now held on computer and are increasingly available on the internet accompanied by relevant codebooks and documentation. Among the more well known data sets are The Violent Intranational Conflict Data Project (VICDP)¹⁸, Dimensionality of Nations (DON),¹⁹ the Conflict and Peace Databank (COPDAB),²⁰ the World Events Interaction Survey (WEIS)²¹ and the PROTOCOL for Assessing Non-violent Direct Action (PANDA).²²

In terms of terrorism databases, limited forms of the ITERATE (*International Terrorism: Attributes of Terrorist Events*) data set produced by Edward Mickolus are available on the Internet²³, although full access is restricted to Yale University students. Indeed, complex factors lie behind the lack of publicly available computerised terrorism data sets. As Chapter 4 will explain the vast majority of publicly available terrorism data sets are now held on some form of computerised database system, where early annual reports for example such as the State

wide publication of information regarding an organisations data sets and its codification procedures may be open to threats of national security.

¹⁶ For a more detailed discussion of coding methodology within conflict studies see: Cioffi-Revilla, Claudio., *The Scientific Measurement of International Conflict: Handbook of Datasets on Crises and Wars, 1495-1988 A.D.* (Boulder, Colorado: Lynne Rienner Publishers, Inc. 1990.)

¹⁷ For an extensive range of information on conflict data sets see: *A Beginner's Guide to Conflict Data – Finding and Using the Right Dataset.* Eck, Kristine Uppsala Conflict Data Program, Department of Peace and Conflict Research, Uppsala University, Uppsala, Sweden (2005).
http://www.pcr.uu.se/digitalAssets/18/18128_UCDP_paper1.pdf [Accessed 02/04/11]

¹⁸ See: <http://mailer.fsu.edu/~whmoore/garnet-whmoore/vicdp/Codebook.pdf> [Accessed 02/04/11]

¹⁹ *Dimensionality of Nations Project: Dyadic Foreign Conflict Variables, 1950-1965.* See:
<http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/05408> [Accessed 02/04/11]

²⁰ *Conflict and Peace Data Bank (COPDAB), 1948-1978.* See:
<http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/07767> [Accessed 02/04/11]

²¹ *World Event/Interaction Survey (WEIS) Project, 1966-1978.* See:
<http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/05211> [Accessed 02/04/11]

²² For a brief discussion on the background to PANDA see: <http://www.vranet.com/FAQ.html> [Accessed 02/04/11].

²³ Part of the ITERATE data sets are available via the ICPSR's website. See: *International Terrorism: Attributes of Terrorist Events, 1968-1977 [ITERATE 2]*. <http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/07947> [Accessed 01/03/11]. For further in-depth discussion of the ITERATE data sets see Chapter 4 of this thesis.

Departments *Patterns of Global Terrorism*²⁴ or the RAND/ST-Andrews²⁵ data sets on terrorism incidents were only published in hard copy format.²⁶ The format and availability of terrorist data sets is dependent upon the type of organisation publishing the data. Issues of security, the type of data set, its public, commercial or academic status, all affect the type of data set that is made available. In the early years of computer availability, the medium on which the data was held, i.e. floppy disks such as the ITERATE data set, CD-ROM or internet access varied among organisations. This format is all but redundant, with the advent of the Internet, secure networks and sophisticated digital archiving technology. Unlike established data sets on conflict, for a variety of reasons that will be discussed later in the thesis, the development of academic data sets on terrorism has never had an overall co-ordinating body to set standards in the development of computerised data sets on terrorism. No professional standards apply in the field and the development of data sets appears to be on an ad-hoc basis, an issue that will be addressed later in the thesis.

For reasons such as these, the study of computerised terrorism data sets within the terrorism studies field has historically been weak.²⁷ This has not been helped by the wide use of headings such as Information Warfare, Computing and

²⁴ In recent years, with the advent of the Internet the U.S. State Department has made available .PDF versions of *Patterns of Global Terrorism*. These can be found at: <http://www.state.gov/s/ct/rls/crt/index.htm> [Accessed 19/02/11].

²⁵ The RAND/St. Andrews data sets were never publicly available via the Internet. For further details see: Hoffman, Bruce, and Donna Kim Hoffman. "The RAND-St. Andrews Chronology of International Terrorism, 1994." *Terrorism and Political Violence*. Vol.7. No.4, Winter 1995. pp.178-229. Also: Hoffman, Bruce, and Donna Hoffman. "Chronology of International Terrorism, 1995." *Terrorism and Political Violence*. Vol.8. No.3, Autumn 1996. pp.87-127.

²⁶ Access to data published by these organisation can be obtained by computer however that would be dependent upon some third party making available the information in a computerised format.

²⁷ With the exception of work carried out by William Fowler at the RAND Corporation [William Warner Fowler, *Terrorism Data Bases: A Comparison of Missions, Methods, and Systems* (RAND N-1503-RC Santa Monica 1981)] no comprehensive overview of the application of computerised databases systems to the study of terrorism has been published. See: <http://www.rand.org/content/dam/rand/pubs/notes/2005/N1503.pdf> [Accessed 09/01/11]

Terrorism, or Cyber-Warfare that are both misleading and inaccurate, whilst other topic headings under Databases and Terrorism, or the general term of Information Terrorism has left classification of the subject area confused and ill-defined.²⁸ This lack of definitional clarity on terrorism data sets has long been reflected in its omission from recognized typologies of terrorism studies, as can be seen even in Jungman's long-established Typology of Terrorism Research.²⁹ Without a clear framework, our understanding of the conceptual, theoretical and practical issues that effect the operation of computerised terrorism data sets is likely to be somewhat hindered. In addition, problems relating to the design of terrorism data sets, the awareness of their current uses and potential future applicability in research and counter-terrorism work require further investigation if the full capability of modern technology is to be realised. Before doing this, however, it will be useful to examine the definitional nature of data sets, chronologies and databases. This will allow a clarification of terms that will provide a sound foundation upon which the thesis argument can be built.

²⁸ Loose classification of terrorism data sets in some literature as chronologies, databases and data banks without thought given to their true classification has caused confusion in the literature. Chronologies on terrorism events data are an arrangement of terrorism events in order of occurrence by chronological date. Databases on terrorism can hold a much more sophisticated schema of data, contained within tables. The data can be relationally linked to allow researchers to perform queries, enter data, and generate reports and graphical data, in addition to further sophisticated functions. Not all database on terrorism are events databases, they could, for example, be based upon terrorist groups or intelligence driven databases containing information on individual terrorists and accompanying profiles, such as the NCTC's TIDE database. Data banks is a rather dated term in computing science from the 1970's.

²⁹ Jongman's typology of terrorism research offers a comprehensive typology and breakdown of areas of research in the terrorism field. No specific classification is given for computerised data sets on terrorism or computing in general. Reference would have to be made to subjects classified under 'Counter Measures', 'Intelligence', 'Preventative' and 'Futuristic Studies' Within these particular areas no common classificatory scheme exists for computerised data sets and terrorism. See: Schmid, Alex P. and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*. (New Brunswick, USA: Transaction Books, 2nd. Ed, 1988.) p.178.

1.5. Defining: data sets, chronologies and databases

Elmasri and Navathe emphasise the significance of an appropriate definition of the term 'database', arguing that they should have the following implicit properties:

'A database is a logically coherent collection of data with some inherent meaning. A random assortment of data cannot be referred to as a database. A database is designed, built, and populated with data for a specific purpose. It has an intended group of users and some preconceived applications in which these users are interested. A database represents some aspect of the real world, sometimes called the **mini-world**. Changes to the mini-world are reflected in the database.'

It is important to differentiate between a database and a database management system (DBMS).

'The DBMS is [hence] a general-purpose software system that facilitates the process of defining, constructing, and manipulating databases for various applications. Defining a database involves specifying the types of data to be stored in the database, along with a detailed description of each type of data. Constructing the database is the process of storing the data itself on some storage medium that is controlled by the DBMS. Manipulating a database includes such functions as querying the database to retrieve specific data, updating the database to reflect changes to the mini-world, and generating reports from the data.The database and software are together called a database system.'³⁰

This issue of clarity over the terminology used to describe a terrorism data set is important. Many terrorism data sets are held on a wide variety of computerised systems and this has led to inter-changeability of the term chronology and database. For example, the ITERATE³¹ chronologies on terrorism, the Pinkerton Risk Assessment Services (PRAS) database (now incorporated into the Global Terrorism Database), the RAND-St. Andrews Chronologies on International Terrorism, and the State Department's Threat Analysis Division Information Management System (TADIMS) database are among numerous titles given to terrorism data sets. The

³⁰ Elmasri, Ramez, and Shamkant B. Navathe. *Fundamentals of Database Systems*. (Redwood City, California: The Benjamin/Cummings Publishing Company, Inc. 1989.) pp.3-4.

³¹ Edward F. Mickolus, Todd Sandler, and Jean Murdock, *International Terrorism in the 1980's A Chronology of Events* Vol. II. 1984-1987 (Ames, Iowa, Iowa State University Press, 1989).

problem of classification arises in relation to the functionality³² of the chronology or database systems. Simple text based chronologies on terrorism have differing design features from that of a fully-fledged database management system (DBMS). Consequently design issues can vary between data sets. The capabilities, for example, of a text based data set such as ITERATE tend to be much more limiting than that of a true database system such as TADIMS.³³ The beauty of the database management system is its ability to retain text and coded variables (fields) and present terrorism data sets, chronologies and databases as part of its basic functionality.³⁴ Regardless of the type of data set in use, the design, collection, and entry of terrorism data into a computerised format requires thoughtful consideration. With this in mind, this thesis now turns to an examination of the early years of terrorism database creation.

1.6. Development of Computerised Terrorism Data Sets: The Early Years

The structure of some of the earliest data sets on political violence bears a strikingly similar format to that of contemporary data sets on terrorism. Developed largely in the 1960's, terrorism events variables were coded used as the main unit of analysis. The most popular technique for analysis was aggregate events data, such as Gurr's *Strife Events Data Sets, Causal Model on Civil Strife, 1961-1965* and Arthur S. Bank's

³² Functionality relates to the actual functional operations of the data set. For example this could include such operations as report generation, querying of the database, input forms, validity checks and mathematical and statistical operators.

³³ A terrorism data set or chronology can be held on a text based computer system and as such this does not constitute a true database management system (DBMS). Generally containing large amounts of un-coded text, they may or may not contain some variables.

³⁴ 'A database management system (DBMS) is a collection of programs that enables users to create and maintain a database. The DBMS is hence a *general-purpose* software system that facilitates the process of defining, constructing, and manipulating databases for various applications' in Ramez Elmasri and Shamkant B. Navathe, *Fundamentals of Database Systems* (Redwood City, CA: The Benjamin/Cummings Publishing Co. Inc. 1989) p.4.

Domestic Conflict Behaviour, 1919-1966.³⁵ Although many of these studies are available on computer via the Inter-University Consortium for Political and Social Research (ICPSR), their original format was either manually held or supported on text-based software.³⁶ The general use of computers and particularly database systems by non-science based researchers was rare. Both computer science and terrorism as established fields were in their relative infancies in the 1960's and thus the perceived benefits from computerisation of terrorism data had not as yet been realised.

1961 saw the first generation of generalised database management system. It was nearly another decade (1970), until the concept of the relational database model, developed by Ted Codd, an IBM research fellow, was conceived. Many of the early database systems were designed for larger commercial users such as American Airlines or for U.S Department of Defense programs.³⁷ Despite the apparent void between availability of systems and application in terrorism research, interest in their use as an intelligence-based tool began to emerge in the late 1960's and early 1970's.

The development by the CIA of their FITE (File on International Terrorist Events) database, operating under the Ramis III system, the Defense Intelligence Agency's STIF (Significant Terrorist Incident Files) database, operating on the DIAL database system and BDM's coded chronology of terrorism, were among the earliest

³⁵ Ibid. pp.139-140. For a comprehensive list of conflict and political violence data sets see: Schmid and Jongman pp.139-175.

³⁶ Access to specific ICPSR data sets can be accessed at the ICPSR's web site at: <http://www.icpsr.umich.edu>

³⁷ For a brief outline of the early stages of database system progress and their consequent development see: Ramez Elmasri and Shamkant B. Navathe, *Fundamentals of Database Systems* (Redwood City, CA: The Benjamin/Cummings Publishing Co. Inc. 1989) pp.18-19.

known computer applications in the field of counter- terrorism.³⁸ All of these data sets were initially designed in the form of coded chronologies on international terrorism, using a mixture of public domain sources and intelligence sources, except for BDM's database, which did not have access to classified information. The CIA chronology had an extensive array of up to 150 variables detailing incidents from 1968 onwards, held in the main chronology, and a series of ancillary files relating to different terrorism information. Both the CIA and DIA chronologies were used primarily for intelligence estimates and forecasting. BDM's terrorism chronology, on the other hand, was used for basic research.

Although the earliest terrorism data sets took the form of chronologies on terrorism incidents, moves towards using computerised databases in a more sophisticated format had developed by the early 1970's. The FBI's Bureau of Alcohol, Tobacco and Firearms (ATF), began operating in 1975, their Explosives Incidents System (EXIS). The database was operated on a mainframe system from the ATF's offices in Washington D.C. The EXIS database's main remit was to hold information on explosives incidents occurring in the United States that were either being investigated by the ATF or had been reported to the ATF.³⁹ Although organisation of the database was maintained in Washington D.C., data input on bombing incidents came from bomb squads at federal, state and local level.⁴⁰

While much of the emphasis on terrorism database development appeared to be based in the United States, efforts in Europe to use computers in counter - terrorism work were being developed in West Germany by the late 1970's. The

³⁸ For other basic details on these data sets see: Fowler (note 3). pp.31-40. The BDM Corporation and their data sets no longer appear to exist. Extensive enquiries within the United States drew little success as to their eventual fate.

³⁹ Revell, Oliver B. 'Counter Terrorism, Planning and Operations.' *The Police Chief*, October 1991.

⁴⁰ Ibid. For a more detailed analysis of the EXIS database see p. 37 of this chapter.

German Police Information System (INPOL) was developed in the mid 1970's and was operational by 1977.⁴¹ The INPOL system was used by police throughout the former West Germany (FDR), both in counter-terrorism work, and in criminal and drug related crimes. The INPOL system was, for its time, a fairly advanced system offering multiple facilities. A centralised database, with regional network access, INPOL maintained a database of wanted terrorists and criminals, including fingerprint files. In addition, INPOL held files on known terrorist groups and individuals, generated from the result of terrorist activity. What made the INPOL system sophisticated for its time was the capability of the system to provide documents on legal advice, technical data and dispatch systems for command and control. With variable coded terrorist details, relevant ancillary database files, narrative documentation and accessibility over national and local police networks throughout West Germany, the INPOL systems provided a model for future development.

Whilst the development of terrorism data sets, like INPOL, in the police and intelligence fields served specific intelligence needs, such classified information remained unavailable to the small, but emerging community of researchers hungry for data. This community comprised of academics, policy analysts and commercial organisations requiring terrorist data to pursue their requisite needs. Unable to obtain classified data, researchers and analysts developed their own computerised data sets. Thomas Snitch, at The American University, developed a coded database using the statistical software SPSS, basing the unit of analysis on assassination

⁴¹ Karl, H. and R Lodde 'German Police Information System - INPOL Organization and Technique.' Paper presented at the International Conference on The Use of Computers in Police Operations. London, November 1977.

attempts world-wide between 1968 and 1978.⁴² In 1972, the RAND Corporation, an independent think-tank based in Santa Monica, California, began research work on the study of international terrorism, eventually developing an extensive collection of computerised chronologies and databases on terrorism (see Chapter 4). Work at RAND, for example, by Waterman and Jenkins, applying computerised heuristic modelling techniques to the study of international terrorism, was well advanced for its time.⁴³ Driven by growing commercial and multinational interest in business risk, the value of terrorism data grew in the early 1970's with companies such as Risks International, Inc. of Virginia, establishing their database of terrorism and political violence, which dates back to 1970.⁴⁴ As a result, terrorism data became 'valuable' in three main respects: first, as a tool in the intelligence and police communities, to help counter acts of terrorism; second, in academic disciplines, to move the boundaries of research from traditional historical, descriptive and theoretical studies to quantitative and empirical based research and, third: terrorism data had commercial value in that it could be sold as part of a consultancy service, to willing corporate directors requiring risk analysis for overseas business.

The late 1960's and 1970's were therefore a time for experimentation and prototype in the field of computerised terrorism data sets. There appears to have been little co-ordination between organisations, and most appeared pre-occupied

⁴² Fowler (note 3) p.39.

⁴³ Waterman, D.A. and Brian M. Jenkins. *Heuristic Modelling Using Rule-Based Computer Systems* (Santa Monica CA: RAND Corp., P-5811, 1977). See: <http://www.rand.org/content/dam/rand/pubs/papers/2006/P5811.pdf> [Accessed 13/06/10].

⁴⁴ Risks International Inc. of Virginia became known as Pinkerton Risk Assessment Services (PRAS). It published its *Annual Risk Assessment* [1970-1997] on world-wide political violence in both hard-copy format and via the Internet until the late 1990's. The entire database was given over to the START project at the University of Maryland, to form the core data for the Global Terrorism Database (GTD) See: <http://www.start.umd.edu/gtd/> Some of the Internet version of Pinkerton's data can be found at: <http://www.pinkertons.com/pinkerton/prasdocs/news/aintro.htm> using the www.archive.org website.

with developing and maintaining their respective data sets. Comparative analysis of data sets was also difficult to assess, and with such a small amount of data to compare, quantitative comparisons of data sets were not meaningful or easy to measure. This point did not go unnoticed by several researchers at the time. As

Fowler noted:

‘the size of chronology-based data sets did not permit adequately reliable quantitative analysis, particularly in the case of interesting categories of terrorist incidents.’⁴⁵

The quantitative analysis of barricade-and-hostage incidents was a particular example of data shortcomings. As Jenkins, Johnson and Ronfeldt note:

‘It is hazardous to draw statistical inferences from so small a universe. The conclusions that may be suggested, or the predictions that seem inherent, are quite tentative. In our analysis of the [77 barricade-and-hostage] cases we have given the actual numbers and the percentages these represent ... to give greater meaning to the imprecise words that are commonly used in place of numbers [Yet] the data do not permit a high level of confidence based upon rigorous quantitative analysis of a sufficiently large population of events.’⁴⁶

The tragic and ironic solution to such a paucity of data was that through time, as incidents of terrorism were likely to occur, data could be coded to permit credible quantitative and empirical analysis of terrorism events.

1.7. Information Technology and Terrorism Studies

Technology and terrorism as a recognisable field in the terrorism literature has been growing over the past few years. It is a crucial as a tool in the assessment and analysis required to counter acts of terrorism. Where the area of computerised data sets on terrorism fits into this field is not clear. Early discussion of the technology

⁴⁵ Fowler (note 3) p.6.

⁴⁶ Fowler (note 3) p.6. Discussed in: Jenkins, Brian, M, Janera Johnson, and David Ronfeldt, “Numbered Lives: Some Statistical Observations from 77 International Hostage Episodes.” *Conflict: An International Journal*. Vol. 1, No. 1, 1978. pp.71-111.

area of terrorism research tended to include such areas as explosive detection systems, aviation security, terrorist weaponry and nuclear issues relating to terrorism. Grant Wardlaw, discussing terrorism and technological change, expresses concern over such issues as armaments, biological agents and major advances conventional weaponry, that if obtained by terrorists could cause immense harm.⁴⁷ These are valid and legitimate areas of concern under the technology heading.⁴⁸ What appears to be lacking is a clear Information Technology field and in particular a focus on computerised data sets on terrorism. Schmid and Jongman do mention the term 'data base' in their book *Political Terrorism*; contextually within the book the database area is not specifically classified under an information technology heading⁴⁹. As Chapter Two will illustrate, there have been real concerns regarding where best to situate the research on terrorism informatics and, indeed, it is only post-9/11 that a much broader literature base has evolved. Very little reference can be found within the technology and terrorism literature to information technology and terrorism as a classified subject area.⁵⁰ Even scarcer is published literature on the application of database technologies to terrorism data sets and more specifically as a tool in terrorism research. As Chapter 4 will demonstrate, it is important to differentiate between the study of computerised data sets on terrorism and the use of computers in the intelligence field. Although both topics have certain common

⁴⁷ Wardlaw, Grant. *Political Terrorism*, (Cambridge: Cambridge University Press, 1984.) pp.25-27.

⁴⁸ For further early discussion of terrorism and technology see: Hoffman, Bruce 'Responding to Terrorism Across the Technological Spectrum' *Terrorism and Political Violence*, Vol6, No. 3 (Autmn 1994), pp.366-390.

⁴⁹ 'Data and Data Bases on State and Non-State Terrorism' (In collaboration with R. Thyse) Schmid, Alex P. and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*. (New Brunswick, USA: Transaction Books, 2nd. Ed, 1988.) Chp. 3. pp.137-174.

⁵⁰ For a broader early discussion of the application of technology to counter-terrorism efforts see: U.S. Congress, Office of Technology Assessment, *Technology Against Terrorism: The Federal Effort*, OTA-ISC-481 (Washington, DC: U.S. Government Printing Office, July 1991).

denominators a fusion of the two topics would not be helpful,⁵¹ in particular because not all databases systems are intelligence systems.

There are several reasons how this paucity of published research work in computerised terrorism data sets could be explained. First, as an established academic field the study of political violence and terrorism has only been developed to any extent in the past forty years. Classification of the subject as entry only appeared in *The New York Times* in 1968. Prior to that the subject was classified under the general heading of violence or low intensity conflict. Second, in the same forty year period, while the development and use of the computers as a viable research tool in the social sciences has advanced considerably, the application of the database technology as a research tool in terrorism studies has at times had a rather chequered history until recently. While mainframe computers have been available for scientific use since the post-war period, their use as a tool specifically in the terrorism field did not occur until the 1970's. Work by Brian Jenkins at the RAND Corporation on Heuristics modelling of terrorism incidents in 1977 was one of the earliest examples of the application of computing to terrorism research.⁵² Consequent development of the RAND chronologies and databases on International Terrorism were to follow in 1980. Development of police surveillance systems by the German Federal Intelligence Service (Bundesnachrichtendienst) - BND, in 1977 after the Scheyler kidnap⁵³ was one of the earliest attempt to use mainframe computers

⁵¹ Put simply, terrorism databases in general deal with events data. They can be held by either academic, private or Government agencies. They are not all intelligence based systems for use in counter-terrorism efforts.

⁵² Waterman, D.A. and Brian M. Jenkins. *Heuristic Modelling Using Rule-Based Computer Systems* (Santa Monica CA: RAND Corp., P-5811, 1977). See: <http://www.rand.org/content/dam/rand/pubs/papers/2006/P5811.pdf> [Accessed 13/06/10]

⁵³ Clutterbuck, Richard. *Terrorism and Guerrilla Warfare*. (London: Routledge, 1990.) Chp.7 pp.61-74.

to gather and establish links between data.⁵⁴ British efforts at similar data gathering techniques was co-ordinated by the Home Office under a project called Holmes.⁵⁵

As Ted Gurr notes, for many academics, increasing interest in the study of political violence as a legitimate topic of research was initially based upon historical, atheoretical and case study approaches to the subject.⁵⁶ Research carried out by Fowler at the RAND Corporation on numerical indexes on terrorism variables in the early 1980's was an early attempt to develop the power of the database using mainframe technology.⁵⁷ Information technology as a recognisable field had not developed in the general science literature let alone the specialised area of terrorism studies. The capability of these systems was generally limited to the retention of variable and text coded data allowing for the creation of chronologies and data sets on terrorism. Few academics had the expertise or financial resources and could not foresee the potential in developing computerised terrorism database systems. Computers were seen among academics as being very much part of the mathematical and computing disciplines, and given that the functional capability of the available systems were anyway somewhat limited, their potential application could not be fully appreciated.

As Fowler notes:

‘The development of large scale data sets on terrorism were left to the larger Think Tank organisations such as the Rand Corporation, The Defence Intelligence Agency (D.I.A.) established 1970 and private corporations such

⁵⁴ Ibid.

⁵⁵ Ibid.

⁵⁶ Gurr, Ted Robert. "Empirical Research on Political Terrorism: The State of the Art and How it Might be Improved.", in Robert O. Slater and Michael Stohl (eds.), *Current Perspectives on International Terrorism* (London: Macmillan, 1988), pp.115-154.

⁵⁷ Fowler, William Warner. An agenda for Quantitative Research on Terrorism. (Santa Monica: Rand P-6591, 1980.) See: <http://www.rand.org/content/dam/rand/pubs/papers/2009/P6591.pdf> [Accessed 07/01/11].

as the BDM Corporation's chronology established in 1965 concentrating on terrorist incidents concerning '...private business and governmental concerns...'.⁵⁸

Others included had a relevant interest in maintaining data on terrorism and governments agencies and intelligence agencies. This also included military agencies both in Europe and North America, their remit being mainly tied to military, scientific and commercial use. Many arts and social science researchers were not particularly comfortable with the use of computers as a research tool. Indeed they did not even envisage it as a tool with which they could use in their work for several years. The invention of the personal computers and more sophisticated mainframe computers were the move forward that would allow terrorism researchers and analyst to use the computer as a tool in terrorism research. However as Chapter Two indicates the wide spread use of personal computers among the academic community has not seen a parallel increase in published literature on computerised terrorism data sets. Certain terrorism analysts developed their own data sets on terrorism including former U.S. State Department employee Dennis Pluchinsky, who developed a database in a private capacity for academic work.⁵⁹ However, for several reasons, terrorism researchers were slow to adopt the database technologies. Principal amongst these was the huge investment of both time and resources required to develop and maintain terrorism data sets to a high academic standard and integrity. Information technology and terrorism research as an established field was in many ways still in its infancy. The arrival of the Internet and the increasing use of computer networks, as well as increased attention being paid to such topics as

⁵⁸ Ibid. (note 3).

⁵⁹ Information obtained from meeting with Dennis Pluchinsky at the U.S. Department of State July 1994.

Cyber-Terrorism, Information Warfare and Information Terrorism⁶⁰ has tended to overshadow the specialist area of computerised terrorism data sets. Instant gratification and retrieval of information (of varying quality) has tended to be at the expense of a serious analysis of the use of computers in terrorism database research. Furthermore the increasing interest being paid to such topics as computer security, intelligence systems, computer viruses and the sabotage of computers by terrorists under the technology banner has again sidelined the issue of terrorism databases. Increasing computer literacy among social scientists and terrorism researchers has tended to take the focus of attention away from the core issues of terrorism databases. The visual attraction of the internet, coupled with an increasing awareness of the volatility of data and information has also tended to obscure the importance of studying the topic of terrorism database technologies as a subject *per se*.

1.8. Quantitative Theory Development

The use of quantitative techniques in terrorism research has grown substantially in the past thirty years. Studies by many academics and analysts have increasingly relied upon the use of terrorism data sets to further theoretical debate in the field. Most terrorism chronologies and databases are coded with a mixture of text variables (for example, incident details, name of terrorist group, and type of incident

⁶⁰ For further discussion on this area see: Matthew G. Devost, Brian K. Houghton and Neal Allen Pollard 'Information terrorism: Political violence in the information age'. *Terrorism and Political Violence*. Vol. 9, Issue 1, 1997, Pages 72 – 83.

– bombing, hijack, chemical attack) in addition to some numeric indices (number of fatalities, number of injured, estimated cost of damage).⁶¹ As James Coleman asks,

‘What is it about quantitative measurement that is so crucial for theory-development? ... [Its power] ... lies in its ability to carry out transformations ... upon input data.’⁶²

Furthermore,

‘If these data are in the form of numbers, and maintain their properties as numbers after transformation, then powerful transformations of algebra, calculus and matrix algebra can be carried out upon them.’⁶³

The computer as a tool in the manipulation of such raw terrorist data sets has, as Fowler argues, an increasingly vital role in quantitative theory development.⁶⁴

Awareness at the Rand Corporation, and among other terrorism researchers, that computers could not only store raw data on terrorist incidents but be used for quantitative empirical research was becoming apparent by the early 1980’s. Fowler’s paper: ‘*An Agenda for Quantitative Research on Terrorism*’⁶⁵ recognised the potential for developing sets of ‘profiles’ *defining* the behaviour of terrorist groups.

These profiles would be numerically indexed in a computerised database. Variables or ‘profiles’ included ‘frequency, severity, quality and effect of terrorist acts’.

Building upon these the creation of aggregate profiles that would reflect national, regional and international behaviour began to be added to database research.

Establishing such a database would allow the use of time-series, process analysis and multivariate calculations. The great beauty of such an exercise is that a computerised

database would allow researchers to model or manipulate the data to form an

⁶¹ The most common numeric variables are: number of injured, number of hostages, number of fatalities, incident totals, database incident number, incident date, financial cost etc.

⁶² Cioffi-Revilla, *op cit*.

⁶³ *Ibid*.

⁶⁴ Fowler, William Warner. *An agenda for Quantitative Research on Terrorism*. (Santa Monica: Rand P-6591, 1980.) See: <http://www.rand.org/content/dam/rand/pubs/papers/2009/P6591.pdf> [Accessed 07/01/11].

⁶⁵ *Ibid*.

empirical foundation for further quantitative research. Fowler suggested its further use as a projection tool, as well as the evaluation of current trends in terrorist incidents. The strength of such databases is their ability to choose varying units of analysis, for example the terrorist incident, and on that basis offer aggregate information based on multi-dimensional criteria. The great power that numbers have over words is their capability for calculation. Increasing requirements for quantitative data on terrorist incidents, groups and other events make the computerised data sets particularly amenable to quantitative research. The value of coded words or text should not be undervalued. At varying levels, textual variables in terrorism data sets offer powerful explanatory information to terrorist incidents or events. For example the terms 'ideology', 'freedom', and 'violence', and 'revenge' do not lend themselves to simple numerical coding. The written word within the data set offers principally a descriptive mechanism for such entities. In addition, it can also offer a more rounded picture of events.

The ability to generate large computerised data sets on terrorism events for quantitative and empirical research does not guarantee that the most useful data sets are being compiled. The ramifications of this for quantitative and empirical research are serious. For example, as Ted Gurr notes in his paper *'Empirical Research on Political Terrorism: The State of the Art and How it Might be Improved'*,⁶⁶ the lack of empirically based research on oppositional terrorism at the expense of chronologies on terrorism incidents as the unit of analysis is problematic. Moreover, at a very obvious level the application of computer technology to any discipline (e.g.

⁶⁶ Gurr, Ted Robert. "Empirical Research on Political Terrorism: The State of the Art and How it Might be Improved.", in Robert O. Slater and Michael Stohl (eds.), *Current Perspectives on International Terrorism* (London: Macmillan, 1988), pp.115-154.

Medicine, Science, Music) is almost automatically seen an advancement in the relevant field. What Jones describes as 'technological utopianism' has provided a strong momentum, as has the perception that new technology by its very nature is an advancement in itself, a feeling that can itself provide a false sense of security.⁶⁷ As will be discussed in chapter 3, terrorism database projects are not always successful, and a false sense of technological advancement and a pseudo-legitimacy of data and information can arise. The very fact that terrorist data is coded into a database does not make it either legitimate or valid. The ease with which data can now be entered upon computerised system requires that some caution be taken when dealing with computerised data sets on terrorism. The availability of software that allows for the fast design and collation of data risks overshadowing some of the fundamental conceptual, theoretical and practical considerations that need to be addressed in the application of database technologies to terrorism research.

1.9. Conclusions

From a scattered and patchy history, the application of database technologies to the study of terrorism and counter-terrorism post 9/11 is a field of research that has been thrust by events into taking action. Chapter 2 of this thesis will assess the key literature that contributed to the early development of the field of study. This not only provides an historical overview of the foundations of research in the subject area. It will discuss the early literature that was foundational in developing terrorism database collections. After all, it was the creation and on-going development of early chronologies and databases on terrorism in the 1960's and 1970's that provided a

⁶⁷ Kling, Rob. *Computerization and Controversy*. (London: Academic Press, Inc, 1996.) pp.85-105.

substantial quantitative continuum for analyst to measure and assess long-term trends in terrorism. Chapter 3 of the thesis will assess the major design and on-going development issues in terrorism database design. Without solid design methodology, data validity and integrity is rendered worthless. In addition to the key issue of defining an act of terrorism and its mapping into terrorism databases, the chapter will also assess source data issues and the sophisticated functionality of terrorism databases systems. It will also discuss some of the key issues surrounding the failure of some terrorism and counter-terrorism database projects. Chapter 4 will provide a detailed overview and discussion of the principle publicly available databases on terrorism. The thesis will present what to date is the most comprehensive outline of twenty key terrorism databases compiled. Chapter 4 will also present an assessment and context for some Government counter-terrorism databases, and illustrate their varying remits. Chapter 5 will discuss current and future trends in the research in a field that has rapidly become a complex matrix of competing demands and challenges. The chapter will address the legal and policy implications for terrorism and counter-terrorism databases post 9/11. Other issues such as data privacy, data mining, mission creep, networked technologies and information sharing will also be discussed. Finally, Chapter 6 will provide a summary and conclusions, with a discussion of the findings and implications for further study.

CHAPTER II

THE PRE-9/11 CONTEXT

2.1 Introduction

With the exception of a few dedicated articles, published literature on the application of database technologies to the study of terrorism and counter-terrorism databases pre 9/11 is minimal.⁶⁸ Indeed, even now, although there are now a number of research papers in this area, there remains no monograph that assesses comprehensively the use of database technologies in terrorism research. The eclectic nature of the field and the lack of an established classification of database technologies in terrorism studies has left the study of the subject area scattered and incomplete. Given the inter-disciplinary nature of the subject and the lack of a cohesive focal point, this chapter will first assess the available literature, pre-9/11, before examining post-9/11 material. This chapter is particularly concerned with the research undertaken, and impact of database technologies, in the field of terrorism and counter-terrorism. As argued in the hypothesis of this thesis, the non-incremental way in which the study of terrorism and computers databases have evolved has meant there has been no 'home' for the subject. Early studies of terrorism academically was carried out in political science and history departments in Universities. Computing science, founded in the discipline of mathematics, eventually evolved into a subject in its own right. For decades each respective

⁶⁸ William Warner Fowler, *Terrorism Data Bases: A Comparison of Missions, Methods, and Systems*. (Santa Monica CA: RAND Corp., N-1503-RC. 1981); A.P. Schmid and A.J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*. 2nd. Ed. (New Brunswick USA Transaction Books 1988); Jeffrey Ian Ross, 'An Events Data Base on Political Terrorism in Canada: Some Conceptual and Methodological Problems' *Conflict Quarterly* 8/2 (Spring 1988).

subjects lived in parallel worlds. Even with 'early cross-fertilisation' of the subject by the RAND Corporation, the study of terrorism databases remained fragmented. The concept of Terrorism Informatics provides a natural niche and relevant and meaningful title to an evolving inter-disciplinary subject area that reflects the real-world. Terrorism informatics applies sophisticated methodologies with information fusion in the management of diverse terrorism related information. It is specifically connected to the use of terrorism data in relation to domestic and international homeland security. This includes, for example the acquisition and integration of terrorism data, which can then be processed and made available for analysis. As argued in the hypothesis of this thesis, applying the encompassing term terrorism informatics provides boundaries. Terrorism informatics boundaries are wide but highly relevant to study of terrorism and counter-terrorism databases. Another benefit of using terrorism informatics as a subject title is that it also includes in its use inter-disciplinary techniques from statistics, mathematics, public policy, linguistics and the social sciences. In many ways it reflects and can respond to the complicated narrative that is terrorism in the 21st Century.

Despite the many classificatory fields of terrorism literature, there has been no natural niche, within existing frameworks, for the study of database technologies and their application to terrorism studies. Published literature relating to database technologies and terrorism studies is spread across many areas within the terrorism field. The diverse sources, for example, quantitative studies, events data, intelligence, counter-terrorism, commercial consultancy, all with varying remits, make it difficult to generalise about the field. Moreover, two principal factors have caused confusion over the classification of the use of computers in terrorism

research.⁶⁹ First, computers are perceived purely as a research tool in the research process. They are viewed as 'background' tools to many areas of terrorism research, and as a result of their diverse use and application, agreement even on a simple title for their use (e.g. Terrorism Informatics') has not been forthcoming. Secondly, the development of the computer as a legitimate area of study within the terrorism field, and not simply a research tool, has further added to an already unsatisfactory lack of classification.⁷⁰ Despite this situation, a small, but important literature base related to terrorism data sets was evolving even from the late 1960s, i.e. the beginning of database use within the terrorism field. This chapter will examine this early research, setting the scene for the post-9/11 analysis in later chapters.

2.2. Early research - monographs

Despite its relative youth as an area of academic study, the literature on political violence and terrorism is substantial. The many classifications (historical, normative, legal, behavioural, social, economic, quantitative, empirical, theoretical, case studies, anthologies, events data, and bibliographic) are indicative of the problems encountered in generalising about such a complex political phenomena. A useful starting point in terrorism studies is Wardlaw's *Political Terrorism*.⁷¹ This provides a comprehensive overview of political violence and counter-terrorist tactics. Balanced with a mixture of history, theory on political violence, and suggested practice in counter-terrorism tactics this work provides one of the first comprehensive introductory approaches to the research field. A large amount of terrorism literature

⁶⁹ This is in addition to the difficulties raised in ethical terms regarding their use, a point to which this thesis will return in chapter 5.

⁷⁰ For a discussion on Information Terrorism see M. Devost, B. Houghton, N. Pollard, 'Information Terrorism: The Debate' *Terrorism and Political Violence*, 9/1 (Spring 1997).

⁷¹ Grant Wardlaw, *Political Terrorism* (Cambridge: Cambridge University Press 1988).

has tended to be based on the historical development of terrorist movements, profiles of their members and leadership. Historical anthologies by Laqueur⁷² and Fromkin⁷³ have provided useful primary source material regarding terrorist activities. Alternatively works by Becker,⁷⁴ illustrating the development of the Baader-Meinhoff group in Germany and Bell's⁷⁵ historical analysis of the IRA and its membership, form part of a large and established field of historically based literature on terrorism, adding further weight to the argument for historical analysis is Laqueur's Terrorism.⁷⁶ Laqueur emphasised the effect of previous historical events to the behaviour of 19th century Russian terrorist group motivations and beliefs. Alternatively, typologies of terrorism by authors such as Walter,⁷⁷ offer one of the earliest sociological perspectives on terrorism – Walter, for example, distinguishes between 'sieges of terror' and 'regimes of terror'. In the conceptual and theoretical literature, an analysis of revolutionary terrorism is offered by Wilkinson⁷⁸ who uses Gurr's frustration-aggression hypothesis to develop a theory of terrorism.⁷⁹ Further work by Wilkinson, such as the seminal *Terrorism and the Liberal State*⁸⁰ concerns itself with the threat of terrorism to liberal democracies. Causal factors and the particular methods of countering acts of terrorism within liberal democracies are also discussed. Of particular relevance to the terrorism, computing and intelligence field is the significance that Wilkinson places on the nature of the intelligence

⁷² Walter Laqueur, *The Terrorism Reader: A Historical Anthology* (New York: New American Library 1978).

⁷³ David Fromkin, 'Terrorism: Origin and Strategy' in *The Struggle Against Terrorism*, ed. William P. Lineberry (New York: H.W. Wilson 1976).

⁷⁴ Jillian Becker, *Hitler's Children: The Story of the Baader-Meinhof Terrorist Gang*, (Philadelphia: Lippencott 1977).

⁷⁵ J. Bowyer Bell, *The Secret Army: A History of the IRA* (London: Blond 1974).

⁷⁶ Walter Laqueur, *Terrorism* (London: Sphere Books 1978). The adopted program of the Narodnaya Volga in 1879 at Lipetsk included the statement: 'We will fight with the means employed by William Tell' (p. 22).

⁷⁷ Eugene Walter, *Terror and Resistance*, (New York: Oxford University Press 1969)

⁷⁸ Paul Wilkinson, *Political Terrorism*, (London: Macmillan 1974).

⁷⁹ Ted Gurr, *Why Men Rebel* (New Jersey: Princeton University 1970).

⁸⁰ Paul Wilkinson, *Terrorism and the Liberal State* (London: Macmillan second edition, 1986)

services and upon having central co-ordination of information to avoid duplication and maintain standards under democratically accountable authorities. Causal factors behind political violence are examined in Ted Gurr's *Why Men Rebel*. This classic etiology, an early example of work on 'root causes', 'uses deductive reasoning and empirical enquiry to synthesise theories about the origin and form of group violence in politics'.⁸¹ From a completely different angle, work in the counter-terrorism and preventative studies field by such authors as Clutterbuck⁸² and Jenkins⁸³ have sought to emphasise the more practical considerations in counter-terrorism research from applied military and security backgrounds.

In terms of the early literature on database technologies,⁸⁴ William Fowler, of the RAND Corporation carried out some of the earliest research work in this specific area in the early 1980's: two papers by Fowler; *An Agenda for Quantitative Research on Terrorism*⁸⁵ and *Terrorism Data Bases: A Comparison of Missions, Methods and Systems*⁸⁶ posits some of the most essential arguments and analysis for the use of computerised database system in terrorism research. In particular, *An Agenda for Quantitative Research on Terrorism* illustrates at a most basic, but fundamental level, the advantages of using computerised databases for aggregate data analysis of terrorism incidents and group behaviour. This early recognition (1980) of the potential of database systems in quantitative terrorism research

⁸¹ Edna Reid, 'Evolution of a Body of Knowledge: An Analysis of Terrorism Research', *Information Processing & Management*, vol. 33, no. 1 (1997)

⁸² Richard Clutterbuck, *Terrorism, Drugs and Crime in Europe after 1992* (London: Routledge 1990)

⁸³ Brian M. Jenkins, *High Technology Terrorism and Surrogate War: the Impact of New Technology on Low Level Violence*, (Santa Monica CA: RAND Corp., 1975) P-5339.

⁸⁴ For a very early and basic analysis of the application of computers to terrorism studies see Aron Rozen and John M. Musacchio 'The Use of a Computerised Database of Terrorist Activities for Threat Assessment', *Proceedings, 1988 Carnahan Conference on Security Technology: Electronic Crime Countermeasures*, University of Kentucky, Lexington, Kentucky, May 10-12, 1988.

⁸⁵ William W. Fowler, *An Agenda for Quantitative Research on Terrorism* (Santa Monica CA: RAND Corp., 1980)

⁸⁶ William W. Fowler, *Terrorism Data Bases: A Comparison of Missions, Methods, and Systems*, (Santa Monica, Calif: RAND Corp., 1981).

(despite the lack of modern computerised systems) demonstrated the usefulness of indexing terrorist variables numerically as a foundation in quantitative research, something that could then be pursued further at an empirical level. Using the terrorist incident as the unit of analysis – i.e. “who did what to whom and when”, Fowler argued that various methods of aggregate modelling could be employed, for example, the use of multivariate modelling, including regression techniques. Time series models could also be employed to detect seasonal variations in terrorist activities, in addition to developing monitoring and forecasting tools. Fowler encouraged the use of numeric databases to study terrorism at varying levels of analysis. For example, at a macro-analytic level databases could be used to monitor terrorist behaviour at international and national levels. Alternatively, micro-analytic analysis using behavioural variables related to geography, political and group attributes could be coded within a database. Fowler’s, *Terrorism Data Bases: A Comparison of Missions, Methods, and Systems* was one of the earliest attempts to outline the conceptual, practical and theoretical problems incurred when designing and using computerised data sets on terrorism. Although Fowler’s paper was published in 1981, his research continues to have resonance. Fowler’s paper is almost unique in that it addresses the specific practical problems encountered by terrorism researchers when attempting to design a computerised database on terrorism, and his appreciation of the need to employ more formal methods for storing information on terrorist incidents highlighted the lack hitherto of the importance of formalising databases. It makes many excellent points that are still valid today, despite the revolutionary advances in computer technology in the intervening period. Fowler recognised the potential applications of computerised

terrorism data sets, in terms of basic research, intelligence and query responses on terrorism data. These relate specifically to the types of users requiring information, rather than the functionality of the system itself. Fowler also outlines the main issues of concern in the design of terrorism database, including such concerns as definition of terrorism incidents, the scope of the database, the method of data selection for terrorist incidents and actual details to be recorded in the database. Other factors effecting the scope and content of the systems were also discussed. For example, time frames and variables that were most commonly used at the time of the publication. In many ways this paper was extremely forward looking for its time. The strength of this work is in the fact that the underlying issues of concern to Fowler in 1981 are just as valid and applicable today.

In terms of the actual use of terrorism data sets, rather than their design, what could be considered a standard reference for any researcher setting up an events data set on terrorism is Taylor and Jodice's *The World Handbook of Political and Social Indicators*.⁸⁷ This is a record of events data on political protest and violence, state coercive behaviour, governmental change and elections from 1948-1977. Although a little dated the strength of this work lies in its rigorous approach to the many issues of concern when establishing data sets. The importance of efficient collection and collation of raw data and its consequent management and analysis is discussed. The authors' recognition of the importance of consistency in codification of variables across national boundaries for comparative use, accessibility of data and the need to document data sets are also emphasised. Crucial to the credibility of any data set, as Taylor & Jodice point out, is reliability of data, on which to base sound

⁸⁷ Charles L. Taylor and M.C. Hudson, *World Handbook of Political and Social Indicators* (New Haven, Conn: Yale University Press 1983) 3rd. Ed.

empirical analysis of political violence.⁸⁸ In addition, recognition of the need for systematic criteria of variables in data sets provides valuable guidance on data set standards. Taylor & Jodice also highlight the issue of academic concern over quality of data sets, the practical considerations involved in the training of coders, inter-coder agreement, cross-time comparability of data sets and the reliability of sources and suggested uses for data sets. These factors all have an important bearing on terrorism data sets design and use.⁸⁹

Schmid and Jongman's *Political Terrorism* is one of the few guides on terrorism to have devoted a specific chapter to 'Data and Data Bases on State and Non-State Terrorism', and provided a comprehensive analysis of the terrorism data set situation at that time. The guide covers computer readable data sets on terrorism as well as manual data sets. Their recognition of the abundance of similar data on terrorism and the need to develop new data sets to further empirical research is highlighted by their survey among academics showing strong reliance on government publications at the expense of independent sources. Although published in 1988, Schmid and Jongman's survey of a large variety of early data sets on conflict and political violence developed in the 1960's and 1970's as well as more contemporary ones, provided an invaluable source of reference, also covering data sets developed by academic institutes, journals and the media. Very little analysis of the actual computer systems retaining these data sets (true database systems or text based chronologies) and functional capabilities was offered, however, and given the time that has now elapsed, most of these data sets have been merged, have become redundant, or have developed into sophisticated internet database systems.

⁸⁸ Ibid., p.176.

⁸⁹ For further discussion of terrorism data sets design see Chapter IV of this thesis.

Moreover, a lack of discussion on issues relating to the design of terrorism data sets, typological classification of data sets, chronologies and databases on terrorism, temper what could be considered a worthy if slightly dated review of terrorism data sets.

At the same time as Schmid and Jongman were writing on terrorist databases, Ted Gurr was analysing the problems encountered in the typological design and use of terrorism data sets Gurr's: 'Empirical Research on Terrorism: The State of the Art and How it Might be Improved' ⁹⁰ makes a serious contribution to terrorism data set issues and merits some attention. Gurr's work is of value for several reasons. Firstly, he appreciates and warns of the concern among terrorism researchers that information obtained from terrorism data sets does not always match the needs of researchers. Secondly, he warns that the typological design of the data set will have a bearing upon the content of the data set. The ramifications of this for quantitative and empirical research are serious. Chosen terrorist variables will determine the limits of the research base. Third, Gurr's concern that the 'right' research questions are being asked has crucial bearing on the consequent research results. He places heavy emphasis on the analytic questions that are being asked and offers appropriate methodologies for answering such questions. The five different levels of analysis: global, national, group, incident and individual would permit the possibility of different questioning at different levels. Gurr also voices concern over the generation of inappropriate or duplicated data on terrorism incidents, for example the creation of numerous chronologies on terrorism containing similar data.

⁹⁰ Ted Robert Gurr, 'Empirical Research on Terrorism: The State of the Art and How It Might Be Improved', in Robert O. Slater and Michael Stohl (eds.), *Current Perspectives on International Terrorism* (London: Macmillan, 1988).

Similar to Ross's concerns, Gurr notes the problems and limits encountered with using the same data set repeatedly for differing research needs.⁹¹ *A Conceptual Framework for Analyzing Terrorist Groups* by Brian Jenkins, Konrad Kellen *et. al* of the RAND Corporation is worthy of some attention.⁹² Its contribution to the literature comes in part from its innovative approach to the analysis of terrorist groups. Of particular interest however is the methodology used in the study; a series of databases on terrorist groups were devised as part of the framework for the project. Twenty-nine terrorist groups were studied from which 150 categories could be identified and categorised into ten areas, (Organisation, Leadership, Demography Ideology etc.). These were then coded and entered into several databases. Of interest to terrorism data set designers is the discussion on code-books, data collection and evaluation, and in particular the differentiation between textual coded data and variable coded data. The author's awareness of the value of using both types of variables in discussing terrorist groups (as opposed to simple aggregate data on incidents) highlights some of the principle design issues in terrorism data sets. The importance of reliability versus the validity of terrorist data is identified making a valuable contribution to the area of data integrity in terrorism data set design.

In a similar vein, Ross' s work on political terrorism in Canada recognised the conceptual and methodological issues encountered in the creation of an events database.⁹³ Ross's concern over the lack of empirical literature on political violence in Canada forms the background to other more general but important issues and

⁹¹ *Op cit*, p.144.

⁹² Bonnie Cordes, Brian M. Jenkins, Konrad Kellen With Gail Bass, Daniel Relles, William Sater, Mario Juncosa, William Fowler, Geraldine Petty, *A Conceptual Framework for Analyzing Terrorist Groups* (Santa Monica CA: RAND Corp., 1985) R-3151.

⁹³ *Op cit*.

concerns in terrorism data sets design. This work was unusual in that it illustrated in detail the potential statistical data that can be derived from a well-designed events database on terrorism.⁹⁴ Among the main benefits was the possibility of demonstrating that terrorists choose among a certain range of options.⁹⁵ Ross also argues that events databases can attach a statistical probability to terrorist choices. In addition, he suggested the possibility of ‘predict[ing] the terrorist’s most likely actions’ which widened the role and capabilities of carefully developed data sets for counter-terrorism purposes. Ross, like other researchers, recognised the well-established debate over definitional agreement on what constitutes an act of terrorism. More importantly however are his concerns over typologies of terrorism and delineation of the different types (for example Mickolus, or Wilkinson) for practical implementation into events data on terrorism. The common and recurring complaint of the ‘lack of good empirically grounded research on terrorism’ is brought to our attention in this paper. Ross developed this further by explaining that “‘empirical research’ implies the use of methodologies of the social sciences’, i.e.:

‘..techniques for ordering information systematically and drawing inferences from that information about the patterns, trends, causes, processes and outcomes of conflict. Since political terrorism is a type of conflict, the full spectrum of techniques for conflict analysis are potentially applicable to it.’⁹⁶

The reference to systematic ordered information fitted particularly well with basic database design theory and its use as a tool in empirical terrorism research. The temptation to focus specifically on terrorism events data as a result of its availability

⁹⁴ *Ibid*, p.47.

⁹⁵ This would be dependent upon the type of data set devised and the variables included in the data set.

⁹⁶ *Ibid*, p. 49. Ross further argues that methodologies do not always mean the analysis of quantitative data and that used appropriately systematic case studies, ‘guided by an explicit theoretical argument or framework’ is possible framework (in Ted Robert Gurr, ‘Methodologies and Data for the Analysis of Oppositional Terrorism’, paper presented for the *Symposium on International Terrorism*, Defense Intelligence College, Washington, D.C., 1985).

at the expense of other techniques of analysis can be limiting. Ross reminds us that events data is not the only methodology for empirical analysis of terrorism. Other techniques such as direct observation, content analysis of terrorist self-reporting, and survey research all have their part to play in empirical terrorism research.

Unlike terrorism data sets, documentation in the international conflict data set field is well established. An understanding of the need to fully document computerised conflict data sets has been recognised.⁹⁷ Cioffi-Revilla's *Handbook of Datasets on Crises and Wars 1495-1988*,^{A.D.}⁹⁸ although concerned with events data on conflict, provides some very useful material on establishing standards in computerised data set development. If purely from a generic point of view Cioffi-Revilla's emphasis on the need for 'information profiles' is an important starting point in the design of any computerised data set. Profiles fully describe the format and entities within the data sets. Such documentation sets a standard for comparative analysis of differing machine readable data sets. Cioffi-Revilla's also provides comparative analysis of space and time coverage of conflict data sets and geographic distribution of conflict. This could, if carefully considered, provide a

⁹⁷ The U.S. National Science Foundation initiated under its Political Science Program a project entitled "Data Development for International Research" (DDIR). This involved supporting existing and new data sets projects, including the Interstate Conflict Datasets Catalog. (ICDC). Longer term aims of developing daily events data and intra and inter-state conflict data sets under the umbrella of (DDIR) have been initiated. A specialised standard the (ICDC) standard has been developed in response to the specialised needs of conflict data set users. The traditional American National Standards Institute (ANSI) standard was considered too limiting for the (DDIR) data sets. See Claudio Cioffi-Revilla, *The Scientific Measurement of International Conflict: Handbook of Datasets on Crisis and Wars 1495-1988*^{A.D.} (Boulder Colorado: Lynne Rienner 1990) pp12-13.

⁹⁸ Claudio Cioffi-Revilla, Computational Social Science, Conflict Analysis and the 21st Century Threat Triad, in *21st Century Information Technologies and Enabling Policies for Counter Terrorism*. Ed. by R. Popp, (IEEE Press, 2006).

useful method for comparative analysis of existing terrorism data sets to highlight the strengths and weaknesses in data collection.⁹⁹

2.3. Early research – journal articles and datasets

The journal *Terrorism and Political Violence*¹⁰⁰ was pioneering in the development of a forum for research and discussion on the application of technology to the study of terrorism and political violence. A small but growing literature field has developed to date: terrorism data sets, the use of on-line databases in terrorism research and Information Technology applications to Terrorism. Bruce Hoffman and Donna Hoffman, for example, provided an overview of the RAND-St. Andrews Chronology of International Terrorism.¹⁰¹ This detailed the criteria for inclusion of incidents in the RAND-St. Andrews chronologies, the information sources used, and also gave aggregate totals of terrorism incidents. A preface providing a profile of the data set demonstrates professionalism in providing background and context to the data set development. Also, as Avishag Gordon notes, the availability of on-line services and CD-ROM as a tool in terrorism research is increasing.¹⁰² Using a variety of on-line databases and searching by key words on ‘terrorism’ ‘international terrorism’ and ‘tactics’ Gordon compares and measures the success of hit rates. Gordon’s use of traditional and non-traditional on-line services (for example

⁹⁹ Some caution is advised. As no consistent criteria or standard similar to the (ICDC) has been established a comparative analysis of existing computerised data sets on terrorism would have to be based upon crude aggregate data of common variables among data sets. This issue is discussed in Chapter IV of the thesis.

¹⁰⁰ *Terrorism and Political Violence* (London: Frank Cass).

¹⁰¹ Bruce Hoffman and Donna Kim Hoffman ‘The RAND-St Andrews Chronology of International Terrorism 1994’, *Terrorism and Political Violence* (London: Frank Cass), 7/4 (Winter 1995) pp.178-229 and ‘Chronology of International Terrorism’ *Terrorism and Political Violence* (London: Frank Cass) 8/3 (Autumn 1996) pp.87-127.

¹⁰² Avishag Gordon, ‘Terrorism and Computerised Databases: An Examination of Multidisciplinary Coverage’, *Terrorism and Political Violence* (London: Frank Cass), 7/4 (Winter 1995), pp.171-177. See also ‘Terrorism and Science, Technology and Medicine Databases: New Concepts and Terminology’, *Terrorism and Political Violence* (London: Frank Cass), 8/1 (Spring 1996), pp.167-173.

'Engineering Index', 'Aerospace Database', 'Medline Express') illustrates the widening appearance of terrorism literature in databases that until recently would have been considered outwith the realms of the subject area. Work published by Devost, Houghton, and Pollard *et al* also discusses the impact of Information Warfare on American national security, a field that is well established on the Internet. Its inclusion in an established journal on terrorism has been long overdue and sets a precedent for further research.

In terms of annual data sets, information on incidents of terrorism began to be produced by governments, academic centres, and private organisations. These publications tended to be the principal, though not exclusive source of terrorism events data used for research purposes. Although difficult to generalise, many of the reports were presented in a chronological format. Not all data sets appeared on an annual basis and some appeared on a periodic basis or materialised as the result of a project-driven contract. For reasons of security and to avoid distortion, the availability of many data sets tended in these earlier years to be in a hard copy format only. Few organisations took advantage of modern computer technology to make available complete data sets on terrorism in CD-ROM format or through the Internet.¹⁰³ The largest sources of data sets on terrorism come from the United States. The size and diverse nature of the U.S. Government dictated that no single agency was responsible for the publication of incidents on terrorism. The State Department, Federal Bureau of Intelligence, American Bomb Data Center in the Bureau of Arm, Tobacco and Alcohol, and the Foreign Broadcasting Information

¹⁰³ There are some exceptions for example the U.S. State Department publishes its *Patterns of Global Terrorism* on the Internet. Web site: [Http://www.state.gov/www/global/terrorism/1996report/](http://www.state.gov/www/global/terrorism/1996report/). See also F.B.I. site: [Http://www.fbi.gov/pubish/terror/year.htm](http://www.fbi.gov/pubish/terror/year.htm)

Service (FBIS) all published literature on terrorism events data. One of the most cited and authoritative sources of record on terrorism is the United States Department of State's *Patterns of Global Terrorism*.¹⁰⁴ This was an annual publication giving regional overviews of incidents of terrorism worldwide. The format was a mixture of narrative analysis of incidents of terrorism and trends, complimented by photographs and graphics. While modern database systems could hold all these entities in a single database format this data was held separately on varying computer systems and then drawn together for final publication. A chronology (text based) of significant incidents, along with statistical reviews (graphics based), formed part of the appendices. Aggregate variables on terrorism were not separated from the main text in the regional overviews, however quantitative analysis could be undertaken from the statistical overview that was present in the appendices. In addition, the U.S. State Department published *Significant Incidents of Political Violence Against Americans* on an annual (now periodic) basis.¹⁰⁵ This is a statistical overview detailing major anti-U.S. incidents of political violence (including terrorism) on a regional basis worldwide. Also listed in a chronological format this publication was heavily littered with graphics, photographs of incidents, maps and tabular statistics on anti-American attacks. Unique to this report was the inclusion of the 'Americans in Captivity' section. *Significant Incidents of Political Violence Against Americans* did, and still does not, claim to be inclusive of all incidents. The exclusion of certain data for classification purposes was mentioned in the initial editorial comments. Aside from the highly visual presentation format this publication lends

¹⁰⁴ US State Department., *Patterns of Global Terrorism*, (Washington, D.C.: US Dept. of State, 1995). See also *Lethal Terrorist Actions Against Americans 1972-1986*, (Washington, D.C.: US Dept. of State, 1987).

¹⁰⁵ US State Department., *Significant Incidents of Political Violence Against American*, (Washington, D.C.: US Dept. of State, 1995).

itself well to database retention; however the data set is formed from an amalgam of work from separate departments from within the State Department.¹⁰⁶

Dedicated information on events data was also provided in *TERRORISM*, a publication produced by the Federal Bureau of Intelligence.¹⁰⁷ This annual publication was a mixture of statistical analysis, trend analysis and topical issues relating to terrorism. A small chronology of terrorism events data is included as well as the definitional criteria given to explain statistical figures.¹⁰⁸ The FBI's *Bomb Summary* detailed bombing incidents in the United States each year.¹⁰⁹ This publication is an interesting mixture of statistical data divided into several categories (incidents by region, state, by target, time of occurrence etc.) that could be used for quantitative analysis. In addition the publication contained numerous graphical presentations, chronologies and practical guidance (graphically based) on handling potential bomb threats. The *Bomb Summary* was a combination of authoritative data on bombings, practical advice on security techniques, graphics, photographs of training, and incident data. Despite its compilation from various databases and file formats its format lent itself well to a wide array of computer-based analyses.

The Office of Civil Aviation and Security (under the auspices of the U.S. Federal Administration) annually published the *Criminal Acts Against Civil Aviation* report. The report presented a wide variety of data on criminal acts against airlines world-wide. Offering geographic analysis of significant acts (bombings, hijackings and attacks) on airlines and their related interests this report offered more specialised

¹⁰⁶ Published by the Bureau of Diplomatic Security's Office of Intelligence and Threat Analysis other departments including the Graphics section, protective intelligence investigations department and regional security officers all contribute to this publication.

¹⁰⁷ U.S. Department of Justice, *Terrorism in the United States 1995*, (Washington D.C.: US Dept. of Justice 1995).

¹⁰⁸ For a ten-year analysis of terrorism in the United States see US Department of Justice, *Terrorism in the United States 1982-1992*, (Washington D.C.: US Dept. of Justice 1992).

¹⁰⁹ US Department of Justice, *Bomb Summary 1995*, (Washington D.C.: US Dept. of Justice 1992).

data dealing specifically with aviation related incidents. Although lacking the subjective visual appeal of other federal agency reports the inclusion of feature articles, trends on hijackings, bombings and attacks on airports meant that it was a comprehensive analysis of threats to the aviation industry. Detailed chronologies on U.S. and foreign carrier hijacking, as well as explosions aboard aircraft, also allowed for some form of trend analysis. The lack of numerical variables in the chronology limited the potential for consequent quantitative analysis; however aggregate totals of incidents by region, target and tactic were supplied in the appendices. Moreover, an admission in the report that not all incidents that were recorded could be verified illustrated two key points: first, an honesty by the reports authors that no data set on terrorism is definitive, something that adds to its integrity, and; second, it further reminds the reader of the problems encountered in collating and verifying such incidents.

In the case of Canada, separate published events data on terrorism had been historically difficult to find, in part due to Canada's close proximity to the United States and the general trend to incorporate Canadian statistics under a North American banner. *Terrorism in Canada 1960-1989*, however, offered a balanced and unusual mixture of analysis, trends, methodology on coding, and several detailed chronologies. In comparison to similar publications much more attention was given to the concept of terrorism, behavioural aspects of terrorism, the motivation behind it and some definitional issues. Detailed discussion on the methodology behind the design of the data set, codification of variables, validation of events and sources used were well outlined, and a broad quantitative coverage of trends and patterns of terrorism effecting Canada were also presented using data derived from the four

chronologies in the report. The latter were unusual in that they differed in three main respects from other comparable chronologies on terrorism: first, separate chronologies on domestic and international terrorism were listed in the same publication; second, a 'Terrorism Support Activity' chronology comprising of 'actions in support of the commission of terrorist acts in Canada either directly.... or indirectly...' were presented, and, finally events that did not meet the prescribed criteria for inclusion in the other chronologies were listed in an 'Excluded Events' chronology.

The British government also produced data sets on terrorism incidents in the United Kingdom in several formats relating to the operation and prevention of terrorism legislation. For example, the Home Office produced statistics on bombings in the United Kingdom, as well as a separate data set for Northern Ireland (something that the Royal Ulster Constabulary (RUC) also did).¹¹⁰ Unlike the American federal publications no definition of what would constitute an act of terrorism is offered in these statistical bulletins. Also in the U.K., the Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St. Andrews, Scotland was one of few academic centres at that time to maintain a large repository of data sets on political violence and terrorism.¹¹¹ Originally established in 1972 by Brian Jenkins of the RAND Corporation of Santa Monica,¹¹² the annual publication of the *RAND-St. Andrews University Chronology of International Terrorism Incidents*¹¹³ appeared, as previously mentioned, in *Terrorism and Political Violence*.¹¹⁴ Covering

¹¹⁰ Royal Ulster Constabulary, *Chief Constables Annual Report* (Belfast: Royal Ulster Constabulary 1996)

¹¹¹ For further discussion of the RAND and RAND-St. Andrews Chronologies see Chapter IV and V of this thesis.

¹¹² Prior to the transferral of the chronologies to the University of St. Andrews, the RAND Corporation published *The RAND Chronology of International Terrorism* (Santa Monica CA: RAND Corp.) on an annual basis.

¹¹³ See Hoffman, *op cit*.

¹¹⁴ *Ibid*.

mainly incidents of international terrorism, and excluding acts of political violence by terrorists against nationals of their own country, a rich and diverse source of information was available. Whilst making no claim to be the definitive source for chronological information on terrorism,¹¹⁵ the rich sources of material used to compile the varying data sets (newspapers, journals, news wires, Internet, terrorist group communiqués etc.) offered terrorism researchers one of the best sources of hard copy and computerised data publicly available in the Western world.

Another academic centre, the Jaffee Center for Strategic Studies produced an annual report surveying international terrorism. Established in 1979 under the 'Project on Low Intensity Warfare' it contained statistical data on international terrorism. Known as *INTER* (International Terrorism) the publication was a well-balanced mixture of trend and regional analysis, various statistical data based on such variables as distribution of terrorism incidents, a chronology and group glossary.¹¹⁶ The strength of *INTER* lay in its middle-eastern regional analysis of events from where the report is produced.

One of the most widely used commercial data sets on terrorism was produced by Edward F. Mickolus, *Terrorism, 1988-1991: A Chronology of Events and Selective Annotated Bibliography*.¹¹⁷ This was a text-based chronology of oppositional terrorism and formed part of an on-going series of bibliographies and chronologies on terrorism events data that began in 1968.¹¹⁸ Useful background

¹¹⁵ Bruce Hoffman, 'The Confluence of International Behaviour and Domestic Trends' *Terrorism and Political Violence* (London: Frank Cass 1997) 9/2 (Summer 1997) p.11.

¹¹⁶ *INTER International Terrorism in 1987* (Jerusalem: The Jerusalem Post 1987).

¹¹⁷ Edward F. Mickolus, *Terrorism, 1988-1991: A Chronology of Events and Selective Annotated Bibliography* (Westport, CT: Greenwood Press 1993).

¹¹⁸ See also Edward F. Mickolus, Todd Sandler, and Jean Murdock, *International Terrorism in the 1980's A Chronology of Events* Vol. II. 1984-1987 (Ames, Iowa, Iowa State University Press, 1989), Edward F. Mickolus, Todd Sandler, and Jean Murdock, *International Terrorism in the 1980's A Chronology of Events* Vol. I. 1980-

detail on how the chronology had been developed, definitional criteria, sources of data, and a summary of aggregate totals of terrorist incidents were used in the first three chronologies. Although a genuine, but unfortunate and inappropriate attempt to use computer bytes to give some quantitative measurement of terrorist attacks in a table format was used in the introduction of the 1988-1991 chronology,¹¹⁹ Mickolus did provide an extensive and detailed code-book of his terrorism data set that was useful for codifying variables. In addition, discussion of how the chronologies were applied in empirical research, for example in bargaining models with terrorist groups (Atkinson, Sandler, and Tschirhart)¹²⁰ and time series analysis (Cauley and Im),¹²¹ gave the reader some examples of applications of the chronology to academic work. However, the fact that it was only published periodically, meant that its use as an annual up-to-date publication was inappropriate. Nevertheless as a cumulative volume of terrorist events data it served many terrorism research projects involving longer time periods. As a result of the historical time period between the events taking place and their publication in the chronology Mickolus included updated information relating to previous chronicled information and its value alone in terms of data integrity and accuracy issues in data set compilation should not be underestimated.

1983 (Ames, Iowa, Iowa State University Press, 1989) and Edward F. Mickolus *Transnational Terrorism: A Chronology of Events, 1968-1979* (Westport, CT: Greenwood Press, 1980).

¹¹⁹ Ibid, p.7. The authors choice of computer bytes to measure what in effect should be numerical figures has rendered the table void. Computer bytes cannot be used for quantitative or aggregate analysis of terrorism incidents.

¹²⁰ Scott E. Atkinson, Todd Sandler and John Tschirhart, 'Terrorism in a bargaining framework' *Journal of Law and Economics* Vol. 30. Pp. 1-21. in Edward F. Mickolus, Todd Sandler, and Jean Murdock, *International Terrorism in the 1980's A Chronology of Events* Vol. I. 1980-1983 (Ames, Iowa, Iowa State University Press, 1989) p. xxii.

¹²¹ Jon Cauley and Eric I. Im, *Intervention policy analysis of skyjackings and other terrorist incidents*. Unpublished manuscript. In Edward F. Mickolus, Todd Sandler, and Jean Murdock, *International Terrorism in the 1980's A Chronology of Events* Vol. I. 1980-1983 (Ames, Iowa, Iowa State University Press, 1989) p. xxiii.

Differing in both style and content the *Pinkerton Annual Risk Assessment* was a commercially based data-set on terrorism published by Pinkerton Risk Assessment Services.¹²² Its target audience was principally the private sector; evidenced in the use of 'risk level definitions'¹²³ in their regional analysis of terrorism. With an abundance of aggregate tables, quantitative and narrative analysis the Pinkerton report was highly detailed in nature, although a slight emphasis statistically on American experiences of terrorism, for example damage to U.S. property, U.S ransom demands and U.S. robberies tended to gear the report to the North American Corporate sector. In a similar vein, other commercial data sets on terrorism were published including the *Security Intelligence Report*, the *Profiles Threat Assessment Group*, and Mizell & Co.'s *Chronologies on Terrorism*. The American Society for Industrial Security published data sets on terrorism for business and corporate clients requiring country profiles or tailor-made analysis of terrorism activity in specific countries or regions world-wide.

