Terrorism 3.0: Understanding Perceptions of Technology, Terrorism and Counter-Terrorism in Spain

**Lawrence Peter Ampofo**

Royal Holloway University of London

Department of Politics and International Relations

Thesis submitted for the degree:

D. Phil in Politics and International Relations

2011

**Declaration of Authorship**

A thesis submitted by Lawrence Peter Ampofo who claims sole and original authorship, for the University of London Degree of Doctor of Philosophy.

Date

# **Abstract**

This thesis tests whether the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives. It focuses on the ways narratives affected the behaviour of Spanish-language audiences through an analysis of policy documents, elite interviews, and internet research methods adapted by the author. The data illuminate shifting understandings of communities of policymakers, journalists, and publics during 2004 to 2011 and is the first such study undertaken in Spain. Five themes are examined: the relation of terrorism in Spain to immigration, the formation of narratives in relation to understandings of terrorism, terrorism and cybercrime within Spain, the nature of communities in relation to understandings of terrorism in Spain and online reaction to the death of Osama bin Laden. The hypothesis is derived from: the theses of Bobbitt (2008) and Barnett (2005) concerning technology’s role in the changing character of the state and terrorist organisations; terrorism studies literature concerning the role of technology in recruitment and communication; and public diplomacy studies suggesting political organisations can communicate effectively to publics through digital campaigns. The main findings are: (i) the availability of technologies has not brought success for government or terrorist organisations; (ii) government narratives were not considered persuasive by online users, refuting top-down communication models; (iii) online communities wish to engage and may contain key influencers to be conduits for government or terrorist narratives; (iv) terrorist organisations now have greater capacity to operationalise visibility and invisibility within their strategies; and (v) partly independent phenomena have been ‘commensurated’ into one ‘nexus’ of concern. The thesis considers how Web 3.0 is likely to bear upon these relationships, recommending that counter-terrorist practitioners conduct further internet research into the attitudes and behaviours of online users to explore ways they can be co-opted into future counter-terrorism strategies.

Table of Contents

Abstract 3

Figures and Tables 8

List of Figures 8

List of Tables 10

Acknowledgements 11

Chapter One: The Socio-Technical Development of the Internet and the World Wide Web 13

Introduction 13

Thesis Outline 18

The Internet, the Web and Society 30

Theoretical Framework Underpinning the Development of the Internet and the Web 35

Evolution of the Internet and the World Wide Web 46

i. The Internet 46

ii. The World Wide Web 47

iii. Iterations of the World Wide Web 48

What Inspires the Development of the internet and the World Wide Web? 52

i. Social and Political Contexts 52

ii. Government 56

iii. Technical Developers 59

iv. Civil Society 63

v. Corporations 67

Conclusion 69

Chapter Two: Terrorism, Counter-terrorism and Public Diplomacy in Spain 71

Introduction 71

Theoretical Approaches to Terrorism in Spain