Pluchinsky's *The Evolution of the U.S. Government's Annual Report on Terrorism: A Personal Commentary* offered a valuable historical insight into the development of the United States Government's (USG) annual publication on terrorism.¹²⁴ Pluchinsky, a former State Department terrorism analyst, detailed the evolution over nearly 30 years of the USG's annual reports on terrorism, from their earliest inception in 1976 as a one-off CIA document *Research Study: International*

¹²² Pinkerton Risk Assessment Services, *Annual Risk Assessment 1994* (Arlington VA: Pinkerton Risk Assessment Services 1994).

¹²³ The assignment of 'security risk levels' also includes other factors such as violent labour agitation, criminal activity and political unrest. The aim is to provide clients with a more rounded picture of events over and above specific terrorist incidents.

¹²⁴ Dennis Pluchinsky, "The Evolution of the U.S. Government's Annual Report on Terrorism: A Personal Commentary, *Studies in Conflict & Terrorism*, 29: 91-98, 2006.

and Transnational Terrorism: Diagnosis and Prognosis.¹²⁵ This eventually became a major publication: *Patterns of Global Terrorism*. In 1977, Pluchinsky outlined the context within which the CIA's Directorate of Intelligence initiated its first annual assessment of international terrorism. The paper entitled *International Terrorism in 1976* was produced "...to set the scope and nature of this activity into historical perspective...". While assessing trends and developments in the field and their likely future impact upon the United States. The final objective was to "apply these judgements and observations to a brief assessment of what may lie ahead during the remainder of 1977". Pluchinsky's paper provided a candid and robust defence of the USG's annual statistical publication on terrorism. The evolutionary processes of the publication, as Pluchinsky highlighted, were many: from the introduction, for the first time, of a definition of terrorism (1981) and a chronology of significant terrorist incidents (1983), as well as changes to the definition of terrorism and international terrorism (1984) and the report being mandated by Congress (1988). The one constant with the USG's annual report on terrorism was change. From subtle definitional revisions of statistical methodology to the addition of appendices on terrorist group profiles (1988) and "foreign terrorist organisations" (1997) Pluchinsky's annual report on terrorism was in constant evolution.

Given the political sensitivities of statistics on terrorism, the reports were open to periodic criticism from both politicians and academics over many years. As Pluchinsky notes "If you create it, they will criticize it".¹²⁶ One of the earliest criticisms was during the Reagan administration when the *New York Times* article "Data on Terrorism Under U.S. Revision" claimed that incidents of terrorism were

¹²⁵ *Ibid.*, p. 9.

¹²⁶ *Ibid.*, 99

“being revised to include ‘threats’ as well as actual acts of politically motivated violence”. The consequences of this, it was claimed, would double the count of terrorism incidents over a twelve-year period. The motivation for the revisions was that it would justify ‘...a more rigid foreign policy abroad’ and be used as an excuse by conservatives to increase surveillance of political dissidents within the United States.

Despite critical analysis and periodic revisions to its format, as will be discussed later, the USG annual reports on terrorism continued to be published until 2003. Its ‘downfall’, as Pluchinsky highlights, came in 2004 when, in an article published in the Washington Post entitled “Faulty Terror Report Card”, two academics from Princeton and Stanford Universities claimed there were underlying statistical and analytical methodology issues with the 2003 report. These public criticisms of the USG reports on terrorism came against a politically sensitive backdrop to events of September 11th 2001 and the need to have accurate data on terrorism incidents. After investigation, the USG acknowledged there were problems and issued revisions in June 2004. As a consequence the methods by which U.S. Governments statistics on terrorism were collated, calculated and presented, was completely overhauled. The result was a new publication titled “Country Reports on Terrorism 2004” containing narrative comment and analysis, whilst the chronologies and statistical element of the reports were transferred to the newly created National Counter-Terrorism Center (NCTC) website.

In addition to the useful historical outline of how U.S. Government statistics on terrorism have evolved, Pluchinsky’s paper offered deeper insight into what had always been a sensitive and controversial area of public reporting. His was paper a

unique insiders view of what became the major statistical reference source on terrorism for almost thirty years. He acknowledged the many up's and downs of collecting data on terrorism, but given the challenges of providing credible statistical analysis that retains integrity amidst a complex political audience, Pluchinsky's paper presents a fair and honest analysis. In particular, he acknowledged that one will never please everyone on the issue of defining an act of terrorism. Until the 'perfect' definition has been achieved, he argued, we should work within the constraints of what we have. Pluchinsky also illustrated 'the ugly' side to U.S.G. terrorism statistics when they are used within a partisan context to push political agendas, thus putting at risk the integrity of the data sets. Despite such shortcomings, Pluchinsky argued that no other country in the world could have provided such extensive data sets on terrorism consistently over nearly thirty years. What further increases its credibility, he argued, was that the report was unclassified after 1986, as mandated by Congress.

2.4. Early research - technical literature

Technical literature on the design and maintenance of terrorism data sets is rarely published and often difficult to obtain. Issues of security relating to the nature of the data being held is among several complex reasons behind the lack of available technical literature, something that will be discussed further in chapter 3. One of the few organisations to publish early technical literature on terrorism sets was the RAND Corporation of Santa Monica. A series of periodic publications gave insight into a less than developed literature base. Research carried out by Dewar and Gillogly in 1984 - *CODA: A Concept Organisation and Development Aid for the*

Research Environment - gave a suggested scheme for the development of a computerised storage and retrieval system for use in policy research, and the RAND Corporation adopted the CODA software to operate their chronologies and databases on International Terrorism.¹²⁷ Dewar and Gillogly's work differed from Fowler's work on database design in that they approached the problem as computer scientists rather than as terrorism analysts. To their credit the authors attempted to fuse the needs of the policy researcher - 'Desiderata' - with the functional capabilities and limitations of existing software and hardware availability at the time. Their work is of value for several reasons: it makes a serious and thoughtful attempt to understand the needs of the policy researcher in quantitative research and tries to 'mould' the CODA system to the user's needs.¹²⁸ This is complemented by discussion of the CODA commands and hardware requirements needed to implement such a system. The authors are realistic about the functional limitations of the CODA system; recognition that itself adds weight to their analysis in that lessons are learnt and further improvements can be suggested, including a 'Wish List' of capabilities. Moreover their work was further augmented by their work with Hammer and together they published the *CODA'S User Manual*, which aimed to provide users of the CODA system with operational advice and contains no research and analysis. As a software user manual it is thorough, technical in nature, and details the full functionality of the CODA system including data entry, recall, the use of operators, indices and menus for querying coded terrorist variables. The literature in this area was supplemented by a brief, but interesting, paper on the *Management*

¹²⁷ Development of CODA began in 1982 as an adjunct to the work on the Air Force Computer Study under project AIR FORCE.

¹²⁸ Often researchers are given a system designed by computer professional and are expected to work with the given system with little thought as to the appropriateness of the given system'.

of the RAND Corporation's *Terrorism and Conflict Databases* published in 1984 by Bonnie Cordes.¹²⁹ Although less technical in nature than the work by Dewar and Gillogly, and Dewar, Gillogly, and Hammer, it is a useful guide to the organisation of the RAND terrorism chronologies and databases in the early 1980's and details the variables coded in the data sets as well as a brief synopsis of each data set.¹³⁰ Updated formats of the RAND and RAND/St-Andrews data sets continued to be published on a periodic basis.¹³¹

Also in terms of early technical literature, the Bureau of Diplomatic Security within The United States Department of State provided terrorism research staff within the Threat Analysis Division with *TADMIS* (Threat Analysis Division Information Management System). This was a user manual published by the Management Information Systems Division of the Bureau of Diplomatic Security at the State Department, and gave guidance to analysts entering data on incidents and threats of terrorism. The manual provided a comprehensive range of information on operating the database. Of particular value was the fact the manual had been written to deal specifically with the needs of terrorism analysts working directly in the field. From a design angle the *TADMIS* manual provided researchers with documentation from a 'live' example of a terrorism database system in operation, which was of benefit in understanding the strengths and weaknesses at an operational, functional and variable level.

¹²⁹ Op cit.

¹³⁰ For further research work on relational database research at RAND see Hobbs paper [move this footnote]

¹³¹ See Description of the *RAND Low-Intensity Conflict/Terrorism Databases*, published by RAND and the *RAND/St.Andrews Terrorism Research Database Categories*. These are occasional descriptors issued giving an outline of the RAND and RAND/St.Andrews terrorism data sets.

2.5 Conclusions

This chapter has examined the very earliest research in the terrorism database field. As this thesis will demonstrate 9/11 changed the landscape regarding the number and variety of databases available, as well as the scope of their use. As this chapter has demonstrated however, there is a significant history of the use of database technology, and it is fair to say that a number of the databases that have achieved particular prominence in the 9/11 world, have their foundation in this very early work. What is important to recognise is that even in this early work there were issues regarding the variety and sources of terrorism data such that to generalise can be difficult given that the published literature base has been created with differing remits in mind, something that remains the case in the post- 9/11 world. There remains a scarcity of specialised literature dealing specifically with the role of the modern computer as both a tool and an area of academic study within terrorism studies. More than this, there remains a significant need for a published literature - both in academic and policy terms - to assess current databases. There is also a paucity of literature relating to the potential benefits of information technology in the counter-terrorism field. It is to these questions that this thesis now turns.

CHAPTER III

DESIGN AND DEVELOPMENT ISSUES IN TERRORISM AND COUNTER-TERRORISM DATABASES

3.1 Introduction

In the post-9/11 world, an array of complex issues effect the design and on-going development of terrorism and counter-terrorism databases. The sourcing, collection and filtering of terrorism data, its codification into a database, and eventual operation, requires serious commitment and substantial financial resources, including specialist subject expertise, technical knowledge, and a sound understanding of the terrorism field. Moreover, the subject of terrorism, by its very nature, is a sensitive political issue. As a result, definitional issues, the remit of the database, the integrity of the data, the choice of database system, security and its on-going operation all have an important influence on the design and development of terrorism databases. Further factors include the type of host organisation developing the database. These can include government agencies, university research centres, businesses and private organisations. By their very nature each organisation will have their own agenda: one that will impact upon the design and development of the database. Added to the many challenges of designing and developing terrorism and counter-terrorism databases is the stark reality that not all projects will succeed. From failure can come reflection and insight that might

otherwise not have proved possible. The pre-9/11 world allowed terrorism and counter-terrorism databases to operate in isolation. That era has come to an end. Major advances in internet technology, networking, and the creation of fusion centers, have presented opportunities unforeseen only a few years ago. The political demands that information be shared and used for the common good to both protect and inform now require that many terrorism database projects share, collaborate, and develop in partnership with other government agencies and institutions. Added to this is the fact that in the post 9/11 world legislation has impacted even more upon database design and development.

With this in mind, this chapter will examine the following three key questions: what are the significant issues that effect the design and on-going development of terrorism and counter-terrorism databases?; what impact does the organisation hosting the database have upon its design and development?; and, what lessons can be learnt from not only successful terrorism and counter-terrorism database projects, but also from projects that have failed?. In attempting to answer these questions, this chapter will examine a series of academic and government database projects established since 9/11. These will be used to illustrate the many challenges involved and will include, amongst others, the Global Terrorism Database (GTD), the Worldwide Incidents Tracking System (WITS) and MIPT's Terrorism Knowledge Base (now disbanded). The chapter will also begin to assess the overall impact of policy and legislation on the design and on-going operation of terrorism and counter-terrorism databases post 9/11, something that will be examined in more detail in chapter 5.

3.2 Data Definition: Defining Terrorism

The issue of defining what constitutes an act of terrorism has remained a constant point of debate for many years. Regardless of whether within the context of a narrative discourse on terrorism, or in the codification of terrorism data into a database system the desire for, and realisation of, perfection in defining an act of terrorism has eluded all interested parties. Pre and post-9/11 the problem remains the same. Narrative discourse on terrorism allows writers the chance to explain and expand upon their arguments using the richness of language the boundaries of which can be almost limitless. Such freedom cannot be enjoyed when designing terrorism and counter-terrorism databases. By their very nature they are 'systems' and have to operate within both conceptual and operational boundaries – and the kernel of any terrorism and counter-terrorism database - indeed the fundamental foundation from which the database is designed and populated - is the definition of what an act of terrorism is.

These issues are hardly new. Nearly thirty years ago, Fowler highlighted many valid definitional problems in designing terrorism databases that hold just as much resonance today:

“Virtually every researcher we interviewed expressed concern about the difficulty of defining a set of consistent criteria for inclusion of incidents in terrorism databases. The problem is one of balancing the desire for comprehensiveness with the necessity for rigor and relevance of the data. Databases that apply clearly defined criteria were criticised for being overly restrictive – in some cases the restrictions are imposed by law ... in others they are dictated by mission ... or by the desire to achieve methodological rigor ... On the other hand, some data bases include information that might be excluded under a strict interpretation of data-based definition ... The data bases are clearly divided on this issue: those used for basic research strive for more rigorous definitions and operationalization of concepts, while those used mostly for intelligence estimates contain data that seem more directly

related to policy questions, whether or not this results in consistent data selection".¹³²

Fowler highlights the many tensions and demands made upon terrorism database designers. Whilst purists could craft and present a 'near perfect' definition of terrorism, the narrative may not translate easily into a credible, fully operational database system.

Almost like a piece of elastic stretched in many directions, the demands on designers can be onerous. On the one hand requirements to have '...consistent criteria for inclusion of [terrorist] incidents...' have to be off-set with expectations of '...comprehensiveness...rigor...and relevance...'. Add to this formula legal constraints, potential political influence, government policy and institutional mission requirements, and any designer is left with a very complex matrix of demands that, in the end, may not please or satisfy anyone. In addition, the type of organisation hosting the database places further definitional constraints upon designers as government agencies such as the National Counterterrorism Center (NCTC), the FBI, and the Australian Secret Intelligence Organisation (ASIO) have a remit that is set out in legal statute.¹³³ Moreover organisations such as these have much wider responsibilities than solely hosting and operating terrorism and counter-terrorism databases. Often terrorism definitions are established prior to the creation of the database, raising the issue of whether to fit the definition to the database or vice versa?

¹³² William Warner Fowler, *Terrorism Data Bases: A Comparison of Missions, Methods, and Systems*. (Santa Monica CA: RAND Corp., N-1503-RC. 1981. www.rand.org/pubs/notes/2005/N1503.pdf [Accessed 18/02/10])

¹³³ There is no such legal requirement is imposed upon academic or private organisations. This is not to say, of course, that these organisations enjoy a free reign. Academic funding bodies, institutional policy and private and commercial financiers may well have an input into how terrorism databases are to be designed and developed, based upon definitional criteria.

Definitional variations have implications in database design not purely from a semantic point of view. Problems can occur too in the translation from a political interpretation to workable definitions in variable coded and text format. In other words the transformation of variables into a computer-coded format that is operationally viable requires considerable thought if accuracy and meaning are to be maintained. Fowler highlights this very problem at both a conceptual level and a practical database level:¹³⁴

‘The definitional problem has two aspects: developing conceptual definitions that delineate the interests of the researcher and the general needs of the application...’

Further complications can arise, as Alex Schmid illustrates, in the actual elements used for working definitions of terrorism given that enormous variations can occur. Many databases, for example, include the elements ‘violence’, ‘political’, ‘fear’ ‘terror’ and ‘purposive; planned, systematic’. Yet other databases include rarely used elements such as ‘publicity aspect’ (RAND and TWEED), ‘criminal’ (PGIS and TRITON) and ‘demands made on third parties’ (TWEED).¹³⁵ As a further illustration of this, and using five major terrorism databases, even a cursory glance at Table 3.1 illustrates the rich variation in language and terminology used in working definitions of terrorism.

¹³⁴ William Warner Fowler, *Terrorism Data Bases: A Comparison of Missions, Methods, and Systems*. (Santa Monica CA: RAND Corp., N-1503-RC. 1981) p.9.

¹³⁵ Alex P. Schmid, *Statistics on Terrorism: The Challenge of Measuring Trends in Global Terrorism*. Forum on Crime and Society, Vol 4 No's 1 and 2. December 2004. United Nations Office on Drugs and Crime, Vienna. Source: http://www.unodc.org/documents/data-and-analysis/Forum/V05-81059_EBOOK.pdf [Accessed 03/03/10]

Table 3.1 – Working Definition of Terrorism in Five Terrorism Databases

Database	Working Definition
Worldwide Incidents Tracking System (WITS)	‘Terrorism occurs when groups or individuals acting on political motivation deliberately or recklessly attack civilians/non-combatants or their property and the attack does not fall into another special category of political violence, such as crime, rioting, or tribal violence’ ¹³⁶
ITERATE - International Terrorism: Attributes of Terrorist Events	“The use, or threat of use, of anxiety-inducing, extra-normal violence for political purposes by any individual or group, whether acting for or in opposition to established governmental authority, when such action is intended to influence the attitudes and behaviour of a target group wider than the immediate victims and when, through the nationality or foreign ties of its perpetrators, its location, the nature of its institutional or human victims, or the mechanics of its resolution, its ramifications transcend national boundaries.” ¹³⁷
Global Terrorism Database (GTD)	<p>GTD 1 (1970-1997) “The threatened or actual use of illegal force and violence by a non state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation.”¹³⁸</p> <p>GTD 2 (1998-2007) “Based on the original GTD1 definition, each incident included in the GTD2 had to be an intentional act of violence or threat of violence by a non-state actor. In addition, two of the following three criteria also had to be met for inclusion in GTD2:</p> <ol style="list-style-type: none"> 1. The violent act was aimed at attaining a political, economic, religious, or social goal; 2. The violent act included evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) other than the immediate victims; and 3. The violent act was outside the precepts of International Humanitarian Law.”¹³⁹
U.S. Department of State	“Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.” ¹⁴⁰
Terrorism in Western Europe: Events Data (TWEED)	‘...terrorism is understood theoretically as a form of violence that uses targets of violence in an indirect way in order to influence third parties, audiences’. ¹⁴¹

¹³⁶ Source: <http://wits.nctc.gov/> [Accessed 19/02/10]

¹³⁷ Mickolus, *op cit*.

¹³⁸ Source: <http://www.start.umd.edu/gtd/using-gtd/> [Accessed 19/02/10]

¹³⁹ “While the original GTD1 employed the definition of terrorism utilized by PGIS, the second phase of data collection for the GTD (GTD2: 1998-2007) coded each incident so as to allow users to identify only those cases that meet their own definition of terrorism.” Source: <http://www.start.umd.edu/gtd/using-gtd/> [Accessed 19/02/10]

¹⁴⁰ Source: <http://www.state.gov/documents/organization/122599.pdf> [Accessed 19/02/10] Country Reports on Terrorism 2008. United States Department of State. April 2009.

¹⁴¹ Source: <http://folk.uib.no/sspje/tweed.htm> [Accessed 19/02/10]

The kernel of any terrorism and counter-terrorism database is designed and built upon two key elements: a definition of terrorism and the unit of analysis; nearly always the terrorist incident.

3.3 – Methodology

Credibility of data within terrorism and counter-terrorism databases is paramount. Dubious data not only damages quantitative and qualitative analysis, it can also present credibility issues for host organisations. Sophisticated web interfaces and advanced querying functionality should not be confused with absolute and total integrity of data. During the 1970's and 1980's with the development of many chronologies on terrorism, a culture of pseudo legitimacy emerged. In other words, by virtue that data was logged on computer, this meant that data was valid. With much greater technological literacy, this mindset has all but disappeared.

Defining the function of a terrorism or counterterrorism database for analysis, research and intelligence purposes is relatively straightforward. What databases are not to be used for, or where they may be imperfect, is rarely acknowledged among designers. One of the few agencies to openly 'disclaim' features of its database is the National Counterterrorism Center. The NCTC openly acknowledges its data sources may be of varying credibility, and that its WITS database is not perfect. This admission is both transparent and healthy. The NCTC clarifies that data within WITS is for statistical purposes only. By inference, one can assume that the WITS terrorism data should not be used for intelligence, counter-terrorism or any other activity. Part of the NCTC disclaimer is outlined below.

'Any assessments regarding the nature of the incidents or the factual circumstances thereof are offered only as part of the analytic work product of the National Counterterrorism Center and may not reflect the assessments of other departments and agencies of the United States Government. Nothing in this report should be construed as a determination that individuals associated with the underlying incidents are guilty of terrorism or any other criminal offense'¹⁴²

Two key points can be gleaned from the above statement. Firstly, despite the NCTC's interpretation of particular incidents and any factual circumstances they have ascribed to the event, one cannot assume that all other U.S. Government agencies will interpret such events data in the same way. While the NCTC aims to collect the universality of terrorism events data, one cannot assume a collective understanding or 'assessment' of particular terrorism events by all U.S. agencies. Secondly, the NCTC abrogates itself from being the judge and jury in potential litigation against individuals, leaving that task for the courts. This illustrates the fine balancing act agencies have to make when running open source, publicly accessible terrorism databases. Do they provide, within reason, as much detail as possible on a particular terrorist incident, or is vague but accurate data acceptable?

In addition to defining what constitutes an act of terrorism, database compilers are often presented with a less than complete picture of events. Where traditionally hard copy documents such as ITERATE and Patterns of Global Terrorism committed facts to print, the great beauty of database systems is their ability to be updated when required. Terrorism incidents are often complex and messy events and change in nature over time. For example, the amount of injured may increase, bodies may be discovered at a later point and responsibility for a particular attack may be immediate, delayed or never established. The fine line between rigorous objectivity

¹⁴² NCTC Website - http://www.nctc.gov/witsbanner/wits_subpage_disclaimer.html [Accessed 02/03/11]

and subjectivity can be testing for analysts attempting to discern between what some might deem to be an act of terrorism and what others would classify as political violence. Subjective judgments need to be kept to an absolute minimum when coding terrorist incidents. The NCTC acknowledges this essentially human dilemma:

‘Users of this database [WITS] should therefore recognize that reasonable people may differ on whether a particular attack actually constitutes terrorism or some other form of political violence.’¹⁴³

This element of ‘reasonable people’ presents the potential for a labyrinthine discourse on what one would consider ‘reasonable’. At some point a coding decision is required. To improve methodological rigour the NCTC uses a series of detailed counting rules.¹⁴⁴ Some of the key exclusions to the database are outlined in Table 3.2.

Table 3.2. Events excluded from the WITS database

Type of Terrorist Attack	Entry into WITS
Failed	Excluded
Foiled	Excluded
Hoaxes	Excluded
Genocidal Events	Excluded

Source: - http://www.nctc.gov/witsbanner/wits_subpage_criteria.html

As with the Global Terrorism Database (GTD), NCTC and previously RAND/MIPT, complex codification issues are referred to a specialist panels for final validation.

¹⁴³ NCTC Website - http://www.nctc.gov/witsbanner/wits_subpage_criteria.html [Accessed 02/03/11]

¹⁴⁴ Ibid.

Many of the large established databases on terrorism and counter-terrorism have in-house panels and external advisors to offer advice on design and methodology, such as the GTD's Advisory Board¹⁴⁵. An innovative move by the NCTC after the inception of its WITS database was the establishment of the NCTC's Brain Trust on Terrorism Metrics. This highly unusual move by a U.S. Government intelligence agency to bridge the security and intelligence divide between 'insiders' and those on the outside has been ground-breaking. In addition to security vetted intelligence officials, the NCTC invited relevant individuals such as academics, security related specialists and other government agencies such as the State Department to contribute to the on-going methodological refinement and development of the WITS database. The easy route for the NCTC would have been to be keep matters internal. In seeking external advice and constructive criticism, a maturity of understanding was established. Reciprocity of ideas and experiences are to be encouraged. Furthermore, the NCTC recognised that not all wisdom resides within its walls. Many of the issues that academics have encountered in terrorism database design are just as applicable to classified and government databases. These include the generic issues of defining an act of terrorism, codifying variables, excluding certain acts and providing accurate and fair narrative on each terrorist incident. The mystique of classified terrorism data will always be attractive to some, by the nature of its limited accessibility. Denial of access to such information has not stopped the creation of many extensive and highly credible open-source databases on terrorism and counter-terrorism. Academics are not functionaries of the law. In fact one could argue the inverse: they have the freedom to develop exactly the terrorism databases

¹⁴⁵ <http://www.start.umd.edu/gtd/about/GTDTeam.aspx> [Accessed 02/03/11]

they desire without the accountability of governments and legislation. This allows them to create open-source terrorism databases, offering a rich resource of data from which quantitative, qualitative and empirical data can further enhance terrorism studies. One would be naïve however to assume that all non-government databases on terrorism are given a completely free reign. The pride element that led in part to a territorial culture of insularity within intelligence agencies such as the FBI, CIA and State Department prior to 2001, was paid for at a very high price. What NCTC has demonstrated is that even the highly sensitive issues of terrorism data and intelligence can be discussed in a safe forum for mutual benefit.

Given the nature of the subject, perfection in terrorism data collection will be forever be elusive. A realist and pragmatic approach to data collection methodologies offers the best solution to this complex area of terrorism research. From the earliest development of terrorism chronologies and databases from the 1960's onwards, the definition of terrorism, coupled with the unit of analysis, determined the universe of data from which the database was populated. This fundamental double act remains the cornerstone of terrorism database design. However, once these foundations have been set in place they can have serious implications for the on-going development of the database. The longevity of terrorism and counter-terrorism database projects, many with temporal periods spanning decades, necessitates continuity in definitional criteria and the unit of analysis. Flaws within the database methodology and refinements and changes in definitions of terrorism can have serious ramifications for quantitative and qualitative data. For example, a change to the NCTC's WITS methodology in 2005, on what was deemed to be an act of terrorism, has meant that retrospective

comparative analysis of terrorist incidents prior to 2004 is not possible. Thus, data from the U.S. State Departments Patterns of Global Terrorism cannot be used with the WITS database without considerable qualification. Many of the well established early databases on terrorism were originally based exclusively on acts of international terrorism. Given the blurring of the binary divide between domestic and international terrorism, database designers have had to re-evaluate their design criteria. This rigidity of definitional criteria has some important merit, in that continuity of data is maintained, however, continuity of data should not be confused with quality, as erroneous data could be consistently entered.

This mixture of technical limitations and definitional criteria being determined by host organisations has meant, for many years, that researchers have played an entirely passive role in their interaction with terrorism and counter-terrorism databases. Books such as ITERATE were referred to, the data was drawn from them and they were cited. In other words, the experience was referential not interactive. Even with the advent of computerised terrorism databases, the user was entirely dependent upon, until very recently, the definitional criteria as defined by the host organisation. A subtle, but important innovation in database web technologies has changed this situation, however. While definitional criteria remain static, users are now, in some cases, able to access multiple definitional criteria within a database, such that users can retrieve data with finer granularity. One of the few open source terrorism databases to offer this facility is the Global Terrorism Database (GTD), START, at the University of Maryland. Table 3.2 below presents three optional definitional criteria by which the GTD can be queried.

Table 3.3. Terrorism Definitional Criteria - Global Terrorism Database (GTD)

Criterion I: The act must be aimed at attaining a political, economic, religious, or social goal. Would you like your search results to require Criterion I to be met?

- Yes. Require Criterion I be met.

Criterion II: There must be evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) than the immediate victims. Would you like your search results to require Criterion II to be met?

- Yes. Require Criterion II be met.

Criterion III: The action must be outside the context of legitimate warfare activities, i.e. the act must be outside the parameters permitted by international humanitarian law (particularly the admonition against deliberately targeting civilians or non-combatants). Would you like your search results to require Criterion III be met?

- Yes. Require Criterion III be met.

One could argue that the next logical step would be to offer researchers the possibility of multiple definitions of terrorism from which data could be queried. Edward Mickolus, for example, produced a typology of terrorism that identified four different types: interstate, international, state and domestic.¹⁴⁶ These classifications were not mutually exclusive, however they did add another angle to design considerations of terrorism data sets and their consequent codification. Multiple definitions would, in theory, permit researchers to model their informational needs around their own understanding of what an act of terrorism was deemed to be. Almost like a piece of clay, one could shape the database to one's own agenda. The great beauty of clay is its manipulative quality. Mapping this analogy onto the design

¹⁴⁶ The definitions are derived from Edward F. Mickolus, "Combating International Terrorism: A Quantitative Analysis," unpublished Ph.D. thesis, Yale University, 1981 pp.218-219. For further discussion on terrorism typologies see Jongman and Schmid (note 6) Chapter 1 pp.39-56

of a terrorism database, could mean in theory, that anything goes. Such a simple analogy is, however, fraught with dangers at both the design and theoretical levels, as designers could then simply generate the definitional criteria for what constitutes an act of terrorism that meets their needs, ignoring the overall integrity of the database, and altering the perception of the terrorist threat. Thus, for example, in 1980 the CIA revised its figures on terrorism incidents to include 'threats' and 'hoaxes', citing in as their reason the fact that established data sources were too narrow. The ramifications of this change were serious in that reported terrorist incidents rose by nearly fifty per cent in one year.¹⁴⁷

Of course not all terrorism data sets are accompanied by working definitions. This is particularly the case for some terrorism data sets produced on the internet, such as the MILNET database of terrorism incidents,¹⁴⁸ whilst other selected chronologies on terrorism such as 'Save Our Sri Lanka from Terrorism' do not provide working definitions either.¹⁴⁹ This lack of definitional criteria in the interpretation by some organisations of an act of terrorism does not necessarily imply that there is a problem with the data set, e.g. that they are inaccurate in their reporting of terrorist incidents or that the quality of sources are dubious, but when a government does not make any provision for defining an act of terrorism this is something entirely different.

As a final example of the significance of definitional issues, John Wigle's introduction of the Worldwide Incidents Tracking System offers a rare 'insiders' perspective on the National Counterterrorism Center's WITS database. Wigle's

¹⁴⁷ A.J.Jongman 'Trends in International and Domestic Terrorism in Western Europe, 1968-1988' , *TPV* 4/4 (Winter 1992) pp.28-29

¹⁴⁸ MILNET URL:<http://www.onestep.com/milnet/terror.htm>

¹⁴⁹ *Save Our Sri Lanka from Terrorism Network* URL:<http://www.case.cioe.com/~sos/terror.html>

paper outlines some of the key methodological challenges at both its inception and on-going development. Patterns of Global Terrorism, the predecessor to WITS, was terminated in 2003. Consequently a 'zero-based review' of terrorism data collection and analysis methods was undertaken by the USG.¹⁵⁰ The end result was the establishment of the Worldwide Incidents Tracking System (WITS) to be hosted by the National Counterterrorism Center. This review, as Wigle notes, not only included key methodological challenges in developing rigorous data sets, but was seen within a wider context of business processes, information technology and staffing requirements. Wigle's paper illustrated a fundamental challenge facing analysts: inconsistencies in the NCTC's definition of terrorism and the operation of inclusion filters for terrorist incidents. As a result of such concerns, these filters were dropped, such that from 2004 onwards, the WITS database tracked both international and domestic acts of terrorism.¹⁵¹ Moreover, Wigle highlighted the difficulty with having dual criteria (terrorist incidents had to be both international and significant) for inclusion in the Patterns of Global Terrorism database. Again these were subsequently dropped.¹⁵²

A particularly valuable section of Wigle's paper is devoted to a discussion of computers, those who use them, and their relationship to decision-making theory. Wigle points to the human ability to categorize and recognize discrete objects, yet their weakness in determining effective aggregate judgements. The author notes: 'Humans often include bias and emotion in their aggregate judgement process,

¹⁵⁰ Further in-depth analysis of the demise of Patterns of Global Terrorism and the establishment of the WITS database is discussed in Chapter Three

¹⁵¹ Discuss this further down the line

¹⁵² For a much more detailed discussion on terrorism database methodology, please refer to Chapter 3.

which hampers their ability to make factual conclusions'.¹⁵³ To minimise such potential issues a computer algorithm is used by WITS to maintain objectivity as far as possible. Wigle's paper is a reminder that not only does terrorism data and collection methods require challenging methodological rigor, but also that the human element of bias and emotions are ever present. This theme was originally presented in the hypothesis of this thesis. Soft qualitative data deals with the many situations that are not always easy to codify into a database system. While codifiers can adhere to rigorous coding schemes, it is almost impossible at times to eradicate totally the presence at some stage of emotions, anger, frustration, tiredness and any other qualitative emotion than cannot be quantified in hard numbers.

3.4. Sourcing Data

Regardless of their remit all organisations or individuals have to adopt certain data collection methods to maintain and build a data set, this requires professional judgements and an adherence to some form of pre-defined criteria. Two principle factors affect the collection method: financial resources and availability of source material. Without appropriate resources to pay for skilled research staff and access to data collections this can be an expensive and time-consuming effort. Even with a respectable financial budget many agencies and organisations absorb large amounts of revenue and time on such data collection efforts. In spite of dedicated resources many terrorism and security analysts are required to undertake other professional duties in addition to the maintenance of terrorism data sets. Analysts at the State

¹⁵³ *Ibid.*

Department's Bureau of Diplomatic Security, as part of their responsibilities, enter on a daily basis terrorism data into TADIMS and the Overseas Security Electronic Bulletin Board (EEB) an on-line database dealing with security related incidents overseas. The culmination of overnight sources and daily news items from CNN, news wire services, National Public Radio as well as classified intelligence data can present a huge volume of data to be analysed and entered into the database. The nature of this data tends to be in a narrative format and often lengthy, twenty or thirty pages for example. In addition the format of newspaper reports varies considerably from that of radio or newswire information. This can add to problems of consistency when translating source material into data set format. A particular issue faced by government agencies is the practical decisions involved in separating classified data on terrorism from unclassified. Where data is used by external users such as the Electronic Bulletin Board compliance with security regulations is a paramount.¹⁵⁴ The amount of terrorist data received and handled at any one time can be substantial. To avoid or keep to a minimum duplication of events data a method called 'cross talk' is employed. This allows analysts to communicate electronically with colleagues to avoid unnecessary duplication of work. This has two advantages: it performs at a basic level some form of data integrity and allows subject specialists to handle their own relevant data.¹⁵⁵ Subject and regional specialists often maintain their own 'private'¹⁵⁶ chronology or database on a specific

¹⁵⁴ In order to identify the author of data entered into the TADIMS and the EEB analysts are required to 'sign' data with their initials. This can help in validity and data integrity purposes for future reference

¹⁵⁵ Furthermore, where analysts may have missed some relevant article the 'cross talk' facility will alert them to information seen by colleagues.

¹⁵⁶ These 'private' chronologies or databases are usually maintained by analysts for the purposes of other security work they are required to carry out. Often held in electronic format they are the cumulative efforts of the analysts building up a large knowledge base upon a particular terrorist group or country. Not all data held in these 'private' databases are used in the main database systems.

terrorist topics; this data where appropriate is entered into the main database systems.

A large amount of funding, however, does not guarantee the quality of the terrorism data set. The choice, availability of source material and methods of coding raw data all play an important role in the quality and validity of the data set. Sources of information for terrorism data sets can vary in quality and quantity depending upon the type of information required. Perhaps more importantly, as Jodice and Taylor note: 'The quality of sources used [in data sets] invariably has an effect on the quality of specific conclusions drawn from the analysis'.¹⁵⁷ In their wide coverage of the practical problems encountered in the development of data sets, Jodice and Taylor outline some of the often more subtle problems with source reliability when compiling data sets. These include issues of prior restraint, and self-censorship in newspapers that can affect the quality of terrorism source data. Editorial prior restraint on the reporting of events and self-censorship of topics dictated from powerful management's or government can inhibit the availability of potentially good source material. Other factors such as regional biases in coverage of North America for example, over sub-Saharan Africa, also affect the availability and quality of terrorism data.¹⁵⁸

3.5. Data Validity

The issue of validity of terrorism events data adds further to source problems. It is important to differentiate between the validity of data from that of reliability and

¹⁵⁷ Charles L. Taylor and M.C. Hudson, *World Handbook of Political and Social Indicators* (New Haven, Conn: Yale University Press 1983) 3rd. Ed.

¹⁵⁸ For an example of regional biases in media coverage of events see Andrew K. Semmel, "The Elite Press, Foreign News and Public Opinion," in Jodice and Taylor (note 27) p.178

consistency of data. The impression that these terms all have the same general meaning can be misleading. The work of Cordes, Jenkins et al, *A Conceptual Framework for Analyzing Terrorist Groups* is among few terrorism data sets to devote some attention to this issue.¹⁵⁹ The authors clearly explain the issue:

‘Reliability in data collection may be defined as the consistent coding of a single item by more than one coder. Validity is the ability of an item to measure what it was intended to measure. Reliability is necessary, but not sufficient, for validity.’¹⁶⁰

Furthermore, the authors recognise that validity can take several forms including content, construct and predictive validity. To test out the predictive validity element the authors assessed terrorism data and created a scheme for attaching responsibility to for an act of terrorism to a certain group.¹⁶¹ The results of the tests showed that research staff can consistently code data wrongly but achieve reliable methods for doing so. The cumulative effect of this can create serious integrity problems for terrorism data sets. Perfection is desirable but impossible. As the authors note:

‘Absolute reliability is impossible to achieve in collecting data on terrorism, because even the most precisely defined concepts in political conflict are subject to judgements when applied to empirically derived information. However, the level of reliability can be estimated and compared with that of similar data-collection efforts.’¹⁶²

The often cited RAND/CIA example, in which the RAND Corporation registered 40 bombings by the same group on the same night, coding this as a single event,

¹⁵⁹ Bonnie Cordes, Brian M. Jenkins, Konrad Kellen With Gail Bass, Daniel Relles, William Sater, Mario Juncosa, William Fowler, Geraldine Petty, *A Conceptual Framework for Analyzing Terrorist Groups* (Santa Monica CA: RAND Corp., 1985) R-3151 p.11

¹⁶⁰ *Ibid.*, p.11

¹⁶¹ *Ibid.*, p.11. Content validity was tested by analysing terrorism data to ensure it was ‘consistent’ and ‘reasonable’ in relation to other items in the database created. The complex issues of construct validity relates to how much the terrorism data ‘made sense’ in relation to the model or hypothesis used in the research project. The authors used specialists for this task.

¹⁶² *Ibid.*, p.11

compared to the CIA's coding of 40 incidents for the same event, presents further dilemmas as to how to treat source data.¹⁶³ Often an oversight, but a serious concern is the issues of updating data set files particularly where the number of causalities have risen or responsibility for terrorist actions are attributed to the wrong group or individuals. The ITERATE chronologies have recently inserted an update section for those very purposes.¹⁶⁴

One of the most basic functions of a modern database system is its ability to offer 'validity checks'¹⁶⁵ or integrity constraints¹⁶⁶ upon the data set. These validity checks are purely functional operations and do not strictly relate to Cordes and Jenkins definition of validity being the '.. ability of an item to measure what it is intended to measure.'¹⁶⁷ The Cordes and Jenkins definition relates to a researchers interpretation of terrorism events data and whether it meets a pre-defined criteria as to be valid for input into a data set. Validity or integrity constraints are a series of pre-defined functional criteria that are invoked when certain declarative rules are broken.¹⁶⁸ Database systems can offer a wide variety of validity or integrity constraints. For example minimum and maximum entry values can be placed upon numerical variables. Other constraints such as entry defaults on a field can insure that a particular entry such as target country, or terrorist group will appear in the data set unless coded otherwise. Validity checks requiring the exclusion of specific words such as 'conflict' or 'guerrilla' can be used to maintain definitional data

¹⁶³ Jongman, *ibid*, p.29

¹⁶⁴ Edward F. Mickolus, *Terrorism, 1988-1991: A Chronology of Events and Selective Annotated Bibliography* (Westport, CT: Greenwood Press 1993) p.13

¹⁶⁵ Validity Check defined as 'A constraint or check on the values entered in a table' *Paradox Relational Database Version 3.5, PAL User Guide* (Scotts Valley, CA: Borland International 1990) p.545

¹⁶⁶ Elmasri (note 4) p.15. The integrity constraint specifies a data type for each data item.

¹⁶⁷ Cordes (note 29) p.11

¹⁶⁸ These declarative rules are pre-programmed criteria. Proper training will have alerted coders of validity checks upon the system.

specifications. Even more powerful integrity constraints could set criteria that terrorism variables entered into one database matches exactly the same variable(s) in a related database. This gives data sets consistency in entry procedures. The repetitive task of bulk data entry whereby mistakes occur can in part be reduced by well-designed systems and appropriate training of coders. Despite the sophistication of many systems and the availability of in-built integrity constraints errors in coding does occur. For example, where an integer between 1 and 10 has been set, erroneous entry of figures even within the pre-defined criteria can occur without being detected. Absolute perfection is desirable but unrealistic when dealing with the entry of terrorism data. Minimisation of potential errors through correct coding procedures can help to reduce integrity problems.

The validation of terrorism event sources through primary source corroboration is one method of ensuring the validity of actual events. Financial and time restraints can often hinder this method of ensuring the quality of source data. An over reliance on using the same source data as a result of familiarity with presentation and out of habit may present some problems. Continual use of the same sources of data without double-checking data from other potential sources may hide potential inconsistencies or inaccuracies of reporting. Although not perfect, easy accessibility on the Internet to almost all major and regional newspapers and news services as well as specialist Web pages such as The Terrorism Research Center can help to provide at least some form of corroboration.¹⁶⁹ One such data set to include a double checking system is the chronology *Terrorism in Canada 1960-1989*¹⁷⁰ by

¹⁶⁹ The Terrorism Research Center, URL://www.terrorism.com/terrorism/links.html

¹⁷⁰ Kellet *op cit*, (note 13) p.40

Kellett et al. The author's set out what they deemed to be three essential criteria before any data could be entered into their terrorism chronology. These were:

'..corroboration by at least one primary source', '..sufficient .. information to classify the event' and 'conformity to the components of terrorism..'.¹⁷¹

The authors used as a minimum, one primary source from a selection of local newspapers in Canada, or other officially recognised primary sources such as *Canadian Criminal Cases*, *Dominion Law Reports* or international newspaper and wire services.¹⁷² What makes this case slightly different from other chronologies on terrorism is the authors decision to create an 'Excluded Events Chronology', this was compiled from terrorism events data that could not be validated or did not have a primary source. Almost as a bonus in this strict procedure, was the discovery of other terrorist incidents that would otherwise have been missed. Not every primary source can provide researchers with all the required details to code in detail a terrorist incident. The most common details, type of attack, target, location, date and number of casualties are relatively easy to obtain in comparison to other important facts. Motivation for an act of terrorism, group or individual responsibility, intended and actual target of terrorism form a much more difficult set of variables to obtain and may require further time and secondary sources to complete data set entries. Non-governmental terrorism data sets do not have the privilege of classified source material that may or may not enhance the qualitative value of the data set. The fact a piece of data may be classified does not necessarily diminish the value of non-governmental data sets. The intrinsic value of classified information may only be relevant to the government agency at hand adding little value to other data sets. The

¹⁷¹ *Ibid.*, p. 40

¹⁷² *Ibid.*, p.79. These primary sources had to form part of the officially recognised criteria.

nature of intelligence data is based upon a mixture of known facts and unconfirmed evidence. For the majority of terrorism data sets criteria and variables are established on the basis of known facts. The data set is not built upon suspected evidence or gut instinct about facts. Sources of information for non-governmental terrorism data sets tend to come from a wide variety of publicly available sources. Several forms of terrorism source data can be identified. Traditional and fairly credible sources such as the New York Times or Foreign Broadcasting Information Service (FBIS) are complemented by electronic news wire services such as Reuters and Associated Press (AP). In addition a vast selection of Internet news services including CNN, the BBC, a the major daily and many smaller newspapers world-wide are published on the Internet.¹⁷³ Other established specialised sources including *The Middle East Journal*, *The East Asian Recorder* the *Africa Diary* can redress the geographic Western biases that can occur in the literature from time to time. Ironically with such choice comes a saturation of information making good selection criteria paramount. Even the impressive capabilities of modern computer systems cannot transform questionable source data into quality information.

The ITERATE terrorism data sets have used such sources as the Washington Post, ABC, NBC, the Foreign Broadcasting Information Service (FBIS), FBIS Daily Reports, the New York Times and Reuters.¹⁷⁴ Assuming the source is of a credible nature there are some advantages in using publicly available sources. Where possible cross-checking of sources can help to validate terrorism events data. A complete picture of events may not be possible from one particular source coverage,

¹⁷³ Some of the smaller regional and local new services available on the Internet can offer coverage of terrorist events that may well have been ignored or given limited coverage by larger national newspapers.

¹⁷⁴ Edward F. Mickolus, Todd Sandler, and Jean Murdock, *International Terrorism in the 1980's A Chronology of Events* Vol. II. 1984-1987 (Ames, Iowa, Iowa State University Press, 1989) p. xii

thus necessitating a wider coverage of sources. Publicly available sources can be susceptible to inaccuracies. Even allowing for this they do provide a forum for comparative analysis of events data. In addition the investigative nature of the journalist may well uncover data that might well have remained unreported.

Without a strategy, the sheer volume of terrorism information available on a publicly accessible basis can potentially overwhelm research staff. Early development of the RAND and RAND-St.Andrews terrorism data sets was based upon the manual collection of source material. This involved the selective cutting and copying of articles from newspapers, academic journals, and news services to be retained in a hard copy format or entered into the CODA system.¹⁷⁵ This is both a time consuming and expensive effort. The potential for backlog in such a process is high unless research staff are able to process all sources of information on a timely basis. To alleviate this problem in part, the RAND-St Andrews research staff use the on-line database services of Lexis-Nexis.¹⁷⁶ This subscription based service, although a relatively expensive product, offered several advantages to the Centre for the Study of Terrorism and Political Violence (CSTPV). Lexis-Nexis contains in excess of 10,000 news publications held in computer format. This offers a far more comprehensive coverage of potential terrorism source material than would be obtainable in a hard-copy format. The cost of purchasing such a broad range of articles would be prohibitive. Its 'clipper' facility is able to return to research staff relevant terrorism articles from previous days events. The RAND-St.Andrews data

¹⁷⁵ CODA software was developed by the RAND Corporation and holds the RAND and RAND-St.Andrews terrorism data sets. See James A. Dewar and James J. Gillogly, *CODA: A Concept Organisation and Development Aid for the Research Environment* (Santa Monica CA: RAND Corp. P-7035 1984)

¹⁷⁶ The Lexis-Nexis service operates out of Dayton, Ohio. With access to over 7300 databases and one billion documents held on-line it offers a substantial selection of material. The Eclipse™ feature (Electronic Clipping Services) returns requested search requests on specified topics daily, weekly by fax, on-line or E:mail. See: URL: <http://www.lexis-nexis.com/lnc/about/background.html>

sets received on average 300 articles every morning. The information offered to research staff is on the basis of key word identifiers stipulated by research staff. A further selection criteria is applied to the source material. Relevant data was then saved in a local P.C. for eventual coding and entry to the appropriate terrorism chronologies or databases.¹⁷⁷ Real time searches for source data on the Internet and other networked services allowed CSTPV staff to maintain an up-to-date and responsive service for researchers.

The apparent wealth of source material on terrorism does not always, of course, satisfy researchers needs. Particularly where data is sought for project-specific terrorism data sets. Jeffrey Ross notes his concern over the lack of statistical information on violence in Canada.¹⁷⁸ The lack of statistical data that, if available, is both inaccurate and out of date is reflective of wider problems in source data. The temptation to abandon such projects can be tempting. Ross suggests however that another approach may be to derive where possible information from non-governmental organisations, independent researchers, police departments and other existing chronologies and newspaper coverage. This process can be a lengthy and at time frustrating process. As Ross notes his experience of collecting source data on right wing organisations was not always a pleasant experience:

‘These supplementary sources, however were not free from drawbacks. First researchers (e.g., academic, journalists, and private) who have conducted research or collected material on one or many right-wing organizations were a mixed lot. They were generally extremely difficult to track down, unco-operative, had confusing political agendas, and mistrustful’.¹⁷⁹

¹⁷⁷ In addition to the Lexis-Nexis service the Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St. Andrews, collected material from an extensive array of other sources. These include hard copy newspapers, journals, academic reports, translation and monitoring services, risk assessment publications, including those of Control Risks (London). Recent developments have been Internet sources.

¹⁷⁸ Jeffrey Ian Ross, ‘Research Note: Contemporary Radical Right-Wing Violence in Canada: A Quantitative Analysis’ *TPV* 4/3 Autumn 1992 p.81.

¹⁷⁹ *Ibid.* p.99. footnote 38.

By its very nature the subject of terrorism and political violence research is an emotive issue. Suspicion as to the researchers motive for collection of terrorism source material can at times result in an uncomfortable experience. Accreditation to an institution and a professional approach by individuals or organisations can help to minimise the more negative aspects of core research.

One of the most widely used sources for terrorism data sets is newspapers. They offer the advantage of regularity of information on a daily basis and depending on editorial judgement provides balanced reporting of events. Neither of these benefits however can guarantee absolute accuracy in statistical data. Coverage of acts of terrorism can be an attractive news story for editors. Their willingness to cover what many would be deem to be an act of atrocity is justified on the grounds of public responsibility to report important news events, and at its most basic level to sell newspapers. Newspapers have not always been a major source for terrorism data. Crelinstein notes that not until 1970 were any articles in the *The New York Times* indexed under the heading of terrorism.¹⁸⁰ And as such this only amounted to four articles. A substantial growth to sixty-seven articles by 1972 was indicative of the increasing interest in the subject area. *The Times* of London also saw substantial increase in articles from 128 in 1972 to 443 by 1977; this in part parallels terrorism activity in Northern Ireland at the time.

The assumption that all terrorism source data can be derived from an English language newspapers overlooks other potential sources. The French Polemological Institute which collected data on political violence used sources such as *Le Monde*

¹⁸⁰ Ronald D. Crelinstein, 'Images of Terrorism in the Media: 1966-1985' *Terrorism*, Vol. 12, No.3 p.171.

and *Neue Zürcher Zeitung* among its principle sources.¹⁸¹ For any researcher language can be a barrier and events can be missed. The attraction of local newspapers is their potential for covering events that may have been ignored by larger national international English speaking newspapers. Language problems are not only restricted to hard copy newspapers. Until very recently key-word searches for terrorism source data on the Internet very much limited to English language pages. This is in part due to the historical development of the Internet in English speaking North America. During 1997 the Internet search engine Alta Vista™ introduced facilities to permits key word searches in over twenty languages. For researchers the problems remains constant: the language barrier. Overcoming this hurdle opens up researchers to an as yet limited, but increasingly developing research base. Many of the established foreign newspapers such as *The Washington Post*, *The Australian*, *The Times of India*, and *The Cape Times* are available on the Internet and offer potential primary source and selective translations of events. The Jordanian Intelligence Service¹⁸² opened an English language version of their own Jordanian site, with a dedicated terrorism page, and other sites such as the Japanese Intelligence Agency website only offer information in their native language. One of the most highly regarded sources for terrorism data is the Foreign Broadcasting Information Service (FBIS) reports on terrorism. Information is derived from television and radio broadcasts, periodicals, news agencies and books. In addition to the daily service, periodic reports on terrorism are published. One factor FBIS is noted for is its over-reporting of events data in Africa. Prokop cites several reasons

¹⁸¹ Jongman (note 11) p.30.

¹⁸² URL:<http://www.petra.nic.gov.jo/gid/004-03.htm>

for this slight over emphasis of events.¹⁸³ The repressive nature of some African regimes that run the state owned media organisations may tend to suppressive true figures. Furthermore, as FBIS provides intelligence information to U.S. government agencies on foreign government policies, and actions, the requirement to over-concentrate on a generally underreported region in the daily American broad-sheets in part redresses an imbalance in reporting.

Source terrorism data for American federal agencies such as the FBI can come from an even wider pool of resources than that of publicly available sources. The very remit of the organisation is in the creation and handling of intelligence data. Established networks of legal attaches based in American embassies permit the generation of terrorism source data.¹⁸⁴ Reciprocal arrangements with foreign counterparts and involvement in the Terrorism, Radicalism, Extremism, Violence International (TREVI) group also provide a forum for co-operation in data exchange. In addition the F.B.I also works closely with agencies such as the United States Secret Service, Immigration and Naturalisation Service and the Bureau of Alcohol, Tobacco, and Firearms (ATF). Some criticism of the F.B.I's data collection methods have been voiced however. Jeffrey Handler's concern over the methods by which agents attempted to collect source arose when he asked for specific data from the FBI. He found some of their data collection methods lacked '...any systematic effort to create uniformity in the type of background data..' that was sought.¹⁸⁵ The lack of a pre-determined pro-format when questioning suspects resulted in many variations

¹⁸³ Diane Prokop, "Preliminary Analysis of the FBIS Database as a Source for African 'International I+W' Analysis" (McLean, VA: International Public Policy Research Corporation, 1980).

¹⁸⁴ William Sessions, 'The FBI's Mission in Countering Terrorism' *Terrorism* Vol.13 No.1 p.5

¹⁸⁵ Jeffrey S. Handler 'Socioeconomic Profile of an American Terrorist: 1960's and 1970s' *Terrorism*, Vol. 13, No. 3. Pp.199-200. This was based upon particular needs of a specific project and relates purely to *source* data methods and not to data coding.

of style in terrorism source data. The type of questions asked by agents was very much left to individual personalities styles and manner at any one particular time.

For intelligence agencies the collection of source data on terrorism is based on a different agenda to the more focused requirements of academics coding terrorist data sets. Longer-term projects with sporadic availability of data and the need for timely information can place considerable pressure on desk officers. The need to evaluate source data in 'real-time' requires considerable professional judgement that can differ quite markedly from source collection methods out-with the intelligence field.¹⁸⁶

Sources of terrorism data are not exclusively restricted to events data methods. Alternative approaches can be employed; this is very much dependent upon the type of data sought and the end requirements for the data. In his study on political terrorism in Canada, Ross identifies four main methods for collecting and empirically analysing terrorism data. These are direct observation, content analysis of terrorist's self reports, survey research and aggregate data analysis.¹⁸⁷ As Ross notes there are problems associated with all these techniques. The direct observation method of terrorists and their activities can present problems with personal security, ethical issues, trust, and comprehensiveness of data. The content analysis method¹⁸⁸ may encounter problems in obtaining legitimate written material by actual terrorist's

¹⁸⁶ For a discussion of the procedures for collection of source data by intelligence analysts see R.H Mathams *The Intelligence Analyst's Notebook* (ANU Canberra: The Strategic and Defence Studies Centre, Working Paper No.151 1988)

¹⁸⁷ Jeffrey Ian Ross, 'An Events Data Base on Political Terrorism in Canada: Some Conceptual and Methodological Problems' *Conflict Quarterly* Vol. 8 No. 2. pp.53-54.

¹⁸⁸ *Ibid.*, p.54. Defined as 'The systematic, quantitative analysis of observations obtained from archival records and documents' in Chava Frankfort-Nachmias and David Nachmias, *Research Methods in the Social Sciences* (London: Edward Arnold 1992) 4th Ed. p.549.

relevant to the research at hand. Survey research approaches to collecting terrorism data can appear an attractive option. As Ross notes:

A well-designed survey can provide five types of information about respondents: facts, perceptions, opinions, attitudes and behavioural reports....[however] The survey method is not without its problems, especially with access and reliability. It is very expensive and can produce highly biased data because of the features of the interview process itself. Difficulties stemming from the mutual suspicion of terrorists and governments are inevitable.’¹⁸⁹

Despite its many potential flaws the events data approach for terrorism data sets sources remains the most popular method.

Terrorism data comes from an eclectic mixture of sources. No one depository meets the requirement needs of all terrorism researchers or analysts. With differing agenda’s such as government/intelligence, academic and commercial operations, generalisations on source data can be difficult. The format can be complex: a mixture of formal and informal publications, classified and publicly available, electronic and hard-copy format. This array of sources forms only the first step in the design process of computerised terrorism data sets. Collected data requires coding. This transformation requires careful consideration if original source data is to be truly represented in the computerised data set. The codification of terrorism data into either a text based system or a database requires some established procedures if accuracy, validity and consistency of data is to be maintained. Jodice and Taylor offer advice on maximising inter-coder-agreement in data set compilation. These include good managerial supervision, thorough and substantive training, periodic testing of data and a recognition that where data does not meet specified criteria it is disposed

¹⁸⁹ Ross, *op cit*, p.55.

of.¹⁹⁰ These factors although appearing to state the obvious are worthy of some consideration. Poor managerial supervision of large data set projects can seriously undermine the quality of work undertaken.

The profile of coders in academically run terrorism data sets tends to be graduate research students who are familiar with the source material and are pursuing research themselves in related disciplines. The background of other coders can vary depending upon the organisation operating the terrorism data set. Input into U.S. federal terrorism databases such as the FBI's Violent Gang and Terrorist Organisations File (VGTOF) is carried out by police and other personnel. Often the coder of data is the analysts as well. This is particularly the case in smaller commercial operations.

The translation from original source to computerised data set format while still maintaining the data's validity can be a challenging task. The format of the original source material can come in varying styles. For example, short newspaper clippings, press communiqués and longer narrative reports, these all have to be read and interpreted for relevant data.

The advantages of a truly modern database system are its capability to offer researchers a whole range of functional capabilities that text based system cannot. These include arithmetical operators such as aggregate totals of terrorist incidents, numbers of casualties or provide powerful querying facilities including 'LIKE' 'NOT' and 'OR' operators as well as providing links between relevant data sets. The generation of forms and reports based upon chosen terrorism data is another extremely useful function of the database system.

¹⁹⁰ Taylor & Jodice, *op cit*, p. 118. For a thorough model see the rest of the document.

3.6. The Codebook

The powerful potential of modern computerised systems should not overshadow some of the fundamental design considerations of terrorism data sets. Codification of terrorist variables requires some form of agreement for data entry. To maintain the integrity of the data set a codebook or coding rules should be established. Although difficult to obtain at times, there are several conflict/political violence/terrorism data sets that have published rules and procedures for coding data.

Several terrorism data sets have produced varying forms of codebooks. Edward Mickolus's ITERATE data sets provides a codebook detailing a summary of all the variables used in the data set.¹⁹¹ This is an extensive codebook clarifying where appropriate reasoning behind coding procedures. For example in the data set each terrorist incident is given a unique event-type code. The codebook clarifies problems where an event may have the characteristics of more than one event such as an airline hijacking that turns into a 'barricade-and-hostage seizure'.¹⁹² Explanation of the numbering of transnational terrorism events assigning an eight-digit code number is also given. Kellett's *Terrorism in Canada 1960-1989*¹⁹³ also contains a detailed methodology and coding procedures for the data set. Variables such as 'level of event' pertaining to international or domestic terrorist incidents in addition to the standard date/time, location, targets and casualty variables are included. Apart from detailing factual information on variables used in a data set the codebook

¹⁹¹ Mickolus *op cit*, p.497.

¹⁹² Edward F. Mickolus, Todd Sandler, and Jean Murdock, *International Terrorism in the 1980's A Chronology of Events* Vol. I. 1980-1983 (Ames, Iowa, Iowa State University Press, 1989) p.509.

¹⁹³ Kellett, *op cit*, p.29.

provides other useful information. It gives researchers the opportunity to explain methodological issues that effect the coding of terrorism information. With many data sets containing hundreds of variables this necessary. Certain codebooks provide additional information on the file structure of the data set. This gives an indication of the design of the data set and its operability. The sheer volume of terrorism data entered into either a chronology or database system could potentially cause serious operational problems in the long run. From a software and hardware angle the retention of large amounts of coded variables and narrative text in single file format could cause a system to crash ¹⁹⁴ or effect the functioning of the data set file. The ITERATE data sets are coded into four files as part of its file management.¹⁹⁵ Codebooks contain relevant information not just for the researcher compiling the data set but also provide a background and context to users in the creation of the data set. While codebooks provide variable information and methodological criteria they give the user little information on the development and history of the data set. Although terrorism data sets may differ in content William Fowler has identified the four most common types of variables that are entered into terrorism data sets. The date of the incident as Fowler notes is usually mandatory. Precision on exact dates can be difficult at times as incidents occur over time. The other key variables - location, target and type of act or incident - generally from the core information base for the data set.¹⁹⁶

3.7. Error Rates

¹⁹⁴ Problems related to limited hard disk space, Random Access Memory (RAM) problems and an inefficient use of file management are among potential problems that could be encountered. This is particularly the case for relational database management system whereby a series of files are linked together, offering efficient use of the systems facilities and powerful functioning capabilities.

¹⁹⁵ The main file for the ITERATE data set is the COMMON file containing most terrorism incidents. The FATE, HOSTAGE and SKYJACK files are supplementary files.

¹⁹⁶ Fowler (note 16) p.17.

Few terrorism data sets contain detailed discussion on error rates when coding data. The work of Cordes, Jenkin's et al, *A Conceptual Framework for Analyzing Terrorist Groups*, discusses in some detail their attempts to measure error rates in the data set.¹⁹⁷ The authors ask if there is an acceptable error rate? Ideally, the answer is no. Their realist approach recognises that errors can and do occur. For their analysis of terrorist groups an acceptability rate of 80 per cent was selected for 'lead' questions used in compiling the data set. Randomly selecting eight terrorist groups the researchers carried out 'blind recoding' of the original questionnaires on the terrorist groups by coders who had not dealt with the original coding. The authors identified two main areas of concern. These were 'individual errors' and 'comparative errors'. The 'individual errors' were perhaps unsurprisingly such factors as inappropriate entries or wrongly coded dates. The 'comparative error' took on a more sophisticated pattern and content. Vagueness in responses to questions about dates appeared to be a recurring pattern, in addition differences in terrorist group numbers was also identified. To complicate matters further problems of subjectivity in coding continuous values such as 'never,' 'almost never,' 'occasionally,' 'almost always,' and 'always' arose. As Cordes and Jenkins note: 'These items typically have lower reliability than items requiring discrete or specific responses'.¹⁹⁸ A recurring problem for this study was in the area of source data. The most common problem was identifying the dates of information detailed in original terrorism source data.¹⁹⁹

3.8. Other Data Collection Methods

¹⁹⁷ Cordes, *op cit*, p.12

¹⁹⁸ *Ibid.*, P.13.

¹⁹⁹ *Ibid.*, p.14.

Publicly available documentation by police and intelligence agencies on data collection and dissemination methods is extremely rare. The sensitive political nature of terrorism data and the consequences of information arriving in the 'wrong' hands limit the availability of such information. The Federal Bureau of Intelligence has published some information in this area under its National Incident-Based Reporting System (NIBRS).²⁰⁰ Established procedures for reporting criminal events have been in place for over 60 years under the FBI's Uniform Crime Reporting Program (UCR). The advent of new technologies and the ever increasing information requirements of the U.S. law enforcement agencies has seen a thorough re-evaluation of data collection and dissemination methods during the past decade. The NIBRS system is an incident-based reporting system. This differs from the traditional summary based UCR program.

Its scope is wide. As the FBI note:

'NIBRS has, in fact, the capability of furnishing information on nearly every criminal justice issue facing law enforcement today, including terrorism, white collar crime, weapons offences...' Furthermore 'The data [is] available from and for all levels of law enforcement - federal, state, and local - aggregated at the level and in the manner which best meets the needs of the data user.'²⁰¹

Development of the NIBRS was carried out over several years and involved the definition of new data elements (incident details) and an initial pilot project in South Carolina.²⁰² The aim of the NIBRS was to permit individual law enforcement agencies to develop computerised systems that suited their own specific requirements at a collection and storage level while delivering data to the NIBRS.

²⁰⁰ National Incident-Based Reporting System (NIBRS) URL:<http://www.fbi.gov/ucr/nibrs.htm>

²⁰¹ *Ibid.*, p.4.

²⁰² *Ibid.*, p.2.

The actual file structure of the data sets developed at a local or state level i.e. relational, network or hierarchical databases do not have to be modelled upon the NBRIS system. This gives a certain degree of flexibility among agencies to choose additional data elements and data values which have already been developed for sophisticated reporting systems. The NIBRS system is able to detect any common data links among the record systems of all the agencies subscribed to the NIBRS. This type of cross-checking of variables among different agencies is a powerful facility that allows the detection of data on individuals or groups that would have otherwise been missed. The difference between this system and the FBI's Violent Gang and Terrorist Group File is that the VGTOF data is contained within one database and data is entered directly into the database from various local, state and federal agencies. The criteria for entry of data into the NIBRS are strict and must meet the UCR's 'Data Collection Guidelines' and 'Data Submission Specifications'.²⁰³ Individual agencies are required to submit test data and operate the required hardware and software facilities to cope with the NIBRS. Offence categories are classified under two main groups. Group A deals with serious and extremely serious offences including Violence, Drugs and Narcotic Offences, Homicide, Pornography and Sexual Offences. Extensive data is collected on all these areas. The Group B categories record only arrest data and includes other lesser offences of drunkenness, liquor law violations and disorderly conduct. Coding of data is based upon a number code identifier. For example 'Drive by-shootings (non-juvenile)' is assigned a code '09'.²⁰⁴ An attractive element of NIBRS is its ability to check certain data entry fields where the data value has not been fully completed with the required information. The

²⁰³ *Ibid.*, p.4.

²⁰⁴ *Ibid.*, p.5.

assignment of an entry 'XX' for example would indicate that a drugs quantity data element has not been coded. The 'XX' coding is an interim entry pending laboratory confirmation. The FBI conducts periodic checks upon these type of fields to ensure that exact details have been entered. This type of facility is particularly useful in terrorist activities when a bombing has occurred, casualties have been reported and may be rising and no confirmation of group or individual responsibility has yet been determined.

The coding of data on terrorist activities by government agencies often contains a wider set of coded variables. The data requirements of law enforcement agencies can differ from academic or commercially based terrorism data sets. The principle differences are their agendas are based upon differing needs. The type and level of coded variables required by government agencies tend to be more intelligence based in their format. The inclusion for example of coded fields or narrative text detailing personal profiles and histories of individuals used in the Interagency Border Inspection System (IBIS)²⁰⁵ or the State Department's Consular Lookout Support System (CLASS)²⁰⁶ differs markedly from chronological data sets such as ITERATE. Legal issues over retention of computerised data on profiles of individuals by academic centre's or commercial organisations such as Pinkerton's or Kroll Associates may leave them open to potential litigation.²⁰⁷

3.9. User Manuals

²⁰⁵ Michael D. Cronin, *Terrorism and America: A comprehensive review of the threat, policy, and law*. Hearings before the Senate Committee on the Judiciary, 103d Congress, 1st. Session 153 (1993) Statement of Michael D. Cronin. Apr.22, 1993

²⁰⁶ *Ibid.*

²⁰⁷ For further discussion on these issues as it relates to data protection see section 4.8 in Chapter IV of this thesis.

Dedicated manuals written specifically to operate terrorism data sets are extremely rare.²⁰⁸ This is for two main reasons. Firstly, security agencies such as the CIA or FBI hold terrorist data that is classified in nature and as result they are not willing to make available information that could compromise security. Secondly reluctance to divulge functional capabilities of computerised systems and more importantly the type of terrorist information held results in these type of documents being classified. An increasingly computer literate population is much more conformable with the use of technology than ever before, a point the FBI has noted.²⁰⁹ Manuals obtained by non- legitimate users could open up a system to potential violation. Almost as important, while manuals can indicate the functionality of a database system they also point the shortcomings of a system that security agencies are reluctant to admit.

For commercial organisations producing terrorism data sets such as Pinkertons, Kroll Associates or Mizell & Co. there is a general reluctance to divulge too much information about computer systems. Security is an understandable concern, however the generation and sale of reliable information to clients is the bread and butter of some of these organisations. Competition can be fierce and divulgence of computerised operations could cause potential security risks. A small but important point to note is that terrorism data set manuals are not necessarily the same as the aforementioned date set 'codebook'. Code-books generally relate specifically to the criteria set and variables coded within the data set, whilst manuals

²⁰⁸ It is important to differentiate between database manuals that are written for general application software such as *Microsoft's Access™* or *Borland's Paradox for Windows™* and dedicated terrorism database manuals provided for the operation of a terrorism database.

²⁰⁹ This refers to concerns the FBI note in their annual publication *Terrorism in the United States 1995*. The FBI voices concern over the use by terrorists of technology, in particular databases to promote terrorist activities. The transmission of secure information by terrorist groups over networks, for example bomb making recipes and computer viruses.

are usually written to help researchers and analysts operate the given software to its maximum functionality.

The RAND Corporation is one of few organisations to have published documentation on the system and software used to hold its terrorism chronologies and databases in Santa Monica until their transfer to the University of St. Andrew's Centre for Terrorism and Political Violence (CSTPV) in 1994. A slightly modified version of the same system operates at St. Andrews. Dewar and Gillogly the authors of *CODA: A Concept Organization and Development Aid For The Research Environment*²¹⁰ outline their thinking behind the development of CODA the software used to operate the RAND terrorism data sets. The main philosophy behind their project in 1982 was driven by the thought of how computers could help as a tool in policy research, in particular their use in the storage of large amounts of text based data combined with the specific needs of policy researchers. Dewar and Gillogly were sensitive to the fact that policy research is not a straightforward process. As they note:

'The key seemed to be that the research process of an individual was essentially an iterative process characterized by both a growing data base and a series of failed attempts at organising the data into a coherent whole (followed ultimately by successful attempt, of course). This led us to an hypothesis about the utility of computers "optimized" for the policy research process and from there to a list of desired characteristics for the associated computer aid.'²¹¹

The resultant 'Desiderata' was a series of functional operations that were explicitly related to the experiences of the policy researcher. The use of quick Boolean tag²¹²

²¹⁰ Dewar, *op cit.*

²¹¹ *Ibid.*, p.2.

²¹² *Ibid.*, p.5. Tag: This is a user-supplied word or phrase that is typically used in CODA for retrieving a piece of data. In other systems this is called a keyword. 'Tag' is used in CODA because it need not be something that actually appears in a record. A given record can have many tags.

searches such as AND, OR, and NOT could help minimise distracting time delay in the researchers thought processes. Other such functions as powerful tag changing capabilities could allow part or complete text documents to be changed by tags or the recall of information by data capability were suggested. As much of terrorism data is based upon date entry this facility was particularly useful. A point worth noting: CODA is not a fully based database management system with large numerical processing capabilities.²¹³ The software was written with policy researchers in mind, with the emphasis being upon text-based information. The vast majority of the RAND and RAND-St.Andrews data sets is in a narrative format. Numbers are used in the data sets for three main purposes: as unique incident identifiers,²¹⁴ date identifiers for incidents and the recording of individual, and aggregate details of injuries and fatalities. CODA was written in 1982 under a UNIX based operating system in the software language C to run on a VAX 11/780. The relevance of this technical detail lies not so much in exact software and hardware specifications but in the context and time period in which CODA was developed and its subsequent use.

The early 1980's saw the advent of what is commonly known as the personal computer or P.C. With limited application packages, processing capabilities, and the operating system MS-DOS still in its infancy,²¹⁵ the P.C. was unable to offer the powerful database facilities of modern systems. The vast majority of work was

²¹³ *Ibid.*, p.4.

²¹⁴ These unique identifiers are crucial to the integrity of any data set. They insure that each recorded terrorism incident is given a unique number avoiding duplicity of records and false data entry. In modern relational database system this is known as a key field. The use of a date field to identify an incident would not be appropriate as several incidents could have occurred on any one day and it would be impossible to determine separately within the database a unique identifier of reference number to a particular terrorism incident. For further discussion on key fields see section 4.15 of this chapter.

²¹⁵ Microsoft Disk Operating System™ (MS-DOS) acts as the file 'manager' of the personal computer. It carries out a series of simple and very complex file management tasks within the P.C. The arrival of this piece of software along with the micro-chip revolutionised the computing industry. It meant individual users were able to run and operate their own computer system without the reliance of a large and expensive mainframe systems.

carried out by large mainframe computers similar to RAND's UNIX system. The system that the RAND and RAND-St.Andrews terrorism data sets are held was specifically tailored to policy researchers needs. The RAND corporation did not intend to sell the software system for commercial purposes which meant that the software could be tailored to users needs more accurately.²¹⁶ The value of Dewar and Gillogly's work is twofold. Firstly it offers a rare insight into the thoughts behind the development of the CODA system. This is not purely from a programming point of view but from the more subtle user requirements of the policy analyst and terrorism researcher. Some of the most basic research techniques used by analysts were considered by the developers of CODA - the need to retain large amounts of narrative text and manipulate it to suite users needs. All too often data is forced to comply with existing database systems and as a result it is not a true reflection of the original data and does not meet the functional requirements of analysts. Secondly, Dewar and Gillogly offer an honest evaluation of some of CODA's shortcomings; this is refreshing and rare. One of its main limitations is the amount of users that can operate the data sets at any one time

Unlike large terrorism data sets such as the State Department's TIPOFF database on counter-terrorism²¹⁷ or the U.S. Federal Administrations Airline Incident Reporting System (AAIRS)²¹⁸ CODA was not designed for a large user audience. As the RAND and RAND-St.Andrews terrorism data sets are used for internal policy and

²¹⁶ Many modern general application database software can now be modelled to users needs without the expense of dedicated written software. However where large organisations maintain very large computer operations such as the FBI's Bomb Data Center, or the FBI's Criminal Justice Information Services Division at Clarksburg, West Virginia these data sets or databases tend to be developed 'in-house'.

²¹⁷ U.S. Department of State, *Assessing Current and Projected Threats to U.S. National Security* Statement by Assistant Secretary of State for Intelligence and Research Toby T. Gati Before the Senate Select Committee on Intelligence Washington D.C. Feb. 5th 1997.

²¹⁸ URL:<http://www.faa.gov>

research purposes external access to the data sets has not been made available.²¹⁹ Concern over the time in which CODA took to load are noted by the authors. Even in the late 1990's this is still a valid concern among relatively modern systems. The length of time it takes for CODA to carry out truncated searches was another concern. They cite the example of a truncated search on the word 'bomb'. This would return records containing the entries bomb, bomber, bombing, bombardment, bombast, bombazine.²²⁰ The method by which CODA searched the data set took quite a considerable amount of time. Despite these and other concerns a genuine attempt was made to meet the needs of policy researchers. Dewar and Gillogly's 'wish list' of other features are just applicable today for terrorism researchers using modern computerised database systems. These included bibliographic facilities, thesaurus and optical data entry tools.²²¹ This paper and the accompanying *CODA User's Manual*²²² although a little dated, offers theoretical context and sound practical guidance on the operation of the RAND/RAND-St.Andrews terrorism data sets.

One of the most common type of searches undertaken in database systems is the use of the Wild Card search. This is a powerful search facility that allow analysts to search any records in TADIMS for words that begin with 'Bomb?' or 'Kid?' The use of the unspecified suffix in lieu of full words offers a potentially wider set of records containing for example the entries Bomb, Bombers, Bombing Bombed.²²³

²¹⁹ The RAND and RAND-ST.Andrews terrorism data sets were never intended to be accessed by an external audience. Software limitations and policy concerns of accessibility of data to external users dictates that the data sets remain within RAND-St.Andrews CSTPV.

²²⁰ Dewar, *op cit*, (note 45) p.12.

²²¹ *Ibid.*, p.15.

²²² J.A. Dewar, J. Gillogly and M. Hammer *CODA User's Manual* (Santa Monica CA: RAND Corp. N-2290-RCC 1985)

²²³ *Ibid.*, Appendix D4. For more examples of querying terrorism data sets see section 4.98 of this chapter.

One of the most important benefits of a true database management system is its ability to offer analysts the facility to explain in a narrative format the circumstances or context in which an act of terrorism occurred. The codification of detailed variables can only explain in part sometimes the background or consequent events following an incident. The TADIMS system permits analysts to enter narrative details on an incident to give a more rounded picture of an event. Complex issues such as ideology or political violence are notoriously difficult to define let alone code within a database. The narrative report within TADIMS allows analysts to explain in greater detail issues that are have not been programmed to be coded or require further detailed description or explanation.²²⁴ As with any well-designed terrorism database TADIMS provides a series of 'Validation Tables' to ensure consistency of data entry on certain key fields. The fields requiring validation are Target Type, Incident Type, Nationality and Country/Region fields. Without some form of established standard on these type of fields the integrity of the database could be undermined. These are core variables in any terrorist data set and some form of pre-defined criteria should be established by the organisation operating the data set.

It would be naive to assume that all database are designed and populated with complete objectivity. Complete objectivity may be an impossible task, especially when compiling data on acts of political violence. Many project-driven data sets such as the Global Jewish Information Network or the National Council of Iran's chronology have by their very nature a political motivation behind their creation. Other databases such as the National Transportation Safety Board's Aviation

²²⁴ TADIMS is able to print just the narrative reports or full detailed reports containing coded variables as well as text.

Accident Database Safety which contains data on civil aviation accidents is designed to perform a more functional role under U.S. Federal laws and regulations.²²⁵

3.10. Database Management Systems (D.B.M.S)

A recurring problem in the field of terrorism data sets has been the interchangeability of the terms terrorism chronology, database and database management system. Clarity over both their theoretical definition and practical application would serve terrorism researchers well as part of the design process. This concern does not arise purely from worries over semantics. Inappropriate classification of terrorism data sets can misrepresent their functionality. Furthermore, the design of a terrorism chronology such as the NewsPage's daily chronology of world terrorism is likely to be a much simpler process than that of a database holding terrorism data with linked entities and relational in nature such as the FBI's National Incident Based Reporting System.²²⁶ A large section of published literature on terrorism data sets uses a broad palette of words to describe computerised terrorism data sets. These range from terrorism data banks, terrorism databases, terrorism data bases, terrorist databases to terrorism chronologies and political terrorism database.

In its simplest form chronologies on terrorism such as the Iterate or Rand-St.Andrews chronologies on international terrorism present a sequential coded data of terrorism events. Most chronologies on terrorism have a minimum of field definition or variable coding. These chronologies do not necessarily have to be held

²²⁵ The Aviation Accident Database contains data describing the aircraft, operations, personnel, environmental conditions, consequences, the probable cause, and contributing factors of civil aviation accidents within the United States, its territories and possessions, and in international waters. See: [Http://](http://)

²²⁶ The NewsPage chronology of world terrorism is a daily compilation of terrorism events derived from an array of media sources. The chronology is not exhaustive. [Http://www.newspage.com](http://www.newspage.com)

on a database system. Chronologies can operate on a text based system. Their ability to carry out more sophisticated requirements is often limited. The benefit of a computerised database or database management system lies in their ability to offer the researcher a multitude of different facilities.

Elmasri and Navathe define a database as 'a collection of related data. By data we mean known facts that can be recorded and that have implicit meaning'.²²⁷ This tight definition although useful requires further exposition. 'A database is a logically coherent collection of data with some inherent meaning. A random assortment of data cannot be referred to as a database.' Elmasri and Navathe further expand on this notion by explaining:

'A database is designed, built and populated with data for a specific purpose. It has an intended group of users and some preconceived applications in which these users are interested. A database represents some aspect of the real world, sometimes called the mini-world. Changes to the miniworld are reflected in the database'.²²⁸

Arguably the terrorism chronology could meet all of the above criteria. To attribute a terrorism chronology with such definitional criteria would be to present it in an overly sophisticated schema. In its simplest form terrorism chronologies are meant to represent 'known facts' on terrorism in an arranged order of occurrence. Some confusion can arise in the classification of terrorism data sets as chronologies can be operated on from software such as a word processor or a spreadsheet, alternatively they can be designed and generated from within a database management system. Chronologies generated from within database management systems can be derived from purpose built databases or generated from existing terrorism databases.

²²⁷ Elmasri and Navathe , *op cit*,pp.3-4.

²²⁸ *Ibid.*

3.11. Alternative approaches to terrorism data set design

Although several academics have voiced their concerns over the design and content of terrorism data sets and the constant referral to the same research base, few have offered an alternative approach to the current unsatisfactory situation. An exception to this general malaise has been some thought provoking ideas by Ted Gurr. His article '*Empirical Research on Political Terrorism: The State of the Art and How it Might be Improved*'²²⁹ presents some alternative approaches to improving empirical research and traditional terrorism data set design. Gurr notes that the majority of quantitative and empirical research is based upon the researcher consulting an established terrorism data set. This 'data first' situation Gurr argues can constrain the type of questions that can be asked of the data set and also limit the type of methodology used.²³⁰ An over-reliance, Gurr argues, on the two major publicly available terrorism data sets, RAND and ITERATE, limits the research base to international terrorism events and excludes incidents of domestic terrorism. As Gurr notes:

'I am convinced by a review of the empirical literature on political terrorism that many, perhaps most, of the important questions being raised cannot be answered adequately with the kinds of information now generally available to scholars'.²³¹

To remedy such a situation Gurr suggests that the analytic question is placed logically prior to the design of a methodology and the consequent collection of data.

There would appear to be some sense in this approach. The attraction for the

²²⁹ Gurr, *op cit*, p.117.

²³⁰ For Gurr 'Methodologies in conflict analysis are techniques for ordering information systematically and drawing inferences from that information about patterns, trends, causes, processes, and outcomes of conflict'. *Ibid*.

²³¹ *Ibid*. p.119.

terrorism analyst is that a relevant data set is established and can be finely tuned to meet the researchers methodological requirements. Furthermore, as Gurr notes the 'question first' approach 'maximises the likelihood that the researcher will get valid answers to the question.'²³² The slight downside to this data design approach is a reminder of the effort and resources required to establish, design and maintain a credible terrorism database. The temptation to use 'off-the-shelf, ready-made' terrorism data sets with their acknowledged imperfections appears to many researchers a more attractive option.

3.12. Database Organisation and Structure

The structure and organisation of terrorism databases can take on many forms. The relationship between entities, variables, values and relations defines the structure of the terrorism database at its most basic level. An entity within a database can be a field such as terrorist group or the most common entity such as the actual terrorist incident. A variable is an empirical property that takes two or more values.²³³ Variables are values that represent an entity within the database. For example where an entity is defined as a 'Source of Ransom' payment the variables could be Government, Corporate, Family, Other, including public collections or private sources. Variables can also be quantifiable, such as number of hours duration of an incident where the entity is duration of incident in hours.²³⁴ Values are representations of a variable and generally take on a numeric format, for example number of people killed. The most powerful component of this structure is the

²³² *Ibid.* p.117.

²³³ Chava Frankfort-Nachmias and David Nachmias, *Research Methods in the Social Sciences*, (London: Edward Arnold 1992), p.54.

²³⁴ Mickolus, *op cit*, , pp.526-527.

relation. Relations within a database are groups of identified entities that are related in some recognised form. Relations must have some inherent meaning, a random cluster of entities or variables is not a relation.

The organisation of databases is divided into three main types: hierarchical, network and relational. The hierarchical database structure or tree structure is based on a hierarchy of entities with pre-defined subordinate entities. The network structure is a complex link of entities with subordinates or superior entities. The relational database structure comprises of one or more two dimensional tables, these are referred to as relations. With the relational data structure data can be stored in multiple tables these tables can then be linked together.

The choice of database system to adopt for holding terrorism data for many researchers will be outwith their control, particularly analysts working for police and intelligence agencies. As part of 'best practice' computer systems departments should always consult their end users to ascertain their particular needs.²³⁵ The past twenty years has seen a gradual shift towards the adoption of relational database management systems, operating at both mainframe level and personal computer level. Research staff operating the RAND-ST. Andrew's database developed a prototype relational database system as part of its on-going policy of technological development. The attraction of adopting a relational system is the relative simplicity of its structure and the powerful functional capabilities it can perform. The relational table comprises of a two way tables with a series of rows and columns. The table contains information about a single type of entity. The table has records which has

²³⁵ Such liaison is carried out, for example the in the U.S. Department of States's Bureau of Diplomatic Security. The Bureau have an appointed member of staff acting as a liaison between themselves and the Management Information Systems Division to discuss any problems or analysts needs regarding the operation of their terrorism database systems.

data about a single occurrence of the entity. The attraction of this approach lies in its relative simplicity. The complex structure of hierarchical and network database structures does not make a particularly easy system for users to understand. With the relational model tables are presented in two-dimensional format. Several other features of the relational design make it a particularly powerful database tool. Apart from the ability to enter terrorism data and query the tables, with correct design procedures it is possible to establish relationships between two or more linked databases and query the linked tables. This is a powerful facility, and addresses Gurr's challenge of linking or merging terrorist information from two separate databases to provide specific data on domestic and international terrorism.²³⁶ Links are established between tables through the creation of common entities or fields. The rigidity of a pre-defined set of relationships as part of the database structure is not required thus allowing the user to establish relationships that meet their own requirements. Furthermore with relational database structures designers are not required to meet narrow informational requirements restricting researchers use of the database.

The move from mainframe to personal computer held terrorism data sets is the result of several factors. Firstly the advent of relatively cheap but extremely powerful personal computers, with the ability to operate sophisticated relational database management system and general application packages is now a reality.²³⁷

²³⁶ Gurr , *op cit*, (note 126), p.118. While it would be perfectly feasible to join (link) a domestic and international terrorism database together the design of both data sets would require very careful consideration to ensure the relationships between the tables have integrity. Gurr mentions both linkage and merging information from separate terrorism data sets. The linkage of two terrorism data sets to establish a relationship between them using a common field e.g. Country is different from merging two data sets. The merger of data sets involves combining one data set (source) with the other (target) data set.

²³⁷ Direct transfer of terrorism data sets from mainframe software to P.C. based applications is not always a simple task. For example the CODA system holding the RAND-St. Andrews terrorism chronologies cannot be

An ever-increasing base of computer literate analysts requiring ever-more sophisticated information has undoubtedly increased the demand for P.C. based systems to hold terrorism data. Communication between mainframe and P.C. based systems has developed at a frenetic pace in the past few years. The advent of network technologies and subsequent explosion of internet use and accessibility by P.C. has added to the on-going momentum. Not all terrorism data sets or databases operate on a P.C. system alone. More powerful mainframe systems that required to provide large user requirements among federal and security agencies need more than a P.C. to carry out their security and operational requirements. For example, restricted access database systems holding terrorism data such as IBIS (Interagency Border Inspection System), the FBI's Terrorism Information System (TIS) database or the Australian Bomb Data Centre's database of bombing incidents operate from a mainframe, mini-computer and P.C. basis, and are operated on Local Area Networks (LAN's) and Wide Area Networks (WAN's).

The move towards P.C based networked systems, backed up by mini or mainframe computers appears to growing. The Jafee Center for Strategic Studies at Tel-Aviv University have recently adopted a new computer system running on a series of Pentium P.C.'s under Window's 95[®] networked to a Windows NT server, using Lotus Notes[®]. The system operated by JCSS's Information Center will enable the establishment of an integrative approach to its information management needs in the areas of International Relations (including terrorism and political violence), Politics, Middle Eastern studies. The University of St. Andrews's Centre for the Study

directly transferred onto a P.C. database application without a large amount of development work. The RAND-St. Andrews system operates however, from a P.C. based interface. The work involved in transferring and re-coding all the terrorism variables would be considerable.

of Terrorism and Political Violence (CSTPV) have recently carried out a feasibility study with the possibility of upgrading its existing computer operations to a Windows based environment, operating its terrorism chronologies under and databases in P.C. based application software.

For terrorism database designers the issue of hardware and software is an important consideration in the daily operation of databases if they are to satisfy researchers and analysts needs. The type of hardware and software adopted is particularly vital if they are required interface with external computer systems, networks or the Internet. Compatibility is the key point. The need to access terrorism data not only locally but perhaps from remote locations, such as police use of the Violent Gang and Terrorist Organisations File require some form a compatibility and standardisation in design. Even among research institutes and agencies holding terrorism data with limited public availability, the need internally for compatibility of systems appears to be growing.

3. 13. Advantages and disadvantages of database management systems

Historically many analysts and academics designing computerised terrorism data sets have had little choice as to the software used in the development of the data sets. Lack of availability of appropriate software and limited knowledge of design procedures resulted in a large variety of differing systems holding terrorism data. Among some of the earliest terrorism data sets to be computerised were the CIA's File on International Terrorist Events - FITE (1968), the BDM Corporation's Terrorism Data Base (1965) and the Defense Intelligence Agency's Significant Terrorist Incident

File - STIF (1970).²³⁸ All of these data sets were coded and took the form of chronologies. Even Mickolus's chronologies on terrorism, one of the few enduring computerised data sets on terrorism is still maintained on a text based system with coded ancillary files.²³⁹ There are several advantages for researchers from a design angle in choosing to hold terrorism data in a chronological format. Firstly, the application software required to hold and maintain the chronologies is relatively inexpensive to purchase. Many modern WindowsTM based text editors, word processors, spreadsheets and HTML (Hypertext Mark-up Language) format for Internet are able to adequately operate terrorism chronologies.²⁴⁰ Secondly, the expertise required at both design and maintenance level is minimal compared to the operation of a fully fledged database management system such Interpol's Criminal Information System (CIS) or the FBI's Violent Group and Terrorist Organizations File (VGTOF). However the design and maintenance of terrorism chronologies should not be completely underestimated. The apparent simplicity of entering incident data into a chronology should not overshadow the basic requirement of any credible data set on terrorism: integrity. Definition, source data and agreed coding procedures all have to be adhered to in the operation of a terrorism chronology. Fowler, Gurr and Ross have voiced about the abundance of chronologies at the expense of other

²³⁸ For further information on these data sets and others see William Folwer, *op cit*, Appendix, pp.33-40.

²³⁹ Mickolus, *op cit*.

²⁴⁰ For an example of terrorism incidents stored in spreadsheet format or imported as a tab delimited text file into database see the Southern Regional Critical Issues Forum Student Database of Violence and Terrorism. This data sets was compiled by Southern Regional CIF students searching the *CNN* Internet Website archives and lists acts of violence and terrorism. [Http://www.tocomplete](http://www.tocomplete). For examples of terrorism chronologies held in HTML format on the Internet see the FBI's Terrorism in the United States 1995. [Http://www.fbi.gov/publish/terror/terrorin.htm](http://www.fbi.gov/publish/terror/terrorin.htm) Alternatively the United States Department of State Counter-Terrorism Rewards program details a chronological list of terrorism incidents in HTML format at [Http://www.heroes.net/pub/heroes/index.html](http://www.heroes.net/pub/heroes/index.html) For other terrorism chronologies in HTML format see Save Our Sri Lanka from Terrorism at [Http://www.case.cioe.com/~sos/terror.html](http://www.case.cioe.com/~sos/terror.html) or the Emergency Response & Research Institute's Bomb Threat Chronology 1997 at [Http://www.emergency.com/bomb0197.htm](http://www.emergency.com/bomb0197.htm)

forms of terrorism data sets, in many respects they have valid points.²⁴¹ However, computerised terrorism chronologies will never be a 'glamorous' tool in the league of sophisticated software development. By their very nature they offer data on terrorism incidents in order of occurrence. The maintenance of accurate, up-to-date terrorism chronologies as an on-going process over a consistently long period of years is a task not to be underestimated. Their basic usefulness outweighs the temptation to opt for overly sophisticated systems for holding basic terrorism data.

The alternative choice by intelligence agencies and academics of designing and operating a terrorism database or database management system requires very careful thought and a considerable amount of resources if the data sets are to be maintained on an on-going basis and have integrity. Database management system offers terrorism researchers several advantages over traditional chronologies on terrorism. In a traditional file approach terrorism chronologies are designed to meet the needs of the researcher or analyst working on certain defined tasks, such as the Deutsch and Magowan's Northern Ireland, 1968-1973: A Chronology of Events or Kohl and Litt's Urban Guerrilla Warfare: Argentina: Chronology.²⁴² Traditional file formats also serve general terrorism chronologies such as Mickolus's ITERATE data sets or McGuire's Security Intelligence Report.²⁴³ Researchers using these data sets are generally restricted to the framework provided by the software. Multiple terrorism chronologies or data sets created in this format produce a certain amount of wastage or what commonly is referred to as redundancy. The need to maintain

²⁴¹ Fowler (note 16), Ted Robert Gurr, 'Empirical Research on Terrorism: The State of the Art and How it Might be Improved', in Robert O. Slater and Michael Stohl (eds.), *Current Perspectives on International Terrorism* (London: Macmillan, 1988) p.144. Ross, *op cit*, p.49.

²⁴² Schmid & Jongman, *op cit*, p.158, p.164.

²⁴³ Mickolus, *op cit*, McGuire, *op cit*,

and update duplicate incident records can cause inconsistency and requires vigilance when comparing data sets. As Fowler notes:

‘Most current data-collection efforts are devoted to the development of chronologies of terrorism. Everyone seems to be collecting the same data over and over again. ...[W]e are suggesting that the data-collection movement has matured to the point that the development of different kinds of data bases would be worthwhile’.²⁴⁴

The advantage of the database schema for terrorism data is that only one single repository of data is established and maintained. Data definition of variables and meta-data on terrorism variables requires only to be defined once. Furthermore several users can access the database for individual needs and requirements. The FBI’s Violent Gang and Terrorist Organizations File (VGTOF) operates on such a basis providing every U.S. law enforcement agency with access to, and where permitted, to add, delete and modify the database.²⁴⁵

The adoption of a database system to hold and manipulate terrorism data provides analysts with several benefits that are not attached to more traditional file handling systems. These benefits include the creation of a system catalogue, insulation between the DBMS and data, data abstraction, powerful querying facilities and the ability to provide users with multiple views of data.

As part of the overall database schema a terrorism database should also provide accompanying documentation describing the design of the database, variables used and any other relevant information of use to database designers and terrorism analysts. Commonly known as the system catalogue, it will detail the file structure of the database e.g. relational, hierarchical or network. The catalogue

²⁴⁴ Fowler , *op cit*,(note 16) p.28.

²⁴⁵ U.S. Department of Justice , *op cit*. For Further information on the Violent Gang and Terrorist Organizations File see Chapter 4. of this thesis.

provides the DBMS with information as part of its operation. The catalogue will also include details on variables within the database. For example, a variable [field] such as number of casualties from a bombing/terrorism incident would normally be assigned as a numeric field within a terrorism database.²⁴⁶ The catalogue would detail this. In addition to a description of the data types used within the database the catalogue permits designers and analysts to store more detailed narrative as to why certain variables have been chosen as part of coding criteria used by agencies or terrorism researchers. This type of data - data about data is called meta-data. The value of meta-data is often underestimated by academics and others when designing databases. Much time and effort is spent on the collection of terrorism data, its coding and eventual operation. The creation of a system catalogue and meta-data is either ignored or regarded as a time consuming luxury. This is unfortunate as many terrorism data sets (chronologies and databases) have undergone considerable change since their original inception. The Pinkerton Risk Assessment Service database on terrorism was originally operated by Risks International, Inc. The Rand Chronologies and Databases on International Terrorism were transferred in 1994 from their original base at the RAND Corporation in Santa Monica CA. to become the RAND-St. Andrews Chronologies on International Terrorism at the University of St. Andrews Centre for the Study of Terrorism and Political Violence. In August 1997 Kroll Associates a major U.S. provider of risk management and corporate intelligence

²⁴⁶ Terrorism databases contain many data types that should be documented within the catalogue.

Common Data Types used in Terrorism Databases and Data Sets

Data Type:	Text	Memo	Number	Date/Time
Variable	Incident	Lengthy narrative on	Number of	Confirmation of exact
Type:	description	incident or other terrorist	casualties,	date and time of
		details	injuries, cost of	incident(s) if
			incident	available.

For further details on data types used within computerised terrorism databases see Chapter 4 of thesis.

(including Country Risk Chronologies™ on terrorism and political violence) announced its intention to merge with the O’Gara Company to become The Kroll-O’Gara Company. The need for documentation and meta-data on terrorism data sets is essential not only for professional documentation, software execution and archival reasons. Over a period of years organisations change, computer systems change, methods of coding terrorism incidents change and professionals working on terrorism data set move on.²⁴⁷ Without such information the task of computer and terrorism analysts operating databases is made much difficult. Publicly available systems catalogues and meta-data on terrorism databases are often difficult to obtain. Classification restrictions with intelligence agencies, non-publication, or a general reluctance to release such information particularly among commercial operators of terrorism data sets has resulted in a paucity of data. Similar-like catalogues and meta-data on terrorism are however not without precedent.

Terrorism data sets such as *Domestic Terrorism: Assessment of State and Local Preparedness in the United States, 1992* and *Political Violence in the United States 1819-1968* available through the Inter-university Consortium for Political and Social Research (ICPSR) are accompanied by data collection descriptions and codebooks.²⁴⁸ Although these are not strictly systems catalogues they offer an excellent example of some of the core type of data elements and meta-data that

²⁴⁷ The responsibility for publishing data on international terrorism was given to the U.S. State Department by the CIA in 1981 as part of its policy of pursuing a lower public profile. The entire data set was back dated and re-coded from 1968 onwards. This re-coding of data is a classic example of changes that should be noted in the system catalogue. The change of calculations brought with it allegations that the Reagan Administration had re-designed the coding of the database for foreign policy purposes, at the expense of true definitional integrity. See: Charles Mohr, “Data on Terrorism Under U.S. Revision,” *The New York Times*, 24th April 1981, p A17 also George Lardner, “CIA Report Adds Thousands of Incidents to Statistics on International Terrorism,” *Washington Post*, 16th June 1981, p A10.

²⁴⁸ Kevin Jack Riley and Bruce Hoffman, *Domestic Terrorism: Assessment of State and Local Preparedness in the United States, 1992* [Computer file]. ICPSR version. Santa Monica, CA: RAND Corporation [producer], 1992. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [distributor] 1996. ICPSR 6566. Many ICPSR data sets provide an abstract, codebook, and data set in File Transfer Protocol (FTP) via the Internet. Large data sets tend to be sent in a compressed Zip format.

should be contained within a terrorism database's system catalogue. Available through user registration and Internet access the ICPSR study description provides a template that all data sets being registered with ICPSR must strictly adhere to. The ICPSR Study Description Manual requires core details on the data set to be recorded in addition to more detailed elements. These fields include: citation, data source and format, date of collection, funding agency, investigators, variable count, universe and time period.²⁴⁹ The work on entering details into a system catalogue may initially be a lengthy process and is often a distraction to the purpose: the creation of a terrorism database. Researchers benefit in the long run in that standard information on terrorism data sets and databases is established; a situation that until now, except for the efforts of Fowler, has been sorely lacking.²⁵⁰ From a research angle it would be unrealistic to assume that meta-data on terrorism data sets provide all the required answers for a comparative analysis of such data sets. Differing definitional criteria on what constitutes an act of terrorism, variance in sources used and a diversity of variables make it difficult to establish standard comparative figures. Furthermore, a multitude of remits from project-specific terrorism data sets such as ATIC to general purpose chronologies and databases such as INTER, add to the complexities of comparing data sets.²⁵¹ Despite problems over quantitative comparative analysis of terrorism data sets the system catalogue provide useful detail on software and hardware systems used in terrorism data set.

²⁴⁹ For a fully detailed list of information required by ICPSR when lodging data sets see: [Http://www.icpsr.umich.edu/template.html#INVESTIGATOR](http://www.icpsr.umich.edu/template.html#INVESTIGATOR)

²⁵⁰ Fowler (note 16). For a summary of terrorism databases see Appendix: Description of Individual Data Bases. This description of terrorism data bases is a little dated with minimal technical detail. It does however, provide useful basic information on some of the earliest computerised terrorism chronologies and data bases.

²⁵¹ Jeffrey Ian Ross, 'Attributes of Domestic Political Terrorism in Canada, 1960-1985', *Terrorism*, Vol. 11 pp.213-233. *INTER International Terrorism in 1987* (Jerusalem: The Jerusalem Post 1987).

Information on time-periods for data sets, changes in coding procedures, geographic spread of terrorism data sets and institutional or individual origins of the data set provide a more holistic view. Furthermore, aside from the functional operation of the database, what systems catalogues do offer is standards, consistency and integrity. The requirement for terrorism database designers to adhere to providing at least a minimum amount of information would provide a benchmark and standard. From this point, consistency can be maintained offering researchers some meta-data with integrity.

The move towards co-ordination and some form of standard in the development of computerised terrorism data sets would be a welcome development. Reluctance particularly on the part of security agencies and commercial providers of terrorism data to do so, is, in part understandable. National security concerns or commercial competition among private organisations collating and selling intelligence and terrorism data has made the issue of co-operation a sensitive issue. Security agencies have in recent years been encouraged and appear more willing to co-operate on the exchange of terrorism information. Initiatives promoting the exchange of 'basic information concerning persons or organizations suspected of belonging to or being connected with terrorist networks' were presented at the G7 (P8) ministerial meeting in Paris in the summer of 1996.²⁵² Equivalent exchanges of information on system catalogues, meta-data and design methodologies used to retain terrorist data appear less apparent. With the proposed development of a forensic science database, which would act as a clearinghouse for

²⁵² United States Department of State. Ministerial Meeting on Terrorism, Paris. Statement by U.S. Attorney General Janet Reno at Ministerial Meeting in Paris, France, July 30th, 1996. For full statement see: [Http://www.state.gov/www/global/terrorism/reno.html](http://www.state.gov/www/global/terrorism/reno.html) For further discussion on co-operation and exchange of terrorism data see Chapter VI. of this thesis pxx-xx.

evidence on terrorist crime, initiated by the FBI and to be used by all G8 members common entry and system procedures will be required.²⁵³

No attempt so far has been made among terrorism analysts or data set designers to create a computerised database of terrorism databases, chronologies or data sets. Such a task however is not without precedent in the field of international conflict. In his *Handbook of Datasets on Crises and Wars 1495-1988*^{AD} Cioffi-Revilla demonstrates a standard format for conflict data set profile using the Interstate Conflict Datasets Catalog (ICDC) standard.²⁵⁴ The template presented in table 3.3 below offers terrorism researchers a framework from which a standard profile could potentially be established.

Table 3.4. Codesheet Model for ICDC International Standard²⁵⁵

Data Set Name:			
DDIR ID: ²⁵⁶	Event Type:	Info.Update ²⁵⁷	IHCD ID:
Principal Investigator(s):			
Generic Event:	Historic Era	Begins:	Ends:
Event Definition: ²⁵⁸			
Source of Event Definition:			

²⁵³ United States Department of State. Combating Terrorism: The Paris Ministerial. Fact sheet released at the Ministerial Meeting on Terrorism in Paris, France, July 30th 1996. p.2. For full statement see: [Http://www.state.gov/www/global/terrorism/fs_achievements.html](http://www.state.gov/www/global/terrorism/fs_achievements.html)

²⁵⁴ Claudio Cioffi-Revilla, *The Scientific Measurement of International Conflict: Handbook of Datasets on Crises and Wars 1495-1988*^{AD}. (Boulder Colorado: Lynne Rienner 1990), pp.13-17.

²⁵⁵ *Ibid.* For a complete explanation of the field descriptors see pp.14-p17.

²⁵⁶ This is the official ID number of the data set.

²⁵⁷ This refers to the most recent update of the data set profile.

²⁵⁸ Event Definition is the operational definition of the basic event unit, derived if possible from the data sets codebook.

Number of Events:
 Actor(s):
 Target(s):
 Event Fields: ²⁵⁹
 Event Source(s):
 Published Data Sources: ²⁶⁰
 Applied Publications: ²⁶¹
 Access to M.R.-Format: ²⁶²
 Remarks:
 References:

The documentation of terrorism data sets in some form of standard profile is beneficial for four principle reasons. Firstly a standard would be established and integrity maintained. Secondly, classification of the data set is established, for example terrorism chronology, database or true-database management system. Thirdly, the content of the data set is understood i.e. data on terrorist group profiles, incidents or tactics. Fourthly, accessibility of terrorism data sets could be made available to other social scientists or researchers via such mediums as CESSDA (Council of European Social Data Archives) on the Internet.²⁶³ Furthermore, the benefits of computerised data set profiles compared to traditional hard copy printed references takes on yet an additional dimension as Cioffi-Revilla argues:

²⁵⁹ This refers to the 'List of the variables coded or measured for each event contained in the dataset.' Revilla, *op cit*, p.16.

²⁶⁰ This is 'Printed publication(s), if any, where the raw dataset may be found'. Revilla (note 140), p.16.)

²⁶¹ The 'Applied Publications' field refers to 'A selection of research publications that have used the dataset'. Cioffi-Revilla, *op cit*, p.16.

²⁶² This refers to the machine readable or computerised format in which the data set can be viewed. When available, ICPSR file numbers are detailed. These data sets are available via the Internet. Terrorism data sets are available in various formats including HTML format and PK. ZIP format. See: [Http://www.fbi.gov/publish/terror/terrusa.htm](http://www.fbi.gov/publish/terror/terrusa.htm) for the FBI's *Terrorism in the United States 1995*. It should be noted the available machine readable format of such terrorism data sets is not always a true indicator of the software used in the original data set or database.

²⁶³ The Council of European Social Science Data Archives (CESSDA) promotes the acquisition, archiving and distribution of electronic data for use by social scientists within Europe for research and teaching purposes. Data sets are accessible through a common interface entry point on their Web page. Internet access to North American archives and other social science data sets world-wide is also provided. Internet Web site: [Http://www.nsd.uib.no/Cessda/IDC/](http://www.nsd.uib.no/Cessda/IDC/) For further discussion on Internet access to social science data sets see Chapter 6 of this thesis page xx.

'... for a book (even in the case of a famous work) most scientists will not be interested in the names and references of others who have used such a book... in the case of a dataset such information on previous uses and applications can be very useful, indeed vital, in learning about ways in which the dataset in question has been used, or it may be critical for obtaining direct practical advice on the analytic potential and limitations of the dataset'.²⁶⁴

The lack of a well developed literature base on the rôle of information technology vis-à-vis terrorism studies, and in general within the wider field of international relations, highlights an evolving problem that needs to be addressed. As Cioffi-Revilla notes:

'Simple descriptive problems such as the ones just mentioned (choosing a proper descriptive structure of information) may often be compounded in new interdisciplinary areas of research such as this - at the nexus between international relations, world politics, conflict and peace research - where there is no professionally set scientific standard for describing electronic media such as datasets, computer programs and graphic files'.²⁶⁵

Several other factors make the choice of adopting a database approach to retaining terrorism data more attractive than that of the traditional filing systems. The D.B.M.S. offers users insulation between the database program and the actual data. In a traditional file the structure of the data file is embedded in the programs that access that file. A change in the structure of the file will need to be reflected in all of the programs that access the file. In a DBMS program the access programs are written independently of the actual database file. This is known as program-data independence.²⁶⁶ The benefits are twofold: changes to the database structure needs only to be made once, integrity and consistency is maintained across all access programs to the database. Computerised terrorism chronologies such as ITERATE

²⁶⁴ Cioffi-Revilla, *op cit*, p.12.

²⁶⁵ *Ibid.*

²⁶⁶ For a fully detailed explanation of these concepts see Elmasri & Navathe, *op cit*, p.8.

which is not supported on a database management system would have to ensure that changes to one part of the chronology were reflected (where relevant) in other parts of the data set.

Multiple access to databases such as the U.S. State Department's Tipoff database, or the FBI's VGTOF database which is accessed by multiple users requiring different forms of data such as reports summaries, individual profiles of terrorist or statistics benefit from program-data independence. The databases are not put at risk from ad-hoc adjustments to its structure by analysts or law enforcement officials using the database.

Many of the benefits of holding terrorism data on a database management system such program-data independence will appear to be rather abstract and irrelevant to most analysts needs. Such functions of the database management system however provide a seamless service in the background that would quickly be noticed if they were not available. Of particular benefit to terrorism researchers and analysts adopting a DBMS system to hold terrorism data is the databases ability to support multiple 'views' of data. These multiple 'views' of the same or different data can take many forms including simple views of tables (databases), input forms for data entry or reports generated from the database. These facilities particularly benefits intelligence agencies and academic organisations, where multiple users of a database have differing data requirements that would not be satisfied through a simple chronological or text based presentation. Advanced systems such as Interpol's Automated Search Facility (ASF) database permits National Central Bureau's (NCB's) to request various forms and 'views' of information such as a suspect individual's phonetic criteria, date of birth, known aliases passport

documents.²⁶⁷ The system can also transfer an individual's photograph and their fingerprint's with related intelligence detail in a variety of languages from English, French and Spanish to Arabic. Such sophistication and detail will tend to be beyond the remit or legal boundaries of academic terrorism data sets. The ability however to generate simple and complex 'views' of terrorism data in the form of summary statistics of terrorist incidents, subsets of data, chronological data, reports and graphics such as pie and bar charts or photographs all derived from the same database or relationally linked databases is an attractive option.

3.14. Conclusions

The post 9/11 era has witnessed the development of many terrorism databases. All of these databases offer insight into some of the key challenges presented to academics, government and private organisations. The issues involved in the design and maintenance of terrorism data sets are often complex and should not be underestimated. A sound understanding of the area of terrorism and political violence combined with computer literate skills, particularly data analysis and database management systems, would be an ideal profile for anyone developing and maintaining a terrorism database. Despite this rare profile, many computerised databases on terrorism operate reasonably well. Requests by researchers and analysts for improved systems are understandable, especially if they are to meet the demands of ever increasing information on terrorism data.

A note of caution however should be sounded. The speed and sophistication of modern computerised systems should not blind analysts to more fundamental

²⁶⁷ Interpol, *The machinery for international police co-operation*.
[Http://193.123.144.14/interpol-pr/Machinery.html](http://193.123.144.14/interpol-pr/Machinery.html) p. 3.

issues that need to be addressed by designers, researchers and analysts. A sound, intuitive knowledge of the area of terrorism, combined with the adherence to professional standards should be a guiding principle in the development and maintenance of terrorism databases. The fact that something is entered on computer neither makes it legitimate or true. Integrity must be maintained. The rush towards newer, faster systems at the expense of integrity and validity would render any terrorism database system useless. Adoption of a more professional approach to the design of terrorism databases would serve both database designers and terrorism analysts well. With increased documentation, such as systems catalogues and user manuals, the potential for databases that move closer to meeting the needs of terrorism researchers and analysts will hopefully be achieved.

The eclectic issues involved in the design of computerised terrorism databases requires not just a generic approach to database design. Complex and sensitive political issues combined with an appreciation of database operations provide a challenge to researchers of some considerable degree. An appreciation of the many issues involved in the design of terrorism data sets provides a stimulus for assessing the actual current availability of computerised terrorism data sets. Knowledge of other terrorism data sets can often be a valuable benchmark from which to assess standards. The next chapter will provide such a comparative analysis.

CHAPTER IV

POST 9/11: AN ANALYSIS OF TERRORISM AND COUNTER- TERRORISM DATABASES: THE PUBLIC, THE PRIVATE AND THE IN-BETWEEN

4.1. Introduction

A multitude of terrorism data sets with disparate backgrounds and varying remits have evolved in the field of terrorism research over the past thirty years. The majority of data sets on political violence however, are based mainly in North America and Western Europe. This imbalance has left knowledge on political violence data sets in the southern hemisphere scattered and incomplete. Moreover, with very little descriptive and comparative information on computerised terrorism data sets, our understanding of the field has been somewhat limited. The work of Fowler, and Schmid and Jongman on terrorism data sets has provided useful early guidance; however, both time and technology have moved on.²⁶⁸

This chapter will assess the variety of elements that are associated with the operation of computerised terrorism data sets. These include factors such as definition, aggregate data comparability, types of data set, and the scope and content of terrorism data sets. The almost anarchic development of terrorism data sets has left their classification ill-defined. Technological advancement in hardware and software systems coupled with increasing computer literacy among terrorism

²⁶⁸ For further details on early analysis of terrorism data sets see: William Warner Fowler, *Terrorism Data Bases: A Comparison of Missions, Methods, and Systems*. (Santa Monica CA: RAND Corp., N-1503-RC. 1981). Also: A.P. Schmid and A.J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*. 2nd. Ed. (New Brunswick USA Transaction Books 1988).

researchers has increased the demand for information on databases that will allow comparison to take place. Furthermore, terrorism analysts increasingly require detailed information on hardware and database software issues, as a basis from which informed decisions can be made on the operation of data sets.

Moreover, this chapter will provide a detailed analysis of the terrorism databases that are currently available. These have different levels of accessibility, from fully publicly accessible, to private subscription-based, to government classified databases. This chapter will examine each of these in turn, with particular reference to publicly accessible databases, given that these are the ones where more information is available. Despite this accessibility, however, there remains no up-to-date comprehensive listing of these, and this chapter will provide one before examining the nature of private and government information in more detail.²⁶⁹

4.2 Examining Terrorism Data Sets

Examining computerised terrorism data sets is complex task, requiring at times many qualifiers to explain a less than coherent subject field. A simple comparative analysis, for example, of existing computerised data sets, based on such factors as aggregate number of terrorism incidents recorded or the number of terrorist variables used, can provide terrorism researchers with little, if any information on the type of data sets appropriate to researchers needs.²⁷⁰ Careful thought as to the type of elements that are compared will provide more appropriate answers to researchers needs. The

²⁶⁹The most recent inventory was the report prepared in November 2003 by the Federal Research Division, Library of Congress, titled 'Inventory and Assessment of Databases Relevant for Social Science Research on Terrorism', by Alice R. Buchalter and Glenn Curtis.

²⁷⁰ Differing definitional criteria on what constitutes an act of terrorism makes cross-aggregate comparisons of terrorism data sets a less than exact science. For a comparison of comparative aggregate totals of terrorist incidents over a series of data sets see: Jongman, A. J. 'Trends in International and Domestic Terrorism in Western Europe, 1968-1988' *Terrorism and Political Violence* Vol 4. No. 4. Winter 1992. pp.26-76.

most common type of comparisons made of terrorism data sets is aggregate data analysis. Research by Jongman illustrates the usefulness and potential difficulties involved in such analysis.²⁷¹ Other comparative factors include definition of terrorism incidents, data selection, geographic spread, scope of the data set and time frames used. All of these techniques provide useful information, however other comparative approaches need to be addressed. The need for additional comparative information has been driven by technological development, accessibility to data, and an increase in different types of computerised terrorism data sets. New and established data sets can be analysed at two further levels. The first is at an operational level, such as information on the type of chronology, database, hardware and software used. The second level is classificatory, for example government, academic or privately operated data sets. With increasing global communications, Internet access, and co-operation between governments, academics and industry within the terrorism field, relevant, up-to-date and standardised comparative data is crucial. In analysing public databases, this analysis will assess the following elements: the official name of the data base, the host institution/organisation, the website, contact details, accessibility, unit of analysis, the scope of the database, the temporal period covered, the principle source material, and the key variables analysed. Early comparative analysis of computerised terrorism data sets in the 1960's and 1970's tended to be somewhat limited, due to the relative infancy of the field and the small research base of data sets from which to work from. Post- 9/11, a large array of computerised data sets on terrorism exist, with diverse remits, and varying quality and accessibility that is often conditional or

²⁷¹ Ibid.

restricted. Moreover, in recent years a new and critical remit for computerised terrorism data sets has been promoted: their use as ‘real-time’ terrorism incident response tools.

Functional classification and description of data sets, chronologies and databases.

Given the large amount of data sets, chronologies and databases discussed below, it is worth providing a simple classificatory description of the differences between each system.²⁷²

Table 4.1 Simple Functional Description of Data Sets, Chronologies and Databases

Classification	Data Type	Notes
Data Set	Numerical, Textual Variables	Data can be imported into spreadsheets, statistical packages and database systems.
Chronology	Numerical, Textual Variables	Generally restricted in functionality, presenting data in chronological format
Database	Numerical, Textual Variables, Graphics, Hyperlinks, Sound, Film Media	Sophisticated software that allows complex storage of data with powerful manipulating features. For example, input of data, deletion, update, querying of data, relational links to other databases, generation of reports, arithmetical and statistical reporting as well as form generation. Sophisticated database software can also host generic data sets and chronologies.

²⁷² A full definition of the term ‘Database’ is outlined in Section 1.5 of this thesis, Chapter 1, page 12.

4.3 The Public Profile

By their very nature, and because of their accessibility, the design and practicality of publicly available databases is particularly significant. Detailed below is an examination of the principal public databases currently available. An analysis of these will allow a wider examination of the current state-of-the-art in terrorism database provision. Each will begin with meta-data, before a more extended narrative. Table 4.2 below classifies each of the 20 public profile databases.

Table 4.2 Classification of Public Profile Data Sets, Chronologies and Databases

	Name	Classification
1.	Global Terrorism Database (GTD)	Database
2.	Worldwide Incidents Tracking System (WITS)	Database
3.	ITERATE - International Terrorism: Attributes of Terrorist Events	Chronology/Data Sets
4.	MIPT Terrorism Knowledge Base	Database
5.	RAND – Worldwide Terrorism Incident Database (RWTID)	Database
6.	Country Reports on Terrorism – United States Department of State	Narrative Report
7.	Terrorism in Western Europe: Events Data (TWEED)	Data Sets
8.	South Asia Terrorism Portal (SATP)	Narrative Report/Data Sets
9.	The International Policy Institute for Counter-Terrorism (ICT) – Terrorist Incident Database	Database
10.	Political Terror Scale (PTS)	Data Sets
11.	The American Terrorism Study	Data Sets
12.	Europol Terrorism Situation and Trend Report (TE-SAT)	Narrative Report
13.	Global Pathfinder	Database
14.	The Institute for the Study of Violent Groups (ISVG) Database	Database
15.	Monterey WMD Terrorism Database	Database
16.	Armed Conflict Database	Database
17.	Iraq Body Count (IBC)	Database
18.	Illicit Trafficking Database (ITDB) International Atomic Energy Agency	Database
19.	Uppsala Conflict Data Program (UCDP)	Database/Data sets
20.	The Minorities at Risk (MIR) Project	Data Sets

Name:	Global Terrorism Database (GTD)
Parent Host	National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland, United States.
Website:	http://www.start.umd.edu/gtd/
E-mail:	infostart@start.umd.edu
Access:	Free
Unit of Analysis	Terrorist Incident
Scope:	Domestic and International Terrorism
Period Covered:	1970-2007 and on-going
Principle sources	Publicly available open-source material
Key Variables	Incident date, region, country, state/province, city, perpetrator group name, tactic used in attack, nature of the target. (See GTD website for other variables)

Global Terrorism Database (GTD)

Introduction

The University of Maryland's National Consortium manages the Global Terrorism Database (GTD), publicly launched in 2007, for the Study of Terrorism and Responses to Terrorism (START). The GTD forms part of a new generation of web-based terrorism databases. It differs from some of its counterparts in that it records domestic, transnational and international incidents of terrorism. The database is Open Source and records processed and structured information on more than 80,000 terrorist attacks.

Historical Background and Database Development

The original source data for the GTD came from data collected by Pinkerton Global Intelligence Service (PGIS) from 1970-1997. Serving the United States private business sector, Pinkerton's original database was designed for risk analysis advice. Its aim was ambitious: to code every terrorist occurrence worldwide, over time. A variety of multi-lingual news sources were used. Pinkerton's definition of terrorism was broad: 'The threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious or social goal through fear, coercion or intimidation'.

In 2001 Pinkerton's donated their entire data sets to START. Initially funded by the National Institute of Justice, START researchers refined, added to, and coded the original Pinkerton data into a new database system, completing the task in December 2005. Additional funding in 2006 from the Department of Homeland Security (DHS) allowed the START team, in collaboration with the Center for Terrorism and Intelligence Studies (CETIS) to update the GTD to 2007. This process was completed by August 2008. In the spring of 2008 a new partner joined data collection efforts with START on the GTD. Researchers at the Institute for the Study of Violent Groups (ISVG) at the University of New Haven CT. began contributing data for integration into the Global Terrorism Database.

An unusual feature of the early version of the GTD was that it was split into two data sets: GTD1 and GTD2. The rationale for the split was historical. The original Pinkerton data covering the period 1970-1997 had a limited set of around 45 variables. This data set was named GTD1. Using the original Pinkerton's generic

incident cards, a web-based entry system was devised to code the 61,637 events (weighted 68,986) into a database system. Data verification was undertaken. Auto-fill fields were also generated to provide additional data where required. Key variables within GTD1 included: group name, type of terrorist incident, date of incident, country, region, city and location. Other main entries included: nature of target, identity of the target, e.g. corporation, nationality of target, weapons used, incident success and damage sustained. GTD1 also coded specific damage to United States interests. Further variables detailed information on kidnappings, hostages, ransoms and hijackings. Despite extensive searches, the 1993 data for GTD1 was found to be missing; this was due to the loss of data in an office move by Pinkerton. START is retrospectively attempting to generate the 1993 data from other sources. With improved data collection methods and the addition of new types of data, the codified data from 1998 onwards was named GTD2. This second database was built and developed on behalf of START by the Center for Terrorism and Intelligence Studies (CETIS). The eventual aim was to codify the GTD1 data set to be compliant with GTD2; thus providing a unitary longitudinal database of terrorist incidents from 1970 until the present day. In the autumn of 2008 the START team completed the synthesis of GTD1 and GTD2; the database simply being referred to as the Global Terrorism Database (GTD). The new GTD database contains over 120 variables of which approximately 75 variables can be used for quantitative and statistical purposes.

Sources

Whereas GTD1 (1970-1997) used single open-source reports collected by Pinkerton, GTD2 and the newly synthesized GTD used an array of independent open source material, or, where available, a single “highly credible” source. These sources included books, electronic archives from news and media organizations as well as legal documentation and journals. The source material for the 1998-2007 element of the GTD was collected by CETIS in association with START. Other material incorporated into the GTD includes data from the University of Ulster’s Conflict Archive on the Internet (CAIN), and the National Abortion Federation Researchers among others. START retains all source materials used in relation to a coded incident in an electronic format called a Reference Source Document (RST). The GTD codebook, containing the database coding scheme and the criteria for the inclusion of a particular incident is available from the START website.

Definition

Both GTD1 and GTD2 worked under their own respective operational definitions. Pinkerton’s definition of terrorism was adopted for GTD1. In addition to standard named terrorist groups, generic variables such as “student protesters” and “rebels” were also included in Pinkerton’s broad definition of terrorism. GTD1 data required that incidents ‘substantially concur’ with the pre-defined criteria.

The GTD2 data set was not restricted to a set definition. The START team did however stipulate minimum criteria. ‘Based on the original GTD1 definition, each incident included in the GTD2 had to be an *intentional act of violence or threat of violence by a non-state actor*’ (Source GTD website). GTD2 avoided the contentious issue of a universally accepted definition of terrorism. The rigidity of any single

definition of terrorism and its association with a particular data set has implications for the design, long-term content and empirical findings derived from the data. The resultant effect, that particular incidents are contained within one database and not others, compounded cross-comparison difficulties. Aware that a universally accepted definition of terrorism is still elusive, designers of GTD2 took advantage of new web based technology, to allow users to configure the database to alternative definitions of terrorism - depending on the researcher's choices from three given criteria, of which two must be included. Within certain constraints, users are now able to filter out data that does not comply with their preferred definition of terrorism, taken from the GTD2 menu. In designing GTD2, researchers coded data covering a variety of definitions of terrorism; therefore offering selective definitions of terrorism within GTD2. This allowed researchers to work with definitions of terrorism that they appealing to a broader group of users. The criteria for inclusion in GTD2 were more rigorous: a minimum of two necessary criteria and two out of three sufficient criteria needed to be met prior to inclusion in the database. This facility is now available with the newly released unitary GTD. The criteria are:

Criterion I: The act must be aimed at attaining a political, economic, religious, or social goal.

Criterion II: There must be evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) than the immediate victims.

Criterion III: The action must be outside the context of legitimate warfare activities, i.e. the act must be outside the parameters permitted by international humanitarian

law (particularly the admonition against deliberately targeting civilians or non-combatants).

The newly synthesized GTD was launched in the summer of 2009. The scope of the data within GTD is extensive. The GTD holds in excess of 27,000 bombings, 12,000 assassinations and 2,900 kidnappings. START engages over 75 data collectors, with expertise in six language groups to build the GTD collections. Source material reviewed for the GTD is substantial. START researchers assessed over 3,500,000 news articles as well as 25,000 news sources for the GTD for 1998 to 2007.

The newly developed GTD website provides users with an extensive array of interactive functionalities. Users are able to search the database in a basic and advanced format. The database can be queried using a browse facility, utilizing either keywords or the advanced search wizard. The resultant information is presented in a tabular format and displays key variables such as date, city country, perpetrator, fatalities and injuries. This is accompanied by narrative descriptions of incidents and, where relevant, graphical data. Users are able to print and e-mail queried results. Further features include the GTD Data Rivers. This allows users to visualize key terrorist variables in the form of stack charts. In addition the website provides a 'This Date in Terrorism' section and a rotating 'Features' web page on news, current research and developments at START. To conclude, here are some sample figures from GTD:

Figure 1: Number of Incidents of Terrorism Worldwide, 1970-2007 (GTD)

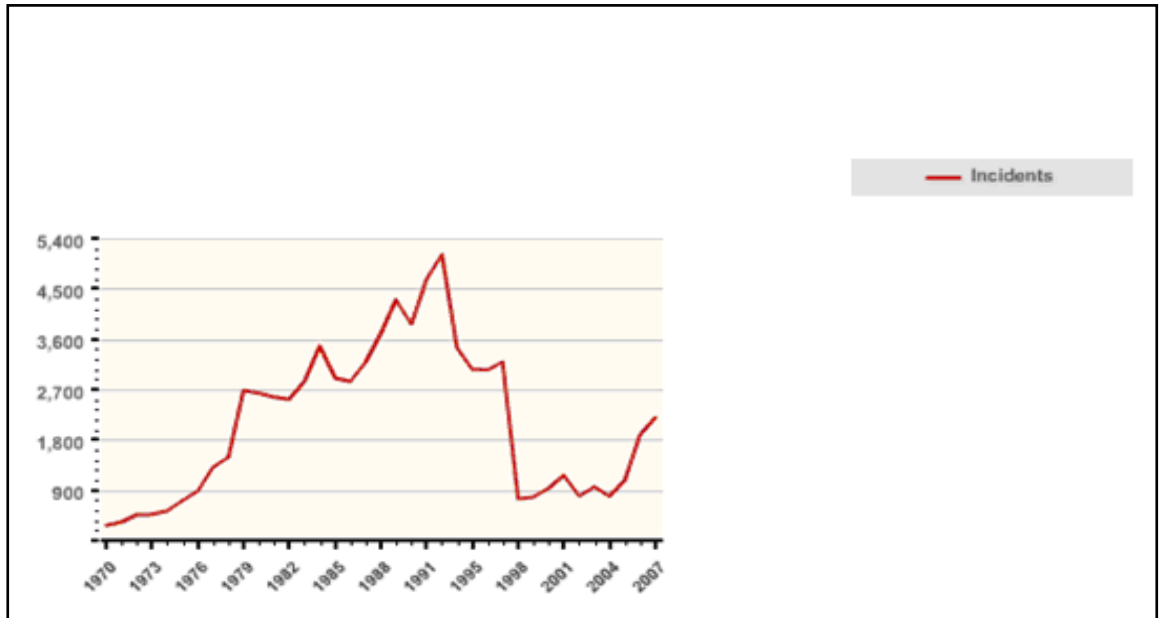


Figure 2: Number of Terrorist Incidents Worldwide, 1992-2008, attributed to Al-Qaeda, according to GTD

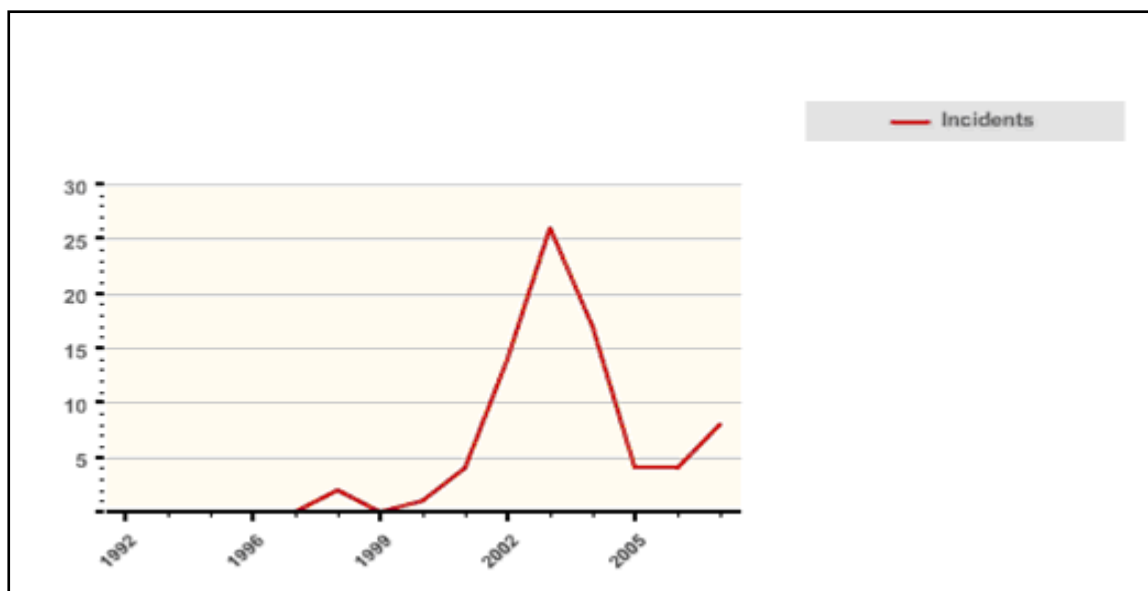
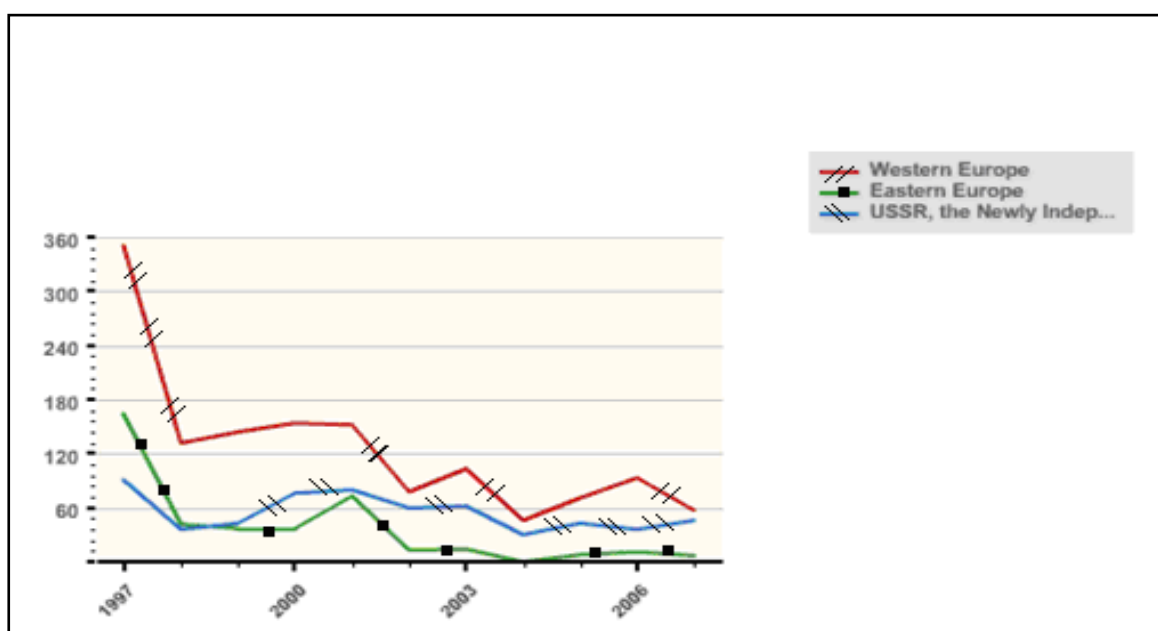


Figure 3: Number of Incidents of Terrorism in Western Europe, Eastern Europe, former USSR & the Newly Independent States (NIS) 1997-2007 (GTD)



Name:	Worldwide Incidents Tracking System (WITS)
--------------	--

Parent Host	United States National Counterterrorism Center (NCTC)
Website:	http://wits.nctc.gov/
E-mail:	N/A
Access:	Free
Unit of Analysis	Terrorist Incident
Scope:	Domestic and International Terrorism
Period Covered:	2004-2009 and on-going
Principle sources	Open-source material and unclassified data
Key Variables	Incident date, region, country, state/province, city, event type, dead count, wounded count, perpetrator characteristics. (See WITS website for other variables)

Worldwide Incidents Tracking System (WITS)

The Worldwide Incidents Tracking System (WITS) is a database of terrorist incidents operated by the United States National Counterterrorism Center (NCTC). The WITS database is presented in a Web-based user interface. The database, publicly unveiled in 2005, contains terrorist incidents from 1/1/2004 to 3/31/2009 and is on-going.

Context and Definition

The National Counterterrorism Center, under Section 2656f of Title 22 of the US Code, provides the United States Department of State with support in meeting the legal requirement to provide annual statistics on incidents of terrorism. This data is held within the U.S. Governments repository of terrorist incidents called the Worldwide Incidents Tracking System (WITS) database.

The NCTC defines terrorism as follows: 'when groups or individuals acting on political motivation deliberately or recklessly attack civilians/non-combatants or their property and the attack does not fall into another special category of political violence, such as crime, rioting, or tribal violence'. Based on these criteria that terrorist incidents are deemed eligible for entry to the WITS database. As a result of methodological changes to the definition of terrorism, only the 2006 NCTC data is directly comparable to the 2005 data. The 2004 data sets were coded on the basis of a narrower definition of terrorism.

Searching the WITS Database

The WITS database offers both simple and advanced searches of terrorist incidents using basic and complex query menus. Searches can be executed using an interactive region/country map, by keywords or simple and more complex query commands. The map facility filters all countries relating to a specific region. The keyword facility allows researchers to ask for specific words: for example 'British Airways', 'Insurgent' or 'Letter Bomb'. Alternatively, wildcard or fuzzy logic searches can be used within keywords, where uncertainty over spelling occurs.

The Simple Search facility queries the WITS database for terrorist incidents by category. These include the date(s) of the incident(s), geographic region, country and characteristics of the perpetrator. For example, secular/political, anarchist or Hindu extremist. Other key fields include characteristics of victims and type of facility targeted. More complex combined searches can be undertaken. Some fields can be queried using exact or multiple values. For example, exact, minimum and maximum values can be placed within the hostage's field. Results are presented in a tabular

report format. This data can be re-ordered on all fields based on ascending/descending order. The data can be exported to spreadsheet for further analysis or transformed into PDF format.

The Advanced Search facility within WITS permits users to specify specific incident criteria from any of the pre-defined fields within the database. The system offers seven different methods for selecting search criteria. The database can be queried by Incident Control Number (ICN), text, date ranges, number values pertaining to specific terrorist incidents, single selection (yes/no/either), multi-selection lists, e.g. arson/firebombing and multi-selection popup screens offering extensive variables. Searches can be undertaken for terrorist incidents by “event type”. These include such variables as armed attacks, bombings, arson and fire-bombings.

Included within the Advanced Search facility of the WITS database is the field “defining characteristics”. The idea is to record, where possible the issues that motivate individuals or groups to carry out a terrorist attack. From this, users are able to retrieve incidents conducted by similar types of groups or individuals, e.g. Sunni extremists. The database also allows users to query terrorist incidents based on victims. Groups or individuals victims can be identified in relation to their ethnic, religious and cultural identities. The system is even designed to identify victims who could have been targeted as a result of their religious, cultural or ethnic identities. Detailed information on numbers of individuals killed, wounded and kidnapped can be retrieved from the WITS database. Where events are on-going, such as kidnappings and the release of hostages, or the status of critically injured changes,

the database is updated. The WITS database also classifies monetary damage as the result of an incident as light, moderate and heavy. All estimates are in U.S. Dollars.

In addition to query driven data, the WITS website provides access to several “.PDF” publications produced by the NCTC. These include ‘NCTC Report on Incidents of Terrorism’ (2006) and ‘A Chronology of Significant International Terrorism for 2004’. The database is also able to generate a series of pre-defined analytical reports. For example, the database will generate a report ‘Number of Damaged Facilities by Targeting Characteristic’ based on user input dates. The WITS database can then store, e-mail or distribute the reports to other interested parties.

Methodology

The NCTC acknowledges that gathering data and coding incidents of terrorism is not an exact science. Incidents occurring in Afghanistan and Iraq have proven especially challenging, in terms of the ability to collect complete data on all incidents. Added to this is the difficulty of differentiating between forms of violence, such as criminal acts and violent sectarian incidents. The NCTC highlights coding challenges e.g. whether a particular incident can be defined as an act of terrorism or insurgency. In certain circumstances, the differences are both complex and subtle.

The WITS website publishes a series of basic ‘counting rules’ used in the compilation of the database. For an incident to be recorded, terrorists must have initiated and carried out an attack. Incidents such as hoaxes and failed or foiled attacks are not included within the database. The WITS data does not include genocidal acts.

The NCTC makes clear that the data derived from its WITS database of terrorist incidents needs to be viewed in a much wider context than the narrower universe of data coded within the system. Among many challenges facing analysts is that data can often be vague or incomplete. The NCTC cautions against crude comparisons of annual aggregate data in efforts to test assumptions about the efficacy of counter-terrorism policies. For the NCTC, the general purpose of the database is to allow users to track terrorist incidents, and provide data and information on the location of the incident, its victims and the individuals/groups responsible for such acts. As a result, researchers may be able to discern trends in the nature of attacks.

The complete WITS data set can be downloaded to other application software including spreadsheet and database (Oracle). The exported “.Zip” files contain all terrorist incident data and related information. Also incorporated within the WITS website is a comprehensive and detailed on-line help facility, allowing users to familiarise themselves with the functionality of the WITS database. Accompanying this is a list of acronyms, and an extensive glossary of definition of terms used within the database. For example, the glossary defines what ‘Near Miss/Non Attack Incident’ means, as used within the context of an incident. A detailed set of Frequently Asked Questions (FAQ’s) explains the rationale and criteria behind some of the most common queries relating to the design and methodology of the WITS database.

WITS NextGen Database

In the Spring of 2010 the National Counterterrorism Center released a completely new interface for the WITS database called WITSNextGen. The WITS NextGen provides researchers with enhanced database functionality coupled with sophisticated reporting and visual presentation tools.

The WITS NextGen provides users with an extensive selection of pre-defined reports which can be generated by selecting an inclusive set of dates. Some of the many pre-defined reports include: incidents [dead, wounded, hostage, total] grouped by country as well as country fatality ranges [e.g. 0, 2-4, 5-9, 10-19]. Other available reports include the number of damaged facilities by targeted characteristic, number of victims by defining characteristic and victim counts grouped by victim type and incident date. Results can then be presented by chart presentation, by a display of individual records, or in a summary format, available for export to spreadsheet. Aggregate totals are detailed within reports and throughout the database where pertinent. Reports can be generated from data derived from searches. Advanced functionality within the WITS NextGen database permits users to create sophisticated report generation of incidents using a series of metric criteria, groupings, 'drilldown' facilities and advanced query editing.

The WITS NextGen allows users to carry out key word searches on specific incidents. To aid users, an incremental suggestion menu of place names, victim types etc. appears, allowing users to choose from an extensive list. Searches can also be refined by date and numeric range. A history of current searches and current reports can also be viewed and saved. Users are also able to apply their own defined filter searches to all or various parts of the database. A further series of extensive tabbed

filters provide detailed search criteria. These include: event type, incident filters, location, victim, perpetrator and facility.

The methods by which users can visualise terrorist incident data within the WITS database has changed radically from the original WITS database. Users view incidents in standard record format, by concept cloud, map, charts and report format. A detailed breakdown of individual incidents is available within the standard record format. In addition to the incident number (ICN) and narrative summary of the incident, an extensive array of variables relating to the incident is provided. Many of these variables are hyper-linked to other related parts of the WITS NextGen database. The concept cloud (restricted to the attack tab in the database) presents users with an alphabetical list of words and phrases that have been used within the narrative summary of each terrorist attack. The more frequently a word or a phrase is used within the narrative summary of selected incidents, the larger the word (font size) will appear on screen. Thus, allowing users to quickly ascertain the frequency of words and phrases that may have some bearing, link, impact or theme on their research. The Map function (restricted to the attack tab only) allows users to view terrorist attacks over a geographical area. This facility is available in both Google Map form and Google Earth (requires plug-in). Coloured clusters on the maps display single and multiple attacks and attack counts. With the new WITS NextGen system users are able to create their own customised line charts, pie charts, 3D Bar charts and stacked bar charts. In addition to viewing results by screen, data can be exported in .CSV, .XML and to Microsoft Excel format. The WITS NextGen website also provides a comprehensive and detailed user guide.

Figure 4: Trends in Person-borne Improvised Explosive Device (PBIED) vs. Suicide Vehicle-borne Improvised Explosive Device (SVBIED) attacks for Pakistan (NCTC 2008 Report on Terrorism)

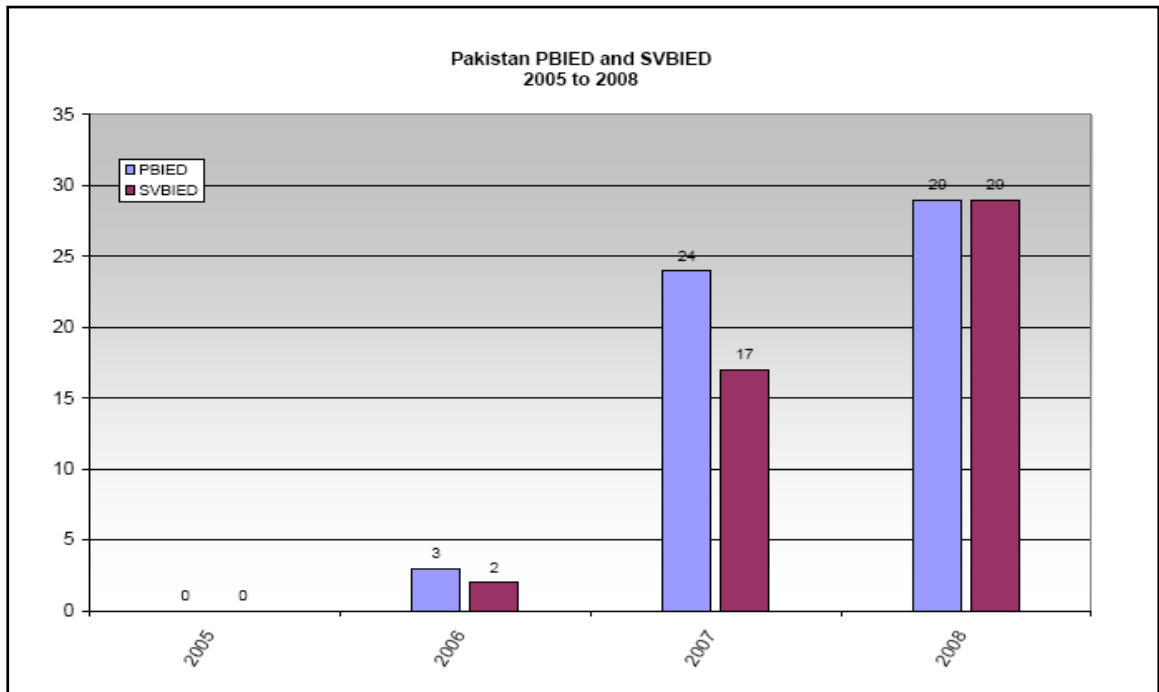


Figure 5: Trends in Person-borne Improvised Explosive Device (PBIED) vs. Suicide Vehicle-borne Improvised Explosive Device (SVBIED) attacks for Rest of World. (NCTC 2008 Report on Terrorism)

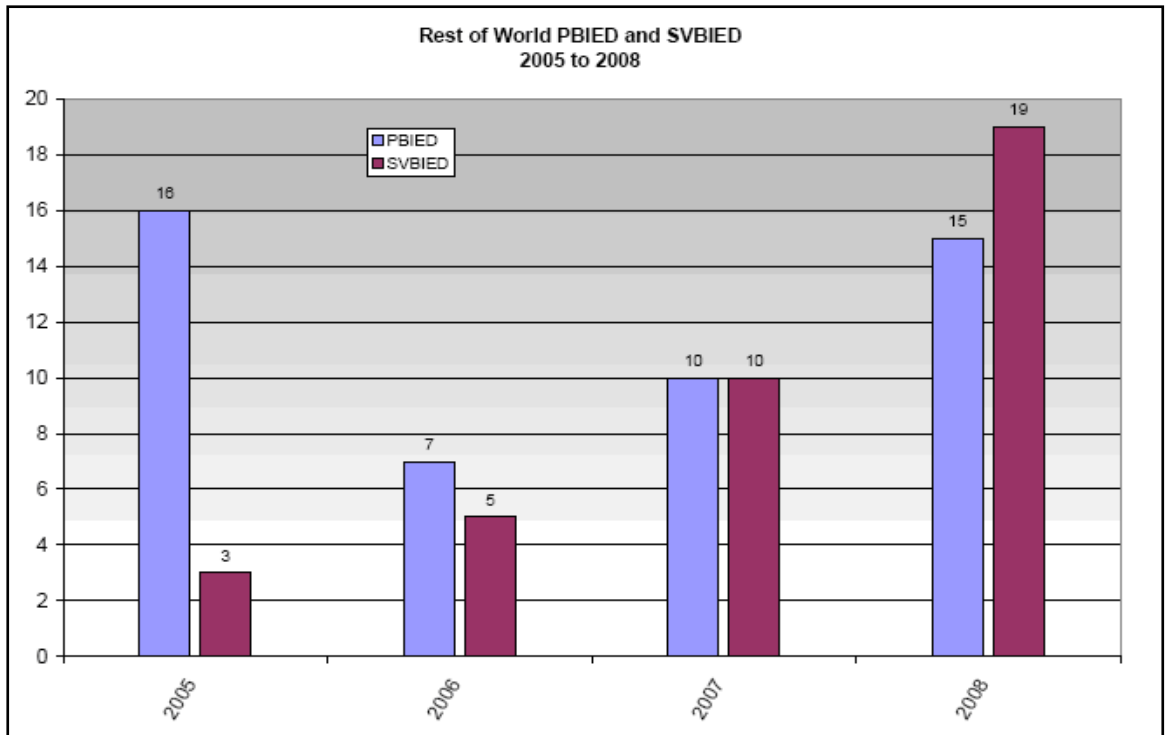


Figure 6: Comparison of Terrorism Fatalities and Incidents by Region (NCTC 2008 Report on Terrorism)

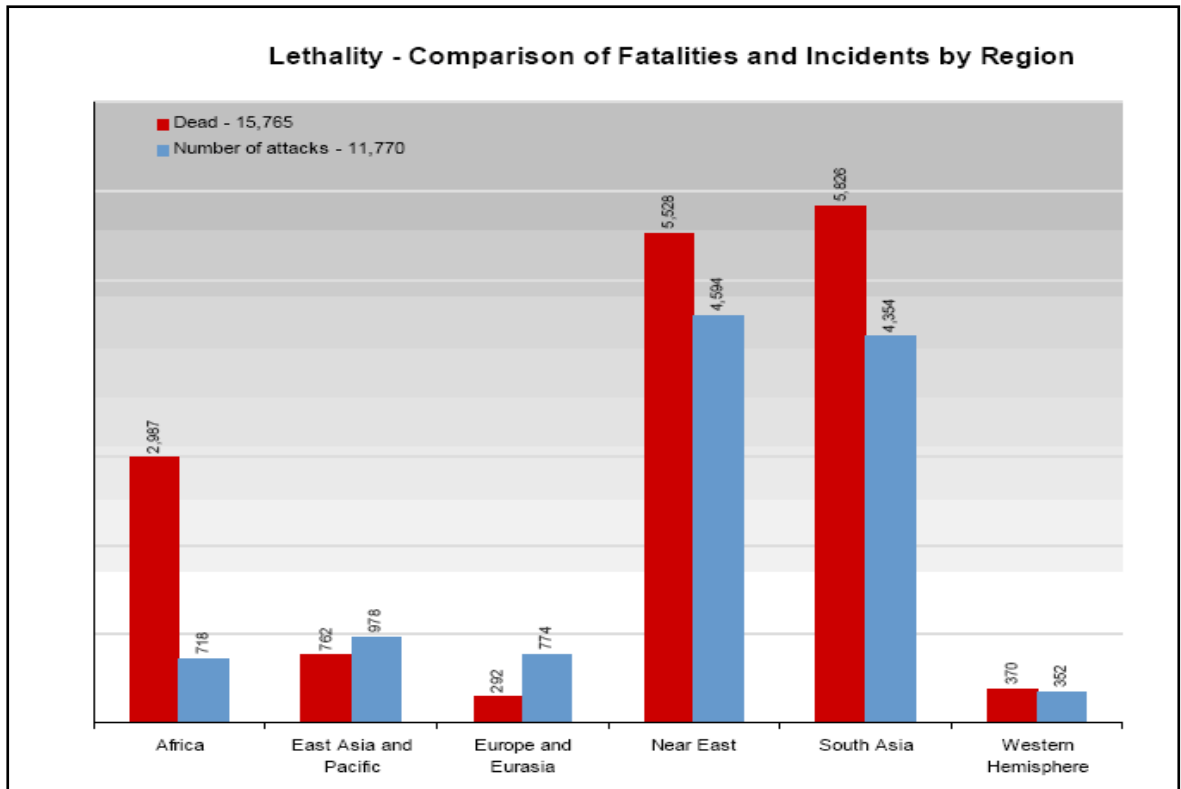


Figure 7: Comparison of High-Fatality Sunni Attacks in Iraq (IZ) and Afghanistan (AF) versus Rest of World (RoW), 2004-2008 (NCTC 2008 Report on Terrorism)

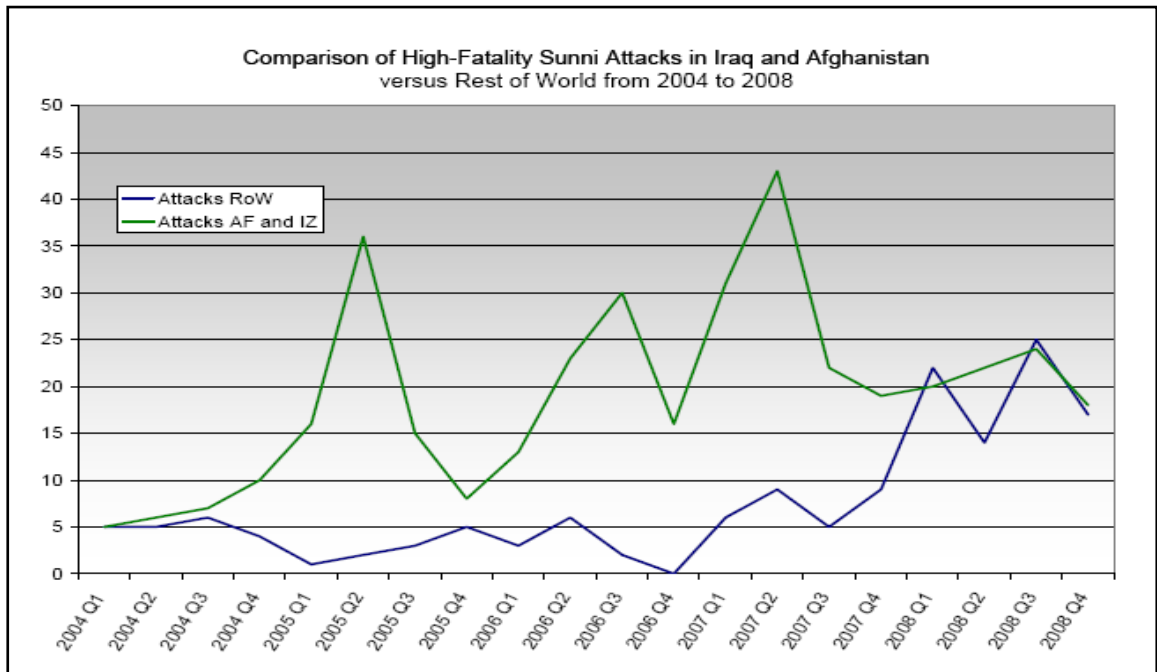
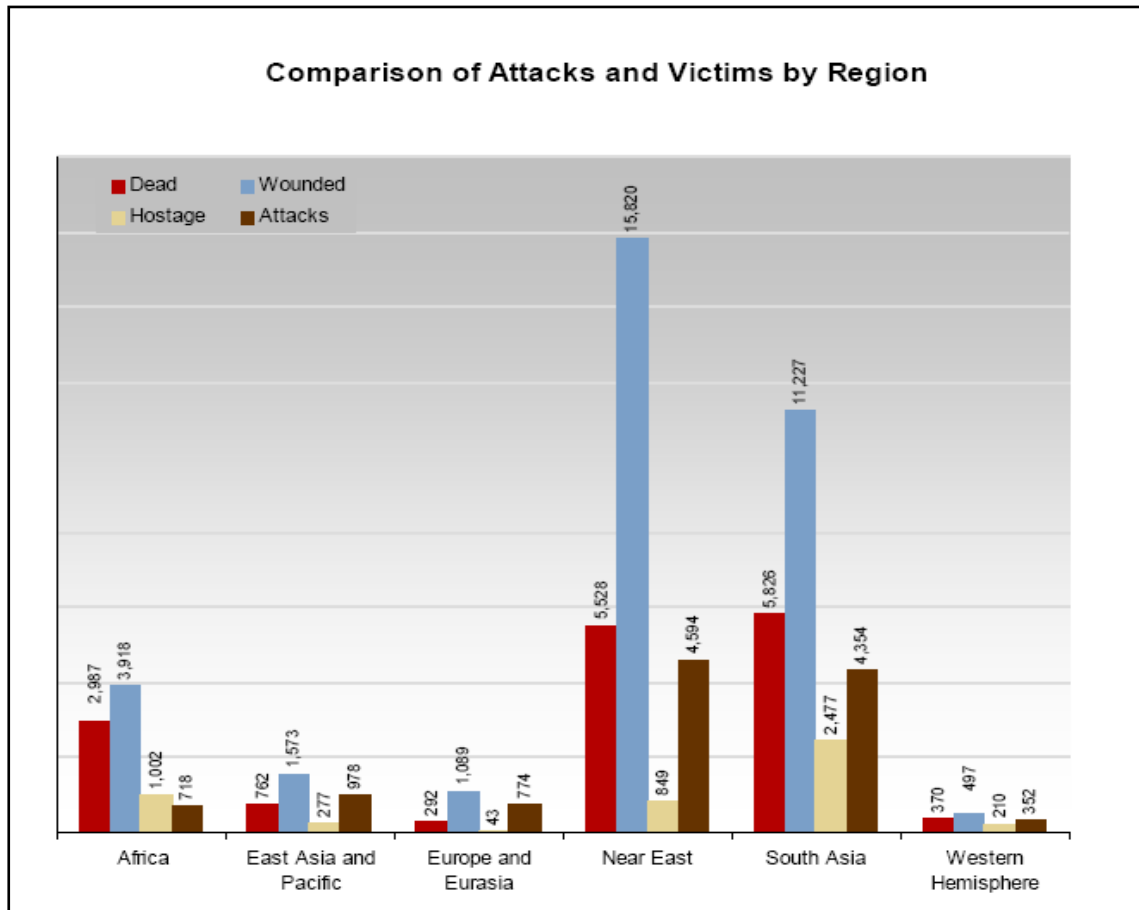


Figure 8: Comparison of Terrorist Attacks and Victims by Region (NCTC 2008 Report on Terrorism)



Name:	ITERATE - International Terrorism: Attributes of Terrorist Events
Parent Host	Vinyard Software Inc., Dunn Loring VA. United States
Website:	http://www.vinyardsoftware.com/
E-mail:	info@vinyardsoftware.com
Access:	Commercial Purchase
Unit of Analysis	Terrorist Incident
Scope:	International and transnational terrorism
Period Covered:	1968 onwards

Principle sources	Open-source material
Key Variables	Date of incident, group initiating action, number of victims, total individuals wounded, terrorist logistical success.

ITERATE - International Terrorism: Attributes of Terrorist Events

Introduction

The ITERATE (International Terrorism: Attributes of Terrorist Events) data sets is one the longest established chronologies on international and transnational terrorism. Produced in the United States, the data set files are available for purchase from Vinyard Software Inc., Dunn Loring, VA. Hard-copy versions of the chronologies have been published periodically by Ed Mickolus, Todd Sandler, Jean Murdock, Peter Flemming and Susan Simmons (Greenwood Press and Iowa State University Press). The ITERATE data sets provide both quantitative and qualitative data and information for use by analysts and researchers within the terrorism and counter-terrorism fields. The data sets can also be used as indices in wider cognate areas of social, political, geopolitical and economic research.

Definition

The ITERATE project defines international/transnational terrorism as: “the use, or threat of use, of anxiety-inducing, extra-normal violence for political purposes by any individual or group, whether acting for or in opposition to established governmental authority, when such action is intended to influence the attitudes and behaviour of a target group wider than the immediate victims and when, through the nationality or foreign ties of its perpetrators, its location, the nature of its institutional or human

victims, or the mechanics of its resolution, its ramifications transcend national boundaries.”

Format and Source Data

The ITERATE data sets records contemporary international terrorism incidents from 1968 up to present day events. The ITERATE data sets are available in two formats: textual and numerical. The textual files, based on a chronology of international terrorism incidents from 1968 onwards, can be uploaded using MS Word or WordPerfect. The numeric data sets (uploaded using MS Excel) are coded into four related, but separate computer files: COMMON, FATE, HOSTAGE and SKYJACK. The coded variables are derived from the data in ITERATE’s textual chronologies of international terrorism. Codification of variables from the data sets inception has been consistent. New attributes are coded with the emergence of new terrorist groups and events. The data sets are updated on a daily basis. The files can operate independently of each other or can be used in association with each other.

The source data used to compile the ITERATE data sets is eclectic. Information is drawn from government agencies, scholars, news media, information services and individuals. Chronologies and databases on international terrorism compiled by the FBI, US Department of State, the CIA and NCTC are all used by ITERATE staff to compile the data sets.

ITERATE derives information from extensive searches of the world’s main news and media organisations, as well as information and research services. Some of the key media outlets used include: Agence France-Presse (AFP), Reuters, Associated Press (AP), CNN, United Press International (UPI), al Jazeera, CNN, the *New York*

Times, *Washington Post* and *Newsweek*. Other source information comes from academic publications and related documents.

In addition to established news media services, the ITERATE staff also compile source information from interviews with academics and government officials working within the terrorism and counter-terrorism field. Where possible, former hostages and individuals with direct experience of particular terrorist incidents have also been interviewed.

The ITERATE files

The files can be cross-referenced with each other based upon a unique incident code for each event. This permits researchers and analysts to link quantitative data to narrative information on terrorist incidents. The vast majority of international terrorism incidents within the ITERATE data sets are contained within the COMMON file. The COMMON file codes the nature and type of incident, the terrorist group(s) involved, if known, and details relating to victims of incidents. This, the largest file, covers the period 1968-2007. The data set is continuous from 1968. At the beginning of 2010 the files held 13,087 cases relating to acts of international terrorism. The COMMON file contains 42 variables. The key variables include: fatalities, victims' wounded, immediate victims of an incident, nationalities of terrorists and terrorist groups as well as the nationalities of victims. Victims attachment to a sovereign states, NGO's and IGO's are also coded. Other variables include type of venue and the location of an act of international terrorism, for example territories,

protectorates and states. Success or failures of particular terrorist logistics are also catalogued.

The FATE file details the post-incident fate of the perpetrators, if established. This could include outcomes such as death, arrest (including numbers arrested) escape, prison term, extradition or asylum. The nationalities of individual terrorists are also recorded. Requests for extradition, the country requesting extradition and the outcome of the request are coded.

The HOSTAGE file details an array of 41 variables relating to hostage situations. This involves such incidents as hostage taking, kidnap, skyjacking and the seizure of land-based transport systems (trains, buses, trucks, cars). The key variables include the nationalities of the individuals involved in the terrorist incident, the duration of the incident and its outcome. Behavioural aspects of terrorists are coded. These include demands for press/media attention, the release of certain prisoners, requests for political change and requests for ransoms, amounts, and ransom sources. Other behavioural traits coded include terrorist's behaviour towards deadlines being met or passing and their relationship towards hostages.

The SKYJACK file contains 27 variables related to terrorist hijackings and includes hijackings undertaken by non-terrorists. These data are also contained within the COMMON file. The key variables include the airlines and aircraft involved in a particular incident along with the incident location, the number of victims involved and any casualties. Negotiating success is recorded. The file also codes the type of weapons used in an incident and the duration of the incident. The flight plan and embarkation point for the hijacker, if known, can also be coded within the SKYJACK file. Further variables within the SKYJACK file include: intended flight

destination, the desired destination of the hijackers, stopovers, and refuelling and actual end point. The logistical success of a particular hijacking incident is recorded and includes such variables as: incident stopped by authorities, aborted by hijackers, apparently completed as planned.

DOTS (Data on Terrorist Suspects)

A recently compiled data set *DOTS* (Data on Terrorist Suspects) produced by Vinyard Software Inc. complements the ITERATE files by recording biographic details of every terrorist coded in the ITERATE chronologies on terrorism. Biographic data within the database includes information on terrorist leaders, perpetrators, financial backers, detainees and defendants. The *DOTS* database covers the period 1968 until present. Vinyard Software Inc. has recently opened a website: www.vinyardsoftware.com .To conclude, some illustrative graphs from ITERATE.

Figure 9: International Terrorism Casualties, 1968-2007 (ITERATE)

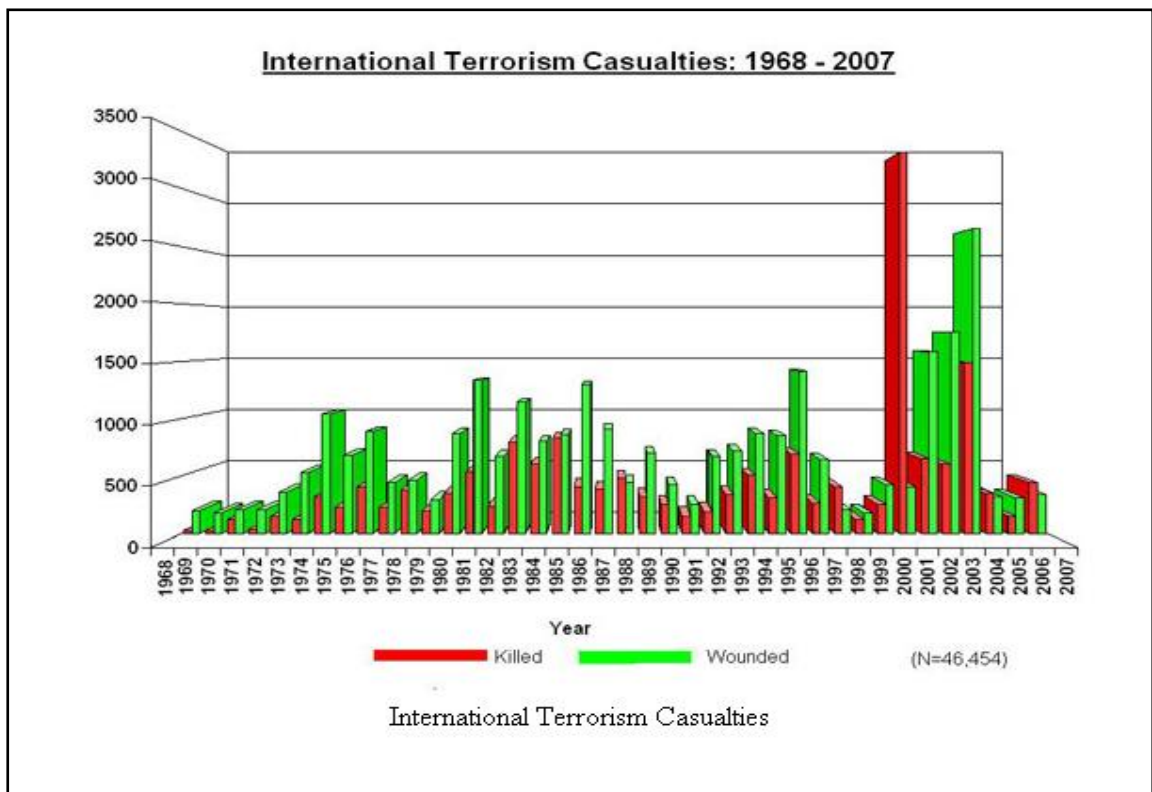
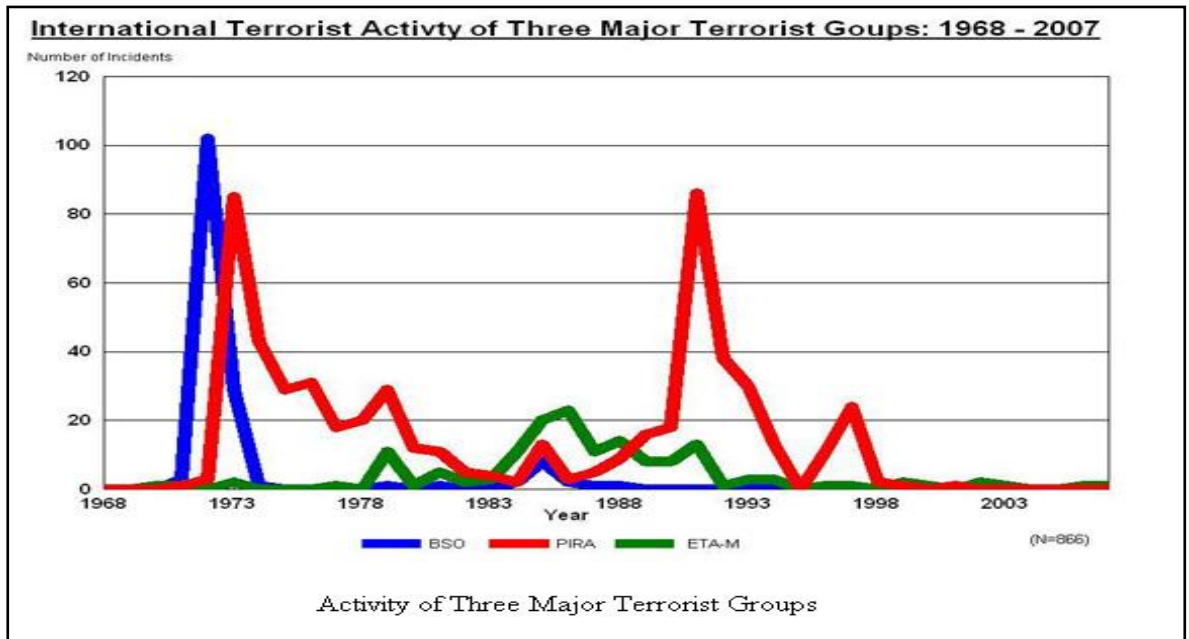


Figure 10: International Terrorist Activity of Three Major Terrorist Groups, 1968-2007 (ITERATE)



- BSO = Black September Organization; PIRA = Provisional Irish Republican Army; ETA-M = Basque Liberation Movement – Military Wing

Name:	MIPT Terrorism Knowledge Base
Parent Host	Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT)
Website:	http://www.mipt.org/
E-mail:	webmaster@mipt.org
Access:	Access was free. Terrorism Knowledge Base has ceased operation in March 2008
Unit of Analysis	Terrorist Incident
Scope:	Domestic and International Terrorism
Period Covered:	1968-2008
Principle sources	Open-source material
Key Variables	N/A

MIPT Terrorism Knowledge Base

(NB: The MIPT Terrorism Knowledge Base ceased operation on the 31st March 2008. However, old MIPT files up to March 2008 can still be seen using the www.archive.org website).

Introduction

The MIPT Terrorism Knowledge Base (TKB) launched in 2004, provided public access to a large collection of information on terrorist groups and their leaders, terrorist incidents and terrorist related court-case information. The TKB was free and completely Internet-based. The knowledge base provided information on both domestic and international terrorism.

Data for the TKB came from four key sources: the RAND Terrorism Chronology 1968-1997; the RAND-MIPT Terrorism Incident Database (1998-2008); the Terrorism Indictment Database at the Universities of Arkansas and Oklahoma; and DFI International, a research, analysis and consultancy organisation.

The TKB portal provided a fully integrated array of textual, graphical and multimedia terrorism data and information. In addition to providing core data on terrorist leaders, groups and incidents, the knowledge base provided contextualised in-depth background material on terrorist group histories, their affiliations, tactics employed and their geographic locations. The format also included biographical details, summaries, interactive maps and the ability for users to generate statistical data and dynamic graphs.

Definition

The TKBs defined an act of terrorism as: 'Terrorism is violence, or the threat of violence, calculated to create an atmosphere of fear and alarm. These acts are designed to coerce others into actions they would not otherwise undertake, or refrain from actions they desired to take. All terrorist acts are crimes. Many would also be violation of the rules of war if a state of war existed. This violence or threat of violence is generally directed against civilian targets. The motives of all terrorists are political, and terrorist actions are generally carried out in a way that will achieve maximum publicity. Unlike other criminal acts, terrorists often claim credit for their acts. Finally, terrorist acts are intended to produce effects beyond the immediate physical damage of the cause, having long-term psychological repercussions on a

particular target audience. The fear created by terrorists may be intended to cause people to exaggerate the strengths of the terrorist and the importance of the cause, to provoke governmental overreaction, to discourage dissent, or simply to intimidate and thereby enforce compliance with their demands'. (Source: TKB's Glossary). RAND verified all terrorist incidents entered within the TKB.

Functionality and TKB Maps

The TKB provided researchers with a wide range of search functions. Users were able to conduct basic searches by keywords or use an advanced search facility. Using drop-down menus, the advanced function allowed users to cross-query all elements of the knowledge base including location, terrorist groups, leaders, terrorist incidents and any related legal cases. In addition, the TKB also contained an Image Archive of terrorist groups, leaders, and attacks. This could be searched by keyword, name of individual or group name.

Another graphical feature of the TKB was TKB Maps. This allowed researchers access to a series of interactive maps giving satellite imagery of relevant geographic areas. Temporal and spatial map images could be generated indicating the location of group attacks, the volume of attacks and the type of targets attacked. Data could be filtered and overlay functions also allowed users to display major infrastructure such as highways, pipelines and airports.

Knowledge Base Directory and TKB Profiles

The Knowledge Base Directory of the TKB provided researchers with the ability to search for information using several variables. For example searches by terrorist

group, their location and ideology. Other search functions permitted a breakdown of terrorist information by country, date or legal cases, ideology and tactic.

TKB profiles offered researchers an eclectic collection of terrorism related information dating back to 1968. Drawing together information on a particular incident and related case data the profiles function of the TKB provided a one-stop dossier for terrorism analysis.

The terrorist incident profile provided factual information relating to the terrorist group, dates, location, targets, tactics and statistical data on numbers injured and killed. Complementing this was the TKB's case profiles. This facility provided legal data and information pertaining to terrorism investigations undertaken by the FBI. This information collected by TKB analysts included indictment data and court documentation. Where available, details of charges, evidence presented within cases and sentencing results were made available. In more complicated court cases cross-referencing of terrorist group connections were indicated. A further search tool gave access to detailed group, leader and membership profiles. This provided researchers with historical background on terrorist groups and their affiliates, as well as information on a terrorist group's philosophy and goals.

Analytical Tools

Using web-based technologies the TKB provided terrorism researchers with a series of flexible analytical tools that could generate a series of tables, charts and graphs derived from terrorism incident data and legal data based upon the indictment and prosecution of terrorists. Pre-defined statistical data on terrorism incidents could

also be accessed. Its rivals and successors have so far not matched the user-friendliness of MIPT's database.

The Incident Analysis Wizard enabled a step-by-step process for users to generate a series of pie-line-bar-and 3-dimensional graphics based upon specific criteria. For example, comparative terrorism trends over time or more detailed data and graphics on injury and fatality ranges.

The Statistical Incident Reports generated a series of interactive reports providing statistical data on terrorist incidents, including such variables as date of attack, target group, perpetrators, incident location and tactics employed. Statistical data taken from indictment data sets and outcome statistics of legal cases could also be compiled using TKB's software. The group comparison function of TKB was even able to compare and present on screen side-by-side statistical analysis of up to a dozen terrorist groups.

Reference Material

The MIPT Terrorism Knowledge Base provided links to a comprehensive collection of terrorism related data and information held within the MIPT Library. In addition to hard-copy and "PDF" documents a large array of CD-ROM, audio/visual material, proceedings, books and governmental documentation could be obtained via the TKB's website. This included *Country Reports*, *Patterns of Global Terrorism*, the FBI's *Terrorism in the U.S.* and MIPT's *Terrorism Annuals*. Some of the TKB data have been transferred to the University of Maryland's Global Terrorism Database.

Figure 11: Worldwide Terrorist Incidents by Year, 1999 - 2005 (MIPT)

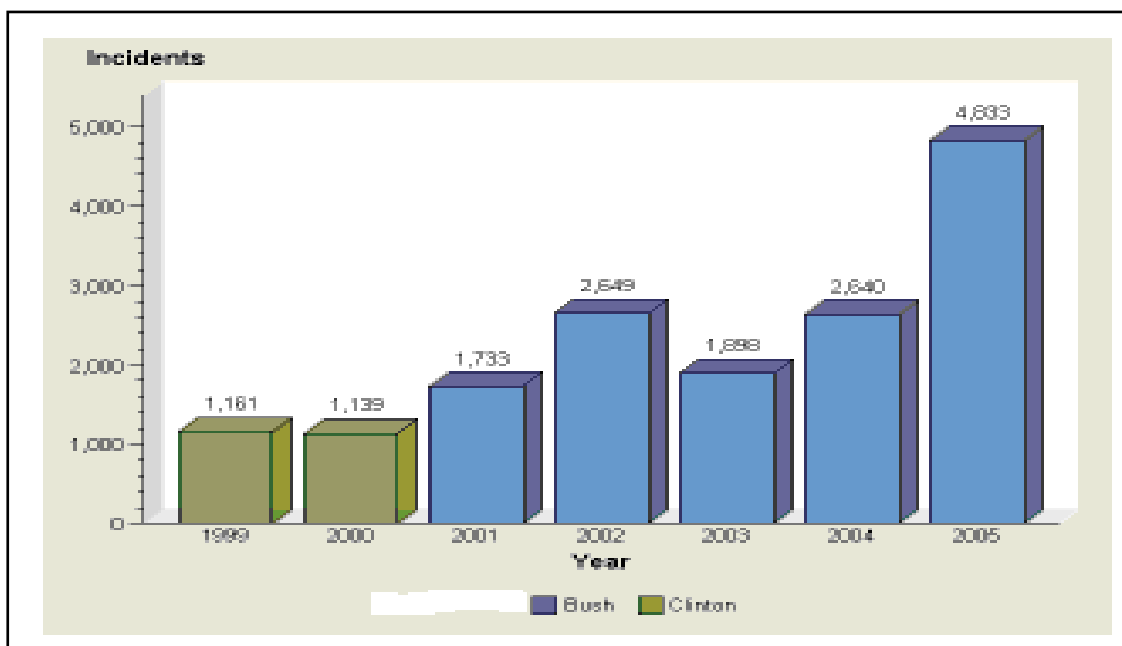


Figure 12: Top Twenty Countries in terms of Terrorist Fatalities per Million People

1968-2006 (MIPT)*

1. Iraq.....	439
2. Lebanon.....	329
3. Israel.....	229
4. Westbank	228
5. Colombia.....	32
6. Cyprus.....	32
7. Algeria.....	30
8. Angola.....	30
9. Afghanistan.....	29
10. Uganda.....	19
11. Chad.....	18
12. Jordan.....	15
13. Kuwait.....	14
14. Greece	14

15.Saudi Arabia.....	12
16.Mauritania.....	12
17.Somalia.....	11
18.Georgia.....	11
19.United States.....	11
20.Canada.....	10

Weighted average for 135 countries.....14

*Excluded from his list were five small countries: Barbados (261 per million), Gibraltar (107 per million), Djibouti (25 per million), Bahrain (18 per million) and East Timor (10 per million). It should be kept in mind that victims of domestic terrorism are counted by MIPT only from 1998 onwards. Source: MIPT as processed by http://www.nationmaster.com/red/graph/ter_ter_act_196_fat_percap-1968-2006-fatalities-per-capita&b_printable=1 (accessed 27 June 2010).

Name:	RAND – Worldwide Terrorism Incident Database (RWTID)
Parent Host	The RAND Corporation, Santa Monica, CA. United States
Website:	http://www.rand.org/ise/projects/terrorismdatabase/
E-mail:	http://www.rand.org/ise/projects/terrorismdatabase/about/contact.html
Access:	Partly free; partly subscription-based
Unit of Analysis	Terrorist Incident
Scope:	Domestic and International Terrorism
Period Covered:	1968-2008
Principle sources	Open-source material
Key Variables	Search term, start date, end date, region, country, perpetrator, tactic, weapon, target

RAND – Worldwide Terrorism Incident Database (RWTID)

Introduction

The RAND Corporation is a non-profit institution with headquarters based in Santa Monica, California. The aim of RAND, which works closely with the US defence establishment is to improve policy and decision-making through research and analysis.

For nearly forty years the RAND Corporation has collected data on terrorism. This was initiated by two key events: the Japanese Red Army's massacre at Lod Airport, Israel, and the Black September terrorist attacks on the 1972 Munich Summer Olympic Games. As a result of these terrorist incidents, the RAND Corporation was asked by the U.S. Government's newly formed Cabinet Committee to Combat Terrorism to examine recent trends in terrorism. As part of this project the RAND Terrorism Chronology was established in 1972. Some card/index system recording international terrorism incidents are thought to have been recorded at RAND before that. The temporal period for the chronology dates from 1968 until the present day. Until its joint venture in 2004 with the Memorial Institute for the Prevention of Terrorism (MIPT), the RAND Chronology dealt exclusively with international terrorism incidents from 1968-1997. From 2004 onwards RAND-MIPT began to record both domestic and international terrorist incidents worldwide, covering the period 1998 to 2008.

The RAND Terrorism Chronology has developed and evolved over the years into what is now a terrorism database system. The core ownership and stewardship of the database has always remained with RAND. However, joint operational running of the chronology and database has periodically been shared with other institutions. What was originally for many years the RAND Terrorism Chronology, became the

RAND-St. Andrews Chronology of International Terrorism (1994-1998) when Bruce Hoffman became director of the Centre for the Study of Terrorism and Political Violence in St. Andrews, and then, after the return of Hoffman to the US, the RAND-MIPT Terrorism Incident Database (2004-2008). With the cessation of the Memorial Institute for the Prevention of Terrorism (MIPT) Terrorism Knowledge Base® (TKB®) in 2008, the RAND component of the data reverted back to RAND. Incorporating the original RAND Terrorism Chronology and the RAND-MIPT Terrorism Incident Database the new database is now known as the RAND Worldwide Terrorism Incident Database (RWTID), covering both domestic (in-country) and international (cross-border/trans-national) terrorism.

Overview of RWTID

The RAND Worldwide Terrorism Incident Database (RWTID) now holds in excess of 36,000 terrorist incidents. Full access to the database is via a Web subscription service, established in January 2009. RAND defines terrorism for the purposes of the RWTID as: '.... violence calculated to create an atmosphere of fear and alarm to coerce others into actions they would not otherwise undertake, or refrain from actions they desired to take. Acts of terrorism are generally directed against civilian targets. The motives of all terrorists are political, and terrorist actions are generally carried out in a way that will achieve maximum publicity' (Source: RAND Website).

On a functional level the RWTID is operated by users selecting and filtering variables from a series of menus. The key variables the database can be queried on are: start date, end date, region, country, perpetrator, tactic, weapon, and target. Other filters allow users to query additional discrete variables: suicide attack, international incident, domestic incident, attacks claimed, coordinated, fatalities

(numbers) and injuries (numbers). The database can also be queried on keywords that could be contained within the narrative description of a particular incident.

The output for the RWTID comes in three formats: incidents lists, pie charts and chronological graphs. The incident lists contain core variables such as date of attack, location and perpetrator, if known. Accompanying this is a narrative description of the incident. The resultant data can also be exported into a spreadsheet format. The pie chart output allows users to generate charts based upon filtered variables from the database. This is presented in a graphical pie format with accompanying statistical data in a table format. For example, this could be the percentage of incidents undertaken by a terrorist group over a particular period of time and a total count of incidents by each respective group. The chronological graphs come in two forms: cumulative graphs and incident frequency graphs. The cumulative graph is generated in a bar chart format and relates to the injuries or fatalities incurred in any particular incident(s) over a specified time period specified within the database. The incident frequency chronological graphs are generated based upon matches occurring from the users search criteria and display aggregate totals based upon a choice of three time intervals: days, months or years.

RAND's Voices of Jihad Database

The RAND Voices of Jihad Database project allows researchers access to a large array of interviews, speeches, statements and publications by jihadist leaders and their supporters. The information is sourced from publicly accessible websites, with the vast majority of material available in English translation form.

The database covers a broad range of areas of what RAND identifies as 'Jihadist ideology'. These include worldviews, for example, on democracy or the role of women. Other areas include the justification of terror, grievances (against the West) as well as strategy and tactics.

Access to the material is via a simple query box. Users are then presented with links to original material and, dependent upon availability, full-text documents.

To conclude, here are some sample figures from the RAND-MIPT database:

Figure 13: Terrorist Incidents by Weapon, RAND-MIPT Terrorism Incident Database, 1 Jan. 2005 - 31 Dec. 2005 (MIPT Terrorism Annual 2006)

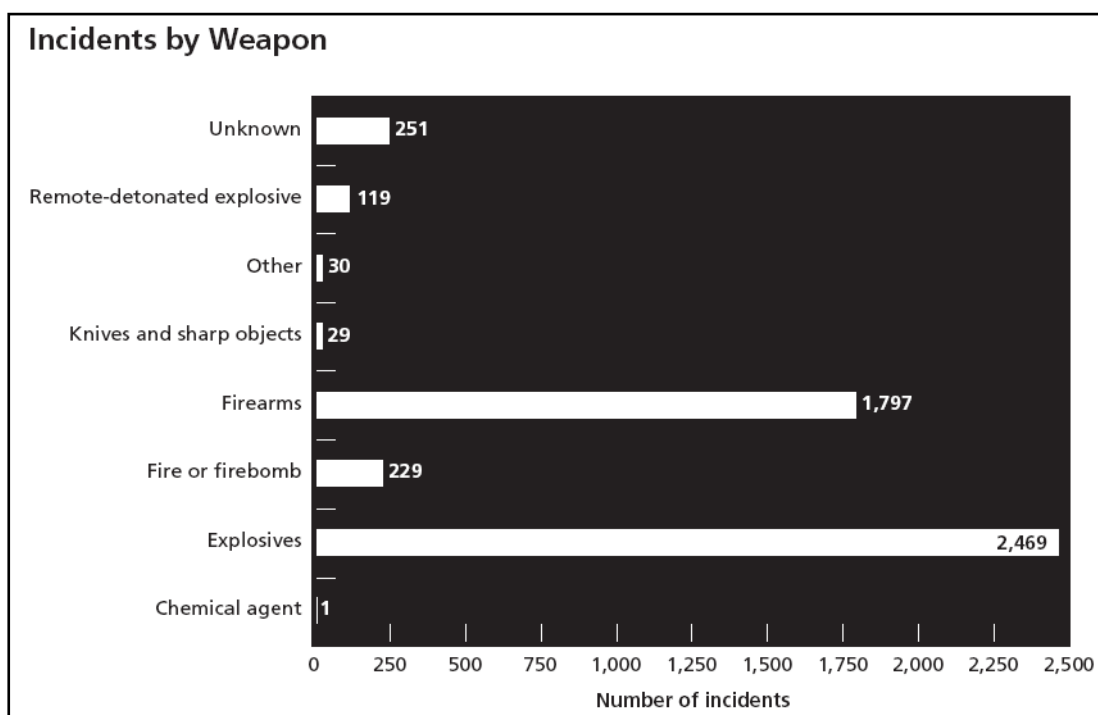


Figure 14: Terrorist Incidents by Target, RAND-MIPT Terrorism Incident Database,

1 Jan. 2005 - 31 Dec. 2005 (MIPT Terrorism Annual 2006)

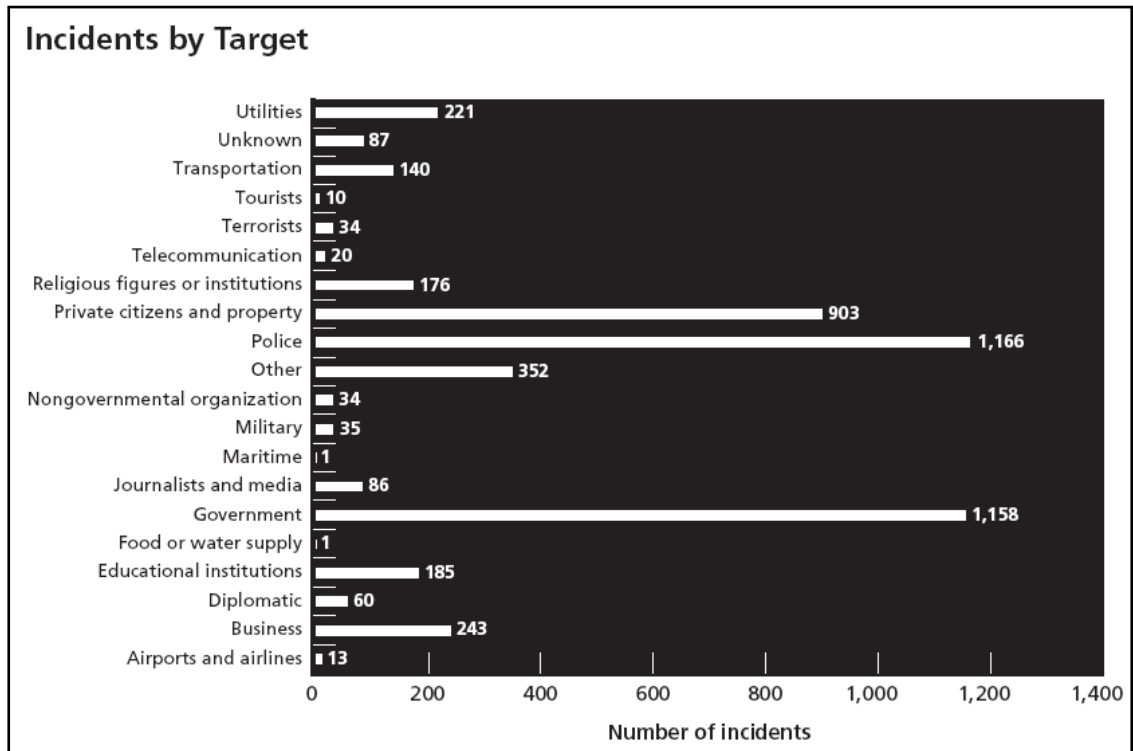
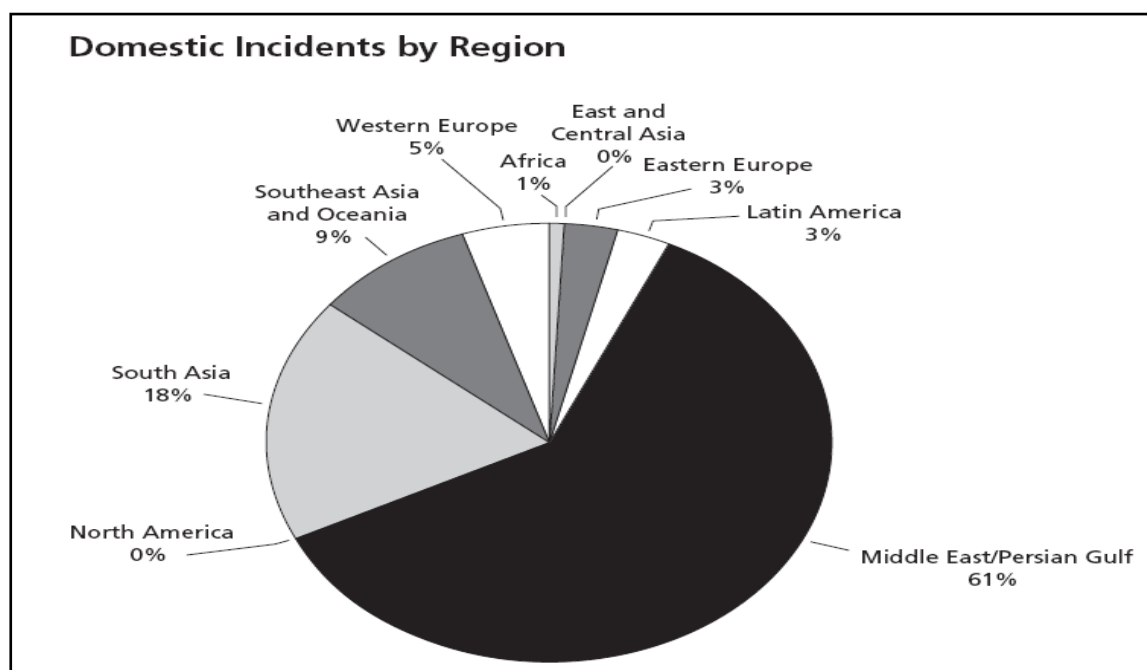


Figure 15: Domestic Incidents of Terrorism by Region, RAND-MIPT Terrorism Incident Database, 1 Jan. 2005 - 31 Dec. 2005 (MIPT Terrorism Annual 2006)



Name:	Country Reports on Terrorism – United States Department of State
Parent Host	United States Department of State
Website:	http://www.state.gov/s/ct/rls/crt/
E-mail:	Via website: http://www.state.gov/s/ct/rls/crt/
Access:	Free
Unit of Analysis	Terrorist Incident
Scope:	Domestic and International Terrorism
Period Covered:	First published 2004. Yearly report
Principle sources	Government sources, unclassified and open-source material
Key Variables	Country by country overview

Country Reports on Terrorism – United States Department of State

Introduction

The Country Reports on Terrorism were first published in 2004, replacing the annual Patterns of Global Terrorism publication. The United States Secretary of State is legally required to present to Congress annually, by the 30th April each year, the Country Reports on Terrorism. The report covers groups and countries as stipulated in legislation.

Historical Background

The United States Government's (USG) publication of an annual report on international terrorism dates back to 1977. Published by the CIA, the first report was titled "International Terrorism in 1976". In brief, the key aims of the report were to outline the scope and nature of international terrorism within a historical context and to discuss trends in international terrorism and their likely bearing upon the United States in the coming year. Numerous modifications to the publication occurred over the years. These ranged from changes of definitions of international terrorism, expanded narrative, addition of statistical appendices, to changes in statistical criteria. Other developments included the introduction of a chronology of significant terrorist incidents, the transfer of the publication to the State Department (1982) and a title change to "Patterns of Global Terrorism" (1984). Over the years the annual report evolved into the United States Government's key publication on statistics, trends and developments in international terrorism.

The final Patterns of Global Terrorism was published in 2004. The reports termination was the result of series of complex data integrity issues questioning the

accuracy of the statistical data in *Patterns of Global Terrorism 2003*. As a result of academic questioning and media and political unease, the U.S. State Department radically overhauled their annual report on international terrorism. Re-named as “Country Reports on Terrorism”, the annual report is confined to narrative commentary. The statistical element on terrorism incidents is now produced by the National Counter Terrorism Center (NCTC) and can be accessed via their website: www.nctc.gov.

Country Reports on Terrorism

The annual Country Reports on Terrorism, published by the U.S. Department of State, provides a comprehensive assessment worldwide of terrorism incidents, commentary on terrorism related issues, factual data and legal requirements. The first chapter of the Country Reports on Terrorism – 2007 is titled “Strategic Assessment”. This offers a backdrop to the overall report. It discusses trends in terrorism for the particular year of publication, as well as highlighting continuing areas of concern. Chapter Two provides an initial overview of the following geographic regions: Africa, East Asia and Pacific, Europe, Middle East and North Africa, South and Central Asia, and the Western Hemisphere. A detailed breakdown of developments within each country is provided. These include, for example, information on government action, counter-terrorism initiatives, new legislation, co-operation agreements and terrorist trials and outcomes. Other information includes combating terrorism finance, terrorist group activity and introduction of new technologies to counter acts of terrorism.

Chapter Three of the Country Report on Terrorism is dedicated to state sponsors of terrorism. The State Department cites five countries that meet their criteria: Cuba, Iran, North Korea, Sudan and Syria. An overview of state sponsored terrorism is given, accompanied by four key sanctions applied to the above states. In summary these are: 1) The banning of arms-related exports and sales. 2) Controls over the exports of dual-use items. 3) Prohibition on economic assistance. 4) Imposition of miscellaneous financial and other restrictions. Detailed narrative explaining respective countries sponsorship of terrorism is provided.

Chapter Four addresses the global challenges posed by Weapons of Mass Destruction (WMD) and danger that any of them might fall into the hands of non-state terrorists. An outline of how the United States approaches the issue of WMD on a diplomatic and strategic level is given. Several other areas are discussed. This includes the types of material that may be used by terrorists in WMD attacks, such as chemical, nuclear, biological and radiological substances and agents. The chapter also highlights concerns that either a state or the resources of a state may be used to conduct a WMD attack. Conversely, worries over emerging non-state facilitators acting knowingly or un-knowingly as a channel for access to resources and expertise that could potential lead to a WMD attack are also raised. Finally, a series of bilateral and multilateral partnerships with the United States, aimed at combating Weapons of Mass Destruction are discussed.

Chapter Five provides updated information on terrorist safe havens. This relates to the requirement by Congress, that the Country Reports on Terrorism provides an update of information on what the U.S. State Department identifies as

terrorist safe havens or sanctuaries, as stipulated in the Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA), section 7120(b).

A list of what the State Department identifies as “U.S. Government Designated Foreign Terrorist Organisations” (FTO) is provided in Chapter Six. An explanation of the terrorist group’s names and their aliases is given. In addition, a series of brief narratives provides a description of the groups, their activities, strength, location/area of operation and any external aid received. The final chapter of the Country Reports on Terrorism provides U.S. legislative requirements relating to the report and key terms used. An annex attached to the report provides statistical information used in the compilation of the document. Discussion includes, how, with support from the National Counter Terrorism Center (NCTC), statistical information for the reports are developed. Other areas covered include data interpretation, methodology, and an academic perspective on the statistical data used in the reports.

Figure 16: Total International Terrorist Attacks, 1982-2003

(Patterns of Global Terrorism 2003)

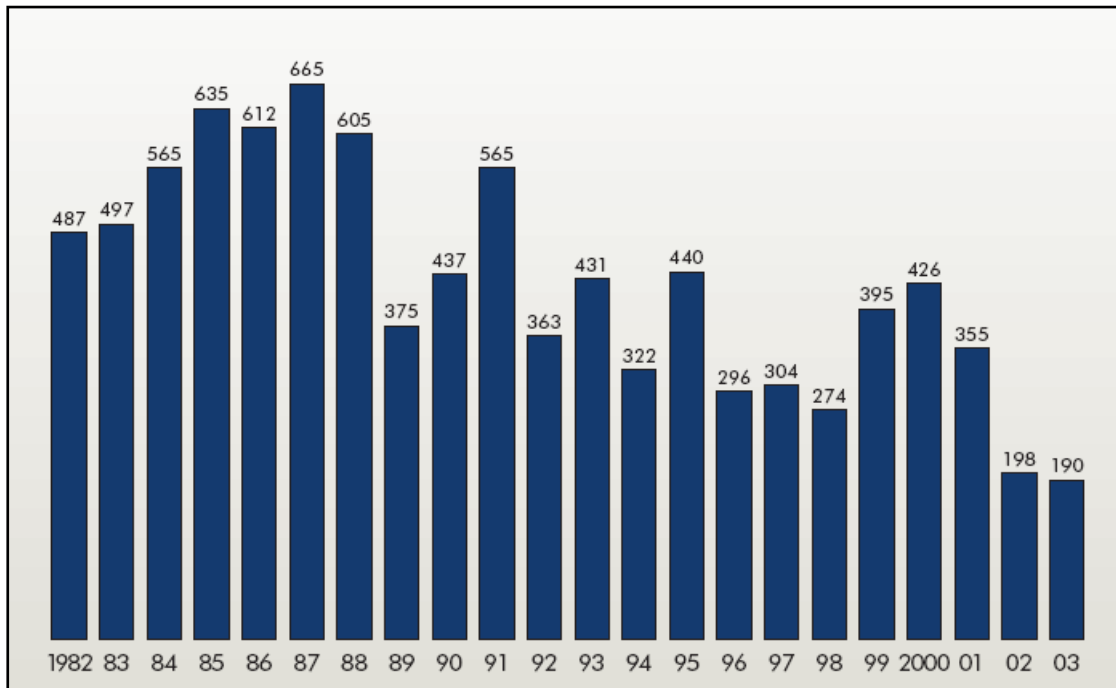


Figure 17: Incidents of Terrorism Worldwide (Country Reports on Terrorism 2008:

National Counterterrorism Center: Annex of Statistical Information)

Incidents of Terrorism Worldwide				
	2005	2006	2007	2008
Attacks worldwide	11,157	14,545	14,506	11,770
Attacks resulting in death, injury, or kidnapping of at least 1 person	8,025	11,311	11,123	8,438
Attacks resulting in the death of at least one individual	5,127	7,428	7,255	5,067
Attacks resulting in the death of zero individuals	6,030	7,117	7,251	6,703
Attacks resulting in the death of only one individual	2,880	4,139	3,994	2,889
Attacks resulting in the death of at least 10 individuals	226	293	353	235
Attacks resulting in the injury of at least one individual	3,842	5,796	6,256	4,888
Attacks resulting in the kidnapping of at least one individual	1,475	1,733	1,459	1,125
People killed, injured or kidnapped as a result of terrorism	74,280	74,709	71,608	54,747
People worldwide killed as a result of terrorism	14,560	20,468	22,508	15,765
People worldwide injured as a result of terrorism	24,875	38,386	44,118	34,124
People worldwide kidnapped as a result of terrorism	34,845	15,855	4,982	4,858

Name:	Terrorism in Western Europe: Events Data (TWEED)
Parent Host	Department of Comparative Politics, University of Bergen, Norway
Website:	http://folk.uib.no/sspje/tweed.htm
E-mail:	jan.engene@isp.uib.no
Access:	Free
Unit of Analysis	Terrorist Incidents in Western Europe

Scope:	Internal terrorism within 18 designated Western European Countries
Period Covered:	1950-2008
Principle sources	Keesing's Record of World Events
Key Variables	Date, month, year, country, type of agent, acting group

Terrorism in Western Europe: Events Data (TWEED)

Introduction

The Terrorism in Western Europe: Events Data (TWEED) was designed and compiled by Dr. Jan Oskar Engene of the Department of Comparative Politics, University of Bergen, Norway. The function of the data set is to allow researchers to analyse patterns of terrorism in Western Europe, whereby these are specifically related to historical and structural pre-conditions (Engene, 1994, 1998, 2004) and (Engene&Skjølberg, 2002). The key unit of analysis within TWEED is the terrorism event, as well as any action undertaken against terrorists or terrorist groups.

The TWEED data set, covering the period 1950-2004, codes data and information on terrorism events covering 18 countries in Western Europe. The data set records only internal (domestic) terrorism events and does not include acts of international terrorism.

Definition

For the purposes of the TWEED data set '...terrorism is understood theoretically as a form of violence that uses targets of violence in an indirect way in order to influence third parties, audiences' (Source: <http://folk.uib.no/sspje/tweed.htm>). Given the

theoretical and abstract nature of the definition for practical/operational running of the data set, the definitional criteria for an act of terrorism is used with reference to concrete terrorist events like bombings, shootings, sieges, explosions, kidnap and armed attacks.

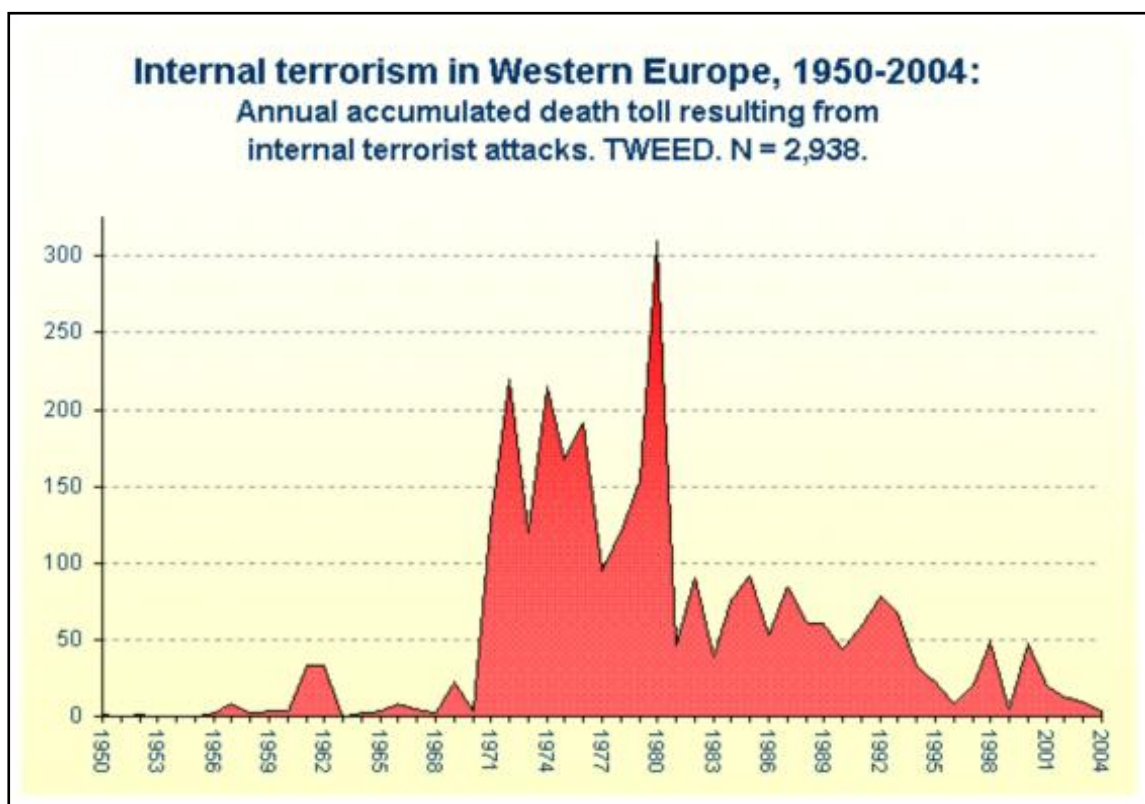
General

Only acts of internal terrorism are coded within TWEED, and only incidents carried out by individuals or groups originating from the designated 18 Western European countries are used within the data set. There are occasional exceptions, whereby an agent from another Western European country perpetrates an incident in one of the 18 countries.

The sole source used for the TWEED data set is *Keesing's Record of World Events* (formerly *Keesing's Contemporary Archives*). Keesing's longitudinal coverage of news events worldwide, dates back to 1931. However, Dr. Engene established 1950 as the start date for his data collection. In comparison, most other terrorism data sets have covered the temporal period 1968 onwards.

The TWEED data set records a total of 2,959 deaths attributed to terrorist agents. A total of 11,026 terrorist events are coded within the data set. The TWEED code-book (as PDF) and data set (SPSS) are both available for download from the TWEED website.

Figure 18: Internal Terrorism in Western Europe, 1950-2004 (TWEED at <http://folk.uib.no/sspje/tweed.htm>)



Name:	South Asia Terrorism Portal (SATP)
Parent Host	Institute for Conflict Management, New Delhi, India
Website:	http://www.satp.org/
E-mail:	icm@satp.org
Access:	Free
Unit of Analysis	Terrorist Incident
Scope:	Domestic and International Terrorism in the South Asia regions
Period Covered:	Varying years dependent upon country
Principle sources	Open source material
Key Variables	Date, incident

South Asia Terrorism Portal (SATP)

Introduction

The Institute operates the South Asia Terrorism Portal (SATP) established in 2000, for Conflict Management, New Delhi, India. The Institute is a registered non-profit, non-governmental organisation. Geographically the SATP covers: Bangladesh, Bhutan, India, Nepal, Pakistan and Sri Lanka. In addition, the Select States of India are included: Assam, Jammu and Kashmir, Manipur, Mizoram, Nagaland, Punjab and Tripura.

The SATP is entirely Web-based. The portal provides a comprehensive mixture of detailed narrative, chronological listings, statistical data, graphs, maps and documentation on terrorist incidents and events in the South Asia regions. Information can be accessed via a series of hyperlinks or by using the search facility within the website. The SATP is organised into a series of sections:

Assessment and Backgrounder

The Assessment section of the SATP provides a yearly in-depth review of the political climate within each country, and details terrorist events and activities over the year. Statistical data and tables from the SATP database are also included within the Assessments.

The Backgrounder section provides an historical context to political conflict and terrorism within regions and countries covered by the SATP. Detailed narrative is provided on the genesis of terrorist groups and the origins of particular conflicts. In addition, developments such as counter-terrorist operations, peace accords and

negotiations between particular parties and their outcomes are discussed. The Backgrounder also includes statistical data on terrorism injuries and fatalities and provides hyperlinks to in-depth information on particular terrorist groups and other related material.

Bibliography and Data Sheets

The website also provides a two-part bibliography listing books and articles for each country covered by the South Asian Terrorism Portal. For each respective country, the SATP Data Sheets provide an eclectic mixture of data including: chronological listings of bomb blasts, terrorist attacks, fatality statistics, insurgency activities, assassinations, conflict maps and elections results. The temporal period covered varies between each country and region. Data is sourced from local news reports.

Documents and Timelines

The Documents section provides terrorism researchers with primary source documentation relating to respective SATP countries and regions. These include legal documentation such as acts and ordinances, treaties and regulations on terrorism related matters. Additional papers are provided in the form of political speeches, statements and committee reports dealing with security, terrorism and conflict.

The Timeline provides a chronological format, broken down by day, month and year, detailing terrorist incidents, arrests of individuals, police/security force action, trials and outcome of trials. The Timeline covers information for the past seven or eight years. Summary information on key historical terrorism and political

events within each country is also provided. Dependent upon the country or region, this covers between the past fifty and a hundred years.

Terrorist Groups

The Terrorist Group section provides a comprehensive list of terrorist groups associated with a particular SATP country or region. Further in-depth information is provided with some of the groups listed. This includes the origins of a particular terrorist group, their objectives and ideology, leadership and group size and organisation. Where available, information is also provided on terrorist group funding, type of weaponry used in incidents, and details of specific terrorist attacks carried out by the group.

The South Asia Intelligence Review (SAIR)

The South Asia Intelligence Review (SAIR) is a weekly publication produced by the SATP and provides a mixture of news and assessments on terrorism and counter-terrorism related activities within the South Asia region. Further assessment and analysis on insurgencies and sub-conventional warfare is also discussed. In addition, the SAIR also covers terrorism policy and response issues as well as social, political and economic topics related to the region. Advance copies of The South Asia Intelligence Review (SAIR) are available via e-mail subscription.

The South Asia Terrorism Portal does not offer systematic aggregate annual data. A typical weekly assessment looks like this:

Figure 19: Weekly Fatalities: Major Conflicts in South Asia, 9 -15 March, 2009 (SATP, *Weekly Assessments & Briefings*, Vol. 7, No. 36, 16 March 2009)

	Civilian	Security Personnel	Force	Terrorist/Insurgent	Total
INDIA					
Arunachal Pradesh	0	0		3	3
Assam	1	0		0	1
Jammu and Kashmir	1	0		8	9
Manipur	1	0		6	7
Left-wing Extremism					
Bihar	5	0		1	6
Chhattisgarh	0	0		2	2
Jharkhand	1	0		3	4
Total (INDIA)	9	0		23	32
PAKISTAN					
Balochistan	2	1		0	3
FATA	8	0		42	50
NWFP	14	0		37	51

Total	24	1	79	104
(PAKISTAN)				
SRI LANKA*	89	NA	360	449

*The Ministry of Defence, Sri Lanka Government, has suspended release of casualty figures.

Media access to areas of conflict is also denied, and no independent sources of data are now available. Civilian data is based on information published by the pro-LTTE Website

Tamil Net. - Provisional data compiled from English language media sources.

Name:	The International Policy Institute for Counter-Terrorism (ICT) – Terrorist Incident Database
Parent Host	International Institute for Counter Terrorism (ICT), Interdisciplinary Center (IDC), Herzliya, Israel
Website:	http://www.ict.org.il/
E-mail:	Via website
Access:	Access status currently unknown
Unit of Analysis	Terrorist Incident
Scope:	Primarily, but not exclusively, terrorist incidents in the Middle East
Period Covered:	1975-2008
Principle sources	Open-source material
Key Variables	Organisation, method used, target type, location, date range, casualties

The International Policy Institute for Counter-Terrorism (ICT) – Terrorist Incident Database

Introduction

The Terrorist Incident Database, is operated by the International Institute for Counter Terrorism (ICT) at the Interdisciplinary Center (IDC), Herzliya, Israel. The ICT, an independent think-tank, is a non-profit organisation. The ICT provides specialist advice and expertise in a broad range of security related fields, including terrorism and counter-terrorism, homeland security and intelligence analysis. The ICT's Terrorist Incident Database is an interactive web-based database focusing primarily, but not exclusively on terrorism incidents in the Middle East.

The Terrorist Incident Database and Terrorist Organizations

The original Terrorist Incident Database dates back to 1975 and now contains in excess of 31,000 incidents. The database is divided into three key areas: Terrorist Organisations, International Terrorism and Arab-Israeli Conflict. This section profiles over fifty terrorist organisations and their national affiliations. Links to each group provides in-depth information on a particular terrorist organisation. This includes an explanation of the group's name, a historical background to the group's development and its ideology and strategy. Detailed narrative on a terrorist group's organisational structure is also given, including leadership, hierarchy and the military arm (if existing) associated with a particular group. If available, information on terrorist group financing and operations to counter-act funding of groups is provided. The terrorist organisations section also displays terrorist group insignia, and provides a chronological listing of terrorist attacks associated with each group. An extensive selection of primary and secondary source articles and documents

relating to each individual terrorist group are also made available within this section of the database.

The Terror Attack Database permits researchers to query international terrorist incidents from 1986 onwards. The ICT updates the database monthly; however, the database is not exhaustive. Using a series of drop down menus, the Terror Attack Database can be queried using a combination of up to six fields: Organisation (name of terrorist organisation), Method Used (tactics – for example, bombing, chemical attack, hijacking, incendiary device), Target Type (for example, embassy, school, airport), Location (worldwide), Date Range (1986 onwards) and Casualties (numbers).

The Arab-Israeli Conflict database allows researchers to search for incidents and casualties related specifically to the Middle East conflict. A combination of six drop-down fields can be searched: Type of Incident (for example, terror attack, internecine violence, violent clash), Terrorist Organisation Involved (these are restricted to Middle East Groups within the menu), Method Used (tactic – letter bomb, suicide car bomb, mortar attack), Targeted (type of place or person targeted), Location (Gaza Strip, Israel, Palestine, West Bank, unknown), Date Range (1986-2006) and Casualties (numbers).

OSINT (Open Sources of Intelligence)

In recent years ICT has expanded its terrorism monitoring systems with the development of OSINT (Open Sources of Intelligence). Based upon open source intelligence the OSINT system is linked to ICT's Incidents and Activists Database. Interactively based, the OSINT system allows data to be linked relationally and cross-

referenced. Holding in excess of 31,000 incidents the database records both foiled and completed terrorist attacks as well as counter-terrorist operations. The system is also able to provide background narrative detail and follow-up information.

Figure 20: All Israeli Fatalities, Monthly, Palestinian – Israeli Conflict, 2000-2003 (www.ict.org.il)

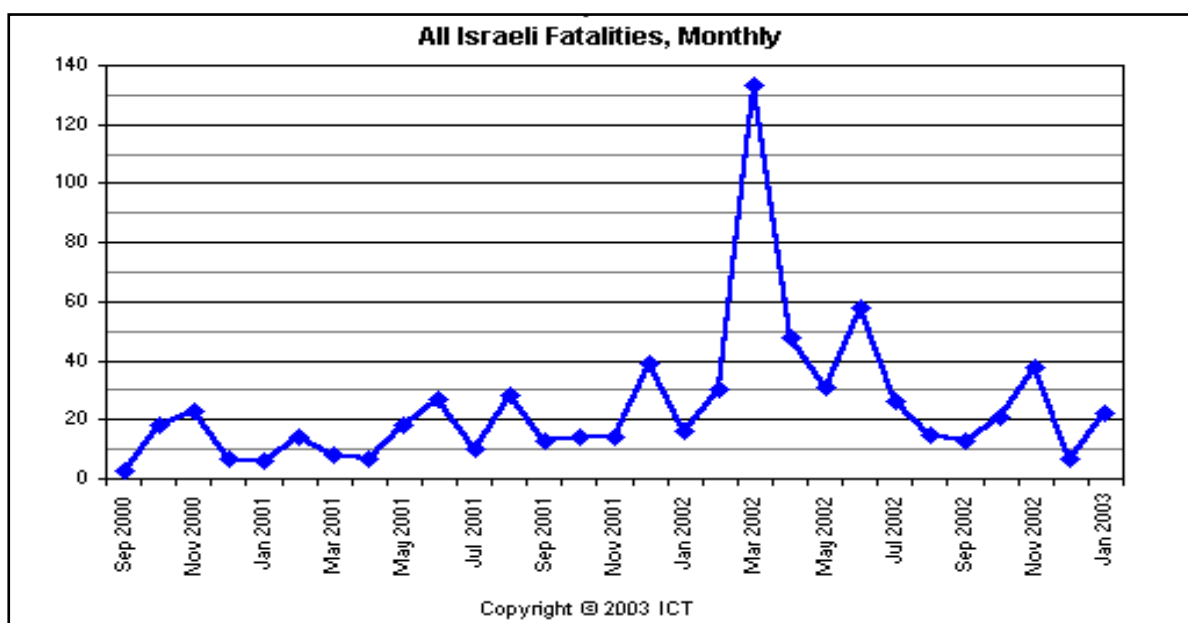


Figure 21: All Palestinian Fatalities, Monthly, Palestinian – Israeli Conflict, 2000-2003 (www.ict.org.il)



Name:	Political Terror Scale (PTS)
Parent Host	University of North Carolina at Asheville, United States
Website:	http://www.politicalterrorsscale.org/
E-mail:	mgibney@unca.edu
Access:	Free
Unit of Analysis	Political Violence and Terror
Scope:	Global
Period Covered:	1976-2007
Principle sources	United States Department of State Country Reports on Human Rights Practices and Amnesty International's yearly reports
Key Variables	Region, income level, OECD status, COW# scale (1-5) per year

Political Terror Scale (PTS)

Introduction

The Political Terror Scale (PTS), originally developed at Purdue University in the early 1980's, is a data set measuring yearly levels of political violence and terrorism by state actors. The PTS covers more than 180 countries with a temporal range 1976 to 2007. The data set is updated annually. Since 1984 Mark Gibney, based now at the University of North Carolina at Asheville, has managed the PTS.

The Data Set

The Political Terror Scale uses as a measurement a scale of 1-5 to determine levels of political terrorism and repressive human rights practices occurring within countries within any one year. The terror scale was originally developed by the independent organisation Freedom House. Although the PTS title implies a focus on political terrorism, it is essentially a data set on human rights violations by states. The term terror used by the PTS '.... refers to state-sanctioned killings, torture, disappearances and political imprisonment...' (Source: [Error! Hyperlink reference not valid.](#)). The data set records primarily levels of state-sanctioned violence. However, some forms of non-state violence are included, for example in civil war situations. The PTS emphasis is on the measurement of actual physical integrity violations rather than levels of general political repression within the state.

Figure 22: Political Terror Scale Levels

Level 5	Terror has expanded to the whole population. The leaders of these societies place no limits on the means or thoroughness with which they pursue personal or ideological goals.

Level 4	Civil and political rights violations have expanded to large numbers of the population. Murders, disappearances, and torture are a common part of life. In spite of its generality, on this level terror affects those who interest themselves in politics or ideas.
Level 3	There is extensive political imprisonment, or a recent history of such imprisonment. Execution or other political murders and brutality may be common. Unlimited detention, with or without a trial, for political views is accepted.
Level 2	There is a limited amount of imprisonment for nonviolent political activity. However, few persons are affected, torture and beatings are exceptional. Political murder is rare.
Level 1	Countries under a secure rule of law, people are not imprisoned for their views, and torture is rare or exceptional. Political murders are extremely rare.
	Source: http://www.politicalterroryscale.org/about.php

The highest level of political terror (scale 5), ranges from terror that has reached the whole population of a country to the lowest (scale 1) where countries have secure rule of law, freedom of expression is permitted, and politically motivated murder and torture is extremely rare. In addition to the scale rating of 1-5, the dynamics of the political terror scales are also based upon more subtle conceptual levels. The assumption is that the measurement of state use of violence can also be based on the trinity of: scope, intensity and range. The first dimension, scope, would indicate the actual type of violence that the state conducts. This could include killings, torture and imprisonment. The second dimension, intensity, relates to how often the state conducts a particular type of violence within a specified period; for the PTS this would be within any one year. The intensity variable also refers to the number of individuals targeted by the state. The third dimension, range, records the actual segment(s) of society encountering state violence.

The PTS uses two sources to compile the data set: the U.S. State Department Country Reports on Human Rights Practices and Amnesty International's yearly report. Both the Political Terror Scale ratings and countries data can be downloaded via the web in spreadsheet format. The PTS website provides users with an interactive map of geographic regions and country breakdown. This lists the PTS scores arrived from both coding Amnesty International and the U.S. State Department annual reports. The scores derived from these two sources do not diverge as much as one would expect. As an instrument to measure state use of terrorism rather than non-state use of such violence, this database is unique. However, it has its measurement problems, placing sometimes countries on the same level that have quite different levels of democracy and adherence to the rule of law.

Figure 23: Increasing Human Insecurity, 1976-2008 (Median Scores)
(www.politicalterrorsscale.org<http://www.ict.org.il>).

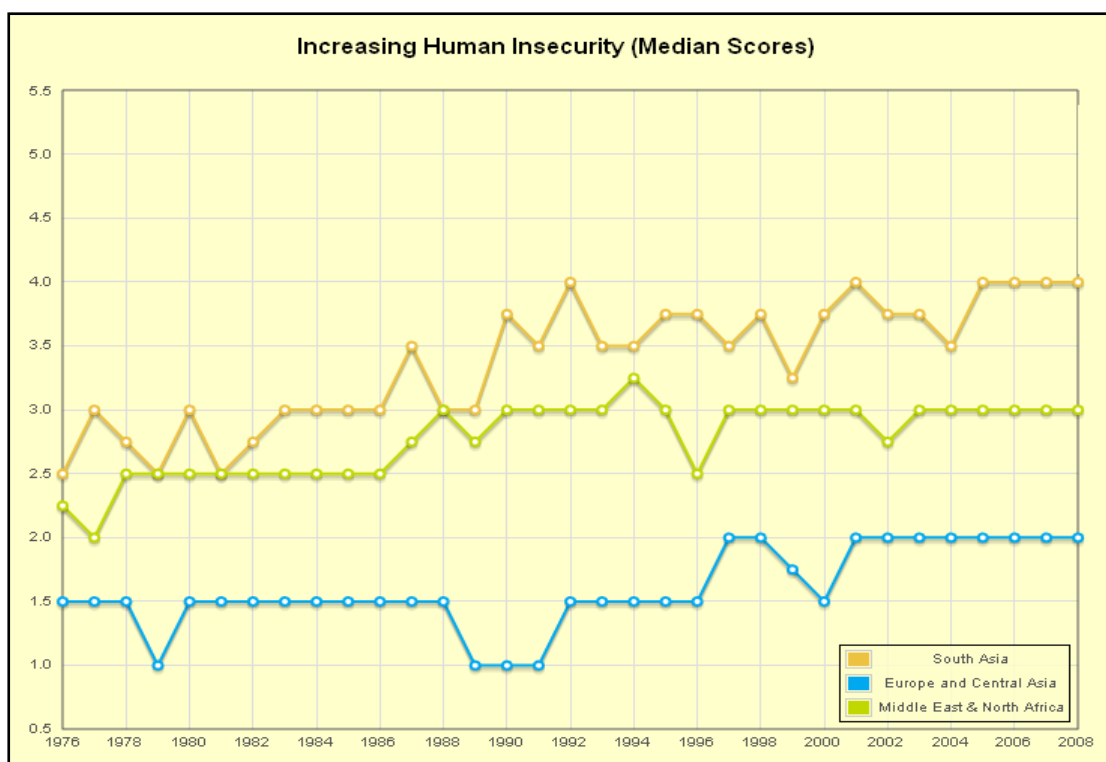
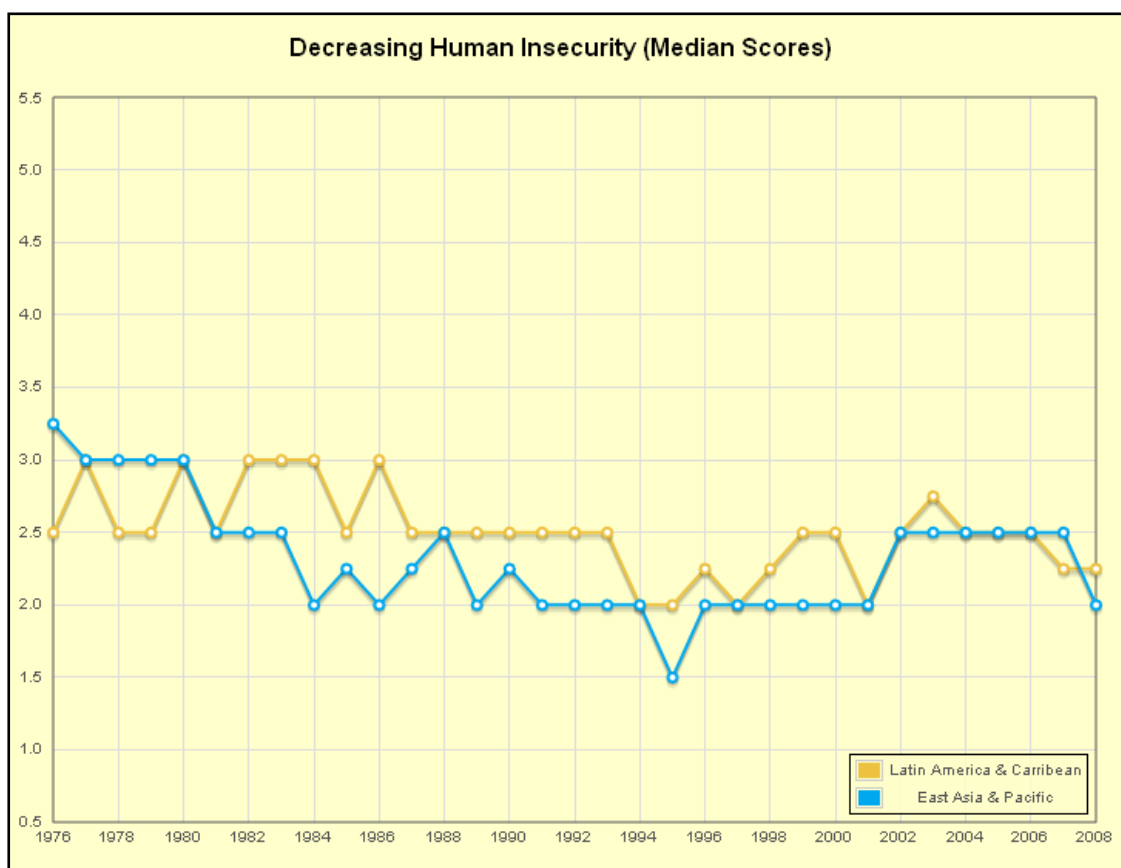


Figure 24: Decreasing Human Insecurity 1976-2008 (Median Scores)

(www.politicalterroryscale.org<http://www.ict.org.il>).



Name:	The American Terrorism Study, 1980-2002
Parent Host	Terrorism Research Center, Fulbright College, University of Arkansas, AR United States
Website:	http://trc.uark.edu/index.php/rschProjects/1 See also: http://www.icpsr.umich.edu/cocoon/NACJD/STUDY/04639.xml
E-mail:	bls@uark.edu
Access:	Free via www.icpsr.umich.edu website. Certain identifying information within the dataset is restricted.
Unit of Analysis	Administrative records data
Scope:	Indictments from federal "domestic security/terrorism investigations" in the United States from 1980 to 2002.

Period Covered:	January 1980 - August 2002
Principle sources	United States District Court case records
Key Variables	Demographic information, terrorist group information, prosecution and defence data. Count/case outcome and sentencing data

The American Terrorism Study, 1980-2002

The American Terrorism Study (ATS) was established in 1989 by Brent L. Smith of the University of Arkansas and Kelly R. Damphouse of the University of Oklahoma. The origins of the project were driven by the paucity of data on acts of American terrorism. Source data for the study came from the Federal Bureau of Investigation's (FBI) Terrorist Research and Analytical Center. In 1989 the Center released a list of individuals who had been indicted following investigation under the FBI's Counterterrorism Program. One of the key aims of the study was to establish an empirical database to permit researchers to evaluate criminological theories and government policy. The American Terrorism Study comprises of two key constituent parts: a statistical database and a series of .PDF files containing case documents. These include such items as indictments, judgment orders and sentencing memoranda.

From the list of persons who had been indicted in federal criminal courts, the results of official terrorism investigations, the research team was able to review each case. The review was undertaken at two venues: the federal district court – the actual location where the case was tried, and the federal regional records center, which held archive records of the cases.

The American Terrorism Study consists of five data sets (Parts 1-5). Each dataset contains approximately 80 variables. The variables are categorized into four key areas: (1) demographic information, (2) information on the terrorist group of which the indictee is a member (3) prosecution and defense data, and (4) count/case outcome and sentencing data (ICPSR).

The basic data set Part 1 – Counts Data contains data ‘on every count for each indictee in each indictment’. Between 1980 and 2002 there were 7,306 counts. Part 2 – Indictees Data contains information on every indictee recorded between 1980 and 2002. This amounted to 574 indictees. Part 3 – Persons Data contains information every person (510 in total) indicted by the federal government as a consequence of a terrorism investigation. Part 4 - Cases Data contains data on every criminal terrorism case that took place as a consequence of a federal terrorism investigation. The final dataset Part 5 – Group Data ‘provides one line of case data for each of the 85 groups that were tried in federal court for terrorism-related activity’ (Source: ICPSR). The FBI has made subsequent lists of data available to the principal investigators. The core ATS dataset is in the process of being merged with the geospatial and temporal projects datasets at the University of Arkansas.

Name:	The European Union Terrorism Situation and Trend Report (TE-SAT)
Parent Host	Europol
Website:	http://www.europol.europa.eu/
E-mail:	Via website
Access:	Free
Unit of Analysis	Terrorist Incidents within the European Union
Scope:	European Union

Period Covered:	2006-2008 and ongoing
Principle sources	Government figures and open-source material
Key Variables	N/A

The European Union Terrorism Situation and Trend Report (TE-SAT)

The European Union Terrorism Situation and Trend Report (TE-SAT) is published on an annual basis by Europol. Its origins derive from the terrorism events of September 11th 2001. The TE-SAT report is presented to the European Parliament on behalf of the Terrorism Working Party (TWP) of the Council of the EU. The remit of TE-SAT is to make available basic factual data, and information on terrorism within the European Union (EU). The TE-SAT report is aimed at interested law enforcement officials, policymakers and the general public. It is a publicly available, unclassified publication, and can be accessed via the Internet. Source information for the TE-SAT report is mostly provided and verified by recognised EU member state law enforcement officials. Additional open source information is also used. As well as factual and statistical information, the TE-SAT report seeks to identify trends and developments in terrorism within the European Union. The most recent report (2010) covers terrorism data for the period 2006-09.

The format of the report is divided into a series of sections. These are: methodology and data collection, a general overview of terrorism in the EU for 2008, Islamist terrorism and ethno-nationalist and separatist terrorism. The remaining sections address left-wing and anarchist terrorism, right-wing terrorism, single issues terrorism and terrorism trends in the EU. Each section contains narrative

commentary and analysis on terrorist attacks, arrested suspects and terrorist activities, as well as data, tables and graphics. Annexes defining terrorist offences, legal and definitional issues and basic statistical data for each EU member country are provided.

The Europol database suffers from the use of different definitions of what constitutes terrorism in different member states – despite the fact that there is a common EU framework definition. It also suffers from the fact that some countries provide a great deal of data (e.g. France and Spain) and many others far fewer (United Kingdom).

Figure 25: Number of failed, foiled or successful attacks and number of arrested suspects for separatist terrorism in member states 2006-2008 (TE-SAT Report 2009).

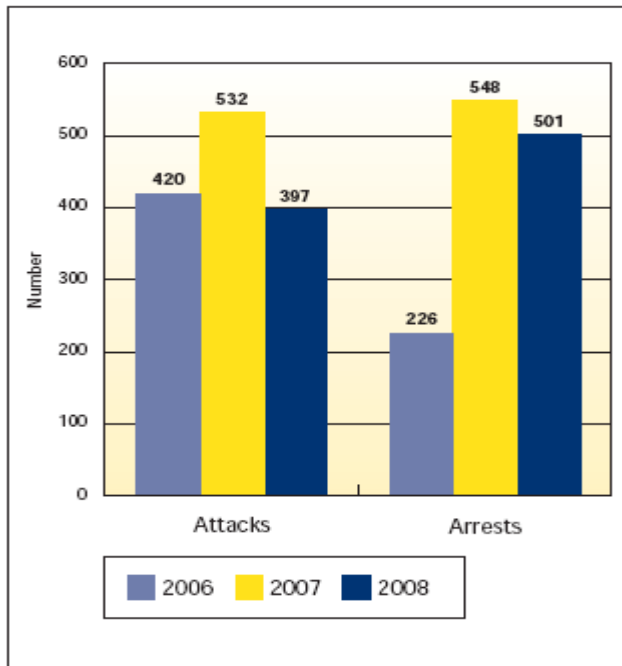
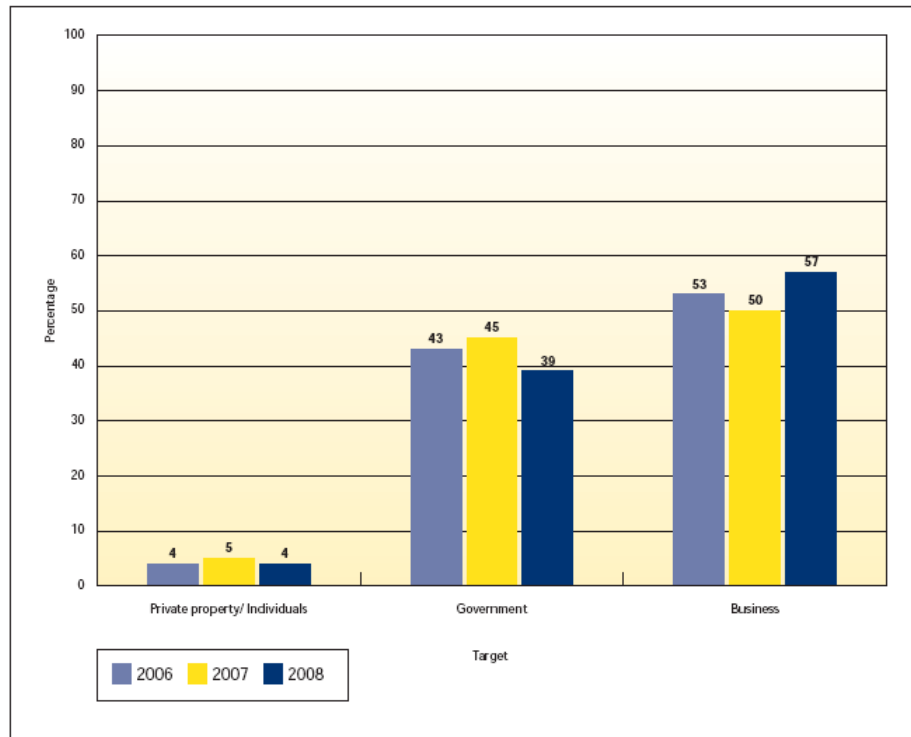


Figure 26: Left-wing and Anarchist Terrorist Attacks by Target, 2006-2008

(TE-SAT Report 2009)



Name:	Global Pathfinder
Parent Host	International Centre for Political Violence and Terrorism Research (ICPVTR), S. Rajaratnam School of International Studies, Singapore.

Website:	http://www.pvtr.org/
E-mail:	iskelvinder@ntu.edu.sg
Access:	Subscription
Unit of Analysis	Terrorist Incident
Scope:	Terrorism globally, but special focus on terrorism and political violence within the Asia-Pacific region
Period Covered:	N/A
Principle sources	Primary documents and open-source material
Key Variables	Profiles of terrorist groups, individuals, terrorist and counter-terrorist incident details, terror attack profiles

Global Pathfinder

The Global Pathfinder is a terrorism database operated by the International Centre for Political Violence and Terrorism Research (ICPVTR) within S. Rajaratnam School of International Studies, Singapore. The Global Pathfinder database collects data on terrorism globally. However, it specialises in terrorism and political violence within the Asia-Pacific area, concentrating on Southeast Asia, North Asia, South Asia, Central Asia and Oceania. Information within the database is open source and proprietary. The database is a subscription-based service.

The Global Pathfinder database is divided into five key areas: 1. Profiles of terrorist groups and individuals. 2. Support Data – terrorist and CT incident details, terrorist attack profiles, information repository, news and sources. 3. Counter-

Terrorism Security – for example agriculture and food, nuclear issues and transportation. 4. Strategic Counter-Terrorism – for example ideology, informatics, legislation and terrorist financing. 5. Country of concern.

The database contains a broad range of documents. These include: primary documents, terrorist training manuals, legal documents, interviews with terrorists and photographic material. Non-English jihadi website documents within the database are translated and analysed by specialists within the ICPVTR. The Global Pathfinder database can also generate reports, graphs and statistical tables.

Name:	The Institute for the Study of Violent Groups (ISVG) Database
Parent Host	Sam Houston State University, TX, in conjunction with the University of New Haven, West Haven CT, USA
Website:	http://www.isvg.org
E-mail:	isvg@shsu.edu
Access:	Restricted
Unit of Analysis	Extremism, terrorism and related trans-national crime
Scope:	Global
Period Covered:	2003 onwards. Currently logging data for previous 20 years
Principle sources	Open-source material
Key Variables	N/A

The Institute for the Study of Violent Groups (ISVG) Database

The ISVG database is based at Sam Houston State University, Texas, USA, but is run in conjunction with the University of New Haven, West Haven CT. It is an open

source database (using more than 9,000 sources) recording information on extremism, terrorism and related trans-national crime. Other data collected includes information on terrorist tactics, logistical activities and CT security operations. The ISVG began its data collection in 2003. It is currently logged data stretching back over 20 years. At present, the database is not fully accessible to the public; access is restricted to ISVG partners and U.S. Government sponsored projects. The ISVG plans from the summer of 2009 to make available web-based access in some format. The collection methodology is human-centric rather than machine centric. The database is relational in design, providing a broad array of functionality. It contains up to 2,000 variables. It lists (as of May 2010) 2471 groups and 27,576 individuals that are linked to terrorism and extremism. ISVG collects data on both violent incidents and non-violent ones (like hostage releases). Its inventory of violent incidents covers 47,999 armed assaults, 4,759 cases of arson, 35,376 bombings and also lists attempted CBRN attacks (10 of the nuclear variety, 46 biological ones and 70 chemical). Individual incidents are coded as well as related tactical and operational information. Given the relational design of the ISVG database, it can be used in conjunction with analysis and visualisation software.

Figure 27: Sample ISVG OmniscopeDataplayer – Incidents by Tactics, Philippines 30/12/00 – 13/6/09
(www.isvg.org)

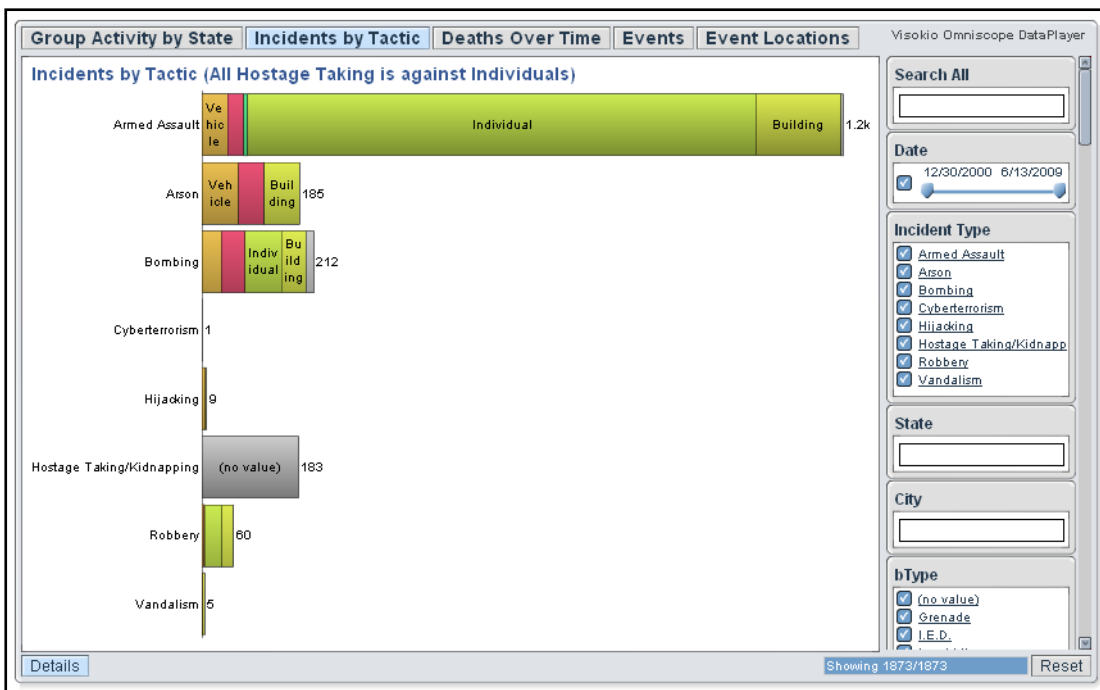
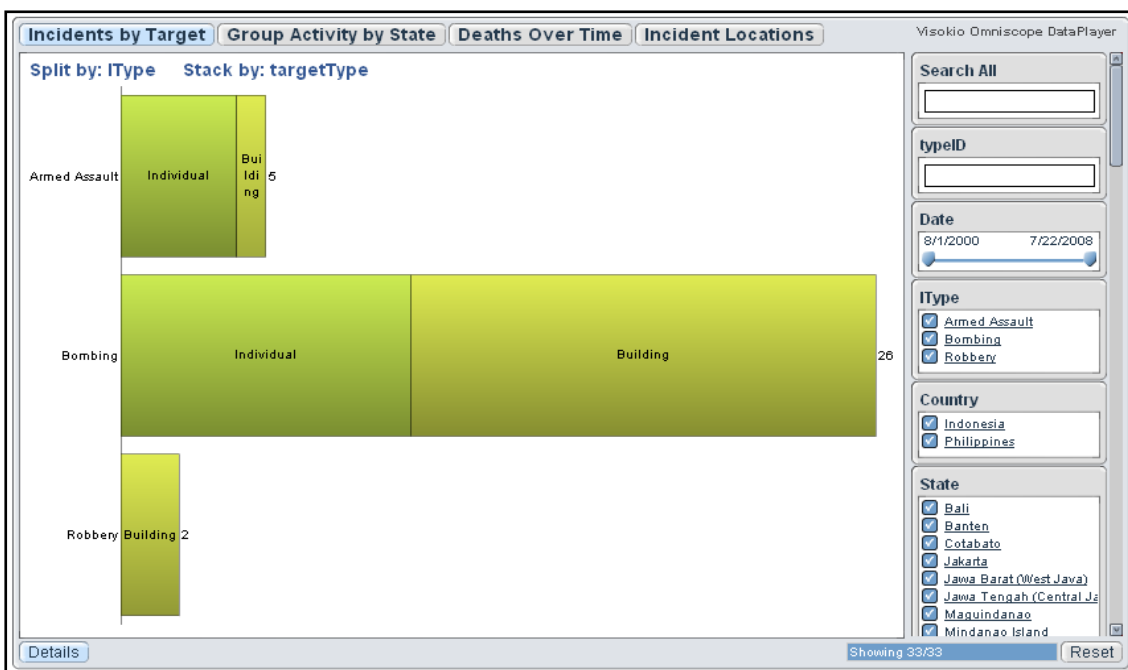


Figure 28: Sample ISVG OmniscioDataPlayer – Incidents by Targets, Jemaah Islamiya 01/08/00 – 22/07/08 (www.isvg.org)



Name:	Monterey WMD Terrorism Database
--------------	---------------------------------

Parent Host	Monterey Institute of International Studies, Monterey CA. United States
Website:	http://montrep.miiis.edu/databases.html
E-mail:	montrep@miiis.edu
Access:	Restricted
Unit of Analysis	Sub-state actors who are involved in the acquisition, possession, threat and use of weapons of mass destruction (WMD)
Scope:	Global
Period Covered:	1900 to present day
Principle sources	Open-source material
Key Variables	N/A

Monterey WMD Terrorism Database

This WMD Terrorism Database is operated by the Monterey Terrorism Research and Education Program (MonTREP) at the Monterey Institute of International Studies. The database records incidents by sub-state actors who are involved in the ‘... acquisition, possession, threat and use of weapons of mass destruction...’ (Source: www.mis.edu). In particular, these are incidents involving chemical, biological, radiological and nuclear materials (CBRN). Incidents recorded date from 1900 to the present day. Sources used to compile the database derive from a large array of open-source materials. These include government documentation, media news services, unpublished material, academic journals and Internet sites. Non-English source material is also used, including documentation in German, Arabic, Russian, Chinese and Korean. The Monterey WMD Terrorism Database holds in excess of

1,100 reported incidents. While access to the database is free, there are restrictions on the type users permitted access and registration is required. Use of the database is normally restricted to United States federal, state and local government employees. In addition, current serving members of the U.S. armed forces are also permitted access.

Name:	Armed Conflict Database
Parent Host	The International Institute for Strategic Studies (IISS) London, United Kingdom
Website:	http://www.iiss.org/publications-old/armed-conflict-database/
E-mail:	Via website
Access:	Subscription
Unit of Analysis	Armed Conflict
Scope:	Global
Period Covered:	2000-2008
Principle sources	Open-source
Key Variables	World map, country list, conflict list, non-state armed groups

Armed Conflict Database – The International Institute for Strategic Studies (IISS)

The Armed Conflict Database (ACD) is a web based interactive database providing access to information on armed conflicts worldwide. The ACD is maintained by the International Institute for Strategic Studies (IISS), based in London. It is a subscription-based service.

The ACD covers three areas of armed conflict: international, internal and terrorism conflict. The international conflict element of the database covers

governments that are engaged in armed border and territorial conflicts over sovereignty. Internal armed conflict refers to conflict between a government and organised group(s). The territory in question controlled either by government or organised group(s) must be sufficient enough to sustain military operations. One area the ACD compiles data on is terrorism. For the purposes of the database **'Terrorism [is] attacks involving one or more factions in significant armed opposition to a state. The intensity in violence in such attacks varies. Violence directly attributable to organised crime is not included'** (Source: IISS Website). The scope covered within the ACD's database range from information on Internally Displaced Persons (IDP's), historical backgrounds to conflicts, the type of weapons used to annual updates and timeline on conflict. The database contains information on 70 armed conflicts. Data within the ACD dates back to 2000/2001. Annual and quarterly reports based on data from the Armed Conflict Database are produced by the IISS. The timelines are updated weekly.

Access to the Armed Conflict Database is via an interactive world map, and clicking on either a continent or a particular country. The Regional Map section of the ACD allows access to all current regional conflicts. Researchers can then navigate to a specific country's conflict pages. The conflict page provides a summary background to the conflict and factual information on the current status of the conflict. This includes the amount of people internally displaced (IDP's), numbers of refugees, fatalities and the type of weaponry used in the conflict. More specific sections with the database include: political developments, military and security developments, humanitarian developments and historical backgrounds to each conflict. A Latest Timeline section provides regularly updated information on conflict

developments. Users are also provided with links to related conflict and official documents as well as IISS publications and materials.

The ACD also provides a search engine facility to retrieve data based on simple queries or more complex query operators. For example: “IRA AND Assassination”. Users of the ACD are also able to access a series or tailored reports sourced from the database. In addition to general queries, the database can generate more specific queries on conflicts to be produced in report format. This also includes the correlation of reports from different years across regions and topics. The database can also query specific variables that can be presented in report format, including graphics such as pie-bar-and line-charts.

Figure 29: Sample Algeria from Armed Conflict Database – The International Institute for Strategic Studies (www.iiss.org).

Latest timelines

Background

Links

Political trends

Military & Security

Human Security

Algeria (AQ Islamic Maghreb/GSPC)

[Print](#)

Latest Update

The Algerian government, under the leadership of President Abdelaziz Bouteflika, made a concerted effort in **2009** to pursue its policy of offering amnesty to members of al-Qaeda Islamic Maghreb (AQIM) willing to surrender their arms. [Read more >>](#)

Year ▶ - select - ▼

Annual Update 2009


Fact Box 2009
[Definitions](#)

Non State Parties	-Al-Qaeda in the Islamic Maghreb/Groupe Salafiste pour la Predication et le Combat (GSPC)
State Parties	-Algeria (gov of)
Type	Terrorism
Political Status	Active
Fatalities	249
Weapons:	
Non State Parties	Artillery , MANPADS , Mines and improvised explosive devices (IED) , mortars , Small arms and light weapons (SALW)
State Parties	Armoured vehicles , Artillery , Fixed-wing aviation , MANPADS , mortars , Rotary-wing aviation , Small arms and light weapons (SALW) , Submersibles , Surface ships


Figure 30: Sample Myanmar from Armed Conflict Database – The International Institute for Strategic Studies (www.iiss.org).


[Latest timelines](#) [Background](#) [Links](#)
[Political trends](#) [Military & Security](#) [Human Security](#)

Myanmar

Print 

Year ▶

Fact Box	Definitions 
Non State Parties	<ul style="list-style-type: none"> -All Burma Students Democratic Front -United Wa State Army (UWSA) -Mon National Liberation Army (MNLA) -Mong Thai Army (MTA) -Democratic Karen Buddhist Army (DKBA) -Palaung State Liberation Army (PSLA) -Kachin Independence Army (KIA) -Karen National Liberation Army (KNLA) -Karen National Union (KNU) -Karenni National Progressive Party Army -Shan State Army - South (SSA- South) -Chin National Army (CNA) -Myanmar National Democratic Alliance Army (MNDAA)
State Parties	-Myanmar (gov of)
Type	Internal Armed Conflict
Political Status	Active
Fatalities	>13,790 since 1985
Refugees	178,845
IDPs	451,000
Weapons:	



Name:	Iraq Body Count
Parent Host	Iraq Body Count
Website:	http://www.iraqbodycount.org/
E-mail:	analyst@iraqbodycount.org
Access:	Free. Archive data upon request
Unit of Analysis	Solely civilian violent deaths from the post-invasion of Iraq 2003
Scope:	Iraq
Period Covered:	2003 onwards
Principle sources	Open source material, official figures
Key Variables	IBC Incident number, type, deaths recorded, targeted or hit, place, date, sources

Iraq Body Count

Introduction

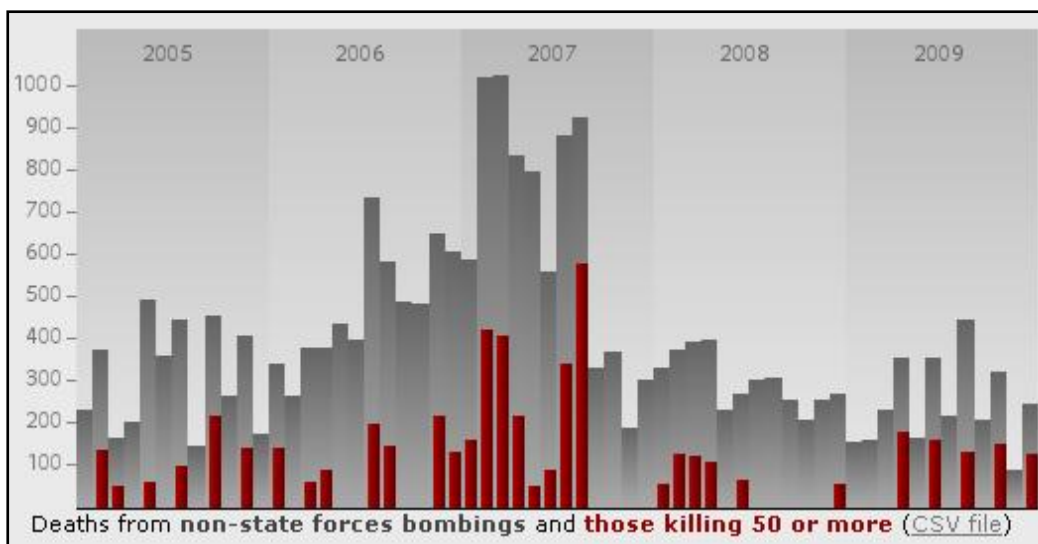
The Iraq Body Count (IBC) was established in 2003. It is a web-based project that records solely civilian violent deaths from the post-invasion of Iraq, as a consequence of the 2003 military intervention by the United States. Deaths recorded within the Iraq Body Count include casualties resulting from the actions of United States led coalition forces. Deaths/crime attributable to paramilitary actions and criminal activity are also included. The Iraq Body Count is a publicly accessible database. All deaths entered within the IBC database are factually recorded deaths. Volunteers operate the Iraq Body Count; they are drawn from a mixture of academic and activist backgrounds.

Overview

Material used to compile the Iraq Body Count database is sourced from an eclectic range of documents. Data is sourced from English-language media reports of deaths and bodies being found as a result of violent events. English translations of original non-English language reports are also used where standards of translation are deemed to be proficient. The vast majority of incidents recorded in the database are obtained from journalist's reports with access to human sources. These include emergency service personnel, police, and survivors of incidents, eyewitnesses and family members. The incidents are crosschecked for validity and to avoid duplication. In addition, supplementary data is also reviewed and extracted from non-governmental organisations, official figures, and hospital and morgue records. The data is used to provide running totals of civilian violent deaths. Two figures are

provided: minimum deaths and maximum deaths. Organisation of the IBC data is divided into two key areas. Firstly, a digital archive of original press and media source material, and secondly, a database with 18 key variables relating to recorded deaths. Access to the press and media archive, where deemed appropriate, is available to legitimate researchers. The database element of the Iraq Body Count is publicly available via the IBC website. The database provides users with two key sections: records of each recorded incident and records of individual deaths as a result of violent events victimizing civilians. The database codes, where information is available, 12 key variables for each incident and 6 key variables relating to individual persons. Some of the key incident variables include: date, time, place, target and maximum deaths. For each individual, the key variables are: name, age and gender. Criteria for entry of incidents to the database require that at least two independent sources be crosschecked and verified. A recent events section provides very recent information on deaths (up to the last 48 hours) that still require full verification and validity checks prior to entry into the IBC database. The database is dynamically searchable and provides data summaries, graphical data and tables as well as analyses of events. Data can be exported from the database in .CSV file format for upload to a spreadsheet.

Figure 31: Deaths from non-state forces' bombings and those killed fifty or more (Iraq Body Count)



Name:	The IAEA Illicit Trafficking Database (ITDB)
Parent Host	International Atomic Energy Agency
Website:	http://www-ns.iaea.org/security/itdb.htm
E-mail:	Official.Mail@iaea.org
Access:	Restricted
Unit of Analysis	Illicit trafficking among States of nuclear and radioactive material and related unauthorised activities
Scope:	Global
Period Covered:	1995 onwards
Principle sources	State-confirmed information and open-source material
Key Variables	N/A

The IAEA Illicit Trafficking Database (ITDB)

The Illicit Trafficking Database (ITDB) was established by the International Atomic Energy Agency (IAEA) in 1995. It records incidents involving the illicit trafficking in and between countries, of nuclear and radioactive material and related unauthorised activities. The principal objective of the database is to allow for the

exchange of authoritative information on the aforementioned activities. The ITDB has since developed into a broader information system generating statistical data for analysis, and the publication of Quarterly and Annual Reports. The database is used by the IAEA in three key areas: the prevention of nuclear and radiological terrorism, as an alert system, and for the enhancement of nuclear security. Membership of the ITDB program is based upon State's voluntarily signing-up. State's signing up for the ITDB program are required to nominate a single national Point of Contact (POC) who will liaise between the respective member State and the IAEA. One hundred State's had joined the ITDB program as of the 1st of September 2008.

Incidents recorded within the ITDB include the theft, possession, loss, use, provision, transfer or disposal of radiological or nuclear materials. These incidents can occur within a state and across international borders. Failed and thwarted attempts in illicit trafficking of nuclear and radiological materials are also entered within the ITDB. Information used to compile the Illicit Trafficking Database come from two main sources: state-confirmed information and open sources. Validation of open-source information on alleged incidents are always sought from the relevant State member(s). The ITDB contained 1340 confirmed incidents as of the 31st December 2007.

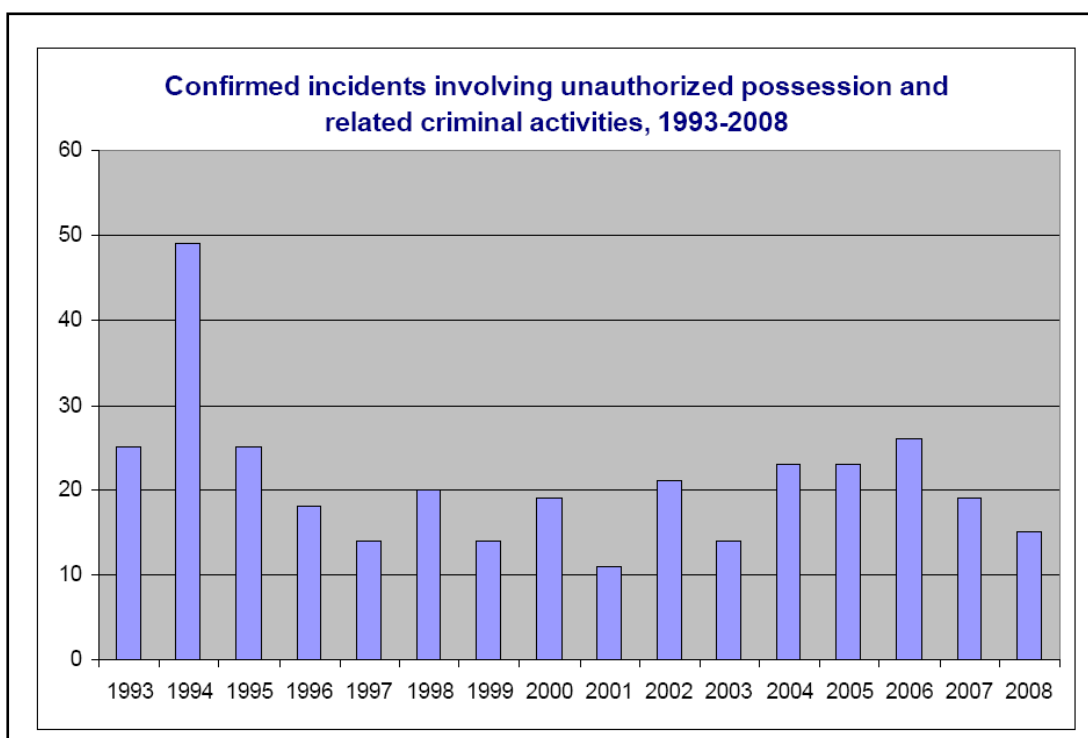
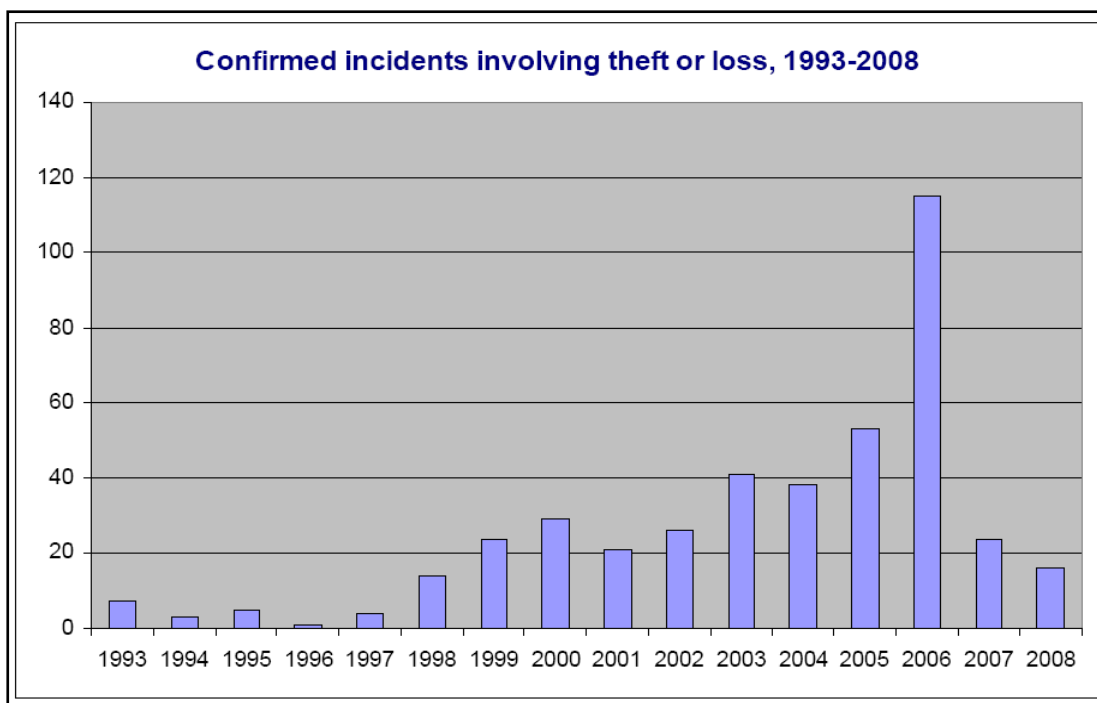


Figure 33: Incidents reported to the ITDB involving theft or loss, 1993-2008 (www.ns-iaea.org)



Name:	Uppsala Conflict Data Program (UCDP)
Parent Host	Department of Peace and Conflict Research at Uppsala University, Sweden.
Website:	http://www.pcr.uu.se/research/UCDP/
E-mail:	conflictdatabase@pcr.uu.se
Access:	Free
Unit of Analysis	Armed Conflict
Scope:	Global
Period Covered:	1946-2007
Principle sources	Open-source material
Key Variables	Location, conflict parties, territory, year

Uppsala Conflict Data Program (UCDP)

Introduction

The Uppsala Conflict Data Program (UCDP) is based within the Department of Peace and Conflict Research at Uppsala University, Sweden. The program holds an extensive collection of quantitative and qualitative data sets on armed violence, some dating back to 1946. Researchers can also use an interactive database on organised armed violence and related peace-making efforts. All the data sets and the database are freely accessible via the UCDP website. A definitional list of UCDP's conflict terminology explaining the key terms used within the data sets is available on the website.

The program allows researchers interested in armed conflict to access relevant data sets that could be used in the analysis of the origins of conflict, its dynamics and resolution. On-going violent conflict data sets have been coded since the 1970s.

Definition and Datasets

The UCDP working definition is: 'An armed conflict is a contested incompatibility that concerns government and/or territory where the use of armed force between two parties, of which at least one is the government of a state, results in at least 25 battle-related deaths in one calendar year'.

(Source: UCDP Website: <http://www.pcr.uu.se/research/UCDP/index.htm>).

UCDP/PRIO's Armed Conflict Dataset

This project is jointly run by the UCDP and Centre for the Study of Civil War at the International Peace Research Institute in Oslo (PRIO). The data set has a global

spatial domain and covers armed conflict where at least one actor in the conflict is the government of a state. It covers the period 1946-2007 and is updated on an annual basis. Key variables coded include: location, year, incompatibility, opposition organisation and intensity level. In addition, a dyadic data set edition of the UCDP/PRIO Armed Conflict Dataset covering 1946-2007 is produced and updated yearly.

UCDP's Conflict Termination Dataset

The Conflict Termination dataset records the start and the end-dates for each armed conflict activity. The dataset covers the period 1946-2007. Termination of a conflict is deemed to be non-activity for a minimum of a year. Non-activity refers to the criteria not being satisfied for incompatibility, levels of organisation and battle-related deaths being less than twenty-five. Examples of data held within the data set include: date of termination, length of conflict termination and the form of termination (e.g. victory, ceasefire or peaceful agreement). The UCDP Conflict Termination dataset can be used in conjunction with the UCDP/PRIO Armed Conflict dataset.

UCDP's Peace Agreement Dataset

The UCDP Peace Agreement dataset records every signed peace agreement initiated between warring parties in armed conflicts between 1989 and 2005. To be eligible for entry into the dataset, a minimum of two opposing primary warring parties must have signed a peace agreement. Some of the datasets key variables include: name of peace agreement, date of signing,

signatories, duration [of peace agreement], third parties and provisions of accords.

UCDP's Non-State Conflict Dataset

The UCDP Non-State Conflict dataset records communal and armed conflict events between a minimum of two groups. The UCDP defines non-state conflict as: 'the use of armed force between two organized armed groups, neither of which is the government of a state, which results in at least 25 battle-related deaths in a year' (Source: UCDP Website). The temporal domain for the dataset is 2002-2006. It is updated yearly.

UCDP's One-Sided Violence Dataset

The UCDP One-Sided Violence Dataset collects data on civilians attacked purposely by a government actor of the state or formally organised groups. A minimum of 25 deaths needs to be recorded for eligible entry to the dataset. The temporal domain for the dataset is 1989-2006. It is updated yearly.

Database

The UCDP website provides an interactive database, updated yearly, on organised armed violence and related peace-making efforts. Using a series of interactive maps, researchers are able to search the database based on three separate criteria: war and minor conflict, non-state conflict and one-sided violence. Alternatively, all three criteria can be included for search purposes. The interactive map highlights the relevant countries and provides a further breakdown of conflict details based on

geographic region and by country. The resultant information provides a detailed historical context on each country's conflicts dating back to 1946. A large array of factual data is included within the database. For example: start/end date of conflict, type of conflict, intensity and number of deaths. Further links within each country, provide, where available, related narrative, statistical data and codebooks on minor armed conflicts and wars, non-state conflicts and one-sided violence. Where preventative efforts on conflicts have been undertaken and peace agreements reached, summaries and full-text agreements can be accessed from the database.

Graphs and Publications

In addition to the datasets the UCDP also make available a series of pre-defined graphs charting data in active conflicts, active dyad levels, warring parties and peace agreement levels. The UCDP armed conflicts data sets are partly published in the SIPRI Yearbook, the States in Armed Conflict and the Journal of Peace Research on an annual basis. Since 2005 the data sets have been published in the Human Security Report.

Figure 34: Conflicts by Region 1946-2007 (UCDP website)

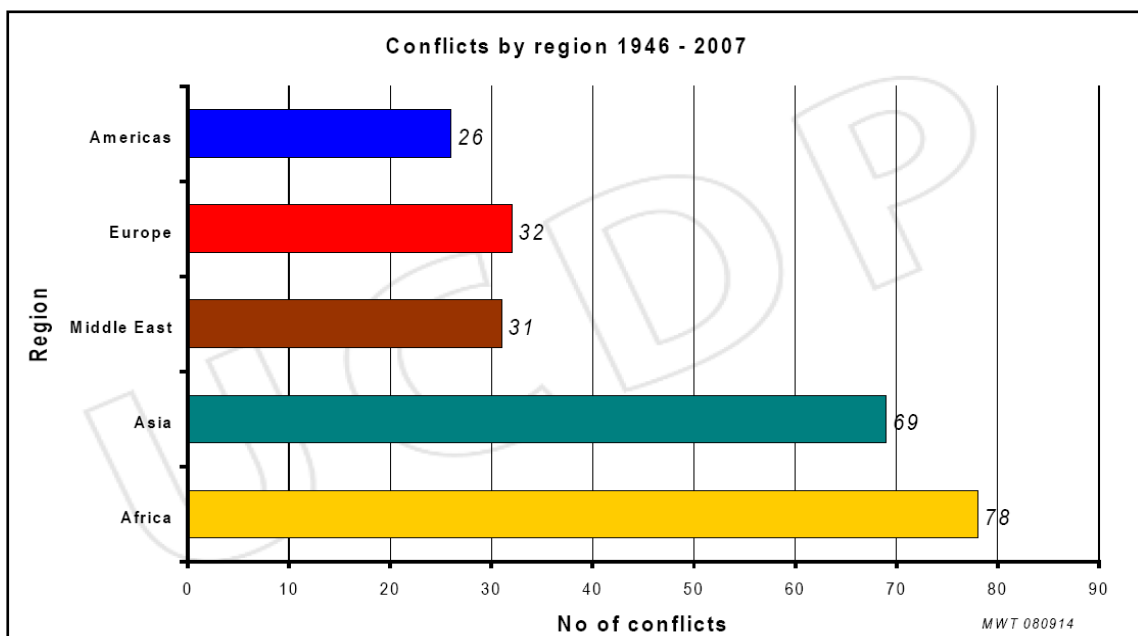
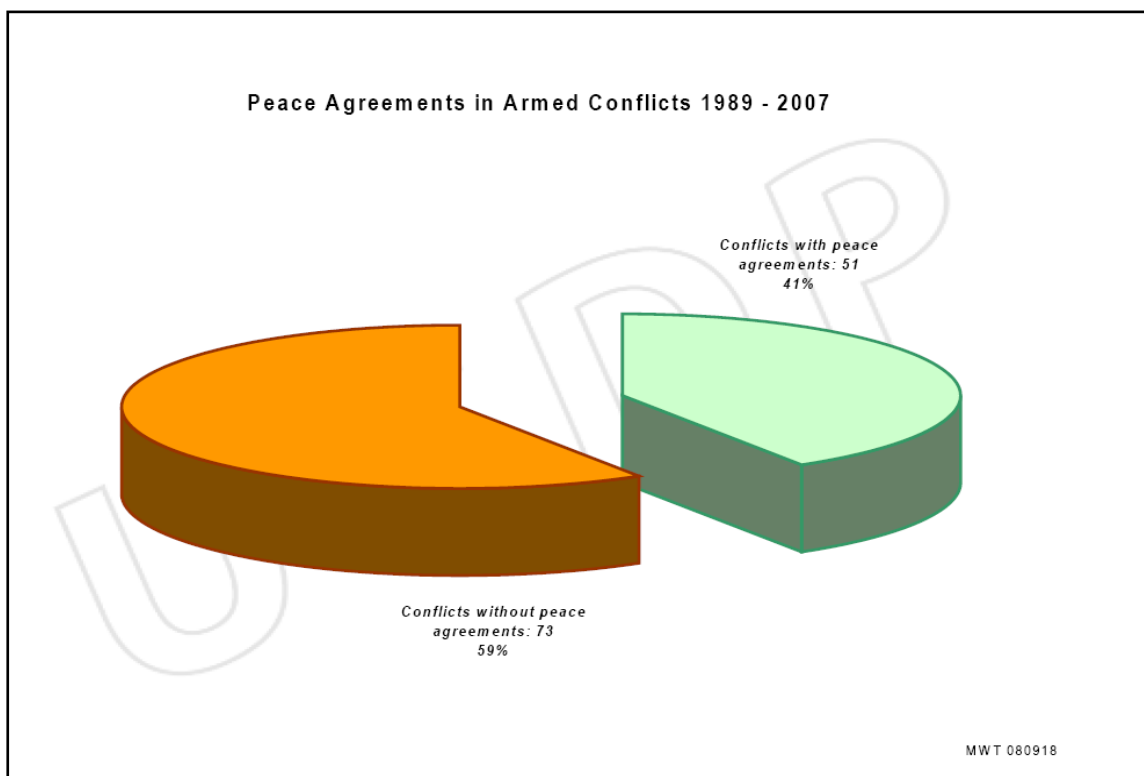


Figure 35: Peace Agreements in Armed Conflicts 1989-2007 (UCDP website)



Name:	The Minorities at Risk (MIR) Project
--------------	--------------------------------------

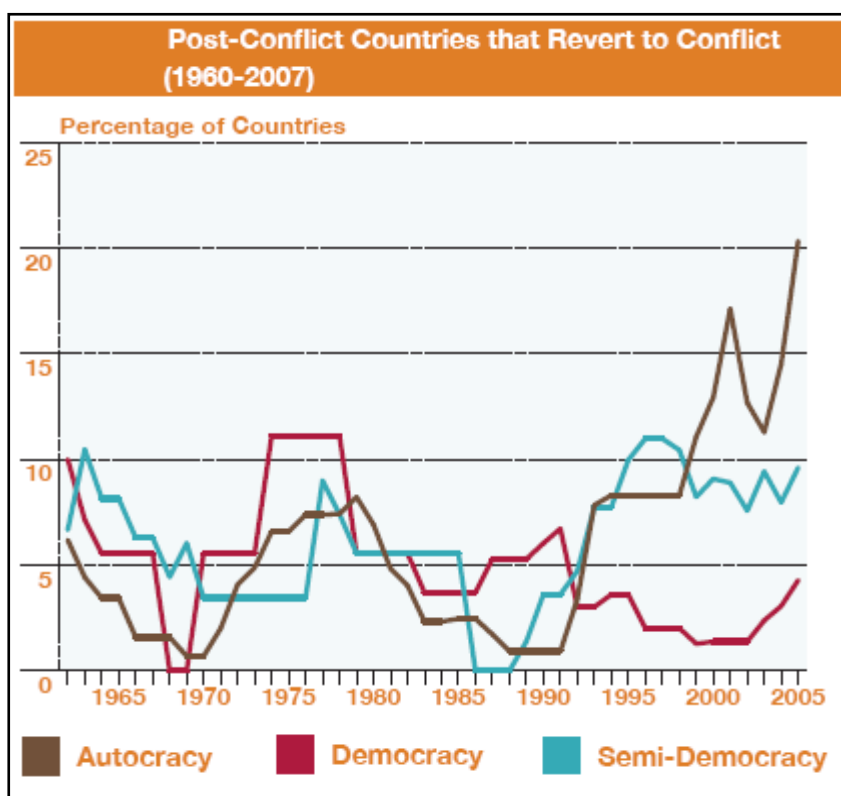
Parent Host	University of Maryland, College Park, MD. United States
Website:	http://www.cidcm.umd.edu/mar/
E-mail:	minpro@cidcm.umd.edu
Access:	Free
Unit of Analysis	Conflicts of politically-active communal groups worldwide whose current population is at least 500,000
Scope:	Global
Period Covered:	1945-2003
Principle sources	Open-source material
Key Variables	See: <i>Minorities at Risk (MAR) Codebook Ver2/2009</i> http://www.cidcm.umd.edu/mar/data/mar_codebook_Feb09.pdf

The Minorities at Risk (MAR) Project

The Minorities at Risk (MAR) project is based at the University of Maryland, College Park. Ted Robert Gurr established the project in 1986. The MAR project examines conflicts of politically active communal groups worldwide whose current population is at least 500,000. Currently, the project holds data and information on more than 282 communal groups. The project has developed in a series of five separate phases. Phase I (1945-1989) covered 227 communal groups. Phase II (1990-1995) covered 275 communal groups. Phase III (1996-1998) covered also 275 groups. Phase IV (1998-2003) covered 287 groups. The Phase V data, released so far, covers the period 2004-2006. The MAR project team monitors each conflict and analyses its status. One of the key aims of the MAR project is to provide researchers with standardised data, allowing for comparative studies and research across various conflicts. A key focus for the project is a data set ‘... that tracks groups on political,

economic, and cultural dimensions' (Source: MAR Website). Access to the MAR project is free and is available via an interactive web-site. Researchers are able to access a large array of information. This includes the Minorities at Risk Database, its codebook and a series of data sets and historical chronologies on conflict. External links to relevant websites are provided. In addition to core data the project also provides access to summaries of group histories, risk assessments and a chronology for each group. Specialist data sets include data on ethno-political organisations in the Middle East and North Africa and the *The Minorities at Risk Organizational Behaviour* (MAROB) dataset.

Figure 36: Post-Conflict Countries that revert to Conflict 1960-2007 (www.cidcm.umd.edu)



4.4 Case Studies: The Private, Government and Commercial

The case studies outlined below is a classificatory scheme for non-publicly available systems

Table 4.3 Classification of Private, Government and Commercial data sets, chronologies and databases.

	Data Sets/Chronologies/Databases included in Case Studies from Section 4.4 onwards	Classification
1.	Terrorism Information System (FBI)	Database
2.	Desist Database (CIA)	Database
3.	OSAC Electronic Database (EDB)	Database
4.	Threat Analysis Division Information Management System (TADIMS) (US Department of State)	Database
5.	TIPOFF (Bureau of Intelligence and Research (INR), US Department of State)	Database
6.	Violent Gang and Terrorist Organisations File (US National Criminal Information Center (NCIC))	Database
7.	Consular Lookout Support System (Class) (US Department of State)	Database
8.	Interagency Border Inspection System (IBIS) (US Customs and Border Protection Data Center)	Database
9.	National Automated Lookout System (NAILS) (US Department of Homeland Security)	Database
10.	Distributed Name Check Database (US Department of State)	Database
11.	Explosives Reference and Search System (EXPRESS) (FBI Bomb Data Center)	Database
12.	Political Violence Research Unit Database (University of Tel Aviv)	Database
13.	Explosives Incident Systems (EXIS) (US Bureau of Alcohol, Tobacco, Firearms and Explosives)	Database

Moving away from the issue of those datasets that are publicly available, there are an array of other databases both government and commercial with varying levels of accessibility and scope. In terms of government databases, those used in counter-terrorism are accorded the highest level of security and secrecy. Their design, operation and accessibility is strictly restricted to accredited intelligence employees, (including terrorism analysts) and where appropriate, designated government officials. They are, therefore, essentially private and classified, and are outwith the

intelligence communities. Public domain information on such data sets is extremely rare.

Two such terrorism databases are the FBI's Terrorist Information System (TIS), and the CIA's Desist database on terrorism.²⁷³ Both these databases are used for intelligence based activity and project-specific work. The FBI's Terrorist Information System is an extensive database by any standards, holding in excess of 200,000 records and details on known or suspected terrorists.²⁷⁴ In addition to this the TIS system holds over 3000 files on organisations or enterprises associated with terrorism. The database is relational in design, permitting intelligence analysts to establish links between such entities as known or suspected terrorists, terrorist groups, weapons, tactics or events. The database is indexed, allowing FBI analysts to search for data on known and suspected terrorist groups. The TIS system can conduct queries (questions) about particular on-going terrorism investigations, retrieving data on terrorist group activities, information about particular associates of a terrorist group, and any contact details that are relevant for intelligence purposes. Although the database is primarily designed to hold terrorist details, the system also codes information relating to groups or individuals with affiliations to terrorist groups such as drug cartels or militia groups. Other public domain

²⁷³ Documentation on the Terrorist Information System (TIS) for obvious security reasons is minimal. Archive material however on the TIS data sets is maintained. The Center for Electronic Records at the U.S. National Archives and Records Administration (NARA) has custody of six data sets known as the Major Investigative Data Base (MIDB), and fourteen data sets known as the Terrorist Information System (TIS), as well as related documentation. The Federal Bureau of Investigation transferred these data sets and documentation to the NARA in 1991 as a part of a larger accession of records known as the CISPES files. These records are security classified and are exempt from disclosure under NARA's general restriction covering information related to law enforcement investigations. This latter restriction conforms to the Freedom of Information Act (FOIA), as amended, 5 U.S.C. 552 (b) (7).

²⁷⁴ The issue of retaining information on suspected terrorists on database systems is a sensitive matter, requiring absolute security and discretion. Intelligence based databases on terrorism such as the U.S. State Departments TIPOFF database are permitted to hold suspected names of individual terrorists without exposing themselves to data protection violation legislation. Academic databases such as RAND-St. Andrews, or the Political Violence Research Unit database at the University of Tel Aviv would open themselves up to potential litigation challenges were they to hold names of suspected terrorists.

information on the Terrorist Information System is virtually non-existent. With the exception of a brief acknowledgement of the Federal Bureau's TIS database, and fourteen related data sets (1981-1990) to be found deep in the U.S. National Archives - no other public domain sources of information appear to be available.

The CIA's Desist database on terrorism, although its existence is barely acknowledged, provides analysts at the CIA and their Counter Terrorism Center (CTC) with data on a whole series of terrorist information.²⁷⁵ The Desist database is thought to have the capability of identifying the geographic locations of terrorists and linking this data with related data on their methods of operations. Other entities held within the database are details on financial sources of funding for terrorist organisations, information on their membership, as well as detailed information on individuals. As with the FBI's TIS database, the CIA's Desist system also holds data on known or suspected associates of terrorist groups as well as data on affiliations with other terrorist organisations. The Desist database, with its powerful relational capabilities, can offer terrorism analysts information at many linked levels, providing an extremely powerful intelligence tool.

Classified terrorism data sets are not solely limited to the CIA or FBI. Other U.S. Federal organisations such as the U.S. Department of State, The U.S. Department of Defense, The Federal Emergency Management Agency (FEMA) and the U.S. Secret Service all have varying types of classified data sets on terrorism.²⁷⁶ On an international level classified terrorist data sets are held by many other

²⁷⁵ For further details on DESIST see: Perry, Mark. *Eclipse: The Last Days of the CIA*. (New York: William Morrow and Co. 1992).

²⁷⁶ For detailed analysis of the U.S. Department of State, FBI, FEMA and other U.S. Government terrorism databases see later sections of Chapter V of this thesis.

national government agencies such as Israel's Mossad, the United Kingdom's MI5, MI6, the RUC, Scotland Yard's anti-terrorist unit SO13 and Special Branch.

The sensitivity of terrorist data requires all the above agencies to maintain data in the securest of formats. This is a challenge in itself from within an agency. When data needs to be transferred to an externally approved police or intelligence organisation through Interpol for example, the risk of interception by illegal means is a worrying reality.²⁷⁷ Interpol deals with many types of intelligence data, including information relating to terrorism. With 176 members, requiring varying forms of data, the challenge is substantial. Interpol transfers classified data in several formats: typed texts, texts with graphs as well as diagrams and tables. Their telecommunications network can also transfer images, fingerprints and photographs and also permits National Central Bureau's (NCB's) to consult relevant databases from remote centres.²⁷⁸ The rapidity with which Interpol's X.400 server dispatches classified information to NCB's does not insure that external agents have not intercepted and deciphered what is intended to be classified data.²⁷⁹ To combat potential violations of security on the transferral of classified data, Interpol have adopted two simple, but practical procedures. They have an encryption system that has been operational since 1991, which identifies the sender of the data, preventing third party access and potential corruption of data. Secondly the encryption system prevents data from being intercepted or identified.²⁸⁰ This security system provides

²⁷⁷ For further details on Interpol's telecommunications network see:
<http://193.123.144.14/interpol-pr/Machinery.html>

²⁷⁸ Ibid. Each member country of Interpol designates a police agency to co-ordinate and liaise with other local and foreign law enforcement agencies. These police agencies are known as National Central Bureau's (NCB's).

²⁷⁹ Ibid. The X.400 standard is an internationally accepted message-handling standard.

²⁸⁰ Ibid.

what is known as ‘end-to-end encryption’ between the source agency sending the data and the target police agency receiving the data.²⁸¹

Government (classified) terrorism data sets by their very nature have an *extremely* low profile in public domain sources and literature. Aside from some conspiracy theories about their purpose, that reside mainly on the Internet, minimal information is available. In many ways their virtual non-existence in published literature is indicative of the success security agencies have had in maintaining terrorism data sets with what their remit has been all along: classified.

4.5. Government (Restricted and Unclassified) Terrorism Data Sets

This second category of computerised terrorism data sets is an unusual mixture of restricted access data sets, partly classified data, and unclassified public access data (i.e. they are ‘in-between’).²⁸² Information on these particular terrorism data sets, although not extensive is available in public domain sources.²⁸³ The Government (Restricted and Unclassified) terrorism data sets vary from Government (Classified) data sets in that they perform both an internal role within respective agencies and provide a public service in an external capacity.

OSAC’s Electronic Database (EDB)

The Overseas Security Advisory Council’s Electronic Database (formerly the Electronic Bulletin Board EBB), is an on-line database service administered by the

²⁸¹ Ibid. To further prevent violations of security the sender of data is assigned an electronic signature using a microchip card that is handled by the X.400 software.

²⁸² Restricted access relates to accessibility strictly limited to designated employees of respective Government agencies holding terrorism data. For a detailed outline of U.S. *Classified National Security Information* see: Executive Order #12958 The White House. April 1995. Also at: <http://foia.state.gov/eo12958/part1.htm>

²⁸³ Information on these data sets can be found at selective Internet sites including: the U.S. State Department, FBI, U.S. General Accounting Office and the Federal Aviation Administration.

U.S. State Department's Bureau of Diplomatic Security. Established in 1987, it has an unusual role in that it serves both the needs of State Department's analysts and that of U.S. businesses overseas. The primary remit of OSAC is to promote co-operation on security matters between United States government and U.S. private businesses world-wide.²⁸⁴ Registered U.S. companies and organisation which are affiliated to OSAC , of which there are over 1500, are able to benefit from an array of different security related information.²⁸⁵ The database has a substantial repository of information, holding in excess of 57,000 security-related incidents. The OASC EDB differs in several respects from traditional terrorism databases. The EDB's external customer base is restricted to officially accredited companies and organisations conducting substantial business overseas, and requires approval to register from OSAC. These companies include Exxon, BF Goodrich, Proctor and Gamble, The Ford Motor Company, American Airlines, IBM and McDonald's.²⁸⁶ The service provided to EDB members is entirely free, except for the cost of operating software provided by a designated vendor. The EDB is very much a practical database service, used by its clients on a daily basis. Its objective is :

'... to provide the kind of nitty-gritty information that will help a corporation assess the security climate in a country and determine if it's safe to travel or keep workers there.'²⁸⁷

²⁸⁴ Pluchinsky, Dennis. *Overseas Security Advisory Council: Electronic Bulletin Board*. Informal paper prepared by Denis Pluchinsky of The Office of Intelligence and Threat Analysis, Bureau of Diplomatic Security, U.S. State Department. 1994. The Overseas Security Advisory Council (OSAC) was established in 1985. In addition to dealing with terrorism threats to overseas businesses OSAC's remit also includes promoting awareness of, and protection of proprietary information and technology, as well security awareness and education.

²⁸⁵ Ibid. In addition to registered companies OSAC has over 25 "Country Councils" which co-ordinate security and terrorism related information for businesses operating within South America, Central America, Africa, the Middle East, Europe and East Asia. The EDB also deals with crime related activity.

²⁸⁶ For further details see: 'Feature: Security Computer Network: Strategic Resources for US Business.' *US Department of State Dispatch*. October 29th 1990. p.227.

²⁸⁷ Ibid.

It contains not only standard information profiles on terrorist groups, but also has an Anniversary Dates file, with a chronological list of significant dates that may have security implications for U.S. personnel working in particular overseas locations.²⁸⁸

Another practical element to the EDB database is its provision of police emergency telephone numbers, addresses and telephone numbers of U.S. diplomatic and consular posts overseas. A series of chronologies exist within the database, although there is no overall definitive chronology on terrorism with the EDB database. One noticeable omission from services provided by the EDB, and for understandable reasons, is aviation threat notifications. This is a sensitive issue at the best of times, especially after the controversy surrounding threat notifications, before the bombing of Pan Am flight 103 over Lockerbie, Scotland in 1988. Potential criticism that EDB members could benefit from aviation threat notifications over the general public would open it up to severe criticism. This emphasis on a 'real-time' practical database service, differs considerably from traditional government databases on terrorism, which normally produces annual chronologies or statistics on terrorism, such as *Patterns of Global Terrorism*, and have no direct contact or liaison with their target audience. The philosophy and practicality behind the EDB is based partly on reciprocity and mutual co-operation. In other words, a two way process exists. Companies act as the 'eyes and ears' of the EDB,²⁸⁹ passing on relevant security information to the State Department, while benefiting from the vast intelligence

²⁸⁸ U.S. Department of State, *Overseas Security Electronic Bulletin Board Users Manual* (Washington D.C. U.S. Dept. of State, Bureau of Diplomatic Security, 1990) pp.4-5.

²⁸⁹ 'Feature: Security Computer Network: Strategic Resources for US Business.' *US Department of State Dispatch*. October 29th 1990. p.227.

resource and professional advice on offer from subject specialists.²⁹⁰ This differs quite markedly from the traditional business customer relationships of commercial organisations offering security and terrorism related information. Companies such as Mizell, Profiles, Kroll and Pinkerton's relationship with their clients is based upon the premise that clients pay for professional advice, information or consultancy. The client expects a service for their payment; mutual exchange of security related information is much less apparent.

Over the years, analysts have build up a good rapport with client companies of the EDB. A two-way process has evolved, whereby both sides benefit and analysts provide a central point from which to receive security related information and to dispense it. As Bartley Railing, an Middle East analyst notes:

'US companies have good contacts and have learned to look out for their security....They want us not only as a resource for information but as a facilitator to help turn it around'.²⁹¹

As with most databases of its size and client spread, OSAC's EDB database is operated on a mainframe system, permitting users to access by modem via telephone lines or Internet connections. Access is only permissible after approved registration by OSAC and passwords have been issued. Companies can access the EDB using personal computers. Although the original EDB system operated by analysts in Washington D.C. was a menu-driven system, a window based system is now in operation. Among the many benefits this brings (apart from general compatibility), is that analysts presented with copious amounts of raw data are able

²⁹⁰ Sources for the EDB database come from a mixture of unclassified U.S. government reports, the media, companies based in a particular geographic region. Verification of reports is conducted by analysts within the Bureau and by checking with companies effected by incidents or security threats within relevant regions.

²⁹¹ 'Feature: Security Computer Network: Strategic Resources for US Business.' *US Department of State Dispatch*. October 29th 1990. p.227.

to quickly copy, paste and edit information onto the EDB database from other sources, saving time and effort. Another unusual, but very useful service on offer to EDB members, is the Private Sector Liaison Staff message system (PLPS).²⁹² This electronic message system encourages corporate users to voluntarily submit information, either in written format or orally by telephone, on security or criminal matters affecting their respective overseas business operations. Incidents that are not picked up by regular intelligence means are sometime highlighted by the PLPS message system. Even if analysts are aware of particular events, the system can often update or supplement information, which helps to add to accuracy and validation to events. The types of submission given have included information on threats and attacks against American personnel and property. Other details have included information on thefts, kidnappings, violent crime and local unrest.²⁹³ Confidentiality is paramount with such information and the Bureau of Diplomatic Security adheres to strict procedures to protect sources when posting details on the EDB.

TADIMS Database

The Threat Analysis Division Information Management System (TADIMS) database, was designed in the late 1980's to support the Threat Analysis Division (TAD) within the Bureau of Diplomatic Security, at the U.S. State Department. Its main remit was to handle daily requests for information relating to terrorism, terrorism trends,

²⁹² U.S. Department of State, *Overseas Security Electronic Bulletin Board Users Manual* (Washington D.C.:U.S. Dept. of State Bureau of Diplomatic Security, 1990.). p.31.

²⁹³ *Ibid.* p.32.

threat assessment and security briefings.²⁹⁴ Although this system is now only used by one division within the bureau, its use and shortcomings merit some brief discussion.

The TADIMS system, at its time of development, was a fairly modern system. It operates by a series of menu-driven screens allowing analysts to enter, delete and update terrorism data.²⁹⁵ The software, written for the WANG VS computer, produces a variety of reports dependent upon analysts requests. TADIMS search facilities for terrorist groups, incidents or other related details, covers most analysts basic requirements. These include searches on range values of terrorism incident dates between specified periods, list searches on specific coded fields, for example BOMB and KIDNAP, and operators such as NOT, and OR. The system can also offer limited wildcard searches. TADIMS general demise, although not complete redundancy, is due mainly to shortcomings in its functionality. The TADIMS system is incapable of producing aggregate totals of numeric variables, such as the total number of people killed in an incident. Its ability to handle common statistical functions is limited, and has no facility to produce graphs, such as bar charts or pie charts. As the TADIMS system does not support a Windows based environment its compatibility with other modern software is severely restricted.

At a fundamental level, the system is not a relationally based database system, such as TIPOFF or the Tel Aviv University's database on terrorism and political violence. Other concerns by analysts over the system, is its inability to group

²⁹⁴ Published information on TADIMS appears to be minimal. Information on the system derived from meetings with Dennis Pluchinsky at the U.S. State Department, Bureau of Diplomatic Security, Washington D.C. in July 1994 and January 1997. For further information on the system see: *Threat Analysis Division Information Management System (TADIMS), User Manual March 1990*, (Management Information Systems Division, Bureau of Diplomatic Security, U.S. Dept. of State).

²⁹⁵ The update facility was not strictly the type of update function that is available from modern database software. If, for example, casualties had risen from the result of a bombing, the update would not be reflected in a cumulative aggregate total. Outdated figures would have to be replaced with new figures.

together information profiles on terrorist groups, or provide simple editing facilities for source data on terrorism, supplied by intelligence agencies, news agencies and other government sources. Although data within the TADIMS system is valid, its limited functionality has vastly reduced its usage. Many analysts within the Threat Analysis Division have now developed their own terrorism related chronologies and databases, running under Microsoft Access. Although this doesn't serve the division with a departmental-wide database on terrorism, it does permit specialists to develop subject-specific terrorism databases that are relevant to their work needs.

TIPOFF Database

Although external co-operation with the operation of terrorism databases is fairly unusual, an increasing amount of liaison and co-ordination within government agencies has increased in recent years.²⁹⁶ One such venture has been the U.S. State Department's TIPOFF database, developed and operated by its Bureau of Intelligence and Research (INR). As part of the State Department's many responsibilities, it is charged with denying terrorists or suspected terrorists and their supporters entry visas to the United States. The TIPOFF database holds detailed information on known or suspected terrorists, which it passes on to the State Department's Consular Lookout and Support System (CLASS) database. This is operated by the Bureau of Consular Affairs who use the declassified information given to them by TIPOFF as part of their security checks, to monitor visa applications to help detect known or suspected terrorist who apply for U.S. entry visas from overseas consular offices.²⁹⁷

²⁹⁶ For further discussion on co-operation and co-ordination of terrorism databases see Chapter V of this thesis.

²⁹⁷ *Ibid.*

This type of co-ordination and co-operation between departments using databases has met with some success. Since TIPOFF's inception in 1987, the database has identified in excess of 722 suspected terrorists as they made visa application for entry to the United States.²⁹⁸ Compared with TADIMS's, the TIPOFF database runs on a fairly modern and sophisticated hardware and software operation. In its earliest days TIPOFF ran as a manual card index system; it now runs under the powerful database management software Oracle. Unlike other terrorism databases such as the Violent Gang and Terrorist Organisations File (VGTOF) or the EDB, which are operated over wide area networks, TIPOFF's operation is run over a local area network. The network runs under Windows NT[®].²⁹⁹ Access is strictly limited to INR staff. TIPOFF has no connection to any other computer system; much of the information INR receives is sensitive intelligence and classified law enforcement data.

The type of data on individuals held on the TIPOFF system is fairly detailed; the aim is to build up a 'thumb-sketch' profile of suspects that is of use to the State Department and other relevant government agencies.³⁰⁰ The type of information, being intelligence based, differs considerably from academic terrorism data sets. The database includes such variables as date of birth, passport number, physical features and known aliases.³⁰¹ The criteria for inclusion in the TIPOFF database is that there is *reasonable* suspicion that an individual or individuals have been involved in known

²⁹⁸ For a brief acknowledgement of the work carried out by the TIPOFF database see : *Assessing Current and Projected Threats to U.S. National Security*. Statement by Assistant Secretary of State for Intelligence and Research, Tobi T. Gati. Senate Select Committee on Intelligence. Washington D.C. February 5th 1997.

²⁹⁹ The TIPOFF database, operating from a local area network file server, runs on a series of 486 100mhz P.C's. using a UNIX based operating system. Information derived from conversation with John Ariza, TIPOFF system manager and developer, Bureau of Intelligence Research (INR), U.S. State Department.

³⁰⁰ These can include the FBI and U.S. Immigration and Naturalization.

³⁰¹ See note 51.

acts of terrorism, or that they (State Department), have reason to believe that suspects operate in terrorist related activities. Intelligence data from TIPOFF is not limited exclusively to one agency. As part of its operation it also provides the Immigration and Naturalization Service (INS) and the U.S. Customs Service with relevant terrorism data when running their computerised Interagency Border Inspection System (IBIS).

The integration of TIPOFF data into the INS and Customs systems offers a powerful facility to detect known or suspected terrorists as they arrive in the United States. Upon presentation to any of the 350 U.S. border entry points the IBIS system is able to run checks to flag-up any suspects registered on the TIPOFF database. Although difficult to gauge or compare against other figures, the TIPOFF database, in conjunction with IBIS has successfully intercepted 196 suspected terrorists from 56 countries since 1991.³⁰²

Interagency Systems

With increasing concern in the United States, and many other countries, of escalating numbers of inadmissible aliens at ports-of-entry, action to stem rising numbers requires high levels of vigilance. Known or suspected terrorists, among many other categories, present immigration services with a formidable challenge. In fiscal year 1992 the U.S. Immigration and Naturalization Service (INS) estimated that over 120,000 inadmissible aliens had arrived in the United States.³⁰³ By October of 1996 INS calculations suggested this figure had risen to roughly 275,000, with 5

³⁰² GAO, *ibid*, Chapter 2:4. These interceptions took place at 44 different U.S. border points, figures for geographic spread are unavailable.

³⁰³ Statement by Michael D. Cronin. *Terrorism and America: A Comprehensive Review of the Threat, Policy, and Law*: Hearings before the Senate Committee on the Judiciary, 103rd Congress, 1st Session 153 (1993).

million illegal aliens residing in the United States. The complexities of guarding against illegal entry have been partly addressed in the United States by the INS's Interagency Border Inspection System (IBIS) database. This database differs from other databases such as the Electronic Data Base (EDB) or TIPOFF in that it is a multi-agency lookout database. The term lookout correctly implies its status as a proactive database used for real-time searches. The IBIS database's multi-agency remit, permits it to carry out queries upon arriving aliens and non-aliens into the United States against other U.S. agency databases. These include the Department of State's Consular Lookout Support System (CLASS), and the FBI's National Criminal Identification Center (NCIC).³⁰⁴ Unlike academic or commercial terrorism data sets, which generally tend to be maintained and used within the limits of university or office boundaries, the IBIS system as its job remit dictates operates over a wide area network (WAN). The system hardware and software has to be robust, handling literally millions of queries per year. For fiscal year 1992, 513 million people sought entry to the United States, through airports, land and seaports.³⁰⁵ While the vast majority of those seeking entrance to the United States do so lawfully, events such as the World Trade Centre and Oklahoma bombings have raised both public and government awareness of the need to intercept and detain known or suspected terrorists at ports of entry. The 1994 World Trade Center bombing played a significant rôle in persuading the U.S. Congress to direct the State Department to

³⁰⁴ Other database systems include the U.S. Customs Treasury Enforcement Computer System (TECS) and the INS's National Automated Immigration and Lookout System (NAILS). For further discussion on the FBI's NCIC 2000 see Chapter VI.

³⁰⁵ Cronin (note 55). More than 85 percent of arriving passengers were processed through IBIS in Fiscal Year 1992.

install its automatic lookout system at all visa-issuing offices worldwide.³⁰⁶ Although the IBIS database would appear to provide a water-tight system of detection, the sheer volume of traffic at some U.S. ports-of-entry results in only partial checks. At land and border entry points, every car number plate is checked against the IBIS system; however name checks on individuals are left to the discretion of inspectors.³⁰⁷ The IBIS database differs considerably from other databases such as the VGTOF, TIPOFF or the Terrorist Information System (TIS). It is not a dedicated database on terrorism activity, although it does handle detailed terrorism information. With its multi-agency remit, it is linked to a complex and sophisticated array of other U.S. government agency databases. One of these databases, maintained by the INS is the National Automated Lookout System (NAILS). Terrorist details, among others are entered into the NAILS system on the grounds of exclusion of entry, based upon national security.³⁰⁸ To add to the complexities, the NAILS database also holds U.S. Department of State records for known or suspected terrorists deemed ineligible for visas. Other agency records held within NAILS include those from the FBI, the U.S. Secret Service and the U.S. Marshals Service.³⁰⁹ Worth noting, is the distinction between IBIS records and the Department of State's CLASS database, accessible from within the IBIS database.³¹⁰ The State Departments' records relate specifically to the eligibility of aliens to be granted visas for entering

³⁰⁶ Statement of Benjamin F. Nelson: *State Department: Efforts to Reduce Visa Fraud*. Testimony, 05/20/97. GAO/T-NSIAD-97-167.

³⁰⁷ Cronin (note 55).

³⁰⁸ The Immigration Act of 1990, passed by the U.S. Congress simplified the categories for excluding aliens. The broad category defined as security also related specifically to known or suspected terrorists..

³⁰⁹ Cronin (note 55).

³¹⁰ Approximately 250,000 of the Department of State's 5 Million CLASS records are available to the NAILS and IBIS's databases.

the United States. The IBIS system is a lookout database on behalf of several agencies, to identify inadmissible aliens, under the Immigration Act of 1990.

The issue of visas for entry into the United States, the responsibility of the State Department, has always been a difficult process. Balancing legitimate access against potential fraudulence, terrorism, drugs or other criminal activity requires timely and accurate intelligence. To help in this process the State Department initiated in 1989 its machine-readable visa program.³¹¹ The creation of a global database holding the names of those ineligible for U.S. visas would be logged onto the system. The automated approach is two pronged. Firstly, by making the visa on the passport machine readable, printed on synthetic material, with an encryption code, potential fraudulence could be minimised. Secondly, the system has access to the Consular Lookout and Support System (CLASS) database. The duality of the system has helped significantly to improve screening procedures. The introduction of both machine-readable visa systems and the CLASS database was patchy however. Their introduction was neither parallel nor comprehensive. The ramifications of the World Trade Center bombing, finally forced the U.S. Congress in 1994 to require all visa-issuing posts to operate the machine-readable and CLASS systems by the end of 1995.

By April of 1997 all visa-issuing posts had the machine-readable visa system installed. In addition, an updated version of the system known as MRV-2 began to replace the original database system from 1996 onwards. The cost of upgrading such systems was substantial. Figures available for fiscal years 1996-1998 indicate the State Department invested in excess of \$68.9 million dollars in the new version

³¹¹ Nelson (note 58).

MRV-2.³¹² While Federal funding explains the considerable provision of resources for such projects, resources of such proportions would be out of the question for academic or even commercially based terrorism data set projects.

Large capital investment in such databases systems does not always guarantee success. Despite considerable capital investment in CLASS, the U.S. General Accounting Office (GAO) noted both technical and policy orientated problems with the CLASS database. Initial technical difficulties can commonly arise in most new database projects operating over local area networks, such as the TIPOFF database or the South Pacific Islands Criminal Intelligence Network (SPICIN), which is linked to a wide area network.³¹³ More serious than the initial inconvenience of broken communication, is the practical impact upon security. When first established, links to U.S. missions in Mexico City, Sydney and Seoul were problematic. With transmission connectivity problems, U.S. officials checking for known or suspected terrorists had to rely on traditional manual methods of search by microfiche. The resultant real-time delay presented the possibility that visa approval could be given to individuals that had been registered with the CLASS database but had not been updated on the microfiche.³¹⁴

The need for real-time information on known or suspected terrorists, accessible on a national or global scale, presents particular difficulties that academic or commercial terrorism data set operators do not encounter. These problems relate to 'live' or real-time operation of the data set. If the data set is required for

³¹² Ibid. MRV-2 (Machine Readable Version 2)

³¹³ For further information on South Pacific Islands Criminal Intelligence Network (SPICIN) see later sections of Chapter V.

³¹⁴ In addition to the CLASS database the State Department also operates the Distributed Name Check (DNC) system. The DNC operates as a backup system from a stand-alone personal computer, holding the CLASS database. It can be accessed by all U.S. missions. The systems transmission capabilities tend to be slow.

intelligence-based work, such as the VGTOF, CLASS or TIPOFF data sets, time can be of the essence. Remote access to such data sets will always present some potential risk. For example, early versions of the State Department's Distributed Name Check (DNC) database, with its slow access, and limited software functionality, meant that U.S. mission staff often by-passed the system in favour of manual searches by microfiche.³¹⁵ Academic terrorism data sets such as the RAND/St.Andrews or the University of Tel Aviv's terrorism database are not maintained and developed on the basis of the need for instant accessibility of data. While bonafide external requests for information may be required quickly, it is worth bearing in mind that academic terrorism data sets are not intelligence-driven real-time operations. With access restricted solely to staff working at their respective centres, immediacy of access to data may be dependent upon other commitments.³¹⁶ For clients using commercially based terrorism data sets over wide area networks, such as Pinkertons, the American Society for Industrial Security (ASIS), Control Risks or Kroll Associates, accessibility to timely information on security advisories is expected. Clients pay for, among other services, access to up-to-date security information.

In addition to transmission and accessibility problems with the CLASS system, the GAO reported other potential vulnerabilities in its operations. Concerns were noted over validation of visas at border security posts. The validation of visa issuance at border points could not be established automatically and relied on manual methods of authentication.

³¹⁵ Nelson, *op cit.* In response to such shortcomings the Department of State's Bureau of Consular Affairs have developed updated versions of the DNC software.

³¹⁶ Staff at both these academic centres conduct database searches on an agreed basis with internal researchers or external clients.

The involvement of several agencies in the use of Interagency databases containing details on known or suspected terrorists present operational problems unique to this type of data set. Integrity problems over entry of information into the CLASS database was highlighted in the GAO's report. These concerns arose over the realisation that not all U.S. missions overseas were adhering to established procedures and controls over entry of data. Five U.S. missions were allowing foreign nationals (FSN's) to check for names in the CLASS database without the supervision of a U.S. officer. Small and technical as this concern may appear, the implications for compromising security are apparent. The reliance on locally employed foreign service nationals to detect and notify U.S. missions of know or suspected terrorists places a very heavy emphasis on trust.³¹⁷ Further concerns over interagency co-operation on terrorism issues have become apparent since the inception of Lookout Committees at U.S. consulates and embassies.³¹⁸ Lookout committees were established after the World Trade Center bombing, to enable diplomatic, political and consular staff to meet regularly and identify the names of suspected terrorists that could be entered into the CLASS database and deny visa applications. The concept of the Lookout Committee depends upon four principle factors: co-operation, co-ordination, intuitive professional judgement and sound intelligence. Surprisingly, the weak link in the equation has been co-operation. Although not identified in the GAO's report officials, at least two embassies questioned the usefulness of such co-operative ventures, as liaison and co-operation appeared to be less than forthcoming. The problems appeared to stem from law and intelligence agencies reluctance to provide terrorism information to embassies and consulates,

³¹⁷ Nelson *op cit.*

³¹⁸ *Ibid.*

for fear of compromising their work and source information.³¹⁹ This type of interagency friction can potentially undermine the validity and integrity of terrorism information held on databases. Conflict of this nature, apparently petty and political in nature, illustrates the potential vulnerability of intelligence-based systems on terrorism that have a large user audience. Compared with most academic terrorism data sets, that reside within the relative safety of University campuses, the potential volatility of such widely accessible databases can be high, as a result of their wide user audience.

The Violent Gang and Terrorist Organisations File

Law enforcement and intelligence agencies in the United States have in recent years developed their own subject-specific computerised terrorism data sets to meet increasingly specialised intelligence requirements. One such data set is The Violent Gang and Terrorist Organisations File (VGTOF), established in October 1995.³²⁰ Operated through the FBI's National Crime and Information Center (NCIC), the VGTOF acts as a pointer system in identifying known members of terrorist organisations or violent gang members. The VGTOF differs markedly in several respects to other agency data sets holding terrorism information. The VGTOF was set up in part to protect not only U.S. citizens, but with an emphasis on helping police identify known suspects, and therefore protecting them in their duties. Many medium to small police departments in the United States do not have the resources to develop and maintain their own national data sets on criminal and terrorist

³¹⁹ The type agency represented on Lookout Committee's includes the Federal Bureau of Investigation, the U.S. Customs service and the Drug Enforcement Agency. Not all U.S. postings including Pretoria and Tokyo have all these key agencies represented.

³²⁰ Episcopo, Peter F. and Darrin L. Moor. 'Focus on Information Resources, The Violent Gang and Terrorist Organizations File' *FBI Law Enforcement Bulletin*. October 1996.

activity. With the spread into smaller communities of criminal and violent activities related to criminal gangs, drug trafficking and political motivated actions, the need for accurate and timely intelligence has increased. The VGTOF has addressed in part some of these needs, while maintaining sensitivity to local intelligence.

As its title suggests, the VGTOF's remit is to hold data on both terrorist organisations and organised criminal groups and gangs. This mixture of information on politically motivated violent group activity, coupled with criminal gang operations, differs considerably from the traditional separation of political and criminal violent events data. For example, nationally published information on terrorism information in the United States such as *TERRORISM in the United States*, strictly limits itself to acts of political violence.³²¹ While the inclusion of both criminal and politically activity in one data set may be unusual, the activities of such terrorist groups and criminal gangs have, over recent years, taken on some similar traits. These include illegal drug and money laundering activities to fund terrorist groups and gang organisations. Unlike simple chronological file formats such as the ITERATE data sets or the Serbian Unity Congress Chronology on Terrorism, the structure of the VGTOF closely reflects its practical operation.³²² The VGTOF classifies its data into two principle file categories: the Group Reference Capability (GRC) file, and the Group Member Capability (GMC) file. Coded details on the respective group and individual members must adhere to strict guidelines laid down

³²¹ US Department of Justice., *Terrorism in the United States 1995*, (Washington D.C. U.S. Dept.of Justice 1995).

³²² Edward F. Mickolus, *Terrorism, 1988-1991: A Chronology of Events and Selective Annotated Bibliography* (Westport, CT: Greenwood Press 1993). Access to the Serbian Unity Congress Chronology of KLA's Terrorism and Aggression can be gained via the Internet at: <http://www.suc.org/politics/kosovo/html/KLA.html>

by the NCIC.³²³ This requirement to adhere to national standards not only offers consistency in entry of variables nationally, more importantly the integrity of the data set is maintained. Another unusual attribute of the VGTOF is the variety of agencies that are permitted to make entries to the data set. Unlike academic terrorism data sets that are mostly maintained by a small specialist group of trained coders, the VGTOF procedures for data entry vary from state to state. For example, in some states a control terminal agency, such as the State Police will enter terrorist and gang details on behalf of the whole state. In other states, local and county police are permitted to enter data. Even more unusual, but reflective of its disparate operation, individual agencies are permitted to create new terrorist or gang records as long as they adhere to established NCIC standards. The type of variable created and coded within the VGTOF data set differs considerably from traditional chronological style terrorism data sets. Information known as 'essential identifying data' describes in detail the attributes of terrorist group and gang members.³²⁴ Information detailing the type of clothing of individuals or gang members, tattoo signs, communication signals, such as hand signs, are logged onto the VGTOF data set. This emphasis on intelligence based identifying criteria is beneficial in two respects. Firstly, it permits local law enforcement agencies to recognise the traits of known or suspected terrorists and gang members operating in their locale. Secondly, as neither terrorists nor criminal gangs recognise or limit their activities to specific states, they can be identified by the VGTOF on a national scale. Whereas traditional terrorism data sets such as Pinkertons or ATIC code basic variables, such as location

³²³ See U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, National Crime Information Center, Technical and Operational Update 94-2, "Violent Gang and Terrorist Organizations File."

³²⁴ Episcopo, *op cit.*

of incident, type of attack, and number of casualties mandatory variables within the VGTOF are much more personal in detail. This difference in emphasis relates primarily to the VGTOF's remit: it is an intelligence based data set, secondly agencies are able to legally hold personal data, a privilege academic and commercially based terrorism data sets do not enjoy.³²⁵ Some of the mandatory variables that are coded include sex, the names of individuals, their race and group affiliation. Optional information held by the VGTOF, highly detailed in nature, and information not always readily available to officers, includes information on an individual's eyes and hair colour, as well as their height and weight. The date and place of birth, if available, of known or suspected terrorists and gang members is also recorded. The value of such data for comprehensive quantitative analysis across terrorist groups and gangs operating in the United States would have to be highly selective, and may be of limited value, particularly as they relate to highly personalised information. At the risk of developing profiles of terrorists based on personal criteria that would promote stereotypes, careful analysis of data would be necessary. To dismiss such highly detailed information as irrelevant, would however, be a mistake. At an operational level, for security and police agencies working in communities, such data can be invaluable. Strongly related to practical intelligence data sets, but missing from standard terrorism data sets, is information pertaining to an individual's known psyche. Such details are contained within a miscellaneous field of the VGTOF. Law enforcement agencies are encouraged to "pack the record" with as much pertinent

³²⁵ Awareness among terrorism analysts of infringing data protection acts, by holding personal information on individuals is not merely a development of the late 1990's. As early as 1981 the Federal Data Protection Commissioner of West Germany advised caution on the retention and use of computerised terrorism data held by police authorities. Terrorism information, he advocated, should only be used for the 'lawful execution of duties'. Furthermore he recommended the erasure of all personal intelligence data once a case had been completed.

information as possible.’ Typical information could detail previous history of groups or individuals carrying guns or using threatening behaviour.

Intelligence based data sets such as the VGTOF stand apart from conventional terrorism data sets in two main respects. Their factual base tends to be cumulative, live and ongoing.³²⁶ Furthermore, as information is added or updated, any information that is found to be invalid must be deleted immediately. This deletion of data is not purely for reasons of integrity, although that in itself would be a valid argument. Law enforcement officials using VGTOF data that is found to be outdated could place themselves and others at risk. Unlike academic or commercial terrorism data sets, intelligence based systems such as the VGTOF are required by law to be audited by Federal authorities. The ramifications of inaccurate data for both police and civilians can be very serious. There is no obligation with managers of commercial or academic terrorism data sets to retain their source documentation. Although in many instances this may occur. By law the VGTOF is required to hold all source documentation and evidence that results in the generation of a Group Reference Capability (GRC) record or Group Member Capability (GMC) record. Eligibility of data for entry into the VGTOF is strict. A weak association of evidence would not be enough to justify the creation and entry of data into the system. Indicative of the seriousness of adhering to these regulations is the potential threat of litigation against a police agency from federal level.³²⁷ Although figures fluctuate,

³²⁶ Few data sets provide updates to previous published data or statistics. One such data set which does provide updates is Edward Mickolus’s series of chronologies on terrorism. His most recent chronology on terrorism provides an update of terrorism incidents from 1950 onwards, which is an unusually long time span in terms of terrorism data sets. Mickolus, Edward, and Susan L. Simmons. *Terrorism, 1992-1995. A Chronology of Events and A Selectively Annotated Bibliography*. (Westport Connecticut: Greenwood Press, 1997.)

³²⁷ The VGTOF is audited twice a year. These audits are conducted by the FBI’s Criminal Justice Information Services Division. Checks are made upon the accuracy of data and the backup and archive material used to support the VGTOF. Information given to the VGTOF by law enforcement agencies requires to be dealt with in the strictest of confidence as it has not been subjected to independent or judicial review. For further

the VGTOF had 445 groups and 180 individuals entered on the system at the end of 1996.³²⁸

Although the VGTOF data sets operates throughout the United States, the federal nature of law enforcement in the U.S. allows certain states to adopt different approaches to its use and operation, sensitising it to local operations. Such states include the State of Texas and the State of Florida. In Texas for example, criminal justice agencies are not permitted to enter data into the VGTOF data sets. This despite it being a state-wide database. This derives from state legislation stating that ‘.a local criminal justice agency may not send information collected under this chapter to a state-wide database.’³²⁹ Strangely enough, despite state restrictions of data entry from Texas, relevant Texan agencies are permitted to use the VGTOF file for intelligence purposes. It would appear mutual reciprocity takes second place to the states interests. Another state which has made provisions for itself, in addition to the VGTOF, is the State of Florida. After initial use, local law enforcement officials decided that the VGTOF was not meeting all their information requirements on terrorist and gang intelligence. A localised database was established in early 1997 to meet the VGTOF’s short-comings, this then fed data into the state-wide VGTOF.³³⁰

The local operational sensitivities of law enforcement agencies can present problems in trying to operate effectively a nation-wide intelligence based system. While reciprocal agreements between states is beneficial to all differing states

information see: George Hisamoto ‘NCIC Violent Gang/Terrorist Organization File’ at: http://caag.state.ca.us/cas/ccupdate/ccup97_2/gangterr.htm

³²⁸ Episcopo (note 72).

³²⁹ ‘TCIC AND NCIC Databases Incorporate New Files.’ Justice Information Management System (JIMS) Newsletter. Summer 1996. <http://www.co.harris.tx.us/jims/news/summer96.html>

³³⁰ U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. National Conference on Juvenile Justice Records: Appropriate Criminal and Noncriminal Justice Uses. Full text available via the Internet on: <http://www.ojp.usdoj.gov/bjs/>

political and practical priorities can take precedent over the concept of a truly national database on terrorism and gang intelligence.

Other U.S. Government Terrorism Data Sets

An array of other computerised terrorism data sets provide the U.S. Federal government with information on interpreting and responding to acts of terrorism. These range from specialist data sets on domestic bombings, aviation data on terrorism, and federal emergency management, to acts of international terrorism directed against U.S. citizens as well as acts of international terrorism in general.

No one central U.S. government agency retains and publishes information on all acts of domestic or international terrorism. The dispersed nature of these data sets although frustrating for novice researchers, provides by default, a healthy separation of data calculation. Reliance on one central data set for definitive statistics on all acts of terrorism has the potential for limiting any reference to secondary government sources, or the possibility of questioning data credibility.

Federal Bureau of Investigation (FBI) Data Sets

The Federal Bureau of Investigation has for many years collected and published data on acts of domestic terrorism. The FBI's remit to collect and disseminate information on acts of terrorism goes beyond the standard delivery of statistics on terrorism. With the advantage of federal funding it has been able to specialise in particular acts of violence, politically and non-politically motivated. With the creation of the Explosives Unit Bomb Data Center (EU-BDC) in 1994, resulting from the merger of

two separate units, concentration of skills has permitted better co-ordination in bomb investigations.³³¹

The EU-BDC Computer Reference Library operates what is thought to be the worlds largest computerised collection of data that can be automatically identified and compared with other bomb data.³³² Its capability by any standards is extensive, and offers FBI analysts facilities well beyond the functionality of academic and commercially based terrorism data sets. The database known as the Explosives Reference and Search System (EXPRESS) differs from other terrorism-based data sets in both its functionality and content of data. A particular advantage of the EXPRESS system is its ability to compare in detail across FBI recorded cases, to detect relevant data or common denominators. While some computerised terrorism data sets such as the Political Violence Research Unit database, at the University of Tel Aviv, operates with the powerful database Microsoft Access™, it cannot match the functional capabilities of the EXPRESS system. This is not to suggest that academic terrorism data sets are the poorer relative. They perform a different function, and are not generally designed and used for intelligence-based purposes.

One particularly capability of the EXPRESS system is its ability to compare cases of bombings using narrative based FBI reports along with photographic evidence for forensic examination purposes. This is a powerful tool. Further advantages include search facilities that can find similar bomb devices and their components, that are used in potentially linked incidents. The nature of this type of

³³¹ For more detailed discussions on the operations of the FBI's Explosives Unit Bomb Data Center see: <http://www.fbi.gov/lab/bomsum/eubdc.htm>

³³² *Ibid.*

data set tends to be forensic in purpose, as such it encompasses not only politically motivated bombings within the United States but other criminal bombing acts.

The sheer array of statistics on terrorism and bombing related incidents in the United States can present a confusing picture of where the data originally derives from. The collation and dissemination of information on bombings and explosive-related incidents is a joint effort carried out by the FBI and the Bureau of Alcohol, Tobacco and Firearms (ATF). Although the resultant statistics are combined, their respective remits to collect data, is by law, carried out separately.³³³ For example, the FBI's Explosives Unit Bomb Data Center is mandated by law to collect and hold bombing statistics reported to them by state and local agencies. At Federal level the statistics on bombings and explosives details are produced by the ATF.³³⁴ A point worth noting, with agency-based systems such as EXIS and AEXIS, is that they are not simply data sets on bombing incidents. The intelligence-based nature of the system means they perform several other functions in addition to merely reporting statistics. For example, the EXIS system, in addition to detailing aggregate totals of bombing incidents, acts as a repository for information on stolen explosives, as well as their recovery. Its new counterpart AEXIS will hold even more detailed data, including the ability to provide information on placement methods of bombs, their initiation and target, as well as details on suspected culprits.³³⁵

³³³ Statistics are collected under Congressional mandate of the Uniform Crime Reporting Act.

³³⁴ For combined FBI and ATF annual bombing statistics see: http://www.ows.aft.treas.gov:9999/exis_owas/owa/f_exis_report1

These annual statistics are derived from the ATF's AEXIS 2000 computerised system and the FBI's Bomb Data Center's system. In addition to the ATF's Explosive Incident System (EXIS) which has operated for the past 23 years, a new database called the Arson and Explosives Incident System (AEXIS) has recently been established. Although the existing EXIS system, as an explosives incident database, has served the ATF well, the need for a specialist database on arson was deemed necessary. For further details see: ATFNEWS FY-97-11. <http://www.atf.treas.gov/press/fy97-11.htm>

³³⁵ For further details of variables held see: http://ows.aft.treas.gov:9999/exis_owas/owa/f_exis_report1

Although acts of terrorism form only part of the information held within these systems, their operation illustrates several points. These systems are truly multi-functional database systems, responding to a plethora of differing needs and requirements. They include the provision of annual statistics for publication, to acting as a repository for explosives material, as well as holding information on suspects, among many other functions.

While an increasing amount of government agencies have established, or are in the process of developing computerised data sets on incidents of political violence, their operation across international boundaries tends to be limited. A mixture of political and national security sensitivity, coupled with a reluctance to share intelligence, has resulted in very few truly internationally co-operative arrangements. One such database project, operational since 1990 and which includes terrorism as part of its remit is the Interpol Explosives Incident System (IEXIS). Running alongside this is the Interpol Trafficking in Arms System (ITAR) database.³³⁶ These two specialist systems although built and maintained separately complement each other's remit. An interesting feature of both the IEXIS and ITAR system is the ability to simultaneously search both databases. The reasoning behind such a facility was that it was felt that increasingly criminal and violent actions can have many common denominators and links that may go unnoticed if left separated.

The Federal Aviation Administration (FAA)

The threat to aviation security from terrorist attacks is ever present. Attacks such as the bombing of Pan Am flight 103 over Lockerbie, in 1988, serves as a brutal

³³⁶ Thurman, Joey V. 'Interpol Computers Keep Track of Firearms, Explosives.' *The Police Chief*. October 1991. pp.53-58.

reminder of the heinous acts terrorist are prepared to commit. Public revulsion at such atrocities, sadly, has not annulled the actions of terrorists to commit similar acts. Bombings at Jorge Chavez International Airport, Lima, Air France offices in Tehran and the hijacking of a Royal Swazi Airline, all in 1993, serve as a sorry reminder that air travellers and the aviation industry must be ever vigilant.³³⁷

As part of its obligations to minimise potential terrorist attacks and counter-act where possible, the U.S. Federal Aviation Administration (FAA) implemented its computerised Civil Aviation Security Information System (CASIS) in 1985.³³⁸ Although CASIS is still used, a new system, of which very little is known, is being phased in to replace CASIS. The new system, known as the Airport-Airline Incident Reporting System (AAIRS), can operate from P.C. based systems over local area networks, connecting into the FAA's main network when required.

Despite the paucity of information on AAIRS, valuable lessons can be learnt from its predecessor, CASIS that will likely be incorporated into the new AAIRS system. The CASIS system when introduced in the mid-1980's operated from a mainframe system, and was used to allow FAA personnel to target resources and monitor trends. Although a subject-specific database, the CASIS system could not strictly be classified as an intelligence-based system, as with the VGTOF or TIPOFF data sets. Its purpose was part intelligence, part trends and analysis. The type of information contained within CASIS is varied, containing chronological details of bombing incidents at airports to the results documented from airport inspections.

³³⁷ These selection of incidents form only a minute proportion of incidents recorded by the Federal Aviation Administration during 1993. For further details see: U.S. Department of Transportation. *Criminal Acts Against Civil Aviation*. Federal Aviation Administration, Office of Civil Aviation Security. Washington D.C. 1993.

³³⁸ For basic information on the role and operation of CASIS see: U.S. General Accounting Office. *Aviation Security. Additional Actions Needed to Meet Domestic and International Challenges*. U.S. General Accounting Office Washington D.C. GAO/RCED-94-38, 1994. pp.42-45.

This mixture of events based data to evidence based information is unusual. In part it reflects the comprehensive nature of the system relative to the period of its design.

While the CASIS system was relatively advanced for its time, the U.S. General Accounting Office (GAO) in its 1994 report to Congressional Committees, identified several weaknesses in the CASIS system.³³⁹ The GAO highlighted problems relating to the FAA's use of CASIS in emerging trend analysis and its allocation of resources.

As the report notes:

'...CASIS does not contain information on the severity of a deficiency or how it relates to airport security as a whole. FAA denotes inspection findings as satisfactory or unsatisfactory. According to officials, this has led to a "check-list" mentality in the FAA security workforce that focuses more on filling out the inspection form than seeking long-term solutions to pressing security problems.'

³⁴⁰

These observations by the GAO illustrate several problems that administrators of terrorism data sets can run into. Firstly, the lack of quantifiable measurement of inspections can so very easily occur if specific fields within the data set are not disaggregated. The simple, and clinical Yes/No, Good/Bad and Satisfactory/Unsatisfactory type of variables provide minimal information to allow for informed decision making. While interpretation of words can cause problems, some form of numerical ranking, for example 1-5, can provide an indication of the seriousness of situations. Detailed breakdown of variables is not without precedent. The Pinkertons *Annual Risk Assessment*, for example, provides in its table of total incidents of political violence world-wide, four levels of identified risk to countries:

³³⁹ Ibid. pp.42-45.

³⁴⁰ Ibid. p.43.

extreme, high, moderate and low.³⁴¹ Although these risk assessment levels are very general, they do provide clients and analysts with some indication of a countries risk status at a glance.

The GAO's concern over the "check-list" mentality of staff using CASIS is indicative of the assumption that just because data has been coded on computer it is legitimate. The FAA's failure to both effectively use the data, and suggest improvements in CASIS's design, again adds weight to the fallacy that legitimacy derives from computerisation of data. Part of the GAO's report on CASIS highlighted one of *the* classic mistakes that can be made from the computerisation of data in general, and can be just as applicable to the design of terrorism data sets. If data is not coded, the problem does not exist. Likewise, if terrorist incidents are not coded, they have not taken place. Any serious student of political violence would dismiss the last statement instantly. Where the CASIS system failed was its inability to detail where the unsatisfactory security conditions derived from. Detailed security information included carry-on baggage screening, passenger screening, airport fences and identification badge control (temporary). As GAO notes:

'...CASIS does not include information to determine whether the unsatisfactory [security] conditions resulted from carelessness on the part of the individuals or were symptomatic of much larger problems.'³⁴²

In its defence the FAA argued that:

'... CASIS was not developed to capture the state of security at the nation's airports. Instead, important information on the strengths and weaknesses of

³⁴¹ Pinkerton Risk Assessment Services. *Annual Risk Assessment 1993*. (Arlington, VA: Pinkerton, 1994.) Much more detailed narrative analysis of regional trends and specific countries risk levels are presented within the *Annual Risk Assessment* compared, for example with *Patterns of Global Terrorism*.

³⁴² GAO, *op cit*, p.44.

air carrier and airport security reside with individual FAA security inspectors.’

³⁴³

As part of its response to the GAO report, FAA officials revised the CASIS system to enable it to incorporate the information noted above.

In concluding its observations on the CASIS system, the GAO made several valid points worthy of elaboration. The GAO highlighted the incompatibility of the CASIS database and its inability to integrate with FAA and other computerised systems.³⁴⁴ This particular problem is not unique to the FAA. Early versions of the RAND databases and chronologies on international terrorism, the ITERATE data sets and the U.S. State Department's TADIMS system, have encountered compatibility problems, particularly their execution on a Windows based operating system environment.³⁴⁵ These problems derive primarily from the time period they were developed. All the above data sets were designed in the 1970's or early 1980's. Operating primarily from mainframe computer system, their compatibility with other system was extremely limited. The advent of Microsoft Windows™ and Apple Mac™ operating system environments, vastly superior software and hardware, as well as sophisticated network technology has revolutionised the scene. Terrorism data sets currently benefiting from the new technologies include the State Department's TIPOFF database and the Overseas Security Advisory Council's (OSAC) Electronic Data Base.

³⁴³ *Ibid.*

³⁴⁴ *Ibid.* p.45.

³⁴⁵ The operating system software acts as the 'manager' of the computer system. The advent of Microsoft Windows operating systems on PC's and Local and Wide Area Networks, has only really developed to any great extent from the early 1990's onwards. The RAND-St. Andrews Chronologies on International Terrorism are now operated on a P.C. based system via a network server. The CODA software is still used. During 1998 a series of prototype files were designed using Microsoft Access database software to run sample data sets from the RAND-St. Andrews Chronologies and data sets.

Nearly seventy five percent of the FAA's security workforce were identified as having problems easily accessing the CASIS system to conduct basic work. A third of their time was spent entering data into the CASIS system.³⁴⁶ Purely on efficiency grounds alone, problems of accessibility and sheer time consumption spent on data entry makes the CASIS database a highly unattractive piece of technology. More importantly, where such a security system is seriously under-performing, the risk of terrorism security breaches will tend to be higher.

One of the most important recommendations of the GAO's report on CASIS was to introduce facilities for carrying out more detailed numerical analysis:

'A first step would be to develop quantitative measures to analyze security inspection data. As noted earlier, most inspection results only indicate whether a satisfactory or unsatisfactory condition exists. A more analytical approach would provide FAA with better information to make decisions regarding security.'³⁴⁷

The lack of quantitative measurement facilities in CASIS highlights a problem not solely restricted to the FAA's system. Many of the early, computerised terrorism data sets developed on mainframe systems in the late 1970's and early 1980's, such as the RAND, TADIMS and the University of Tel Aviv's data sets, were unable to offer even basic aggregate data analysis. While numerical variables such as number of causalities were either coded or entered among narrative descriptions of incidents, the software was unable to calculate data on numerical variables. These functions among many other basic and complex numerical and statistical functions are now available to data sets such as the TRPUV and TIPOFF.³⁴⁸

³⁴⁶ GAO, *op cit*, p.45.

³⁴⁷ *Ibid.*

³⁴⁸ In addition to basic arithmetical functions for calculating data the GAO suggests that some form of scaling procedure be introduced for compliance with specific security regulations, where such issues cannot be easily

Publicly acknowledged short-comings of security related government run database systems such as CASIS is rare, and is to be welcomed. Balancing security considerations with the public's right to know of potential weaknesses in a system is always a finely tuned consideration. The particular sensitivity of aviation, a mass form of transport, illustrates the acute need to handle these matters with care. The FAA's report tackles the weaknesses of the CASIS system head on, and makes practical and realistic suggestions for improvement in both hardware and software operations that are now entirely feasible.

Other Government Computerised Data Sets

In recent years the amount of computerised data sets handling terrorism and security related issues has increased significantly. The general and subject-specific terrorism data sets mentioned above form part of an even wider series of computerised networks that operate within the United States and beyond. Again publicly available information on these data sets tends generally, though not exclusively, to derive from North America.³⁴⁹ Among the more relevant data sets that encompass terrorism issues is the South Pacific Islands Criminal Intelligence Network (SPICIN). Its unusual and rather large title reflects its enormous geographic remit: the Commonwealth of Australia, New Zealand, the Federated States of Micronesia, the French Society Islands, Western Samoa, and the Solomon Islands are among its twenty one country membership.

quantified, but require some indication of having met regulations. For further examples of database numerical and statistical functions see Chapter VI of this thesis.

³⁴⁹ For a useful list of security related computerised databases see: U.S. General Accounting Office. *Investigators Guide to Sources of Information*. Chapter 4, Electronic Databases. GAO/OSI-97-2

The SPICIN system, in part fills an intelligence gap in a geographic area of the world that is both very large to cover and often underreported. With heavy coverage of terrorism events in the Northern Hemisphere, particularly North America, Europe and the Middle East, attention on terrorism activity in much of the Southern Hemisphere tends to be minimal. Admittedly, compared with other regions of the world, Australasia and the Pacific regions have considerably less incidence of terrorism activity than their Northern counterparts. The U.S. State Department's *Patterns of Global Terrorism 1996* makes no mention of terrorism activity in the region for that year. Pinkerton's however, identify activity in Vanuatu and Australia in their 1996 report.³⁵⁰ The regions low terrorism activity should be no excuse for the non-recording of incidents. The SPICIN system is not a dedicated database system for terrorism activity in the South Pacific. It deals with the collation, coding and reciprocal exchange of terrorism information, drug intelligence data and other criminal activity among relevant agencies in the Pacific region.³⁵¹

Other lesser-known systems that encompass terrorism related information, among many other areas of security, include: the FBI's Fingerprint Identification Records System (FIRS), the National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS) and Sentry. The Sentry system is operated by the U.S. Federal Bureau of Prisons, and contains information on all prisoners held with jail in the United States since 1980.³⁵²

Illustrative of such new developments in the field have been comments made by Kay C. Goss of the U.S. Federal Emergency Management Agency (FEMA). In a speech

³⁵⁰ U.S. Department of State. *Patterns of Global Terrorism 1996*. U.S. Department of State Publication. Office of the Secretary of State, Ambassador-at-Large for Counterterrorism, Washington D.C. 1997. Pinkerton Risk Assessment Services. *Annual Risk Assessment 1996*. (Arlington, VA: Pinkerton, 1997.)

³⁵¹ For further information on the operations of SPICIN see: http://www.fas.org/irp/gao/osi-97-2/soi_ch4.htm

³⁵² For more detail on these computerised systems see: http://www.fas.org/irp/gao/osi-97-2/soi_ch4.htm

before the NATO Civil Emergency Preparedness Symposium meeting in Moscow, Goss outlined the essential elements – still relevant today - required in the handling terrorism incidents co-ordinated at local, state and federal level.³⁵³ These include:

‘Pre-positioned resources, which allows all levels of government to have the necessary databases, communications links, inventories of assets, equipment, availability of experts, and other critical requirements.’³⁵⁴

The ‘necessary databases’ which Goss refers to do not have to be strictly limited to data sets on known terrorist groups. Their value may be of limited use in the immediacy of injuries, death and the need for crisis management. What Goss argues for, is that pragmatic and practical advice be made available to FEMA and other agencies in handling terrorism incidents. In the aftermath of a terrorism incident, databases could hold, for example, information on local medical specialists, fire and safety personnel, as well as trained counsellors. This holistic approach to the use of terrorism data sets, with their acknowledged shortcomings, could offer a powerful integration of infrastructure data in handling critical post-incident events.

Goss highlights the three levels of terrorism incident crisis management. These, in part, compliment some of the functions of existing terrorism data set such as the VGTOF, IEXIS and TIPOFF.

‘Crisis management includes proactive measures for prevention, immediate incident and post-incident response, including command of the operational response as the on-scene manager for an incident.’³⁵⁵

³⁵³ Presentation given by Kay C. Goss. *America Preparing for the Consequences of Terrorism*. The United States Federal Emergency Management Agency (FEMA) Before the NATO Civil Preparedness Symposium. Moscow, Russia April 22nd 1997.

³⁵⁴ *Ibid.*

³⁵⁵ *Ibid.*

What may be more realistic however, is a move towards relationally linked terrorism databases that are maintained separately by respective specialists, and drawn upon as required.³⁵⁶

For FEMA and other agencies involved with post-terrorism incident management, one of the crucial factors involved in successfully minimising casualties is time. As operational tools, computers can execute commands within milli-seconds; much faster than the most competent human. Through networks such as the Internet, information can be accessed almost instantly, on a global scale. Particularly where chemical and biologically based attacks occur, the need for an almost instant response is paramount if lives are to be saved. As Goss notes:

‘Expert advice in terrorism, on the other hand, may make the difference between life and death for thousands, particularly if chemical or biological weapons are used. There are so many different types of agents that could be used, with many variables in medical response, that expert advice must be quickly available to any community.’³⁵⁷

As attractive a scenario as this may paint, instant accessibility to local, national or global expertise must be qualified in one vital respect: the frailty of human decision-making. Acknowledgement of this ever-present weak link in the chain, should not be a deterrent for dedicated professionals to fully grasp the exciting potential of new technology. The increasing mobility and accessibility of computerised systems in the form of mini-computers that can be activated in or around the scene of a terrorist incident has not been lost on FEMA:

‘That’s another reason why pre-positioned and easily accessible databases are so invaluable. Thankfully, computerized access to vast sources of

³⁵⁶ The notion a fully integrated crisis management terrorism database closely mirrors the argument for a macro world-wide database on terrorism. Attractive as this may sound, the practical implications in terms of funding and maintenance could be prohibitive, unless funded by Government. As such, without considerable investment in development and maintenance, the projects credibility and integrity could be jeopardised.

³⁵⁷ Goss, *op cit.*

information makes quick answers to questions a possibility – and, where chemical or biological agents are involved, time is of the essence.’³⁵⁸

4.6. Academic Terrorism Data Sets

Academically maintained computerised terrorism data sets form one of *the* major sources of reference for academics and analysts researching the field of terrorism.³⁵⁹

Increasing interest in the subject area is not, however, reflective of the amount of computerised terrorism data sets available. Confusion between the availability of terrorism data sets via computer and the development and maintenance of computerised terrorism data sets needs to be clarified. Only a handful of academic and policy institutions world-wide could seriously be described as maintaining and developing substantial computerised data sets in the field of terrorism. Where some confusion arises, is that a number of sources, both government and academic, provide links to terrorism data sets, on computer via the Internet. These include: the United States Department of Justice, Department of State, the FBI and the Northern Ireland Office among others.³⁶⁰ These are discussed at length in Chapter V of this thesis.

The principal academic institutions holding such data sets are the Centre for the Study of Terrorism and Political Violence, at the University of St. Andrews, Scotland, (until recently, in conjunction with the RAND Corporation of Santa Monica)

³⁵⁸ *Ibid.*

³⁵⁹ Studies using academic terrorism data sets include: Jongman (note 16), Sandler, Todd. ‘On the Relationship between Democracy and Terrorism.’ *Terrorism and Political Violence*. Vol. 7. No.4. (Winter 1995.) pp.1-9. Ross, Jeffrey Ian. ‘Research Note: Contemporary Radical Violence in Canada: A Quantitative Analysis.’ *Terrorism and Political Violence*. Vol.4. No.3. (Autumn 1992) pp.72-101.

³⁶⁰ The subtle, but crucial difference between the maintenance and development of computerised terrorism data sets and the availability of terrorism data sets via such mediums as the Internet is important. None of the academic data sets discussed above are available on-line via the Internet or a Wide Area Network. Certain government agencies do however make available terrorism data sets via the Internet. These include the FBI, ATF, Northern Ireland Office and the U.S. State Department. These data sets are pre-dominantly presented in a Hyper Text Mark-up Language (HTML) format and do not give users direct access to a computerised database. One of the few exceptions to this rule is OSAC’s electronic database and the Israel Interdisciplinary Center, Herzliya. For further discussion of these issues see Chapter VI of this thesis.

and the University of Tel Aviv's Political Violence Research Unit (PVRU).³⁶¹ Although not strictly deriving from an academic institution, the series of ITERATE chronologies and data sets published by Edward Mickolus at Vinyard Software, form another major source of academic reference. Smaller computerised projects, and subject-specific in content, include the Attributes of Terrorism in Canada (ATIC) data sets developed and maintained by Ian Jeffrey Ross and a series of South African data sets maintained by the University of Natal, South Africa. The remit of academically based terrorism data sets differs considerably from their government and intelligence based counterparts. They are maintained and developed primarily for use in research-based activities. They have no intelligence role, although they are often consulted by external media, commercial organisations and research analysts for information. Access to the full data sets over such mediums as the Internet generally is not permitted.

RAND-St.Andrews Database on Terrorism and Low-Intensity Conflict

The RAND-St Andrews data sets on terrorism and low-intensity conflict, in the league of computerised terrorism data sets, can be considered to be one of the longest established data sets of its kind. Its long history merits some attention. Originally developed in 1972, at the RAND Corporation, a U.S. policy think tank, they have been maintained and developed for over quarter of a century.³⁶² That is a considerable amount of time, considering the fact they are computerised, and require on-going

³⁶¹ Until December 1998 the Centre for the Study of Terrorism and Political Violence maintained and operated what was known as the RAND-St.Andrews computerised chronologies and data sets on international terrorism. The RAND Corporation in co-ordination with the University of St.Andrews developed and maintained these data sets from 1994 until 1998.

³⁶² The original RAND data sets on terrorism were initially developed by Brian Jenkins, Geraldine Petty and latterly by Karen Gardela and Bruce Hoffman.

maintenance and development. As mentioned in Chapter IV of this thesis, the RAND chronologies and data sets were designed and built at RAND using custom-built software called CODA. The advantage for terrorism researchers was that their own particular research requirements were incorporated into the functional capabilities of the CODA system in its early design.³⁶³ At the time, these were basic facilities, such as text fields to hold narrative on terrorism incidents as well as basic editing facilities. Annual hard copy publication of the *RAND Chronology of International Terrorism* provided external researchers and analysts with access to data held at RAND.³⁶⁴ The RAND chronologies included narrative comment on trends in international terrorism, including terrorist tactics, regional trends in international terrorism and specific attacks on American targets. In addition to the annual RAND Chronology of International Terrorism, a breakdown of terrorist incidents by perpetrator, tactic, target and region was also provided. The data sets operated from a mainframe computer system running under the UNIX operating system software.³⁶⁵ For its time the RAND system was fairly advanced. Shortcomings however in its ability to carry out arithmetical and statistical operations for quantitative analysis of terrorism events meant that these often had to be calculated manually.

The mid 1990's saw major changes as RAND's Santa Monica headquarters with the funding for long-term terrorism projects such as the data sets under some pressure. The move by Dr. Bruce Hoffman of RAND to the Department of International Relations at University of St. Andrews, Scotland resulted in the RAND terrorism data sets being moved from its Santa Monica headquarters to the Centre

³⁶³ See: Dewar, James A. and James J. Gillogly, *CODA: A Concept Organisation and Development Aid for the Research Environment* (Santa Monica CA: RAND Corp. P-7035 1984).

³⁶⁴ Hoffman, Bruce and Karen Gardela. *The RAND Chronology of International Terrorism for 1986*. (Santa Monica, CA: RAND Corp., R-3890-RC, March 1990).

³⁶⁵ Dewar, *op cit*.

for Terrorism and Political Violence (CTPV) at the University of St. Andrews, Scotland.³⁶⁶

In addition to the RAND data sets, and the considerable terrorism research material already held at St. Andrews, Control Risks Ltd. of London, a leading security/risk consultancy business, agreed to donate on a regular basis its archival material on terrorism and twentieth century conflict data. The cumulative results of this merger of resources meant that the Centre for Terrorism and Political Violence at St Andrews held one of the world's most formidable collection of terrorism research material, and was complemented by on-going development of the newly titled RAND-St.Andrews Chronologies on Terrorism and Low Intensity Conflict.

As a source of data, the RAND-St.Andrews data sets provided a rich and comprehensive collection of electronic and hard copy material, for undertaking terrorism research. The computerised data sets allowed researchers to carry out trend analysis of terrorist behaviour, their methods and motivation. Contextual analysis of terrorist attacks, principally by means of text fields, as well as coded variables, provided researchers with a macro view of events. Other forms of analysis that could be undertaken using the data sets included group and policy analysis.

One of the strengths of the CTPV data sets in addition to its chronologies on international terrorism, is the computerised ancillary data sets and archive material on terrorism and low-intensity conflict data. These topics included: maritime and aviation security, emerging conflicts data, organised crime, religious fundamentalism as well as ethnic violence and genocide among many other topics. This truly eclectic collection of specialised terrorism and low-intensity conflict data, both computerised

³⁶⁶ The re-location of the RAND data sets to St. Andrews was part of an agreed arrangement between both centres to maintain and develop the data sets.

and manual, provided researchers with one of the richest collections of data to be found in any University within North America or Western Europe.³⁶⁷

The establishment of the RAND-St.Andrews chronologies at the University of St.Andrews not only provided a superb collection of research material but importantly provided a focus from which other terrorism analysts and researchers were encouraged to contribute to a research field that requires considerable attention. As discussed in earlier parts of this thesis, there continues to be very little academic research work written on the application of computerised database systems to the terrorism research field. This void has not gone unnoticed. The leading academic journal in the terrorism field *Terrorism and Political Violence* which published the RAND-St Andrews Chronologies on International Terrorism, has encouraged contributions to the database field. Professor Paul Wilkinson, its co-editor, aware of the lack of published literature has invited contributions among others on: domestic terrorism databases, analysis of trends in terrorism and counter-terrorism, the impact of terrorism on victims as well as socio-economic, cultural and religious databases on terrorism. In addition, Wilkinson also promotes the need for further research to be carried out into database design and management, technical issues as well as emerging trends in Information Technology.³⁶⁸ The call for more research into technical and management issues relating to terrorism data sets, as well as Information Technology is to be welcomed. Although there has been a slow

³⁶⁷ For further details of the RAND-St.Andrews data collections see: Hoffman, Bruce and Donna Kim Hoffman. 'The RAND-StAndrews Chronology of International Terrorism, 1994.' *Terrorism and Political Violence* Vol.7.No.4. Winter 1995. pp.178-229. The forward to this article by Professor Paul Wilkinson of the University of St. Andrews provides a detailed context to the terrorism database field and outlines the plans for the databases development at St. Andrews.

³⁶⁸ *Ibid.*

response, contributions by Gordon as well as Devost, Houghton, Pollard et al. have set in motion the development of a vastly under-researched literature base.³⁶⁹

While at the Centre for Terrorism and Political Violence, the RAND-St.Andrews chronologies began to broaden the methods by which it collected source data. The advent of the Internet and clipping services such as Lexis-Nexis enabled research staff to access a much broader forum of literature. Reliance mainly on hard-copy source material has been a trait of most terrorism data sets, until the arrival of electronically accessible material via such mediums as the Internet. Increased access to source material however does not guarantee the perfect data set. Data has to be captured, accurate and coded. Even then the chances of logging every incident of terrorism occurring world-wide is almost impossible. Claims by any data sets administrator to have the most authoritative collection of recorded incidents should always be tempered with reality that the recording of acts of terrorism, domestically and internationally is an imperfect science. One of the great strengths of the RAND-St.Andrews data sets was acknowledgement by its director that while the chronology attempted to be as inclusive as possible absolute perfection was neither possible nor realistic. As Hoffman notes:

‘It should also be emphasised that the data contained in the Chronology is intended to be illustrative only and does not purport nor claim to be a definitive listing of every international terrorist incident that has occurred everywhere since 1968. Its value, accordingly, is as a means of identifying terrorist trends and projecting likely future terrorist patterns.’³⁷⁰

³⁶⁹ Gordon, Avishag. “Terrorism and Computerised Databases.” *Terrorism and Political Violence* Vol.7. No.4. Winter 1995. pp.171-177. Devost, Matthew G., Brian K. Houghton and Neal Allen Pollard. “Information Terrorism: Political Violence in the Information Age.” *Terrorism and Political Violence*.Vol.9. No.1 Spring 1997. pp.72-83. For much further detailed discussion of the application of Information Technology to terrorism research see Chapter V of this thesis.

³⁷⁰ Hoffman, Bruce. ‘The Confluence of International and Domestic Trends in Terrorism.’ *Terrorism and Political Violence*. Vol.9 No.2. (Summer 1997). pp.11.

The end of 1998 saw major changes in the operation of the RAND-St.Andrews data sets. With the return of Dr. Hoffman to the RAND Corporation in December of 1998, the RAND-St Andrews chronologies and data sets on terrorism reverted back to their original home base at RAND in Santa Monica.³⁷¹ The data sets are to be known as the RAND Database. The future development of the RAND Database is as yet unknown. From a software perspective, the retention of the data sets on the CODA system will likely become increasingly untenable. The CODA system although having provided years of service is quickly reaching, if not already reached, its sell by date. Although the continuity of CODA has been one of its strengths, the adoption of readily available relational database software supported in a Windows environment is long overdue.

A small, but crucial point worth noting, is the potential fate of the original RAND data sets had RAND decided not continued their maintenance. Any stoppage in their maintenance could seriously have put at risk the future of the data sets. Their move to the University of St.Andrew's CSTPV ensured their continued development at time when their future within RAND was uncertain. Data sets of this type of magnitude require to be maintained constantly. They cannot be treated as a hobby or a passing interest in the subject field. To have intermittent or periodic recording of data not only threatens their integrity, but makes the task of coding back-logs of data an almost impossible task. These projects are for the long run; temporary respite even for a few weeks or months can seriously jeopardise the data sets operation.

³⁷¹ Although Dr Hoffman has taken a new position as Director of the RAND's Washington bureau the newly titled RAND Database is to be run from RAND's Santa Monica headquarters.

Although little is known of RAND's plans, the Centre for Terrorism and Political Violence at St.Andrews has indicated some of its plans for the future development of computerised data sets on terrorism.³⁷² Instead of replicating existing terrorism chronologies and data sets, which would be a vast waste of both financial resources, and time, it plans to develop new databases on post-conflict resolution. These would encompass such areas as South Africa, Northern Ireland and Israel. Other areas that are planned for computerised database development include data sets on international organised crime, issues relating to multi-national peace keeping and peace-enforcement operations. This deliberate move to cover other areas of terrorism and conflict research is refreshing, and will broaden the availability of research data in a field requiring much attention.

The Political Violence Research Unit Terrorism Database ,University of Tel Aviv

The Political Violence Research Unit (PVRU) terrorism database, rates along with the RAND and RAND-ST.Andrews data sets as one of the longest established computerised data sets on terrorism and political violence. The data sets were established by Professor Ariel Merari in 1978 at Tel Aviv University's JaffeeCenter for Strategic Studies.The data sets were originally held on a manual card-index system; this followed a very similar pattern to the early development of other data sets such as TIPOFF and the Pinkerton's PRAS data sets.³⁷³ As is often the case with terrorism data sets, their development and maintenance forms part of a larger project. The TPVU terrorism data sets in their early phase provided the core data to support the

³⁷² See http://www.st-and.ac.uk/~www_sem/IR/about.html

³⁷³ (PRAS) - Pinkerton Risk Assessment Services data sets.

Jaffee's Project on Terrorism and Low Intensity Warfare from 1978 until 1989.³⁷⁴

The JaffeeCenter's annual publication of the INTER terrorism data sets, derived its data from the Jaffee project.³⁷⁵ The data sets moved from the JaffeeCenter in 1989, with the creation of the Terrorism and Political Violence Unit (TPVU) under the directorship of Professor Merari.

Continuity over the years in the use of software to support terrorism data sets has varied among agencies and organisations. The dilemma between upgrading software to provide improved functionality, and the cost, design, training and maintenance implications can be a difficult act to balance. The TPVU data sets have encountered several changes in software, unlike the RAND and RAND-St.Andrews terrorism data sets, which have had long software continuity with CODA. For example, the TPVU's terrorism data sets have undergone several changes: from operating under a card-index system, mini-computer and mainframe software, to its present Microsoft Access database system.³⁷⁶ The TPVU's current hardware and software system provides in part, a model from which other systems designers could learn from.³⁷⁷ The availability of sophisticated software and hardware is no guarantee

³⁷⁴ Terrorism data sets can be free-standing, such as the U.S. State Departments Patterns of Global Terrorism, the ITERATE data sets or the RAND-St.Andrews data sets on terrorism. Alternatively they can be developed to support large on-going projects. These include: The Project on Terrorism and Low Intensity Warfare (as above), the FBI's Violent Gang and Terrorist Organisations File (VGTOF) or the U.S. State Departments TIPOFF data sets.

³⁷⁵ *INTER International Terrorism in 1987* (Jerusalem: The Jerusalem Post 1987).

³⁷⁶ Information derived from communications with Professor Ariel Merari, Tel Aviv University, July 1998. Also from communications and meetings with Zvika Adar, TPVU administrator, Edinburgh September 1998. The TPVU terrorism data sets were originally computerised from 1979-83, under the supervision of Professor Merari. Initially, only acts of Palestinian Terrorism (International) were coded on computer. From 1983 all events data were computerised. The TPVU terrorism data sets operated on a VAX computer system run by DIGITAL Inc. hardware, the software used to hold the data sets was written specifically for the project and was known as X-FIC. Over the years the system was transferred to the University's main VAX computer. Requiring closer control of the data sets from within the TPVU, a programmer was employed to code them to run under Microsoft Access database software.

³⁷⁷ Currently (1999) the data sets run under Microsoft Access, operating from a COMPAQ ProSignia server running under Microsoft Windows 95. The tables are relational in design. Data can also be entered via scanner and the World Wide Web (WWW). Current development includes plans to make the data sets partly available in

of a quality data set. The TPVU's data sets do, however, provide a comprehensive collection of terrorism and political violence events data, with specific emphasis on Middle East terrorism.

The TPVU data sets are organised over three main database files, with relationally linked tables. The files are: Terrorist Events, Terrorist Groups and rather unusually - States' Attitude towards Terrorism. The Terrorist Events file offers an impressive collection of coded and narrative data. Key fields used to describe events include standard variables such as: date of event, place of occurrence and target. Further detailed variables provide more subtle but crucial information. For example, the data set differentiates between claimed respondents to acts of terrorism and the actual perpetrating organisation. Operational tactics as well as arms and equipment used by terrorist groups are also recorded, if available. A simple field titled 'Success Event' requiring a Yes/No entry, provides a quick, if crude assessment of an events 'success'. Calculated carefully, using specific Microsoft Access functions, this field could provide a simple aggregate comparative analysis of terrorist groups successes or failures. The criteria for assigning a Yes or No to an incident would have to be clearly defined. Even more detailed variables coded within the file includes geographic routes taken by terrorist's to carry out acts of violence. Others include 'Demands' and resultant 'Threat[s]' from terrorist groups.

The Terrorist Groups file is substantial, containing information on over one thousand sub-national groups. This file offers highly detailed information on the many attributes of terrorist groups, providing excellent profiles and data for further research. Details in narrative form include terrorist group history, general

Hyper-Text Mark-up Language (HTML) format, as is used on the Internet Web pages. Other plans include running the data sets from various platforms including: Windows 95/98, Unix and AppleMac systems.

descriptions of the groups activities, strategies, ideologies, leadership and membership as well as their geographic spread of activity. Other variables include preferred tactics and modes of operation, state support as well as identified links to other terrorist organisations. One particular variable in the Terrorist Groups file, which is rarely formally recorded - even among terrorism data sets - is details on the public attitudes towards terrorist groups.

The third file in the TPVU data sets addresses an area of terrorism research requiring considerable attention: the 'States Attitudes toward Terrorism'. Details such as state support for terrorist groups, ideological positions, counter-terrorism activities, law-enforcement, special anti-terrorist units and extradition treaties, are among a gamut of state related approaches to terrorism activity held on file. The lack of publicly available data sets produced by government on this specific topic, is in part understandable. Apart from obvious sensitive political, security and operational reasons, few governments are willing to publicly record let alone acknowledge even a small percentage of the above activities. Publication of such data could by default result in governments being accused of implicit involvement in actions such as state sponsored terrorism. Academic centres such as the TPVU offer at a minimum integrity, un-biased analysis and objective rigour from which such sensitive data can be compiled.

Despite the TPVU's wide-ranging coverage of terrorist activity, the practicalities of maintaining a truly global database on terrorism were recognised by its owners as being rather ambitious. The drive for total inclusivity of events data can often weaken research bases. From 1989 onwards the TPVU's data sets changed emphasis, concentrating, with the exception of several categories, on Middle East

terrorism at both domestic and international level.³⁷⁸ This pragmatic move was both a recognition of the limits of one institution trying to sustain global coverage of events but also strengthened their resources on coverage of Middle East activities, its natural 'back-yard'.

The TPVU data sets, as a well established repository of events data on terrorism, provide not only a rich source of reference for research, but redress geographically the Western bias in reporting and maintenance of such data sets. On the grounds of pure objectivity in the recording and assessing events data, this healthy situation can only be encouraged. The current hardware and software specifications of the TPVU data sets also provide a very useful prototype for other researchers interested in developing terrorism data sets. The considerable time period over which they have been developed and maintained, coupled with the TPVU's willingness to refine and improve the data sets functional operations, illustrates the potential benefits that can be derived from new technologies.

The ITERATE Data Sets

The ITERATE (International Terrorism: Attributes of Terrorist Events) data sets form one of the longest established series of data sets and chronologies on terrorism. Published over five volumes, in varying titles, and recording incidents from 1968 onwards, they can be classified as partly academic and commercial data sets. The

³⁷⁸ The TPVU continues to records acts of international terrorism world-wide related to hostage and aviation incidents.

principal author over all five editions, Edward Mickolus has compiled a considerable collection of terrorism events data, presented mainly in chronological format.

The ITERATE data sets differ in several respects from other computerised terrorism data sets. The data sets are publicly available for purchase in both hard copy and computerised format. They are one of few terrorism data sets that can be bought on floppy disk and run remotely from the purchasers computer. Unlike *Patterns of Global Terrorism*, an annual publication, the ITERATE data sets are published on a periodic basis as and when the author deems the publication to be viable. Despite several shortcomings, outlined below, the task of maintaining and producing such a comprehensive set of data is substantial, particularly over the time period covered.

The ITERATE data sets could not be classified as a true database of terrorism incidents. The chronological listing of events within the data set is held within a text-based system. Although this has served the authors over the years well its usefulness operationally can be limiting. For example, calculation of statistics for quantitative purposes within the data sets has to be carried out using external statistical software, such as SPSS. The computerised format of the data sets is held on text-based software, thus limiting the potential for the generation of forms, reports, querying and statistical functions. Even within the hard-copy version of the chronologies the ability to calculate aggregate totals can be a potentially lengthy process given the narrative format in which the data is presented.

As is often the case, quantity of data gives no guarantee of quality. As Eubank notes on his review of the latest chronology: *Terrorism, 1992-1995: A Chronology of Events and a Selective Annotated Bibliography*:

'The descriptions, admittedly not analytical, range from a very few lines to several pages, with the World Trade Center bombing an example of the latter. Immediately preceding this event is a recording of "...PKK members attacked Turkish interests in Zurich and Geneva. 93062430-31", (p.430). Thus it is hard to know what to make of many of these descriptions, being similar in content. ...Admittedly not each event is of the same importance as every other, but it would be helpful if some had been a bit more informative.'

Eubank's reference to the brevity of some incident descriptions could in part be explained by lack of data. However, if incidents are recorded, some form of minimum criteria for variables would be helpful, not only for basic information purposes, but also to allow minimum comparative analysis of basic variables. The voluminous nature of the manual data sets and the limiting functionality of its computerised equivalent render the ITERATE data sets awkward to use for detailed analysis, cross-referencing, identifying links and emerging trends and patterns in terrorism behaviour.

In his 1988-1991 chronology of terrorism Mickolus has erroneously attempted to quantitatively measure aggregate trends in terrorism attacks by month and year, using computer bytes as the unit of measurement. Mickolus recognises that calculating terrorism activity and trends is not at times an easy task:

'Determining trends in terrorism has always been methodologically controversial.At the risk of being self-referential, I have attempted to create a surrogate measure of such media attention [of terrorist attacks] by looking at the coverage of incidents by this chronology. As the chronology is based primarily on media accounts around the world, tallying the amount of coverage by the chronology gives a rough idea of the richness of data presented in the media for each month's incidents.'³⁷⁹

³⁷⁹ *Op cit.*

Unfortunately Mickolus's use of computer bytes as a surrogate measurement of media attention renders the table and his consequent analysis of the figures completely null and void. Computer bytes provide absolutely no useful or meaningful measurement of aggregate or quantifiable data. The format and software program in which the file is saved, will determine to quite an extent the size of the file in bytes. Furthermore a small amount of bytes is no reflection at all on total fatalities of an incident or the amount of coverage. For example, the statement '275 people were killed in a terrorist bombing' saved in computer bytes amounted to 11 kilo bytes whereas three full pages of text only amounted to 15 kilo bytes of memory.³⁸⁰ Unfortunately Mickolus repeats the same mistake in his latest issue of Terrorism 1992-1995.

As a series of data sets on terrorism the ITERATE and consequent chronologies on terrorism provide yet another alternative to government based statistics and information on terrorism events. Although a little awkward to use in terms of indexing and general searching of the data sets they make a valuable contribution the terrorism set field and are well used among academic researchers. Mickolus's willingness to receive contributions and comments on his series of manual and computerised data sets provides a healthy forum in which their quality can be hopefully monitored and improved.

³⁸⁰ This small, but useful example was carried out using Microsoft Word for Windows 95 Version 7. An explanation of the pitfalls of using bytes as a form of measurement in terrorism data was given to the author (Mickolus) at a meeting in July 1994.

CASE STUDY: SOUTH AFRICA

To help redress this problem a research visit to the newly emerging South Africa and Namibia was undertaken to look at established data sets on political violence.

Objectives

The objective of the study tour was to assess the quality, breadth and type of political violence data sets available in South Africa and Namibia.

Research Findings

Data sets on political violence and conflict in South Africa are held by research institutes, the universities and non-governmental bodies. Official government statistics on political violence are also published. These publications tend to be periodic and are not always considered completely reliable.

Across all the main centres holding data on political violence in South Africa the quality of the information gathered and coded was found to be of a very high standard. Quality can be measured in the reliability and breadth of sources used to compile the data set. This includes material such as newspaper cuttings and the reporting of incidents by independent agencies and monitoring services. Other such factors as validity and consistency of data entry of variables to the data set (e.g. type of incident, number of casualties and groups responsible) was found to be of a high standard. One of the largest and most comprehensive data sets on political violence and conflict in South Africa is held by the Human Science Research Council of South Africa. The H.S.R.C. currently operates three computerised data sets on political violence in South Africa. The largest - The Conflict Monitor Database, was first

established in 1970. This database holds in excess of 15,000 records and holds data on collective action protest events. A smaller though extremely detailed data set on political violence and conflict in the KwaZulu Natal region of South Africa has operated since 1986. A newer project established in 1990 on political violence protest within South Africa is also held. Each of these data sets holds in excess of 70 variables. This is a substantial amount of variables for any data set, and highlights the in-depth detail available on conflict and violence events. The data sets include such variables as social categories of victims, deaths, injuries, police involvement and response type and time as well as weapons used. The inclusion of police response details in the data set is particularly unusual. This is in part due to the general mistrust of the security forces and the demand for credible information on police and security forces responses to incidents. The data set derives its sources from a large array of public documents, newspapers and independent monitors. These data sets are purely variable coded, enabling the use of statistical software for trend analysis and G.I.S. for time and spatial analysis.

The data sets at the H.S.R.C. are not published regularly. However, bona fide academics requesting information can obtain relevant details. Charges are made for commercial requests. The system is fully computerised and uses Paradox database management system to hold the data. Where more complex statistical requirements are needed the statistical package SAS is used.

Another main source of data on political violence in South Africa can be found at the Human Rights Committee of South Africa. Operating mainly a text-based system, it has its own data sets on political violence and also deals with such

issues as labour unrest, the security forces, torture and political detentions. The data set has operated since mid 1990 and is used by academics, government and NGO's. Their work tends to be more orientated towards conflict, however they do maintain significant material on incidents of political violence. For validity purposes cross-checking of incidents with the Human Science Research Council is carried out to maintain qualitative standards. The committee produce a monthly report: *The Human Rights Report*, containing statistical and narrative evidence on acts of political violence.

Within the universities one of the biggest research projects undertaken in South Africa on political violence is at the University of Natal, Durban. The Conflict Trends in KwaZulu Natal Indicator Project (linked to the Human Science Research Council project) monitors political violence and conflict in the KwaZulu Natal region of South Africa. The KwaZulu Natal, an area noted for endemic political violence in the past is of particular interest to researchers. This data set was established in 1986 and currently holds 12,400 records on incidents (not overtly criminal in nature) involving two or more people. It details such variables as to where an incident occurred, who participated in the incident, and the political affiliation of groups/individuals responsible for the incident. In addition details pertaining to police response to incidents is also recorded, as well as the number of injuries and deaths. The sources are taken from the local newspapers, Durban human rights groups, and political parties. Discrete variables are coded bi-monthly. Researchers coding the database have encountered problems with the reliability of sources of information. The highly sensitive nature of political violence in South Africa has led to a distrust of the authorities, police and security forces in their validation of events.

Lack of co-operation from the authorities in giving accurate information has been a recurring problem. In addition many acts of political violence go unreported out of fear of reprisal. The project uses SPCC for statistical analysis. The data set is completely coded. Data is not published in a monthly or annual format, however statistics from the data sets do appear in issues of the journal *Crime and Conflict*.

Another large project holding data on political violence in South Africa is the Clipping Service of the Institute for Contemporary History at the University of the Orange Free State. The Institute operates a very large newspaper clipping service covering 64 newspapers throughout South Africa. The subjects collected by the Institute is of a more general nature than the specialist data sets, however clippings on incidents of terrorism and conflict feature heavily. The majority of information is held in a manual format. A computerised index of key words and a thesaurus is used to provide information. The clipping service was established in 1970 and offers a rich source of information on political violence and conflict in South Africa. Other sources used also include parliament, government and private papers. It is one of the largest repositories in South Africa.

Many other medium to small projects monitoring political violence in South Africa have been established. These include a political violence project run by the department of psychology at the University of Witwatersrand and a data set on violence and conflict operated by the Centre for Inter-Group Studies in Cape Town. The Institute for Race Relations in South Africa also publish political violence data periodically.

Official publications and statistics on political violence are produced in an annual yearbook. The Commissioner of the South African Police publishes an annual

report on violence. This includes the number of incidents and arrests related to violent crime (both political and non-political) within South Africa. As figures are not separated it is difficult to gauge the accuracy of events. A credibility problem with official statistics on political violence may in part reflect the number of independent projects being undertaken to monitor violence in South Africa. The police also issues from time to time periodic bulletins on statistics of violence.

A survey of data sets on political violence in Namibia gained very little information. Due to its recent independence from South Africa (1990) statistics relating to Namibia were very difficult to find. The government does not publish statistics on incidents of violence in Namibia. Details of incidents are very often found among South African literature prior to 1990. Incidents of political violence are reported from time to time in *The Windhoek Observer* and *The Windhoek Advertiser*. Approaches to Government officials on the topic of political violence data were met with bemusement.

My research visit to South Africa was both surprising and encouraging. The amount of data sets on political violence and conflict found in South Africa were more numerous than expected. A healthy spread of institutions and agencies undertaking data collections, underpinned with well established data collection methods has ensured a rich resource of data available on political violence and conflict in South Africa. In addition, the length of time in which these data sets have been established provides researchers and analysts with a long term view of political violence trends in South Africa. The same cannot be said for Namibia. This was not unexpected. Due to its strong historical ties with South Africa and relatively new status as a new country little detail on incidents of political violence can be found.

General Implications and Conclusion

The wider implications of the availability of South African generated data on political violence is significant. A largely untapped source of high quality data on political violence and conflict exists and is being further developed. General reliance on the mainstream data sets such as ITERATE, RAND/St.Andrews and the US. Department of State's Patterns of Global Terrorism can further be complemented by data sources much closer to the heart of events in South Africa. This should be encouraged. The widespread use of computers in most of the above projects also permits potential use of such data in a larger more comprehensive computerised database project world-wide.

4.7. Conclusions

The eclectic nature of computerised terrorism data sets reflects not only a wide and disparate collection of data, it also mirrors the anarchic development of a subject field sorely in need of some structure and cohesion. The isolated development of governmental, academic and commercial terrorism data sets has resulted in an ill-defined classification of terrorism data sets, with potential users either unaware of their existence and even less aware of their remit or functional capabilities. Without a broader perspective, analysis of terrorism events data can be limited to a small universe of data sets that risk over exposure at the expense of other quality data sets. Part of this limited perception of terrorism data sets derives from the lack of a simple framework from which classification, content, organisation and functionality can be assessed and compared. Section 5.5 of this chapter presents such a

framework. Quality data on terrorism data sets provides a basis from which informed decision can be made.

The insular development by agencies and organisations of computerised terrorism data sets can be explained in part by the remit and content of the data sets. Security and insecurity among developers have engendered a culture of isolation which can be difficult to break. National security issues, political sensitivities, commercial competition, academic pride and occasional acts of goodwill and reciprocity illustrate a less than coherent subject field. Still within relative infancy both in content and technologically, the field of computerised terrorism data sets has yet to mature to the point that a coherent professional set of standards are established within this sub-discipline of terrorism research.

Given the acknowledged frailties, there appears to be an emerging and diverse set of computerised data sets on terrorism that can offer intelligence analysts and researchers more than standard information gleaned from chronological events data. Terrorism chronologies have their place, and make a valuable contribution to research the research field. The new data sets such as TIPOFF, VGTOF and Electronic Database, along with the more established data sets such as ITERATE, RAND and the TPVU data sets illustrates the continuing interest in a specialist field that needs focus, imagination and a strong commitment to continuity once data sets have been established. The comparative analysis of computerised terrorism data sets can be a difficult task given the wide array of definitional remits, hardware and software specifications and content data and without context, judgements as to their applicability in either research, intelligence or commercially based work can be misleading.

CHAPTER V

TERRORISM AND COUNTER-TERRORISM DATABASES POST

9/11: A COMPLEX MATRIX WITH FUTURE CHALLENGES

5.1. Introduction

Undoubtedly, the defining moment for the development of terrorism and counter-terrorism databases in the past forty years occurred on the 11th of September 2001. The field of study was irrevocably changed. The catastrophic events of that day had ramifications across the whole gamut of counter-terrorism efforts by governments and security agencies. No less immune from these events, the academic field of terrorism studies was also struggling to come to terms with the enormity of 9/11. What emerged very quickly from the shock and chaos of the New York and Washington terrorist attacks, was a cardinal weakness in intelligence systems. By 2001 the Internet was widely available, computer networks were well established in Government, and database management systems were becoming ever more sophisticated. In the counter-terrorism field some databases such as the U.S. State Departments TADIMS systems and the FBI's Violent Gang and Terrorist Organisation File (VGTOF) had been operating for over a decade. In academia, the ITERATE chronologies on terrorism and Pinkerton Terrorism Database had been operating for over three decades. A classic, but necessary question: so what went wrong? In relation to the specific focus of this thesis, three important areas can be identified: systems, intelligence (including HUMINT) and politics. Critical to the operation of databases systems, networks and the Internet is the concept of the system.

Moreover, the concept of the system should be acknowledged within the wider conceptual idea that Government, intelligence agencies and academics all work within political systems. Where boundaries within a system are confused, are not explicitly stated, and are unresponsive to users needs or completely ignored, problems are inevitable. The intelligence element of terrorism and counterterrorism analysis provides the unique qualities of intuition, experience, objectivity and raw source data such as interpersonal contact with individuals on the ground. Even the smartest terrorism database system would have trouble codifying the subtle elements of anger, ideological belief, nationalism, cynicism or even joy and elation. Finally, to blame politics as the *raison d'etre* for the events of 9/11 would seem obvious, yet unsatisfying. To have an effective terrorism and counter-terrorism strategy, actors must abide by legal and political frameworks that politicians create. While terrorists have the freedom to reject the norms of the body politic, terrorism and counter-terrorism agents must abide by an imperfect system. The elements of systems, intelligence and politics are not mutually exclusive. On the contrary, quite the opposite. By their very nature, this trinity of elements requires that the 'dots' be joined up to enable a cohesive and effective terrorism and counter-terrorism strategy. The reality on 9/11 was, however, quite different. Within the intelligence agencies and government, such as the FBI, CIA, the U.S. State Department and U.S. Immigration Service a territorial culture had emerged. Each respective government agencies had their own statutory remits, which were at times driven by internal power agendas and external political sensitivities to what their counter-parts in government were doing. Even official definitions of terrorism varied between Federal agencies. Interoperability of database systems was limited. While their sense

of allegiance to the protection of the United States was never in doubt, the systemic way these agencies went about their business meant that the bigger picture was not always evident. In other words, localised power politics and departmental management of counter-terrorism efforts took precedence over the need to respond to a rapidly changing macro view of global terrorism events. The result was a series of government 'islands' with no connecting bridges. Simply interconnecting government by using technology misses the point. What was lacking was a synthesis of technology, human intelligence and political will power to address the complicated world of domestic and international terrorism in the 21st Century. The blurring of the binary divide between the domestic and international incidents of terrorism added to a much more sophisticated schema that required urgent attention. For example, the move from purely nationalists, separatists and regional terrorism causes to a more pan-global activity in the form of al-Qaeda and its regional franchises, such as al-Qaeda in the Islamic Maghreb (ALM) and al-Qaeda in the Arabian Peninsula (AAP). Ironically, these terrorist groups could see the advantage of systematically embracing technology and the Internet to operate a distributed network of alliances. Geography became an irrelevance. Technology was both the glue and conduit to allow them operate and promote their causes from anywhere in the world.

In responding to the events of 9/11, Governments, intelligence agencies, academics and commercially interested terrorism database providers have all been faced with a wide range of complex challenges. Even after a decade, these challenges are ongoing and in many ways still evolving.

Chapter 5 will focus on some of the key issues that have impacted upon terrorism and counter-terrorism databases post-9/11. In particular, it will ask, what have been the main legislative requirements placed upon the intelligence communities to improve the quality of terrorism and counter-terrorism databases? In addition, many policy ideas have been generated in response to 9/11. This chapter will assess some of the key policy recommendations, particularly focussing on the work of the Markle Commission. The chapter will then turn to look at the legal requirements for Government and intelligence agencies to share and integrate terrorism and terrorism related data; this has in many ways been a culture shock for all concerned. Moreover, while the cultural shift and political will power to share terrorism related data may be improving, to share data, one must have interoperable systems. Technical capability does not always coincide with political and legal requirements. Some of these issues will be addressed. Among the principle worries about the creation of large government terrorism databases has been the issue of privacy. Chapter 5 will discuss the issue of privacy in relation to the wider impact the use of terrorism databases has had upon the general public. For example, what are the concerns about issues of accuracy in identifying correct individuals at airports, wrongly placed on a watchlists? Conversely, while the wrong people may be logged, the real terrorists may be missing. Other critical debate has centred on the subject of mission creep. Is it overstated? In other words, are terrorism and counter-terrorism databases stretching their tentacles into areas of people's lives that should be out of bounds?

5.2. The 9/11 Commission

Following the terrorist attacks of 9/11, the National Commission on Terrorist Attacks Upon the United States³⁸¹ was established on the 27th November 2002.³⁸² The commission, established by an act of congress, was signed into law by President George W. Bush. The principle aim of the commission was:

‘...to prepare a full and complete account of the circumstances surrounding the September 11, 2001 terrorist attacks, including preparedness for and the immediate response to the attacks. The Commission is also mandated to provide recommendations designed to guard against future attacks’.³⁸³

Furthermore, the 9/11 commission was specifically tasked under section 604 of U.S. Public Law 107-306 to investigate:

‘... “facts and circumstances relating to the terrorist attacks of September 11, 2001,” including those relating to intelligence agencies; law enforcement agencies; diplomacy; immigration, nonimmigrant visas, and border control; the flow of assets to terrorist organizations; commercial aviation; the role of congressional oversight and resource allocation; and other areas determined relevant by the Commission for its inquiry’.³⁸⁴

The commission’s investigative remit was wide and varied. In addition to the obvious investigations into Al Qaeda’s organization of the 9/11 attacks, the commissions work touched upon many areas relevant to this thesis’s research: the application of database technologies to the study of terrorism and counter-terrorism. In particular, investigators looked at the areas of intelligence collection, analysis, and management. Further specialist groups investigated border security, law enforcement and intelligence collection, terrorist financing, and commercial aviation

³⁸¹ Commonly known as ‘The 9/11 Commission’.

³⁸² See: <http://www.9-11commission.gov/report/index.htm> [Accessed 08/04/11]

³⁸³ *Ibid.*

³⁸⁴ *Ibid*

and transport security.³⁸⁵ One recurring theme binds the above investigative topics: pre 9/11 all of these areas of Government security required the use of database systems. While many database systems were in place, their effective operational use and wider system connectivity to security relevant cognate groups left much to be desired.

The commission's research uncovered a wealth of database problems prior to 9/11 that illustrated the fractured nature of intelligence systems. One such example was the case of Ahmed Ressam, an Algerian born member of al-Qaeda who entered Canada in 1994, claiming political asylum and using a fake passport and documents.³⁸⁶ Living in Montreal, Ressam supported himself from the proceeds of low level theft and benefit fraud. Despite having a criminal record (he was arrested four times) and travel to terrorist training camps in Afghanistan in 1998 and 1999, his profile remained below the security services radar. Along with associates Ressam planned to attack a U.S. Airport on the 1st of January 2000. Ressam's associates could not obtain the requisite Canadian documents; he therefore planned to carry out the attack on Los Angeles International Airport (LAX) himself. On departure for the United States, Ressam's passport was run through a variety of INS databases that failed to alert authorities. His passport was genuine, but had been obtained fraudulently. Ressam was finally apprehended by authorities in Port Angeles, WA after acting suspiciously. While in theory, the database correctly did not identify Ressam's passport as suspicious, the database systems in place failed to alert other

³⁸⁵ Further investigative teams also assessed issues of response to the 9/11 attacks at National, State and Local level, as well as International Counter-terrorism policy.

³⁸⁶ National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004. pp.176-179.

cogs in the intelligence wheel that may have set alarm bells ringing. Another intelligence failing identified by the 9/11 Commission relates to the many U.S. Government databases set up for terrorist, criminal, immigration and financial information.³⁸⁷ These databases, each with varying remits, holding different kinds of data and accessibility rules have for years presented intelligence agencies with many challenges. Legitimately, they may well contain different types of users data relevant to an organizations needs. If the domestic scenario for the United States was challenging, attempts to agree access to foreign Governments terrorism related data often involved protracted negotiation. Even if successful there was no guarantee that terrorism data had been digitized or could be integrated into existing U.S. database systems. Add to this, suspicion by other sovereign states as to why the U.S. intelligence community needed access to their data, without reciprocal arrangements, and one is presented with a highly politically sensitive scenario.

A vital weakness in the intelligence communities was their failure to recognize the value of other non terrorism and counter-terrorism databases. The 9/11 Commission picks up on this point.³⁸⁸ While terrorism and counter-terrorism databases are critical in the fight against terrorism, many other databases that are not deemed 'intelligence' systems can be highly useful. No individual lives within a complete vacuum. To operate, terrorists need to communicate (e-mail, mobile phone, Internet); they may need to travel (book flights and hotels); and purchase material (clocks, wiring, chemicals). Often these transactions require payment by credit card. Even if cash is paid, a receipt is produced. What is increasingly difficult to avoid in all

³⁸⁷ *Ibid.* p386.

³⁸⁸ *Ibid.* pp.416-417.

of the above transactions is the use of database systems in some form or other. The routine and banal occurrence of billions of such transactions daily, masks a potential source of terrorist data that can potentially build a highly detailed profile of an individual or terrorist groups activities.

What Government, and in particular intelligence agencies have failed to recognize, is the relevance of what would appear on the surface to be a completely disparate set of data. For example, what does the FBI's Terrorist Financial Database³⁸⁹ have in common with the *Interagency Border Inspection System (IBIS)*³⁹⁰ and the Advanced Passenger Information System (APIS)³⁹¹ Everything. A terrorist could withdraw funds from a 'legitimate' bank account to book a flight to a city near the border to enable them to cross the border by car for a 'vacation'. Yet again the common denominator is the need for effective databases and systems in place. One of the weaknesses of U.S. government databases pre-9/11 was that they were modeled around a 'hub and spoke' system.³⁹² Its weakness lay in the fact users could only send and retrieve information to and from an agency's internal mainframe hub. This did not allow for any cross-checking with other Government and intelligence agencies. In many ways the technology suited the cultural mindset that each agency had ownership of their data. Given the 'competing' demands for resources, the focus was on building strong internal information systems on subject specific databases.

³⁸⁹ See: <http://www.fbi.gov/news/testimony/usa-patriot-act-terrorism-financing-operations-section> [Accessed 08/04/11].

³⁹⁰ For further information see: U. S Congressional Research Service. *Terrorism: Automated Lookout Systems and Border Security Options and Issues*. (RL31019; June 18th, 2001) <http://www.fas.org/irp/crs/RL31019.pdf> [Accessed 08/04/11].

³⁹¹ http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/apis/ [Accessed 08/04/11].

³⁹² National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004. P. 418.

Ironically this type of thinking missed two key points. Firstly, technology had matured to the point that integrated and cross-network databases systems were perfectly feasible by the year 2000. Notwithstanding the usual technical challenges and glitches that any new databases systems project would be presented with, integration and cross-referencing of terrorism data sets was possible. Secondly, the introspective culture among Government and intelligence agencies missed the critical point that terrorism in the year 2001 had moved on. The binary domestic/international criteria had changed. A much more sophisticated series of terrorism events were taking place against a globalised backdrop. The communications backbone for this was the Internet. The outdated hub to spoke terrorist group structure was morphing into a much more de-centralised network of terrorist groups, reflected in such groups as al-Qaeda. Government and intelligence agencies needed to respond to this new world, by adopting a much more integrative database approach to counter-terrorism needs. The 9/11 Commission therefore recommended a decentralized network model, whereby in addition to hierarchical needs, relevant terrorism data could be shared horizontally. The concept one 'global' database on terrorism data was a non-starter. The strength of a decentralized systems was that intelligence analysts and police could draw from an eclectic range of database, reflecting the reality of real-life events. To reassure respective agencies an "information rights management" strategy was recommended allowing analysts access to specific data without complete access to the network. The Markle Foundation labeled it a "trusted information network".³⁹³ It is not without some

³⁹³ A broader discussion of the work of The Markle Foundation is presented later in this Chapter. For information on the Markle Foundation see: <http://www.markle.org/>

irony that the trust word was promoted to label the network schema. In particular, a culture of trust needed to be engendered *within* Government intelligence agencies to fight the very external agents (terrorists) they least trusted and who put U.S. national security at risk. While it would be naive to assume some collegial system would evolve, there was recognition by the 9/11 Commission that to safely bring the territorial barriers down, a safe mechanism was needed, encouraging a culture of trust.

Another example of ineffective use of databases systems identified by the 9/11 Commission related to the U.S. Government's analysis of terrorists travel strategies.³⁹⁴ While often the focus of attention is around the terrorist event, the lead-up to such incidents can often provide vital clues to intelligence authorities. Up until the 9/11 terrorist attacks, no U.S. government agency was charged with analyzing terrorist travel strategies. The 9/11 Commission highlighted the potential for terrorists to exploit border security weaknesses. Where travel strategies and arrangements can be identified, useful information can be gleaned. For example, patterns may be identified, or frequency of travel may be indicative of some form of pre-planning. Other pertinent questions a database may flag up to an alert border official could be: was the method of entry to the U.S. unusual?; was a flight paid for by cash or credit card?; if so who was the registered owner of the card? All mundane details, however, even ordinary events have their part to play in building a wider picture of terrorist's movements. It is such normalcy that terrorists strive to melt into. Indeed the 9/11 Commission identified that at least fifteen of the

³⁹⁴ National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004. P. 384.

nineteen September 11th terrorists ‘were potentially vulnerable to interception by border authorities’.³⁹⁵ The report argues that, from inspection of their travel documents and patterns of travel, had effective databases systems been in place, between 4 and 15 of the 19 hijackers could have been intercepted. Moreover, at least three hijackers could have been identified. In other words, intelligence data was available, however, the ‘dots’ were not joined up.

While it is easy to blame ineffective border control database systems, as part of the overall intelligence failings of 9/11, these particular weakness’s needs to be placed in some context. Border security and immigration legislation prior to 9/11 was not geared for counter-terrorism efforts. The focus was on the routine task of upholding immigration legislation, preventing entry of illegal aliens and processing legitimate travelers and migrants. This presented an opportunity to al-Qaeda; they could exploit the loopholes, as outlined below:

‘Because they [al-Qaeda conspirators] were deemed not to be bona fide tourists or students as the claimed, five conspirators that we know of tried to get visas and failed, and one was denied entry by an inspector. We also found that had the immigration system set a higher bar for determining whether individuals are who or what they claim to be – ensuring routine consequences for violations – it could potentially have excluded, removed, or come into further contact with several hijackers who did not appear to meet the terms for admitting short-term visitors’.³⁹⁶

As the 9/11 Commission identifies, this low threshold, with a lack of ‘consequences for violations’ was combined with two key weaknesses: INS’s inability to deliver on its basic commitments, and to provide an effective counter-terrorism strategy. Thus, database systems can have an effective part to play in counter-terrorism strategy,

³⁹⁵ *Ibid.* p. 384.

³⁹⁶ *Ibid.*

only if, however, the wider intelligence framework they are designed around is responsive to both its original remit (for example immigration) and embraces an effective counter-terrorism strategy.

Key Recommendations of the 9/11 Commission

The many recommendations outlined in the 9/11 Commissions report extends well beyond the focus of this chapter. Discussed below however, are some of the 9/11 Commissions key recommendations as they relate to application of databases technologies to the terrorism and counter-terrorism field.

The creation of the National Counterterrorism Center (NCTC) in August 2004 was the direct result of a key recommendation of the 9/11 Commission.³⁹⁷ The NCTC hosts the Worldwide Incidents Tracking System (WITS) database³⁹⁸ and the Terrorist Identities Datamart Environment (TIDE)³⁹⁹ database among others. The NCTC succeeded the Terrorist Threat Integration Center (TTIC). The Commission was keen that the NCTC differed from its predecessors, 'breaking the mold' of other national government organizations. The NCTC would be both a centre for joint operational *and* joint intelligence, drawing upon the expertise of several intelligence and government agencies. Instead of a high boundary wall the NCTC was tasked to source expertise from other agencies such as the FBI and CIA that would encompass intelligence on domestic and international terrorist organizations. To strengthen it

³⁹⁷ President George W. Bush established the NCTC by Executive Order 133354 in August 2004. See: http://www.nctc.gov/docs/eo_13354.pdf [Accessed 10/04/11]. The NCTC was codified into U.S. law by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). See: <http://www.nctc.gov/docs/irtpa.pdf> [Accessed 10/04/11].

³⁹⁸ See the WITS database: <https://wits.nctc.gov/FederalDiscoverWITS/index.do?N=0>

³⁹⁹ http://www.nctc.gov/docs/Tide_Fact_Sheet_October_2010.pdf

further, much of the analytical expertise from within the CIA's Counterterrorist Center and the Defense Intelligence Agency's (DIA) Joint Intelligence Task Force – Combating Terrorism (JITF-CT) would be integrated into the NCTC. This move, to create an eclectic intelligence community, was responsive to and reflective of a post 9/11 world, whereby good intelligence could only be acquired from a cross-pulling of resources. However, as the Commission notes: 'The most serious disadvantage of the NCTC is the reverse of its greatest virtue'.⁴⁰⁰ By this it refers to the potential worry that while the NCTC may be the U.S. Government's central repository for terrorism data, too much power may be vested in one agency. Other intelligence agencies may have their concerns. This point did not go unnoticed by the 9/11 Commission and U.S. Secretary of Defense Donald Rumsfeld as noted below:

'We [the 9/11 Commission] recognize that this is a new and difficult idea precisely because the authorities we recommend for the NCTC really would, as Secretary Rumsfeld foresaw, ask strong agencies to "give up some of their turf and authority in exchange for a stronger, faster, more efficient government wide joint effort.'"

The ceding of power can be a difficult exercise for any large organization at the best of times. The realization was however, that for any post 9/11 counter-terrorism effort to succeed, it would need to be a collaborative project. Given the new global terrorism landscape, intelligence agencies may have had little choice in the matter. The problem remains, however, in terms of coordination of such intelligence. As the Commission acknowledged:

"Each intelligence agency has its own security practices, outgrowths of the Cold War....Current security requirements nurture over-classification and

⁴⁰⁰ National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004. P.406.

excessive compartmentation of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though these costs – even in literal financial terms – are substantial. There are no punishments for not sharing information. Agencies uphold a “need-to-know” culture of information protection rather than promoting a “need-to-share” culture of integration.”⁴⁰¹

As illustrated above, the foundations of many security practices within the U.S. Intelligence Agencies were formed during the Cold War. Mainframe computers were in their relative infancy, while database systems were virtually unheard of until the mid 1960's. The stand-alone nature of computer technology at that period also reflected the technological and political vacuum that intelligence agencies operated within. A culture of insularity was built and sustained, as the technology was not available to share and reciprocate intelligence. The concept of sharing database information among agencies was both technologically extremely difficult and politically highly contentious. While this rigidity in classification of information continued for many decades, database and network technology surged ahead. Externally, major organizations such as businesses, education, and transport were all starting to embrace and view the concept of network and database technologies as integral to their future development. Combined with an ever increasing public appetite for the Internet, the fusion of all interested players further spawned the increasing phenomena of globalization. Intelligence agencies, it must be noted, were using technology, but generally with an insular mindset. With the misguided concept

⁴⁰¹ Ibid. p.417.

that the more classified certain data was the 'safer' it was; ironically this could be the opposite. As noted above the 9/11 Commission highlights in its report '[there were] ... few rewards for sharing information'. It was almost as if the concept of sharing intelligence was perceived as a weakness, and perhaps a betrayal of the very essence of classification.

5.3. U.S. Border Screening

Among the key recommendations cited within the 9/11 Commission Report was the creation of robust and effective U.S. border screening mechanisms at airports, sea ports and land entry to the United States, for both domestic and international travelers. Given the modus operandi of the 9/11 terrorist attacks, using aircraft as the principal weapon of attack, improving future airport security was cardinal to any counter-terrorism effort within transport infrastructure. The failure of intelligence and database systems to flag any of the 9/11 terrorists on any of the four flights hi-jacked that day, was a testimony to the weakness and shortcomings in U.S. airline security.

While the obvious remedy may appear to advocate stringent airport and transport security systems that would rout out every single potential threat, the 9/11 Commissioners were mindful that a very fine balancing act had to be made. On the one hand the freedom of the individual to go about their lawful business epitomizes the very ethos of American liberty and enterprise, yet at the same time never again could airport and border entry points be so porous as to let slip even one terrorist, intent on causing devastation.

In response to this situation the United States Government created a dual identifier system based upon biometric technology which includes a photograph of every individual and fingerprints of both index fingers. This is operated under the US VISIT scheme (United States Visitor and Immigration Status and Indicator Technology program⁴⁰²). In creating the US VISIT program the Commission was keen that it mopped up the existing 'patchwork' of database systems under one cohesive security database that both consolidated and integrated passenger data. The US Visit program has not, however, been without its critics. For example, the US watchlist has been criticized by the American Civil Liberties Union (ACLU) for being "bloated and full of inaccuracy". By 2007 the ACLU claimed the U.S. Government had compiled 750,000 "terror suspects" on its watchlist database.⁴⁰³ In addition, part of the controversy emanated from their use not only within the United States, but their operation in other sovereign countries, such as Japan.⁴⁰⁴ As the 9/11 Commission notes: 'The further away from our borders that screening occurs, the more security benefits we gain'.⁴⁰⁵ This statement illustrates several key changes in security strategy. Firstly, the US Government has been keen to adopt the spatial advantages that network database technologies has to offer. No longer will US intelligence agencies rely on weeding out potential terrorists at points of entry to the United States. Reciprocal counter-terrorism database agreements with other Governments means that known or suspected terrorist can be identified many thousands of miles away from their intended airport or port of departure. Secondly, the verification of

⁴⁰² See: <http://www.dhs.gov/files/programs/usv.shtm> [Accessed 08/08/11]

⁴⁰³ See: <http://search.japantimes.co.jp/cgi-bin/nn20071108f1.html> [Accessed 17/08/11]

⁴⁰⁴ *Ibid.*

⁴⁰⁵ National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004. P.389

passenger details, both domestically and now internationally, requires that intelligence agencies must operate out-with their 'safe fiefdoms' in a world where reciprocity and information sharing among trusted partners is becoming the norm.

Despite the criticisms of the watchlist databases, and there have been many, some of which will be illustrated at a later stage in this chapter, the US Government has been resolute in implementing a comprehensive database watchlist system, based on the 9/11 Commission recommendations.

While sophisticated database technologies can in part address some of the intelligence failings of 9/11, another vital element of the post 9/11 intelligence world was the acknowledgement by the 9/11 Commission: that no one single agency could possibly handle the labyrinthine schema that was the U.S. intelligence community. Leadership was required from the very top. In other words, the White House would be expected to take the lead. While the technological challenges requiring all U.S. intelligence agencies to co-operate fully on sharing terrorist data were potentially difficult, three further challenges added to the weighty burden placed upon Government. The trinity of legal, policy and the political dynamic could only be succeed if driven from the Presidential and Executive level. Congressional legislation, policy consistency and above all political consensus were critical to the establishment of a credible Intelligence Community (IC) that could begin to meet the challenges of 21st Century counter-terrorism operations. The result was improved congressional oversight of the United States intelligence operations, the creation of the National Counterterrorism Center and the Office of the Director of National

Intelligence (DNI). The DNI serves as the head of the United States key 16 intelligence agencies.

What Progress?

What progress in terrorism database technology has actually occurred from the recommendations of the 9/11 Commission, a decade after those tumultuous events? There have been several improvements worth illustrating; however, there have been some notable failings that serve as a reminder of the need for on-going vigilance.

Not only did the U.S. intelligence agencies fail to apprehend any of the 19 bombers that September morning, the terrorists preparation in the lead-up months to 9/11 fell below the radar of intelligence and counter-terrorism officials. While some individual's action and movements may have been thought slightly suspect or unusual, no overall coherent picture of emerging plans was identified. Even as early as late April 2001 some of 9/11 terrorists were arriving into the United States with cash and travelers cheque's, thus avoiding any electronic footprint from bank accounts or credit cards. This situation has been redressed with the coordinated work of several U.S. Government agencies. The Terrorist Screening Center, the DHS, the NCTC and other U.S. Federal agencies now analyse travel-related data in order to better comprehend, understand and crucially 'anticipate' the travel movements of known terrorists or terror suspects.

Several database have come online in recent years including the Terrorist Screening Database (TSDB),⁴⁰⁶ the Advanced Passenger Information System (API), Passenger Name Records (PND) and the Electronic System for Travel Authorization (ESTA). The TSDB is an amalgam of 12 previously operating terrorist watchlists into one consolidated Terrorist Screening Database; what the FBI describes as “one-stop shopping” for relevant Government screeners.⁴⁰⁷ Travelers are not permitted to know if their name resides on the TSDB. Since its implementation, the watchlist has denied travel to both private and high profile public figures, such as former Presidential candidate John Anderson who was wrongly flagged on the database. One of the most high profile passenger denied boarding a flight to Boston was the late Senator Edward M Kennedy in 2004.⁴⁰⁸ While astonishment and perhaps a little humour at the thought of such an eminent U.S. politician being labeled as a risk to U.S. national security filled many newspapers columns, there is a far more serious side to this type of incident. Many innocent member of the public have been caught unawares in the same situation – without the accompanying media interest. Among the most common situations to arise is where passenger’s names have been misspelled, passengers have changed their names or their name bears some close resemblance to known terror suspects. The TSDB is not totally without redress. Passengers who are continually stopped without good reason and identified as a “mis-identified” person can apply to have their name removed from the TSDB. The TSDB system is a real-time system, while the systems attempts to deal with the

⁴⁰⁶ For further information see: http://www.fbi.gov/about-us/nsb/tsc/tsc_faqs [Accessed 08/08/11]

⁴⁰⁷ For further details see: *Homeland Security Presidential Directive 6: Directive on Integration and Use of Screening Information to Protect against Terrorism.*
http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm [Accessed 08/08/11]

⁴⁰⁸ For further information see: <http://www.nytimes.com/2004/08/20/us/senator-terrorist-a-watchlist-stops-kennedy-at-airport.html>

immediacy of a check-in desk or Homeland Security official. The time taken to fix erroneous entries to the TSDB cannot be carried out in real-time. While mistakes are inevitable from time to time with any database system, confidence in the efficacy of such terror watchlists has arisen. A 2007 report by the Office of Inspector General (OIG) under the U.S. Department of Justice entitled *'Follow-up Audit of the Terrorist Screening Center'* outlined detailed problems watchlists.⁴⁰⁹ Among concerns raised was a report that the watchlists were operating under two interconnected versions. The OIG found that inspection of 105 records executed under the TSC's routine quality assurance reviews, 38 percent were found to be erroneous or contained inconsistencies. Added to their concern the monthly increase in entries to the watchlist database was averaging 20,000 per month with a running total of 700,000 entries by April 2007. As the OIG notes:

“A single omission of a terrorist identity or an inaccuracy in the identifying information contained in a watchlist record can have enormous consequences. Deficiencies in the accuracy of watchlist data increase the possibility that reliable information will not be available to frontline screening agents, which could prevent them from successfully identifying a known or suspected terrorist during an encounter or place their safety at greater risk by providing inappropriate handling instructions for a suspected terrorist.”

The relentless increase in numbers, with quality assurance procedures that were problematic presented the challenge of providing improved data integrity procedures while simultaneously attempt to handle a vast quantity of data that required being available on a real-time basis.

⁴⁰⁹ *'Follow-up Audit of the Terrorist Screening Center'* Audit Report 07-41, September 2007. Office of the Inspector General, U.S. Department of Justice, Washington D.C. United States <http://www.justice.gov/oig/reports/FBI/a0741/final.pdf> p.ii

By far the most notorious case relating to shortcomings in terrorist watchlists in recent years was what became known as the ‘Christmas Day Bomber’ incident. Umar Farouk Abdulmutallab, a 23 year old Nigerian, concealed plastic explosives in his underpants, while travelling on Northwest Airlines flight 253 from Amsterdam to Detroit on the 25th of December 2009. From a failed attempt to blow up Flight 253 over the Eastern Board of the United States, the individual was tackled, restrained and subsequently arrested on arrival into the United States. This particular incident had implications on several levels. Firstly, it brought to the forefront the issue of terrorist watchlists as a critical element in counter-terrorism efforts. Not only were intelligence officials and politicians hugely concerned that the tactics of Abdulmutallab had almost caused a catastrophic air incident, the ramifications on land could have been even more disastrous. Yet, even more concerning, was the fact that he was not flagged up by the terror watchlists and apprehended, given the background knowledge of the individual. The subsequent findings of the the U.S. Senate Select Committee on Intelligence presents fourteen key points of failure.⁴¹⁰ A complex matrix of shortcomings is outlined, ranging from ‘human errors, technical problems, systemic obstacles, analytical misjudgments, and competing priorities’.⁴¹¹

One of the most revelatory passages in the Senate report refers to the issue of language in watchlist databases. As point 2 of the report notes:

‘Abdulmutallab was not placed in the “Terrorist Screening Database” (TSDB), on the Selectee List, or on the No Fly List Conclusion:

The standards to place an individual on the Terrorist Watchlists were interpreted too rigidly and may be too complicated to address terrorist threats. Although U.S. Embassy officials in Abuja recommended that

⁴¹⁰ *Attempted Terrorist Attack on Northwest Airlines Flight 253*, U.S. Senate, 111th Congress., (S Prt. 111-119). (2010).

⁴¹¹ *Ibid.* p.2.

Abdulmutallab be placed on the No Fly List, the determination was made at CIA Headquarters and at the NCTC Watchlisting Office that there was only sufficient derogatory information to enter Abdulmutallab's information in the general "Terrorist Identities Datamart Environment" (TIDE) database, but not sufficient derogatory information to place him on any of the watchlists. Because of the language of the watchlisting standard, the manner in which it was being interpreted at the time, or both, analysts responsible for making the watchlisting determination did not believe they had the ability to give additional weight to significant pieces of information from the field, such as the report that resulted from the meeting with Abdulmutallab's father.⁴¹²

Rigid interpretation of standards for database entries can be a laudable and necessary requirement to uphold database integrity in many instances. However, when dealing with potential terrorist classification, the information available on particular individuals can often be fuzzy, 'soft' qualitative information that requires a fine sense of intuition and wise experienced judgment. Add to this, as illustrated above, geographic distance between local analysts on the ground and intelligence officers in Washington D.C. and one can end up with differing interpretations of severity of threat. Even the subtleties of language in the above statement when interpreting the term 'derogatory information' resulted in Abdulmutallab's eligibility for one database but not another. This semantic dilemma and subsequent interpretation remains an on-going challenge for analysts. A useful method of strengthening these potential systemic weaknesses is to provide (as the report mentions) some kind of weighting system, that provides a more finely tuned interpretation of a potential terrorist eligibility for watchlist entry. Combined with Chiefs of Stations local angle on affairs, watchlist entries can be more reflective of localized situations.

⁴¹² *Ibid.* p.4.

One of principal organizations to feel the wrath of politicians from the Abdulmutallab incident was the National Counterterrorism Center (NCTC). Senators wasted no time in reminding officials that the NCTC's [mission was]:

“to serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism”

⁴¹³

A mixture a under staffing in the NCTC's Directorate of Intelligence, with their focus predominantly on Yemini AQAP's operators, meant that other regions of AQAP's coverage were not given sufficient attention. In addition, while Abdulmutallab's name was registered with the Terrorist Threat Identities Datamart (TIDE) the NCTC failed under the legislative requirement of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) to further enhance their intelligence on the individual. If further information had gathered, his name may well have been added to the U.S. watchlists and consequently been flagged when travel commenced. In addition a further criticism of the NCTC was its failure to '*connect the reporting on Abdulmutallab*'.⁴¹⁴ The 'connecting' was the dual task of 'analyzing and integrating all intelligence...' received on the the perpetrtrator. What the Senate Committee states unreservedly is that the NCTC it duty bound by law to carry out such tasks, and just as importantly was perfectly capable of doing so, it simply failed to do so. Such shortcomings are easy to comment on with hindsight. The NCTC has achieved much since its creation in 2004. Among some notable public successes has been the development of its state of the art Worldwide Incidents Tracking System (WITS),

⁴¹³ *Ibid* p.7.

⁴¹⁴ *Ibid*. p.7.

which super-ceded the U.S. State Departments *Patterns of Global Terrorism*.⁴¹⁵ More specifically, in its quest for improved methodological rigor, NCTC's willingness to involve non-governmental specialists on counter-terrorism to serve on its Terrorism Metrics Brain Trust, has shown a level of transparency and openness that few other intelligence agencies have shown to date. Despite the many positives, when near catastrophic terrorism events occur on its patch, politician demand accountability.

Complex information systems, pressurized staff and political agendas with limited resources can all too easily lose sight of the basics, which then morphs into systemic failure. This eclectic set of failures illustrates that while one could design the most rigorous database systems, they are always dependent upon external elements: human factors, political judgments, and analytical interpretation, all of which cannot simply be scripted into computer code.

With the improvements in travel watchlist databases a much wider intelligence database net has been cast both spatially and temporally, in order to pre-empt potential terrorist attacks. The use of dedicated travel databases combined with existing intelligence systems has undoubtedly closed many potential security loopholes.

⁴¹⁵ The move from *Patterns of Global Terrorism* at the State Department to the WITS database at NCTC was not just a simple transition from hard-copy publication to electronic. A complete methodological revision was undertaken, with the State Department producing a yearly narrative report called *Country Reports on Terrorism* and the NCTC providing statistical data that could be presented both publicly and used 'behind the scenes' as part of a much wider counter-terrorism intelligence operation. Due to methodological revisions the WITS database cannot be retrospectively compared to *Patterns of Global Terrorism* data.

5.4. Information Sharing

As discussed at several stages in this thesis, one of the key weaknesses of terrorism and counter-terrorism databases prior to 9/11 was the fragmented, disparate and often disconnected nature of database intelligence systems. In order to close many security loopholes and provide a comprehensive network of 'joined-up' database systems, a more robust and cohesive strategy needs to be adopted. The concept of Information Sharing as a pivotal element in post 9/11 database technology has surged ahead relentlessly over the past decade. Among these developments has been the introduction of over 70 fusion centers. One of their key responsibilities has been to promote the sharing of terrorism related information among the principle U.S. intelligence agencies. These agencies include the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the United States Military and the U.S. Department of Justice (DOJ). In addition to the 'big players' terrorism related information is also passed up the chain of command from local county state level police departments. The benefits of a fusion center approach to information processing is that a massive array of data can be captured and processed from a disparate collection of data points in order to join the 'intelligence dots together'. This provides law intelligence officials with a more cohesive pictures of potential terrorist related data that might otherwise have been missed had fusion not taken place. While the benefits of fusion centers appear attractive, their introduction has

not been without criticism.⁴¹⁶ A key criticism has been that they go well beyond their original remit into a whole new array of areas that Fusion Centers were never originally designed to operate. For example, Fusion Centers have been accused of excessive secrecy, generating information that is both erroneous and incomplete and of developing and using data mining software. Further criticisms have included Fusion Centers involving the Military and private sector businesses to conduct intelligence activities, including Mission Creep. In particular the American Civil Liberties Union (ACLU) has been critical of their potential to violate privacy laws and civil liberties.⁴¹⁷ Among the several concerns the ACLU has had over Fusion Centers has been the issue of 'Ambiguous Lines of Authority', whereby it argues:

The participation of agencies from multiple jurisdictions in fusion centers allows the authorities to manipulate differences in federal, state and local laws to maximize information collection while evading accountability and oversight through the practice of "policy shopping."⁴¹⁸

When a complex set of jurisdictions inter-play, to collect, analyse and eventually disseminate terrorism information, lines of authority and ultimately responsibility, can potentially be lost. The tiers of U.S. federal, state and local legislation do not always chime together. Creating both horizontal and vertical synthesis may well be an unlikely scenario or even desirable by certain political actors.

Another concern for Civil Liberty activists is the use of private organizations in their work with Fusion Centers. For privacy activists, Government has crossed the line

⁴¹⁶ U.S. General Accounting Office. *INFORMATION SHARING, Federal Agencies are Helping Fusion Centers Build and Sustain Capabilities and Protect, but Could Better Measure Results*. GAO-10-972 Washington D.C. 2010. <http://www.gao.gov/new.items/d10972.pdf> [Accessed 11/09/11].

⁴¹⁷ See: <http://www.aclu.org/technology-and-liberty/whats-wrong-fusion-centers-executive-summary> [Accessed 28/08/11]

⁴¹⁸ *Ibid.*

between the role of the state and its obligation to protect its citizens and the use of profit making companies that may use some information to their advantage. The ACLU has voiced an array of concerns. For example, some fusion centers have contracted out the storage and analysis of data to private vendors. The ACLU cites the decision by the Texas Department of Homeland Security to award a \$1.4 million dollar contract to the Northrop Grumman Corporation to operate a database that would amass a wide selection of government and law enforcement data and consumer dossiers,⁴¹⁹ that would eventually be used by the Texas Fusion Center. According to reports in the *Texas Observer* the database project failed, amid allegations of mismanagement and that it was unclear who had access rights or what eventually had become of the database contents.⁴²⁰ This example illustrates several potential problems when Government mixes the public with the private. Firstly, the very essence of the role of the state as the ultimate guarantor of an individual's safety and liberty could potentially be questioned when sensitive terrorism related data is outsourced to private enterprise. Given the severe economic constraints that Governments find themselves in, the attraction of a commercial organization that can provide the desired product for less cost can be tempting. This economic argument has proven successful and profitable in many countries. For example, the de-nationalization in the United Kingdom in the 1980's of car production, telecommunications and airlines such as British Airways has both relieved the public

⁴¹⁹ The consumer dossier element of the database was further sub-contracted out to a private data company called ChoicePoint. This company has not been without controversy. The U.S. Federal Trade Commission fined the ChoicePoint a total of \$15 million dollars after the company acknowledged that it the personal financial records of 163,000 consumers had been compromised. See: <http://www.ftc.gov/opa/2006/01/choicepoint.shtm> [Accessed 21/08/11]

⁴²⁰ See: <http://www.texasobserver.org/archives/item/15072-2472-the-governors-database-texas-is-amassing-an-unprecedented-amount-of-information-on-its-citizens> [Accessed 21/08/11].

purpose of liability and returned generous profits to shareholders.⁴²¹ Furthermore, the belief that private enterprise has the specialist knowledge to successfully operate terrorism related databases, given their sophisticated schema, may well persuade Government of the efficacy of this route. In other words, can issues of national security, specifically large databases of individuals details be sourced safely to the private organizations that primary objective is to make profit? A more subtle point, but just as crucial, relates to employees loyalty to an organization. For instance, should an employee of a private vendor, handling sensitive terrorism related data, view their primary loyalty to their employer, from whom they are dependent upon a salary, or to the primacy of the state, which ultimately is sworn to defend the individual. With access to a breadth of personal information, the ACLU is concerned that:

“Companies participating in fusion centers could be tempted to use their access to sensitive information to retaliate against company critics, competitors or troublesome employees, or to gain an advantage in difficult labor battles”.⁴²²

This externalisation of sensitive terrorism and terrorism related data also adds another dynamic. A whole series of power conflicts, as cited above, could undermine the integrity of data. It would be more than a little naïve to assume that the internal machinations of Government security agencies are without their own internal power-politics. However, even with tacit acknowledgement of such behaviour, there is a clear set of boundaries. These boundaries provide Government and the citizens with the guarantee that state will robustly guard sensitive data and that it is processed safely within a clear framework of responsibility with intelligence

⁴²¹ The customer experience is a vast discourse that goes beyond the remit of this thesis.

⁴²² *Whats Wrong with Fusion Centers?* American Civil Liberties Union, Washington D.C. 2007. p.14. http://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf Accessed [14/08/11].

agencies. While many private organisations provide the highest standards of data integrity, some fall short of the benchmark. Complicated sub-contracting of intelligence field work and data processing can obfuscate management lines of responsibility. In addition, the clandestine nature of gathering terrorism related intelligence has meant that not all private enterprises involved in Fusion Center intelligence gathering are publicly declared.

5.5. The Markle Foundation

The lengthy reflective process of addressing the events of 9/11, required a multifarious approach which not only dealt with political strategy, but grasped the need to integrate sophisticated database and network technologies into overall counter-terrorism thinking.

As a consequence, the work of the Marke Foundation,⁴²³ based in New York, provided a series of groundbreaking recommendations, recognised within the *9/11 Commission Report*,⁴²⁴ which encompassed an eclectic combination of the political, technological and human elements that could contribute to an effective post 9/11 counter-terrorism strategy in the United States. The Markle Task Force, comprising of bi-partisan members and national security specialists produced a wide ranging set of reports dealing with Information Sharing within Government and the intelligence communities. Among these were *Creating a Trusted Network for Homeland*

⁴²³ See: <http://www.markle.org>

⁴²⁴ National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004. p.419.

*Security*⁴²⁵, *Mobilizing Information to Prevent Terrorism*,⁴²⁶ and *Protecting America's Freedom in the Information Age*.⁴²⁷ What made the contribution of the Markle Foundation refreshing, was their ability to view terrorism related intelligence and data from a wider perspective. Firstly, they argued, information residing within intelligence systems had to be both discoverable and secondly, accessible. The discoverable element would appear to be an obvious statement. However, one should not confuse retention of data with the ability to link or retrieve data. One particularly pertinent example is provided in their 2002 report *Protecting America's Freedom in the Information Age*.⁴²⁸ The authors illustrate that if certain software had been operating prior to 9/11 a whole series of linkages between the 9/11 perpetrators could have been established relating to addresses and frequent-flyer accounts. Invoking a cliché about hindsight detracts from the slightly more subtle point: information about the 9/11 attackers was already available on computer databases systems, the information had not been discovered, nor the dots joined. Adding to the weakness in systems, Markle argues that even if information on the attackers had been available, it was not always accessible, crucially in a timely manner. Therefore, on the most basic level, some of the most important variables⁴²⁹ in running an effective counter-terrorism database intelligence system were flawed.

⁴²⁵ Markle Foundation Task Force, "Creating a Trusted Network for Homeland Security" December 2003. http://www.markle.org/sites/default/files/nstf_report2_full_report.pdf [Accessed 21/09/11].

⁴²⁶ Markle Foundation Task Force, "Mobilizing Information to Prevent Terrorism" July 2006. http://www.markle.org/sites/default/files/2006_nstf_report3.pdf [Accessed 21/09/11].

⁴²⁷ Markle Foundation Task Force. "Protecting America's Freedom in the Information Age" October 2002. http://www.markle.org/sites/default/files/nstf_full.pdf [Accessed 21/09/11].

⁴²⁸ *Ibid.* p.28.

⁴²⁹ Variables: discoverability, accessibility and timeliness

Both these sequential and linear information processes have since been strengthened among the large array of new post 9/11 database intelligence systems.

In the ten years since 9/11, it is often easy to cite failure, shortcomings and concerns in Government attempts to build effective terrorism and counter-terrorism database project. For example, the short-live Total Information Awareness (TIA), subsequently named Terrorism Information Awareness program under the George W. Bush administration.⁴³⁰ Many concerns around this database centred upon privacy, data mining and 'mission creep' issues. Others included the eventual collapse of the Multistate Anti-Terrorism Information Exchange Program (MATRIX) database project, developed for the Florida Department of Law Enforcement.⁴³¹ The project was abandoned after cuts in Federal funding and public outcry about state surveillance and privacy concerns. Despite such shortcomings, there has been some recognition that not all that Government attempts are doomed to failure, with the legacy of wasted time, money and resources. In an acknowledgment that the U.S. Federal Government has achieved some relative success, Zoe Baird from the Markle Foundation, wrote an op-ed for the *Washington Post* presenting an upbeat message declaring: 'A lesson of 9/11: Washington can work'.⁴³² The op-ed argues that:

'There has been a virtual reorganization of government, a shift in thinking that inspires reform in the way agencies, people and technology collaborate and communicate. The need-to-know culture is being replaced by a need-to-share principle; information is increasingly decentralized and distributed. Informal and flexible groups of analysts from different parts of government and the private sector are able to work together and share expertise'.⁴³³

⁴³⁰ See: Electronic Privacy Information Center <http://epic.org/privacy/profiling/tia/>

⁴³¹ See: American Civil Liberties Union 'THE MATRIX: Total Information Awareness Reloaded' <http://www.aclu.org/FilesPDFs/matrix%20report.pdf>

⁴³² See: http://www.washingtonpost.com/opinions/a-lesson-of-911-washington-can-work/2011/08/26/gIQAtvv8gJ_story.html [Accessed 27/08/11].

⁴³³ *Ibid.*

This change in mindset is to be welcomed. As with any deeply engrained culture, change does not always come easily. Rigid hierarchical thinking and inflexible database systems do not sit easily with the modern complex matrix that sophisticated terrorism informatics now operate in. The move towards distributed database technologies⁴³⁴ has allowed analysts the opportunity to access intelligence across a wide panoply of potential terrorist information 'footprints'. For example, bank/credit card details, mobile telephone records, e-mail and Internet connectivity. While much attention is paid by counter-terrorism analysts to the use of social networking sites by terrorists and their associates,⁴³⁵ their adoption for use across the U.S. intelligence networks prior to 9/11 was virtually non-existent. There has been a sea change in this area. The vertical and hierarchical chain of commands that previously were required for one agency to communicate to another has been transformed. Agencies such as the NCTC, FBI and Homeland Security are now routinely able to connect with each other using highly sophisticated database systems and social networking software. There are several benefits. Firstly, a more 'collegial' and collaborative culture is encouraged, which by-passes highly formal communication protocols between agencies that may miss critical data. Secondly, some of the most important terrorism intelligence data is nuanced or embedded within other information. In addition, levels of interoperability between terrorism and counter-terrorism databases are much higher than a decade ago. Many of the technical challenges over operating system software and interoperability of database

⁴³⁴ Distributed database technologies means that not all data resides in one central system, it is distributed across a series of computers systems at various physical locations.

⁴³⁵ See: "Social Networks link Terrorists" PC World Australian, January 2009.
http://www.pcworld.idg.com.au/article/272364/social_networks_link_terrorists/

software have been overcome. For example, as cited above, U.S. watchlist databases are now interoperable with Japanese security counterparts.

However, successful counter-terrorism success post 9/11 not only demands that database systems speak together, it also requires humans are able to handle the copious amounts of high volume of data made available literally by the minute, on a daily basis. To be able to discern between what is routine and what is critical is a tradecraft that can take many years to master. Human experience and basic gut instinct cannot be de-lined to a binary level or coded on a microchip. Where technology has assisted analysts post 9/11 is the ability now to share thoughts with other agencies on a real-time basis providing a finer level of granularity. The human element, has been one of the great strengths of the work carried out by the Markle Foundation. Their emphasis has not only been on the technicality of terrorism databases and the political issues, but their emphasis on the individual and people such as outlined in their briefing: *Meeting the Threat of Terrorism: Cultural Change*

⁴³⁶ Key to the Markle Foundations thinking, is the development of some type of metric to measure the benefits derived from an information sharing culture.

For example:

‘...given the importance of enabling information consumers to find information, an early metric for discoverability would measure what percentage of an agency’s data holdings are registered in a directory of data indices.’⁴³⁷

Further examples include:

‘Enhanced metrics improve agency and individual accountability for meeting certain benchmarks or milestones and significantly reduce the voluntary

⁴³⁶ Markle Foundation Task Force, ‘Meeting the Threat of Terrorism: Cultural Change” See: http://www.markle.org/sites/default/files/MTFBrief_CultureChange.pdf [Accessed 12/09/11]

⁴³⁷ *Ibid.*

aspect of exposing select data with data indices. Penalties would be widely known, applied consistently, and proportionate to the misuse or failure.⁴³⁸

A quantifiable metric to measure discoverability offers the chance for terrorism database designers to refine and improve methodological rigor in the database schema, in addition to providing some measurement of discoverability weaknesses. Furthermore, for the first time, metric assessments could be used to provide some measurement of success in terrorism information sharing. Also, in-built, is a mechanisms for accountability and even penalties where deemed necessary.

5.6. Legislation Post 9/11

The ramifications of September 11th 2001 saw major new legislation introduced by the United States Senate and House of Representatives that had a profound impact upon the U.S. Intelligence agencies and the way in which they conducted their counter-terrorism operations. Within weeks of the 9/11 attacks the *USA Patriot Act* was signed into law on October 26th 2001.⁴³⁹ Given the brevity of time for the drafting of the legislation, its contents were wide ranging and highly controversial, particularly among advocates of privacy rights and civil liberty activists. The legislation permitted much wider access by security and intelligence agencies to e-mail accounts, landline and cell phone accounts, financial transactions and medical records. Given the global implications of Al-Qaeda's operations and their associates, restrictions on the collation of foreign intelligence were eased. Significantly, for the first time domestic terrorism was to be included in the United States definition of terrorism. Eventually this inclusion would be reflected in the NCTC's TIDE database

⁴³⁸ *Ibid.*

⁴³⁹ USA Patriot Act full name: Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism *Act of 2001*. United States Congress (Pub L. 107-56- Oct 26, 2001. 115 Stat. 272

and their WITS database which records both domestic and international acts of terrorism. In many ways this legislation set in motion the creation of many sophisticated terrorism and counter-terrorism databases. These databases would stretch their tentacles deep into the heart of Americans personal lives, business operations, Government business and foreign interests. Another of the earliest and most significant pieces of legislation was the introduction of the *Homeland Security Act (HSA)* of 2002.⁴⁴⁰ A new era had arrived for the United States Intelligence Community; they were to experience their biggest shake up in culture, operations and organization since the start of the Cold War. With the signing into law of the act, on November 25th 2002 by President George W. Bush, the United States Department of Homeland Security (DHS) was also established. As a result, over twenty existing U.S. intelligence and counter-terrorism agencies were subsumed into the newly created DHS.⁴⁴¹ Significantly, the position of head of the DHS was also made at cabinet level, with Tom Ridge serving as the United States first ever Secretary of Homeland Security.

Another pillar of post 9/11 counter-terrorism legislation was the enactment of the *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*.⁴⁴² Among key developments, the IRTPA act set in law the creation of a Director of National Intelligence (DNI). It also laid the legislative foundations for the creation of the National Counterterrorism Center (NCTC) and the subsequent development of the

⁴⁴⁰ (Pub.L. 107-296, 116 Stat. 745, enacted November 25, 2002), 116 Stat. 2135. See: United States Congress, 'Homeland Security Act' : http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

⁴⁴¹ Among the agencies absorbed by the DHS were: the U.S. Secret Service, the U.S. Coast Guard and the Immigration and Naturalization Service (INS), the Federal Emergency Management Agency (FEMA), and the U.S. Customs Service.

⁴⁴² United States Congress, 'Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)'. Pub. L. No. 108-458, 118 Stat. 3638. See: <http://www.nctc.gov/docs/irtpa.pdf>

TIDE and Worldwide Incidents Tracking System (WITS) database on terrorism events worldwide. The act covers a comprehensive array of terrorism and homeland security issues, encompassing reform of the FBI, transportation security, border protection and immigration.

The above legislative programs introduced over the past decade has provided the legal framework from which has emerged a transformed U.S. Intelligence Community that is more reflective of, and responsive to, the complicated domestic and global political narrative that is 21st century terrorism.

5.7. Conclusions

As discussed, the status quo was not an option for U.S. intelligence and security agencies in a post 9/11 world. Responses to the terrorist attacks were initially swift, politically and militarily, with the invasion of Afghanistan on October 7th 2001, by American and UK forces, and the Afghan United Front (Northern Alliance). However, the impact of new technology and legislation upon the operation of the United States intelligence community has changed forever the way Americans think about their own security.

Database systems form an integral part of any counter-terrorism intelligence system. Several key thematic issues have changed the way in which terrorism and counter-terrorism databases operate. Firstly, as illustrated above, a much more cohesive systems approach to collating, analyzing and using data has emerged. Bridges have been built to connect the 'dots' of intelligence data. In other words, a much more integrative, interoperable series of networked database technologies have been built. This in turn has strengthened the knowledge base on terrorists and potential perpetrators. It is also in this area of study that the term terrorism informatics has a

crucial role to play. The above post 9/11 world of counter-terrorism has needed to respond using a multi-pronged approach. The use of legislators, statisticians, social scientists, computer scientists and information systems specialists requires that some cohesive title be given to the complex interdependent world of counter-terrorism. Again, where terrorism informatics has its strengths is in its ability to host such a wide gamut of inter-disciplinary topics under one common title. Only a few years ago many security analysts would have scoffed at the idea that such a divergent field of subjects could have any meaningful relationship together. What has emerged is a field of study – terrorism databases – that now truly reflects the real 21st century world. From airports, banking, hotels, travel, security, economics and I.T. to name a few – the world is truly interconnected. Acts of terrorism are committed within that very world. It therefore makes sense to develop over time the sub-field of terrorism informatics, so that it can best serve the needs of academics, and the Intelligence and security communities in minimizing if not preventing acts of terrorism.

In addition, lessons from the 9/11 Commission have been learnt. Namely, that counter-intelligence officials can no longer take a passive approach to potential terrorists pre-event movements. Where database systems have proven invaluable is their ability now to glean complex data on individuals that can alert agents to potential situations. Success in such matters can come at a price. Privacy issues have been and will continue to be an on-going issues for Government and civil liberty activists. The freedom of movement to fly, open a bank account and use a credit card, have not escaped the scrutiny of the state to ask questions. Even the innocent have been apprehended, after appearing on watchlists. Also, controversially, can the

defence of the state be, in part, carried out by business enterprises whose bottom line is to make profit and satisfy shareholders?

A second theme to emerge from the development of terrorism and counter-terrorism databases post 9/11 has been the quality of intelligence and human intelligence (HUMINT). Rigorous database design methodology and thousands of terabytes of digital data can be rendered useless if humans are unwilling to cooperate effectively in the use of such terrorism data. Cutting edge technology can provide a pseudo sense of legitimacy that can mask systemic and cultural shortcomings. What has changed, as illustrated above, is the cultural mindset of intelligence and security agents. A zero tolerance for self-serving power bases and a drive to rid the almost competitive culture of inter-agency rivalry has transformed fundamental thinking about how terrorism database technology in the U.S. is operated. The arrival of what the Markle Foundation calls a 'Trusted Information Network' has engendered a more horizontal and reciprocal database schema, that works for the common good. What also has emerged post 9/11, is revised thinking on the rich value of human intelligence and experience. The fusion of this priceless asset with modern technology strengthens immeasurably the value of terrorism and counter-terrorism databases.

Finally, a third thematic issue, the political dynamic has driven and influenced the enormous sea-change in counter-terrorism database technologies since 2001. Major legislative reform of the Intelligence services, their structure and increased accountability to both the U.S. Legislature and Executive has been seismic. The creation of the Department of Homeland Security, its wide-sweeping powers and its absorption of many other security related agencies, has brought under one umbrella

a disparate and at times fragmented intelligence community. Also, with the creation of the NCTC and its ability to draw upon specialist knowledge from many other arms of Government, the information sharing culture of post 9/11 is flourishing.

Having embraced technology, with the richness of human knowledge and combined this with new structural agency support, despite its many shortcomings, the post 9/11 world of terrorism database technologies is stronger and more powerful than at any point in history.

CHAPTER VI

SUMMARY AND CONCLUSIONS

6.1. Introduction

This thesis set out with the aim of answering the following questions: first, what is the quality, practical value and impact of database technologies in the field of terrorism and counter-terrorism post 9/11?; and second, how can the application of database systems improve the quality of terrorism and counter-terrorism research? Also, it argued that the study of computerised terrorism databases has had very little direction. The subject area needs to be drawn together under the classification of 'Terrorism Informatics' if its full potential is to be realised.

In addition the thesis argued:

5. That despite the fact that computerising terrorism data sets has allowed for more sophisticated levels of interrogation, this still does not deal with the issues surrounding the problem of soft qualitative data.
6. The application of computerised databases to terrorism research requires a high level of inter-disciplinarily. This includes the disciplines of international relations, computer science and other techniques (empirical, quantitative, content analysis, link analysis etc.) derived from a variety of social science disciplines, e.g. economics and psychology. The task of integrating such an eclectic array of subjects requires a systems approach to the fusion of computers and the study of terrorism.

7. The inevitable shift towards a more technologically based response to countering acts of terrorism requires the field of Terrorism Informatics to be more formally recognised for the full potential of technology to be realised.

6.2. Summary

The thesis was particularly concerned with the information aspects of terrorism and counter-terrorism in general, and database management systems specifically. The scope of databases used in this thesis was mainly limited to publicly available data sets, databases and chronologies on terrorism. The rationale was simple. Given the large amount of documentation already available on publicly available databases, there was enough source material to provide a substantial discourse. However, as has been illustrated, there is very few comprehensive monographs covering the wide array of terrorism and counter-terrorism databases post 9/11. This thesis sought to redress this issue. Private and classified databases were in the main excluded from this thesis. Given the volume and difficulties associated with access to such classified database systems, the focus of this thesis remained firmly in the public domain. Further research on the subject of classified terrorism and counter-terrorism databases would, however, be a valuable future research project.

The thesis drew upon a wide range of publicly accessible sources of information. These included opens source material, as well as a number of case studies. Given the wide accessibility now in electronic form of such databases as the Global Terrorism Database (GTD) and the NCTC's Worldwide Incident Tracking System (WTS) database, this study was able to make use of the commensurate amount of primary and secondary source material now available electronically. The thesis illustrated the

lengthy temporal development of quantitative data in International Relations in the 1930's to the complex statistical use of terrorism data in the 21st Century. Through a variety of field visits, outlined in Appendix B of this thesis, the opinions of those people currently working in the field of terrorism research, as to the efficacy of particular data sets has been considered. These were highlighted throughout the thesis.

Using a number of case studies throughout the thesis, this thesis demonstrated that the historical development of early terrorism data sets and chronologies on terrorism were primarily Government run systems, with the exception of a few privately owned data sets. The thesis argued that with the sheer cost of mainframe computers with limited functionality and accessibility to a small universe of data available in the late 1960's, the concept of joined-up integrated networked database technology was decades away. Following a review of the historical context for the use of databases in Chapter 2 of this thesis, Chapter 3 set out to trace the design and development of terrorism and counter-terrorism databases, and the issues that can arise in their design and management.

The thesis was able to outline the complex matrix of issues that present when attempting to design terrorism and counter-terrorism databases. The classic and recurring issue of how to define an act of terrorism was discussed. Given the variations in definitions between and within Government(s), academics and other interested parties, arriving at a definitive answer is simply impossible. What the thesis was able to demonstrate, was, that with sophisticated software technology, users are able to refine their criteria for an act of terrorism, within agreed boundaries. This functionality would have been impossible only a few years ago. The

thesis then went onto to discuss the difficulties associated with terrorism database methodology, including sourcing primary data, data validity and error rates. To add to this complicated narrative, the thesis was able to provide evidence that simple cross-comparison of terrorism databases and data sets can be fraught with problems. While simple aggregate totals comparing events data may have some use, the underlying spatial, temporal and methodological design of the database may render cross-comparison difficult to achieve. The thesis also clarified the difference between data sets, chronologies on terrorism and terrorism and counter-terrorism databases. The inter-changeability of the terms has added to confusion about their remit and functionality.

Following this, Chapter 4 outlined the many public, private and 'in-between' terrorism and counter-terrorism databases from a post 9/11 perspective. The thesis demonstrated that there has been a large variety of terrorism data sets and databases that have been developed over the past forty years. Not all have survived, as discussed, for example the MIPT's *Terrorism Knowledge Base* (TKB). Furthermore, the thesis was able to demonstrate that even although some terrorism databases have had a considerably longevity, their original founding hosts have relinquished the database, renamed the database, or merged the data with other databases. For example, the MIPT data was in-part returned to RAND and the Pinkertons database was encompassed within the newly formed Global Terrorism Database (GTD). One particular problem with such mergers is the paucity of meta-data accompanying databases. In surveying terrorism databases, the thesis discovered an eclectic mixture of systems. It found that they were hosted by a mixture of academic, Government and private organisations. What appears to be the main reason behind

the predominance of Government funded projects is the sheer costs involved in the design and on-going maintenance of databases on terrorism. Ironically, it appears as technology has become relatively cheap, the cost of sourcing data and employing staff to run the database and the on-going commitment (which in theory could be years) can be prohibitive. The research undertaken for this project also illustrated the difficulty in retrospectively coding terrorism events data. From the survey of terrorism and counter-terrorism databases undertaken, the thesis illustrated that the largest proportion of these databases reside within North America followed by Western Europe. There are some exceptions, notably in Israel and South Africa. As a result of this imbalance, there is a paucity of databases based within Central and South America, the Africa's, the Middle East and Asia-Pacific. In researching and analysing these databases, to the authors knowledge, this post 9/11 analysis of the twenty key terrorism databases in Chapter 4 of this thesis is the largest comprehensive assessment of terrorism databases ever undertaken.

Finally, Chapter 5 finally examined the complex world of terrorism databases post 9/11. The chapter demonstrated that no contemporary terrorism database system can sit within its own narrow confines. It illustrated that terrorism and counter-terrorism databases post 9/11, needs to be placed within a wider political, legal and technological context. In addition, while many benefits can be derived from network based database technologies, they do have their critics. The thesis demonstrated the many concerns among civil liberty groups about privacy issues, for example in travel watchlists and increasing trends in mission creep. One particular issue was the relationship between the citizen and the state, and the increasing use of commercial vendors to collect, store and use private citizens data for counter-

terrorism purposes. The thesis also assessed the 9/11 Commission Report and its recommendations. Chapter 5 demonstrated that a more systematic, integrative and transparent culture needed to be developed. What the thesis was able to demonstrate was a revolution in information-sharing across a vast array of intelligence and Government database system. Using the legislation introduced in the immediate years after 9/11, the thesis was able to illustrate the most fundamental change to the structure of the Intelligence Community (IC) since 1947. This in turn allowed the thesis to show the extent to which new agencies, a cultural change in thinking and a more 'trusting' approach within the Intelligence Community was in everyone's interest. This new approach needed to reflect the new technologies and globalised stage upon which terrorism operates in the 21st Century.

6.2. Conclusions

The technological leap and change in terrorism tactics over the past forty years has been immense. From crude bombing devices to sophisticated cyber activities, terrorists have, in recent years shown a keen willingness to embrace the technological revolution. Often one step ahead of their avowed Governmental enemies, they have lead often where others have followed. Quick to grasp the potential of the Internet and network technologies, many terrorist groups have been more than adept at using technology to their advantage. Be it propaganda videos, Internet chatter, blogging or scam financial trading for fund raising, the distributed typology of database systems, and internet domain hosting has provided an excellent vehicle with which to pursue their cause.

As demonstrated within this thesis, the same levels of success with internet based technologies cannot always be attached to academic and counter-terrorism intelligence databases prior to 2001. It took the horrific events of that day to change irrevocably a political and intelligence narrative that was essentially fragmented, insular, outdated and highly ineffective.

Ten years later, formalisation of terrorism and counter-terrorism data has advanced both the quantitative and qualitative value of data almost beyond recognition. From the most basic events based chronologies on terrorism, held on a card-index system, data can now be accessed globally and deliver analysts with the most sophisticated schema of data that would have been unimaginable in 1968.

What can be learnt from this study that could be carried forward for future research? Outlined below is a series of recommendations for future best practice in terrorism database design.

1. A comprehensive feasibility study should be undertaken to assess the viability of developing new terrorism databases. Is the project duplicating existing data (as is often the case). Can, for example, a new database compliment rather than replicate existing data? Furthermore, are their sufficient funds available to provide long-term finance for what can be an extremely costly lengthy project?
2. Meta-data should always be provided as part of the development stage of any terrorism database. This would allow future designers the ability to understand and improve methodological rigor.

3. Designers should, where possible, design a terrorism database platform that can be functionality as integrative and interoperable as possible, to permit future synthesis of data with other databases.
4. The nature of database technologies is changing at a ferocious pace. Designers of databases need to think beyond the standard terrorism events data approach, to data modelling that meets the needs of terrorism researchers and is not dictated by computer programmers alone. At all stages of such projects terrorism analysts should be involved, to ensure the end-product meets the users requirements.
5. There may be a case for developing regional terrorism database units that would focus purely on local source data. For example, in the Africa's, South America and Asia-Pacific. This would help overcome language and cultural barriers, whereby data can be under-recorded due to language difficulties. As long as there was agreed methodological rigor, regional terrorism database units could then 'bolt-on' regional data to a centralized system.
6. Consideration should be given to the possibility of designing terrorism databases that can also be widened to include 'peripheral' issues that provide greater contextualisation of events. For example, one could attach other data sets such as failed terrorist attempts, hoaxes, socio-economic indicators, political election results, poverty indicators as well as drug, gang and conflict data. No terrorism event occurs without context. Synthesis of such data into a sophisticated database schema could provide rich events data sets for social scientists to analyse.

7. Provision should be made, that in the event of a terrorism database discontinuing, that no data should be lost, or left languishing on a hard-disk. Many terrorism databases are in theory and also in practice projects that will continue ad-infinitum. Financial resources cannot always be guaranteed forever. The Global Terrorism Database at the University of Maryland has made such provision. In the event that the GTD funding is halted or the database discontinues, the data will be placed within the *Inter-university Consortium for Political and Social Research (ICPSR)* at the University of Michigan.
8. The creation of a Terrorism Informatics forum, within a University environment or Government funded think-tank would provide a focus for key stakeholders from Homeland Security, Academia, Business, and the Intelligence community to regularly discuss and push the boundaries of the field. This type of forum is not totally without precedent, the Institute for Electrical and Electronic Engineers (IEEE) has already developed its own Intelligence and Security Informatics sub-field.

A key fundamental point needs to be made. There requires a carefully considered synthesis of sophisticated databases technologies to be mapped onto to a complex 21st Century globalised world of terrorism. As illustrated in Chapter 4 of this thesis, too often have databases been limited in their ability to 'talk' to other terrorism databases. Some form of agreed best practice among vested organisations could in part help to resolve the same recurring design and methodology issues. Concerns about compromise on security should not be an obstacle to such interaction. Many of the refinements in database methodology can easily be tested using mock data

that reflects real-life situations. Security and intelligence organisations can be more transparent with their counter-parts using tiered levels of security access. This would allow the safe discussion of problems and issues without compromising safety and security. Despite the many different U.S. agencies holding terrorism related data, often the recurring problems are common to their colleagues in the intelligence sector. Much also can be learnt from an open dialogue with the academic community. Given the sophisticated front-end interfaces that such databases as the Global Terrorism Database (GTD) presents, academics specialists have a wealth of knowledge and experience to share. Furthermore they are not encumbered by the same security restrictions and political agendas that Government place upon the intelligence communities. Where there is a paucity of data is in the amount of feedback users provide on their satisfaction with the use of such databases. This can be a difficult issue to address. Some users would rather not be identified. For perhaps differing reasons, users of academic databases are not always content to identify themselves. Future research might include some form of questionnaire undertaken by a University research centre. Often users can provide valuable insight into a databases shortcoming's that designers are unaware. An improvement to any terrorism database is a constant cyclical process. The end user must feature in that process for the database to be of value.

As illustrated in this thesis, one must always be mindful of the issues of privacy and data integrity. Ever sophisticated data mining techniques, surveillance and identity issues will continue to present Governments and non-government groups with ever increasing challenges. The sheer volume of terrorism data available, as well as related 'innocent' data such as credit card and phone account

details all provide the potential for ever increasing scrutiny by the state. As consumers we already experience this moulding of adverts/brands, our likes and dislikes to our everyday internet searches. It is no coincidence that adverts sitting at the side of ones search engine just happens to be local, or is a product that one has previously purchased. Applying this scenario to state surveillance and the retention of our personal data in the name of counter-terrorism may require that the individual has some form of data protection identity or system of redress.

Academics and counter-terrorism analysts must also remember that numbers, graphs, maps and pictures can only tell part of the story. As this thesis has demonstrated, what database technologies have still to achieve and is impossible to code in the 21st century, is the human element; the human experience. Terrorism databases cannot, to date, code such entities as 'gut instinct' 'hate' 'anger' and 'fear'. The list is endless. One could attempt to dis-aggregate the elements down to the finest, most detailed level of granularity, and yet one would still fail. Hence, the need for a systems approach whereby academics and terrorism analysts can use the very best of technological advances coupled with a political framework that works to everyone's advantage. It is the political framework that this chapter now turns.

The thesis has demonstrated one of the key lessons from 9/11 was a complete lack of 'joined-up' counter-terrorism strategy. The territorial culture of intelligence agencies and isolated development of databases resulted in a highly fractured, almost brittle world of counter-terrorism databases. While academic database can survive as stand-alone systems, this state of play for counter-terrorism database post 9/11 is unthinkable. Three key foundations need to be in place. Firstly, a legal framework that is both effective and protective of its citizens, when drafting

terrorism legislation in relation to terrorism and counter-terrorism databases. Given the rapidity of terrorism database technology development, regular revision of terrorism database legislation would be valuable. This would not only be a useful reflective exercise but would highlight any potential loopholes in legislation that agencies and individuals are able to exploit given improved database functionality. Secondly, all relevant government agencies should fully adopt integrative network technologies that permit terrorism analysts to safely cross-reference data from the many databases available. A new generation of information sharing professionals with highly honed skills in intelligence analysis is now emerging. Their role will be ever-evolving and responding to technological change. However, one prime asset than will forever serve them well is their ability to synthesise their human knowledge and experience with cutting edge technology to produce terrorism knowledge bases of the highest standard.

A decade after 9/11, much has been achieved in the development of terrorism and counter-terrorism databases. Mistakes have been made, and will, from time to time be made again. The overarching picture however is of a robust decentralised network of terrorism databases that are now enhancing the full power of the Internet and network technologies.

Finally, the political will-power must be in place to support intelligence and security agencies in fostering a culture of meaningful reciprocity in the fight against terrorism in the 21st Century.

APPENDICES:

Appendix A –

List of Publicly Accessible Terrorism Databases included for Chapter 4

Appendix B –

Field Visits undertaken pre and during Thesis research

Appendix C –

Poster Presentation - IEEE 2010 International Conference on Intelligence and Security Informatics, Vancouver, Canada

APPENDIX A

List of Publicly Accessible Terrorism Databases included for Chapter 4

1. Global Terrorism Database (GTD)
2. Worldwide Incidents Tracking System (WITS)
3. ITERATE - International Terrorism: Attributes of Terrorist Events
4. MIPT Terrorism Knowledge Base
5. RAND – Worldwide Terrorism Incident Database (RWTID)
6. Country Reports on Terrorism – United States Department of State
7. Terrorism in Western Europe: Events Data (TWEED)
8. South Asia Terrorism Portal (SATP)
9. The International Policy Institute for Counter-Terrorism (ICT) – Terrorist Incident Database
10. Political Terror Scale (PTS)
11. The American Terrorism Study
12. Europol Terrorism Situation and Trend Report (TE-SAT)
13. Global Pathfinder
14. The Institute for the Study of Violent Groups (ISVG) Database
15. Monterey WMD Terrorism Database
16. Armed Conflict Database
17. Iraq Body Count (IBC)
18. Illicit Trafficking Database (ITDB) International Atomic Energy Agency
19. Uppsala Conflict Data Program (UCDP)
20. The Minorities at Risk (MIR) Project

APPENDIX B

Field Visits undertaken pre and during Thesis research

1. Australian Bomb Data Center (Canberra, Australia)
2. FAA (Washington D.C. United States)
3. United States Department of State (Washington D.C. United States)
4. Office of Diplomatic Security, United States Department of State, (Washington D.C. United States)
5. RAND Corporation (Santa Monica, CA, United States)
6. RAND Corporation (Washington D.C. United States)
7. University of St. Andrews (RAND-St.Andrews database)
8. MIPT – Meeting with Chip Ellis (McLean, VA, United States)
9. Federal Aviation Administration (FAA) (Washington D.C. United States)
10. National Counter Terrorism Centre (NCTC) (McLean, VA, United States)
11. National Counter Terrorism Centre (NCTC) Terrorism Metrics Brain Trust (McLean VA, United States)
12. Terrorism Incidents Conference (NCTC) (McLean, VA, United States)
13. ITERATE – Vinyard Software Inc. (Dunn Loring, VA, United States)
14. Served on the NCTC Terrorism Metrics Brain Trust (2008)
15. Attorney General for Australia's Office (Canberra)
16. Global Terrorism Database – GTD (START – University of Maryland)
17. Institute of Strategic Studies (Pretoria, South Africa)
18. Pinkertons (Washington D.C.)
19. 2010 IEEE International Conference on Intelligence and Security Informatics (Vancouver Canada)
20. Terrorism.com Washington D.C.
21. United States Library of Congress (Washington D.C. United States)

APPENDIX C

A Systematic Review of Databases on Terrorism

Neil G. Bowie¹ and Alex P. Schmid²

¹ Centre for the Study of Terrorism and Political Violence (CSTPV), School of International Relations,

University of St. Andrews, Scotland. Email: ngb@st-andrews.ac.uk

² Director, Terrorism Research Initiative (TRI). Email: apschmid@gmail.com



University of
St Andrews

Introduction

At the turn of the 21st Century, terrorism and political violence is one of the defining issues for governments, security agencies and individuals concerned with maintaining democracy and the rule of law. If sound judgments are to be made, the analysis of terrorism events data by policy makers, analysts and academics requires data, information and analysis of the highest quality. The need for information has produced a plethora of databases or terrorism.

The vast majority of databases on terrorism and counter-terrorism are operated and funded by governments. Given the nature and sensitivity of these databases, access is often highly restricted. Originally developed as chronologies on terrorism incidents, they have evolved into sophisticated database management systems primarily using the 'terrorist incident' as the unit of analysis. While information and analysis of these databases can be very limited, there are several terrorism and terrorism related databases that are partly or fully publicly accessible. Our review focuses on these databases. Some of the principal databases include: The Global Terrorism Database (GTD), the Worldwide Incidents Tracking System (WITS), ITERATE – International Terrorism: Attributes of Terrorist Events and

the RAND Worldwide Terrorism Incident Database (RWITD).

Objectives

The design and on-going development of the vast majority of public domain databases is a major undertaking for any organization. Some terrorism databases have had a lengthy pedigree, such as the RAND terrorism database, stretching back to 1972. Others have encountered sporadic development, periodic lapses in operation and change of remit, ownership and name. This legacy has at times been messy and confusing.

In the review we sought to investigate:

1. What are the main public domain databases on terrorism?
2. What type of organizations fund and operate these databases?
3. What is the format of the databases their functionality and key variables used?
4. Can some key comparative statistics be obtained across the spectrum of terrorism databases?

Methods

In our review presented in the forthcoming 'Handbook of Terrorism Research' (Schmid et al. 2010), we outline twenty databases from

which some systematic information could be obtained. The vast majority of these databases are in the public domain. The review contains key information such as the unit of analysis, scope of the database temporal and spatial period covered and key variables. A detailed narrative for each database provides historical background and context, the definitional criteria, the source material used and database functionality. Where available, we have provided statistical and graphical data for each terrorist database to give further depth and insight. While the majority of databases use the 'terrorist incident' as the unit of analysis, we also review some databases that use alternative units of analysis, such as 'armed conflict'. With one exception, the review does not include private or commercially run databases on terrorism.

Results

Our review discovered that the majority of public domain databases on terrorism are hosted by universities, specialist research centres or form part of larger government research projects. The substantial financial resources required to develop and maintain these databases means that, other than private or commercially funded projects, the databases are funded directly or indirectly by government. While the majority of the twenty databases now cover international

and domestic incidents of terrorism, their geographic base (host organization) is predominantly within the United States. Four of the databases originate in Europe, two in Asia and one in the Middle East. Temporal coverage of incidents in the databases range from 1950 to the present day. Year by year comparison of the databases can be problematic as temporal periods vary between databases and methodologies have changed over time. Furthermore, definitions of terrorism vary between databases. Most of the databases have adopted or are in the process of adopting new web-based technologies.

Conclusion

Given the eclectic nature of these databases, to avoid unnecessary duplication and to enhance the universality of terrorism data, some moves towards fusion of data should be encouraged. Also, widening the scope of the unit of analysis would provide a richer informational context in which the analysis of acts of terrorism can be studied.

Literature Cited

Alex P. Schmid et al. *Handbook of Terrorism Research*. New York, Routledge, December 2010. ca. 750 pp. ISBN: 978-0-415-41157-8

Examples of Databases included in the Review



The Political Terror Scale (PTS)

Host: University of North Carolina at Asheville, United States

Web: <http://www.politicalterroryscale.org>

The PTS measures annual levels of political violence and terror in over 180 countries, from 1976-2007. The scale element refers to a measurement scale of 1-5, with level 5 being the highest level of political violence and terror. Data used to compile the PTS is sourced from two reports: The US State Department Country Reports on Human Rights Practices and the yearly country reports of Amnesty International.

RAND Database of Worldwide Terrorism Incidents (RDWTI)

Host: The RAND Corporation, United States

Web: <http://www.rand.org/nsrd/>

The RAND Corporation originally developed their RAND Terrorism Chronology in 1972. Over the years the Chronology has evolved into what is now the RAND Database of Worldwide Terrorism Incidents (RDWTI) holding in excess of 36,000 domestic and international terrorism incidents. The full database is accessible via a subscription service. Limited access to the database is publicly available free of charge.

Global Terrorism Database (GTD)

Host: National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland, United States

Web: <http://www.start.umd.edu/gtd/>

The Global Terrorism Database was launched in 2007, with the original data being collected from 1970 by the Pinkerton Global Intelligence Service (PGIS). The database covers both domestic and international acts of terrorism from 1970-2007. It holds in excess of 80,000 incidents.

The Worldwide Incidents Tracking System (WITS)

Host: US National Counterterrorism Center (NCTC)

Web: <http://www.nctc.gov/wits/>

WITS was publicly launched in 2005. The database replaced the US Department of State's annual publication *Patterns of Global Terrorism*. The database covers both domestic and international acts of terrorism. Data held on WITS dates back to 2004. The WITS database is available in two formats: the original WITS Classic Site and the new Next Generation Site launched in April 2010.

SELECTED BIBLIOGRAPHY

- Alexander, Yonah., and J.M. Gleason. Behavioural and Quantitative Perspectives of Terrorism. (Pergamon: New York. 1980)
- Alexander, Yonah., and David C. Rapoport. The Morality of Terrorism: Religious and Secular Justifications. (New York: Pergamon Press Inc. 1982)
- Alexander, Yonah and Dennia A. Pluchinsky. European Terrorism Today & Tommorrow (Brassey's [US], Inc. 1992)
- American Civil Liberties Union. THE MATRIX: Total Information Awareness Reloaded (Washington D. C. 2003)
- American Civil Liberties Union. Whats Wrong with Fusion Centers? (Washington D.C. 2007).
- American Society for Industrial Security. Security Online. (Arlington Virginia: American Society for Industrial Security. Summer 1992.) Vol. 6/No. 2.
- American Society for Industrial Security. Security Online. (Arlington Virginia: American Society for Industrial Security. Spring 1994.)
- Arnold, Stephen, E. "Researching Terrorism." Information Today. July/August 1992.
- Arnold, Stephen, E. "Databases Focus on Terrorism." Link-Up. July/August 1992.
- Ashford, Oliver M ., Prophet or Professor ? - The life and work of Lewis Fry Richardson (Bristol: Adam Higler Ltd, 1985)
- Beanlands, Bruce, James Deacon and Anthony Kellett. Terrorism in Canada 1960-1989 No. 1990-16. (Ottawa: National Security Co-ordination Centre, Solicitor General Canada. 1990.)

Bequai, August. Technocrimes: the Computerization of Crime and Terrorism.
(Lexington Books, Lexington, MA. 1986.)

Bryman, Alan., and Duncan Cramer. Quantitative Data Analysis for Social Scientists
(London: Routledge, 1990.)

Central Intelligence Agency, The World Factbook 1993. (Washington: CIA, Office of
Public and Agency Information. 1994.)

Central Intelligence Agency, The World Factbook 1996. (Washington: CIA, Office of
Public and Agency Information. 1997.)

Cioffi-Revilla, Claudio., The Scientific Measurement of International Conflict:
Handbook of Datasets on Crises and Wars, 1495-1988 A.D. (Boulder,
Colorado: Lynne Rienner Publishers, Inc. 1990.)

Clutterbuck, Richard. Terrorism, Drugs & Crime in Europe after 1992. (London:
Routledge. 1990.)

Cordes, Bonnie., Management of the RAND Corporation's Terrorism and Conflict
Databases. (Santa Monica: Rand)

Cordes, Bonnie, Brian. M. Jenkins, Konrad Kellen et. al. A Conceptual Framework for
Analyzing Terrorist Groups. (Santa Monica: Rand - R-3151. 1985.)

Dougherty, James E. and Robert L. Pfaltzgraff, Jr. Contending Theories of
International Relations. (New York: Harper & Row, 1990.)

Fowler, William Warner. Terrorism Data Bases: A Comparison of Missions, Methods,
and Systems. (Santa Monica: Rand N-1503-RC, 1981.)

- Fowler, William Warner. An agenda for Quantitative Research on Terrorism. (Santa Monica: Rand P-6591, 1980.)
- Frankfort-Nachmias, Chava and David Nachmias. Research Methods in the Social Sciences. 4th ed. (London: Edward Arnold, 1992.)
- Groom, A.J.R. and C.R. Mitchell International Relations Theory: a bibliography (London: Frances Pinter, 1978.)
- Gurr, Ted Robert. "Empirical Research on Political Terrorism: The State of the Art and How it Might be Improved.", in Robert O. Slater and Michael Stohl (eds.), Current Perspectives on International Terrorism (London: Macmillan, 1988), pp.115-154.
- Hoffman, Bruce, and Karen Gardela, The RAND Chronology of International Terrorism for 1986 (Santa Monica: Rand - R-3890-RC, 1990).
- Hoffman, Bruce. Inside Terrorism (London: Victor Gollancz, 1998.)
- Holsti, Kalevi J. International Politics. (Englewood Cliffs, New Jersey., Prentice-Hall. 1990.)
- Hudson, M.C., and Charles L. Taylor, World Handbook of Political and Social Indicators. Vol 1. (New Haven, Conn: Yale University Press. 1972.)
- Jongman, Albert J and Alex P. Schmid. Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature. (New Brunswick, USA: Transaction Books, 2nd. Ed, 1988.)
- Koplowitz, Wilfred D. Teaching Intelligence. (Washington: National Intelligence Study Center. 1980.)
- Laquer, Walter. Terrorism. (London: Sphere Books Ltd. 1980.)

Markle Foundation. Task Force on National Security in the Information Age. Protecting Americas Freedom in the Information Age. (New York: The Markle Foundation. 2002.)

Markle Foundation. Task Force on National Security in the Information Age. Creating a Trusted Network for Homeland Security. (New York: The Markle Foundation. 2003.)

Markle Foundation. Task Force on National Security in the Information Age. Implementing a Trusted Information Sharing Environment. (New York: The Markle Foundation. 2006.)

Markle Foundation. Task Force on National Security in the Information Age. Mobilizing Information to Prevent Terrorism. (New York: The Markle Foundation. 2006.)

Markle Foundation. Task Force on National Security in the Information Age. Nation at Risk: Policy Makers Need Better Information to Protect the Country. (New York: The Markle Foundation. 2009.)

Markle Foundation. Task Force on National Security. Meeting the Threat of Terrorism: Cultural Change. (New York: The Markle Foundation 2010)

Merari, Ariel, and Anat Kurz. INTER International Terrorism in 1987 (Jerusalem: Jaffee Center for Strategic Studies, 1987.)

Mickolus, Edward F. and Peter A. Flemming. Terrorism, 1980-1987: A Selected Annotated Bibliography. (New York: Greenwood Press, 1988.)

Mickolus, Edward F, Todd Sandler and Jean M. Murdock. International Terrorism in the 1980s: a Chronology of Events. Vol. II, 1984-1987 (Iowa: Iowa State University Press, 1989.)

Mickolus, Edward F, Todd Sandler and Jean M. Murdock. International Terrorism in the 1980s: a Chronology of Events. Vol. I, 1980-1983 (Iowa: Iowa State University Press, 1989.) [CHECK OUT ORDER OF THIS BY DATE]

Mickolus, Edward. Transnational Terrorism - A Chronology of Events 1968-1979. (London: Aldwych Press, 1980.)

Mickolus, Edward F. Terrorism, 1988-1991 : A Chronology of Events and a Selectively Annotated Bibliography. (Westport, Connecticut: Greenwood Press. 1993.)

Mickolus, Edward, and Susan L. Simmons. Terrorism, 1992-1995. A Chronology of Events and A Selectively Annotated Bibliography. (Westport Connecticut: Greenwood Press, 1997.)

Mizell and Company. A Chronicle of Terrorism and Crime in the Hotel Environment. Mizeell and Company, Bethesda, Maryland, 1991.

National Commission on Terrorist Attacks Upon the United States (2004). The 9/11 Commission Report. (New York: W.W. Norton & Company, 2004.)

Oots, Kent Layne. A Political Organization Approach to Transnational Terrorism. (Westport, Conneticut: Greenwood Press. 1986.)

Pinkerton Risk Assessment Services. Annual Risk Assessment 1993. (Arlington,VA: Pinkerton, 1994.)

Reid, Edna Ferguson. "An analysis of Terrorism Literature: A Bibliographic and Content Analysis Study." Ph.D diss., University of Southern California, 1983.

Sloan, Stephen. Simulating Terrorism. (Oklahoma: University of Oklahoma Press, 1981.)

Taylor, Charles L., and M.C. Hudson. Word Handbook of Political and Social Indicators. Vol. 2.(New Haven, Conn: Yale University Press. 1982.) [check these all out]

Terrorism and America: A comprehensive review of the threat, policy, and law: Hearings before the Senate Committee on the Judiciary, 103d Cong., 1st Session 153 (1993). (Statement of Michael D. Cronin) Publication No: J-103-9. Pp.153-156.

United Kingdom Government Statistical Service. Research and Statistics Directorate. Statistics on the Operation of Prevention of Terrorism Legislation. Home Office Statistical Bulletin, Issue 4/97, 1997. U.S. Department of Justice. Federal Bureau of Investigation. Terrorism in the United States 1991. [Washington D.C.] Terrorist Research and Analytical Center, Counterterrorism Section, Intelligence Division. 1992.

U.S. Congress. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub.L. 108-458 118 Stat. 3638 (Washington D.C. 2004)

U.S. Congress. Homeland Security Act (HSA) (Pub.L. 107-296, 116 Stat. 745, 116 Stat. 2135). (Washington D.C. 2002)

U.S. Congress USA Patriot Act. Public Law 107-56 Stat. 115 Stat. 272 (2001) (Washington D.C. 2002).

U. S Congressional Research Service. Terrorism: Automated Lookout Systems and Border Security Options and Issues. (Washington D.C. RL31019; June 18th, 2001)

U.S. Department of Defense. Terrorist Group Profiles. [Washington D.C.] 1988

- U.S. Department of Justice. Federal Bureau of Investigation. Terrorism in the United States 1982-1992. [Washington D.C.] Terrorist Research and Analytical Center, Counterterrorism Section, Intelligence Division, 1992.
- U.S. Department of Justice. Federal Bureau of Investigation. "Focus on Information Resources. The Violent Gang and Terrorist Organizations File." FBI Bulletin October 1996. [Washington D.C.]
- U.S. Department of Justice. Federal Bureau of Investigation. Bomb Summary 1992. [Washington D.C.] F.B.I Bomb Data Center. 1992.
- U.S. Department of Justice, Office of the Inspector General. Follow-up Audit of the Terrorist Screening Center. Audit Report 07-41 (Washington D.C. 2007.)
- U.S. Department of State. Bureau of Diplomatic Security. Lethal Terrorist Actions Against Americans 1973-1986. [Washington D.C.]: U.S. Department of State Publication. Bureau of Diplomatic Security, 1986.
- U.S. Department of State. Bureau of Diplomatic Security. Significant Incidents of Political Violence Against Americans 1988. [Washington D.C.]: U.S. Department of State Publication 9718. Bureau of Diplomatic Security, 1989.
- U.S. Department of State. Bureau of Diplomatic Security. Significant Incidents of Political Violence Against Americans 1989. [Washington D.C.]: U.S. Department of State Publication 9767. Bureau of Diplomatic Security, 1990.
- U.S. Department of State. Bureau of Diplomatic Security. Significant Incidents of Political Violence Against Americans 1991. [Washington D.C.]: U.S.

Department of State Publication 9953. Bureau of Diplomatic Security, 1992.

U.S. Department of State. Bureau of Diplomatic Security. Significant Incidents of Political Violence Against Americans 1995. [Washington D.C.]: U.S. Department of State Publication 9953. Bureau of Diplomatic Security, 1996.

U.S. Department of State. Bureau of Diplomatic Security. Significant Incidents of Political Violence Against Americans 1992. [Washington D.C.]: U.S. Department of State Publication 10067. Bureau of Diplomatic Security, 1993.

U.S. Department of State. Libya's Continuing Responsibility for Terrorism. [Washington D.C.] 1991.

U.S. Department of State. Patterns of Global Terrorism 1988. [Washington D.C.] U.S. Department of State Publication 9705. Office of the Secretary of State, Ambassador-at-Large for Counterterrorism, 1989.

U.S. Department of State. Patterns of Global Terrorism 1989. [Washington D.C.] U.S. Department of State Publication 9743. Office of the Secretary of State. Office of the Coordinator for Counterterrorism. 1990.

U.S. Department of State. Patterns of Global Terrorism 1990. [Washington D.C.] U.S. Department of State Publication 9862. Office of the Secretary of State. Office of the Coordinator for Counterterrorism. 1991.

- U.S. Department of State. Patterns of Global Terrorism 1991. [Washington D.C.] U.S. Department of State Publication 9963. Office of the Secretary of State. Office of the Coordinator for Counterterrorism. 1992.
- U.S. Department of State. Patterns of Global Terrorism 1993. [Washington D.C.] U.S. Department of State Publication 10136. Office of the Secretary of State. Office of the Coordinator for Counterterrorism. 1994.
- U.S. Department of State. Terrorist Tactics and Security Practices. [Washington D.C.] U.S. Department of State Publication 10099. Bureau of Diplomatic Security. 1994.
- U.S. Department of State. State Department: Efforts to Reduce Visa [Washington D.C.] Testimony GAO/T-NSIAD-97-167 U.S. Department of State Publication, 1997.
- U.S. Department of State. Country Reports on Terrorism 2004. (Washington D.C. 2005).
- U.S. Department of State. Country Reports on Terrorism 2005. (Washington D.C. 2006).
- U.S. Department of State. Country Reports on Terrorism 2007. (Washington D.C. 2008).
- U.S. Department of State. Country Reports on Terrorism 2008. (Washington D.C. 2009).
- U.S. Department of State. Country Reports on Terrorism 2010. (Washington D.C. 2011).
- U.S. Department of Transportation. Criminal Acts Against Civil Aviation. Federal Aviation Administration, Office of Civil Aviation Security. [Washington D.C.] 1993.

- U.S. General Accounting Office. Aviation Security. Additional Actions Needed to Meet Domestic and International Challenges. (Washington D.C.: U.S. General Accounting Office. GAO/RCED-94-38, 1994.)
- U.S. General Accounting Office. INFORMATION SHARING, Federal Agencies are Helping Fusion Centers Build and Sustain Capabilities and Protect, but Could Better Measure Results. GAO-10-972 (Washington D.C. 2010).
- U.S. National Counterterrorism Center (NCTC). Report on Terrorism 2007 (Washington D.C. 2008).
- U.S. National Counterterrorism Center (NCTC). Report on Terrorism 2008 (Washington D.C. 2009).
- U.S. National Counterterrorism Center (NCTC). Report on Terrorism 2009 (Washington D.C. 2010).
- U.S. National Counterterrorism Center (NCTC). Report on Terrorism 2010 (Washington D.C. 2011).
- U.S. Senate Judiciary Committee and Subcommittee on Technology, Terrorism and Government Information. Washington D.C. October 9th 2002.
- U.S. Senate Attempted Terrorist Attack on Northwest Airlines Flight 253. 111th Congress., (S Prt. 111-119). (Washington D.C. 2010).
- Wardlaw, Grant. Political Terrorism, (Cambridge: Cambridge University Press, 1984.)
- Weber, Robert Philip., Basic Content Analysis. (Beverly Hills, California: SAGE Publications Ltd. 1985)

Wilkinson, Paul. Terrorism and the Liberal State. (London: Macmillan Press Ltd, 1977.)

Wilkinson, Paul and A.M. Stewart. Contemporary Research on Terrorism (Aberdeen: Aberdeen University Press, 1987.)

Wilkinson, Paul. Technology and Terrorism. (London: Frank Cass & Co. Ltd, 1993.)

Wilkinson, Paul. Terrorism: British Perspectives. (Aldershot, England: Dartmouth Publishing Co. Ltd, 1993.)

Computing Science

Ahituv, Niv., and Seev Neumann. Principles of Information Systems for Management. 2nd. Ed. (Dubuque, Iowa: Wm. C. Brown Publishers. 1986.)

Brookes, Cyril H. P., Phillip J. Grouse, D. Ross Jeffrey, and Michael J. Lawrence. Information Systems Design. (Sydney: Prentice-Hall. 1982)

Brookshear, J. Glenn. Computer Science: An Overview (California: The Benjamin/Cummings Publishing Company, Inc. 1988.)

Date, C.J. An Introduction to Database Systems. Vol. I 5th Ed. (New York: Addison-Wesley Publishing Company, Inc. 1990.)

Elmasri, Ramez, and Shamkant B. Navathe. Fundamentals of Database Systems. (Redwood City, California: The Benjamin/Cummings Publishing Company, Inc. 1989.)

Kendall, Julie E., and Kenneth E. Kendall. Systems Analysis and Design. (Englewoods Cliffs, New Jersey: Prentice-Hall International. 1988.)

Salcedo, Gregory B., and Martin W. Rudy. PC World Paradox 3.5 Power Programming Techniques. (San Mateo, California: IDG Books Worldwide, Inc. 1990)

Technical Documentation

American Society for Industrial Security. Various Publications Literature. (Arlington, Virginia. 1994)

American Society for Industrial Security. Security Online A Guide to ASISNET - The ASIS Electronic Network. Spring 1994. (ASIS. Arlington, Virginia.)

Campbell, Colm, Tom Hadden and K.S. Venkateswaran. A Database on States of Emergency, Report of a Feasibility Study. (Belfast: Queen's University of Belfast, Centre for International and Comparative Human Rights, 1992.)

Dewar, James A, and James J. Gillogly. CODA: A Concept Organization and Development Aid for the Research Environment. (Santa Monica: Rand P7035) 1984.

Dewar, James A., James J. Gillogly and M.Hammer. CODA User's Manual. (Santa Monica: Rand N-2290-RCC) 1985._

Hobbs, Walter V., RDB: a Relational Database Management System [Draft]. (Santa Monica: Rand. 1992)

Netmap. The Netmap Intelligence Analysis Systems. Netmap Ltd. London. 1992.

Paradox 4.0. User's Guide (Scotts Valley, CA: Borland International.1992)

Rand Corporation. Description of the RAND Low-Intensity Conflict/Terrorism Data Bases. (Santa Monica: Rand)

Rand Corporation. CODA (Santa Monica: Rand)

Brief technical documentation on operation of CODA

_____ Security Online A Guide to ASISNET - The ASIS Electronic Network. August 1993. (ASIS. Arlington, Virginia.)

_____ Security Online A Guide to ASISNET - The ASIS Electronic Network.
December 1993. (ASIS. Arlington, Virginia.)

_____ Security Online A Guide to ASISNET - The ASIS Electronic Network.
Summer 1992. (ASIS. Arlington, Virginia.)

U.S. Department of State. Threat Analysis Division Information Management System
- TADMIS, User Manual. Threat Analysis Division, Office of Policy
Coordination, Bureau of Diplomatic Security, 1990.

U.S. Department of State. Overseas Security Electronic Bulletin Board. Users Manual.
Bureau of Diplomatic Security, U.S. Department of State. 1988.

U.S. Department of State. 'Assessing Current Projected Threats to U.S. National
Security.' Statement by Assistant Secretary of State for Intelligence and
Research Toby T. Gati Before the Senate Select Committee on Intelligence.
Washington D.C. February 5th 1997.

U.S. Department of State. Security Computer Networks: Strategic Resources for U.S.
Business. U.S. Department of State Dispatch. October 29th. 1990. Vol 5, NO.
23.

U.S. Department of State. Electronic Services. U.S. Department of State Dispatch.
June 6th. 1994. Vol 5, NO. 23.

U.S. Department of State. Overseas Security Electronic Bulletin Board. U.S.
Department of State Note. 1994

Vinyard Software. Iterate III Version 5 (Dunn Loring, VA: Vinyard Software, 1994.)

Journals

- Bertalanffy, Ludwig Von., "General Systems Theory." General Systems, Yearbook of the Society for General Systems Research, I (1956)
- Boulding, Kenneth. "General Systems Theory -- The Skeleton of Science." General Systems, Yearbook of the Society for General Systems Research, I (1956)
[this is a reprint from another journal]
- Bruce, Steve. "The Problems of 'Pro-State' Terrorism: Loyalist Paramilitaries in Northern Ireland." Terrorism and Political Violence. Vol.4. No.1, Spring 1992. pp.67-88.
- Crelinsten, Ronald, D. "Images of Terrorism in the Media: 1966-1985." Terrorism: An International Journal. Vol.12. No.3, 1989. pp.167-198.
- Churcher, P.R. "A Common Notation for Knowledge Representation, Cognitive Models, Learning and Hypertext." Hypermedia Vol. 1 No.3. 1989
- Clutterbuck, Richard. "Terrorism and The Security Forces in Europe." Army Quarterly 1981.
- Cordes, Bonnie. "Euroterrorists Talk About Themselves: A Look at the Literature." Paper presented at an International Research Conference on Research on Terrorism. Aberdeen University 15-17 April 1986.
- Dugard, John. "International Terrorism: Problems of Definition." Paper delivered at the annual meeting of the American Society of International Law. 1973.
- Enders, Walter., and Todd Sandler. Evaluating Policies Aimed at Thwarting Terrorism: A Var-Intervention Approach. (Iowa: Iowa State University. 1990)
- Gaddis, John Lewis., "International Relations Theory and the End of the Cold War." International Security, Vol. 17, No.3 (Winter 1992/93), pp. 5-58

- Gordon, Avishag. "Research Note: Terrorism and Science, Technology and Medicine Databases: New Concepts and Terminology." Terrorism and Political Violence. Vol.8. No.1, Spring 1996. pp.167-173.
- Gordon, Avishag. "Terrorism and Computerized Databases." Terrorism and Political Violence. Vol.7. No.4, Winter 1995. pp.171-177.
- Greer, Steven C. "The Supergrass System in Northern Ireland." Paper presented at an International Research Conference on Research on Terrorism. Aberdeen University, 15-17 April 1986.
- Harvey, Charles., and Jon Press. "Relational Data Analysis: Value, Concepts and Methods" History and Computing Vol. 4 1991. pp.98-109.
- Hazelton, William A. and Sandra Woy-Hazelton. "Terrorism and the Marxist Left: Peru's Struggle against Sendero Luminoso." Terrorism: An International Journal. Vol.11. No.6, 1988. pp-471-490.
- Hoffman, Bruce. "Terrorist Targeting: Tactics, Trends, and Potentialities." Terrorism and Political Violence. Vol.5, No.2. Summer 1993. pp.12-29.
- Hoffman, Bruce. "The Confluence of International and Domestic Trends in Terrorism." Terrorism and Political Violence. Vol.9, No.2 Summer 1997. pp.1-15.
- Hoffman, Bruce, and Donna Hoffman. "Chronology of International Terrorism, 1995." Terrorism and Political Violence. Vol.8. No.3, Autumn 1996. pp.87-127.
- Hoffman, Bruce, and Donna Kim Hoffman. "The RAND-St. Andrews Chronology of International Terrorism, 1994." Terrorism and Political Violence. Vol.7. No.4, Winter 1995. pp.178-229.

- Jenkins, Brian M. and D.A. Waterman. "Heuristic Modeling Using Rule-Based Computer Systems." (Santa Monica: Rand - P-5811)
- Jenkins, Brian Michael. Combatting Terrorism Becomes A War (Santa Monica: Rand P-6988. 1984)
- Jenkins, Brian Michael. The Lessons of Beirut: Testimony before the Long Commission. (Santa Monica: Rand - N-2114-RC. 1984)
- Johnston, Alexander. "Politics and Violence in KwaZulu-Natal." Terrorism and Political Violence. Vol.8, No.4. Winter 1996. pp78-107.
- Jongman, A.J. "Trends in International and Domestic Terrorism in Western Europe, 1968-1988." Terrorism and Political Violence. Vol.4, No.4. Winter 1992. pp.26-76.
- Llera, Francisco J, Jose M. Mata and Cynthia L. Irvin. "ETA: From Secret Army to Social Movement - The Post-Franco Schism of the Basque Nationalist Movement." Terrorism and Political Violence. Vol.5. No.3, Autumn 1993. pp.106-134.
- Lopez, George A. "Teaching about Terrorism: Notes on Methods and Materials." Terrorism: An International Journal, Vol 3, No. 1-2. pp.131-145. 1979.
- Mathams, R.H. "The Intelligence Analyst's Notebook." The Strategic and Defence Studies Centre. Working Paper No. 151. Australian National University, Canberra, 1988.
- McClellan, George G. "The Terrorists Among Us." Security Management
- McLelland, Charles A. "Systems and History in International Relations: Some Perspectives for Empirical Research and Theory." General Systems, Yearbook of the Society for General Systems Research, III (1958).

- Merritt, Richard L. "Confluence of Interest and Possibility: Roots of Quantitative International Politics Research." *International Studies Notes*. Vol.17. No.2. Spring 1992. (American Graduate School of International Management. Glendale, Arizona. 1992)
- Mizell, Louis, and Aura L. Lippincott. "Armoured Transport Companies: Attacks and Robberies." *Clandestine Tactics and Technology*. Vol. XIV. Report Issue 11, 1989.
- Mizell, Louis, and Bleu K. Lawless. "Guerrilla Warfare in Peru: Tactics, Targets, and Trends." *Clandestine Tactics and Technology*. Vol. XIV. Report Issue 7, 1989.
- Moxon-Browne, Edward. "Terrorism in France." *Conflict Studies* No.144. 1983.
- Nimmich, Kenneth W. "FBI Role in Countering Terrorism." *Terrorism: An International Journal*. Vol.14, No.2. April-June 1991. pp.123-127.
- Pluchinsky, Dennis A., "Academic Research on European Terrorist Developments: Pleas from a Government Terrorism Analyst." *Studies in Conflict and Terrorism*, Vol 15, pp13-23. (London: Taylor & Francis. 1992.)
- Pluchinsky, Dennis A., "Middle Eastern Terrorism in Europe: Trends and Prospects." *Terrorism*, Vol.14 pp67-76. (London: Taylor & Francis. 1991)
- Poland, James M. "Teaching 'Terrorism' in Criminal Justice: Benefits and Problems." *Journal of Police Science and Administration*. Vol 14. No. 3. 1986.
- Quigley, Robert C. "Terror Marches On." *Security Management*. January 1991.
- Waterworth, John A., and Mark H. Chignell. "A Manifesto for Hypermedia Usability Research." *Hypermedia* Vol. 1 No.3 1989. (London: Taylor Graham. 1989.)

- Rapoport, David C. "The International World as Some Terrorists Have Seen It: A Look at a Century of Memoirs." Journal of Strategic Studies. September 1987.
- Reid, Edna, O. "Using Online Databases to Analyze the Development of a Speciality: a Case Study of Terrorism." Proceedings of the 13th National Online Meeting, New York, 5-7 May 1992.
- Revell, Oliver B. "Counter Terrorism: Planning and Operations." The Police Chief. August 1990
- Ross, Ian Jeffrey. "Hypothesis about Terrorism During the Gulf Conflict, 1990-1991." Terrorism and Political Violence. Vol.6, No.2. Summer 1994. pp.224-234.
- Ross, Jeffrey Ian. "The Relationship Between Domestic Protest And Oppositional Political Terrorism In Connection With The Gulf Conflict." *Journal of Contemporary Criminal Justice*. Vol.11, No.1. February 1995. pp. 35-51.
- Ross, Jeffrey Ian and Ted Robert Gurr. "Why Terrorism Subsides A Comparative Study of Canada and the United States." *Comparative Politics*. Vol.21, No.4. July 1989. pp.405-426.
- Ross, Jeffrey Ian. "Low-Intensity Conflict in the Peaceable Kingdom: The Attributes of International Terrorism in Canada, 1960-90." *Conflict Quarterly*. Vol. XIV. No.3. pp.36.62.
- Ross, Jeffrey Ian. "Research on Contemporary Oppositional Political Terrorism in the United States: Merits, Drawbacks and Suggestions for Improvement." From Kenneth D. Tunnell (ed.) *Political Crime in Contemporary America*. (New York: Garland Publishing, Inc. 1993).

- Ross, Jeffrey Ian. "Attacking Terrorist Attacks: Initial Tests of the Contagion between Domestic and International Terrorism in Canada." *Low Intensity Conflict and Law Enforcement*. Vol. 1. No.2. Autumn 1992. pp.163-182.
- Ross, Jeffrey Ian. "An Events Data Base on Political Terrorism in Canada: Some Conceptual and Methodological Problems." Conflict Quarterly. Spring 1988, Vol.8. No.2. pp.47-64.
- Ross, Jeffrey Ian. "Attributes of Domestic Political Terrorism in Canada, 1960-1985." Terrorism: An International Journal. Vol.11. No.3, 1988. pp.213-234.
- Ross, Jeffrey Ian. "Contemporary Right-Wing Violence in Canada." Terrorism and Political Violence. Vol.4, No.3, Autumn 1992. pp.72-101.
- Rozen, Arnon, and John M. Musacchio. "The Use of a Computerized Database of Terrorists Activities for Threat Assessment." Paper presented at Carnahan Conference on Security Technology: Electronic Crime Countermeasures. University of Kentucky, Lexington Kentucky, May 10-12, 1988.
- Scheid, Stephen B. "Explosives Incidents System: A Computer Approach to Explosives Incidents." The Police Chief October 1991.
- Shultz, George., "The Uses of Military Power." Survival Feb/Jan 1985.
- Smith, P. and T.C. Tan. "RADA - An Intelligent Research and Development Advisor." Expert Systems for Information Management. Vol.2. No.2 1989.
- Stephens, Jerone. "An Appraisal of Some System Approaches in the Study of International Systems." International Studies Quarterly. Vol 16. No.3. 1972. pp.321-pp.349.

Thurman, Joey. "Interpol Computers Keep Track of Firearms, Explosives." The Police Chief. October 1991.

U.S. Department of the Treasury. Bureau of Alcohol, Tobacco and Firearms. 1993 Explosives Incidents Report. Bureau of Alcohol, Tobacco and Firearms. Washington D.C. 1994.

Vincent, Billie H. "Aviation Security and Terrorism." Terrorism: An International Journal. Vol.13. No.6, 1990. pp.397-439.

Wardlaw, Grant. "The Terrorist Threat to Australia and the Region." Paper prepared for a seminar on 'International Terrorism and the Australian Experience' Sponsored by the Australian Institute of Jewish Affairs. Melbourne 8-9 June 1986.

Weinberg, Leonard and William Lee Eubank. "Cultural Differences in the Behaviour of Terrorists." Terrorism and Political Violence. Vol.6, No.1 Spring 1994. pp.1-18.

Wellings, Lytton J. "A powerful new toll to assist the Analyst or the Investigator." Law Enforcement Intelligence Analysis Digest. Winter 1989 -Summer 1990.

White, Robert W. "The Irish Republican Army: An Assessment of Sectarianism." Terrorism and Political Violence. Vol.9. No.1, Spring 1997. pp.20-55.

Yannakoudakis, E.J., F.H. Ayres and J.A.W. Huggill. "An Expert System for Quality Control in Cataloguing and Document Identification." Expert Systems for Information Management. Vol 2. No.2 1989.

Internet Web Site Sources

American Civil Liberties Union, The:

<http://www.aclu.org>

American Society for Industrial Security (ASIS):

<http://www.asisonline.org>

Australian Federal Police:

<http://www.afp.gov.au>

A U.S. Terrorism Chronology:

<http://www.totse.com/files/FA004/terrorn1.htm>

C2 Corporation, Counter-Terrorism & Intelligence Resources Repository:

<http://www.c2corp.com/terror.html>

CAIN Project:

<http://cain.ulst.ac.uk/help/caindex.htm>

The Counter-Terrorism Page:

<http://www.interlog.com/~vabiro/coming.htm>

Canadian Security Intelligence Review Committee:

<http://www.sirc-csars.gc.ca/annual>

Central Intelligence Agency (CIA) :

<http://www.odci.gov>

Center for National Security Studies (CDT):

<http://www.cdt.org>

The Center for The Study of Terrorism and Low Intensity Conflict:

<http://www.darksideresearch.com/~cleaner/about.html>

CNN:

<http://cnn.com>

Control Risks Group:

<http://www.crg.com>

Counter-Terrorism & Security:

<http://www.worldonline.net/securitynet/CTS/index.html>

Centre for The Study of Terrorism and Political Violence (CSTPV):

http://www.st-and.ac.uk/~www_sem/IR/cstpv.html

Council of European Social Science Data Archives (CEESDA):

<http://www.nsd.uib.no/ceesda>

Department of Homeland Security, The

<http://www.dhs.gov>

Emergency Response & Research Institute:

<http://www.emergency.com>

Electronic Privacy Information Center:

<http://www.epic.org/privacy/terrorism/>

FAS - Intelligence Resource Program:

<http://www.fas.org/irp/threat/terror.htm>

Foreign & Commonwealth Office Travel Advice:

<http://193.114.50.10/travel/default.asp>

Federal Emergency Management Agency (FEMA):

<http://www.fema.gov>

Foreign Military Studies Office - Research Links:

<http://leav-www.army.mil/fmso/RESRCHLK.htm>

Federal Bureau of Investigation (FBI) :

<http://www.fbi.gov>

Federation for American Immigration Reform, Terrorism Chronology

<http://www.fairus.org/04153804.htm>

Federal Trade Commission:

<http://www.ftc.gov>

Global Hindu Electronic Network: Bharat (India)

George Washington University - Terrorism Studies Program:

<http://www.gwu.edu/~terror/interns.html>

http://193.123.144.14/INTERPOL.COM/PPF/comps_it/unisy_14.htm

Global Conflict Analysis:

<http://www.erols.com/tferleman/index.htm>

Global Terrorism Decoded:

<http://www.globalterrorism.com>

IASSIST:

<http://datalib.library.ualberta.ca/iassist/iassist.intro.html#TOC>

ICT - The Interdisciplinary Center, Herzliya:

<http://www.ict.org.il/home.cfm>

Indicator Crime and Conflict:

http://www.und.ac.za/und/indic/cc8_97.htm#abstract

i2 Limited - Analysts Notebook:

http://193.123.144.14/INTERPOL.COM/PPF/software/i2_1.htm

International Relations and Security Network (ISN):

<http://www.isn.etz.ch>

International Federation of Data Organisations (IFDO):

<http://sada.anu.edu.au/other/ifdo.html>

The Information Warfare Database:

<http://www.georgetown.edu/users/samplem/iw/>

INTERPOL (Ottawa, Canada):

<http://www.rcmp-grc.gc.gc.ca/cgi-bin/rcmpbold.pl/html/interpol.htm?terrorism+database>

Inter-University Consortium for Political and Social Research (ICPSR)

<http://www.icpsr.umich.edu>

Jaffee Center for Strategic Studies:

<http://www.tau.ac.il/~jcspb/infocenter.html>

Jane's IntelWeb:

<http://intelweb.janes.com>

Japan Times, The:

<http://www.japantimes.co.jp>

Jordanian General Intelligence Department:

<http://petra.nic.gov.jo/gid/001-01.htm>

Kim-Spy:

<http://www.kimsoft.com>

Kroll Associates:

<http://www.krollassociates.com>

Lexis-Nexis:

<http://www.lexis-nexis.com>

Markle Foundation:

<http://www.markle.org>

Milnet:

<http://www.onestep.com/milnet/terror.htm>

Mizell & Co. International Security:

<http://www.crime-terror-safety.com/index.htm>

National Counterterrorism Center (NCTC):

<http://www.nctc.gov>

National Security Institute:

<http://nsi.org>

National Criminal Justice Reference Service (NCJRS) :

<http://www.ncjrs.org>

National Technical Information Service

<http://www.ntis.gov>

The National Transportation Safety Board:

<http://www.nts.gov>

New York Times, The:

<http://www.nytimes.com>

Northern Ireland Information Service:

<http://www.nio.gov.uk>

Naked in Cyberspace:

<http://www.pimall.com/nais/nake.html>

Office of International Criminal Justice (OIJ):

<http://www.acsp.uic.edu/index.shtml>

Overseas Security Advisory Council (OSAC):

<http://ds.state.gov>

P.C. World (Australia):

<http://www.pcworld.idg.com.au>

PTD: Political Terrorism Database:

<http://polisci.home.mindspring.com/ptd.html>

Pinkerton Risk Assessment Services (PRAS):

<http://www.pinkertons.com>

Precognitive Technological Design Inc.:

<http://www.precog.com/dds.shtml>

Project On Insurgency, Terrorism and Security (POINTS):

<http://www.paladin-san-francisco.com/library.htm>

Reference Center For Terrorism In India:

<http://www.rbhatnagar.csm.uc.edu>

Save Our Sri Lanka from Terrorism (SOSL - Network):

<http://www.case.cioe.com/~sos/terror.html>

Serbian Unity Congress

<http://www.suc.org>

South African Data Archive (SADA):

<http://www.hsrc.ac.za/sada/>

South African Media Information System:

<http://inch.uovs.ac.za>

Sourcebook of Criminal Justice Statistics:

<http://www.albany.edu/sourcebook/1995/ind/TERRORISM.ind.html>

Terrorism & Security Monitor:

<http://www.intelligence-net.com/terrmain.htm>

The Terrorism Research Center:

<http://www.terrorism.com>

Terrorism Research Institute:

<http://www.terrorism.org>

Texas Observer, The:

<http://www.texasobserver.org>

The Terrorist Profile Weekly Archive Site:

<http://www.dibona.com/terror/index.shtml>

Terrorist Group Profiles:

<http://web.nps.navy.mil>

U.K. National Criminal Intelligence Service:

<http://www.ncis.gov.uk>

U.K. Home Office News Bulletin:

<http://www.coi.gov.uk/coi/depts/GHO/coi1059c.ok>

Uniform Crime Reporting (UCR) Summary System:

<http://www.fbi.gov/ucr/>

U.S. National Counterintelligence Center:

<http://www.naic.gov>

U.S. General Accounting Office (GAO) :

<http://www.gpo.gov>

U.S. National Crime Information Center (NCIC):

<http://www.fbi.gov/2000/2kv1n.htm>

United States and International Government Military and Intelligence Agency Access:

<http://204.180.198.56/ajax/ajax.htm>

U.S. Department of the Treasury:

<http://www.treas.gov>

U.S. Army:

<http://www.army.mil>

United States Department of State:

<http://www.state.gov>

Unsys - HOLMES 2 Computer System:

U.S. Department of Defense Directives:

<http://www.defenselink.mil/pubs>

United States Information Agency (USIA):

<http://www.usia.gov/topics/terror/terror.html>

U.S. National Archives and Records Administration:

<http://www.nara.gov>

Virtual World of Intelligence - Terrorism:

<http://www.dreamscape.com/frankvad.terrorism.html>

The Violent Intranational Conflict Data Project (VICPD)

<http://wizard.ucr.edu/~wm/vicdp.html>

Washington Post, The:

<http://www.washingtonpost.com>

Miscellaneous

McGuire, Frank. Security Intelligence Report. Vol. 8. No.24. (Interests, Ltd., Silver Spring, Maryland. 1993)

McGuire, Frank. Security Intelligence Report. Vol 9. No.12. (Interests, Ltd., Silver Spring, Maryland. 1994)

McGuire, Frank. Security Intelligence Report. Vol 9. No.14. (Interests, Ltd., Silver Spring, Maryland. 1994)

Office of Technology Assessment. "The Terrorist Threat." Technology Against Terrorism: The Terrorist Threat. Office of Technology Assessment. Congress of the United States. 1993.

Office of the Data Protection Registrar. Data Protection Act 1984. The Guidelines. 3rd Series. Data Protection Registrar, United Kingdom. 1994

Pinkerton. Daily Risk Assessment. Friday July 22nd. 1994. (Pinkerton Risk Assessment Services. VA., USA. 1994.)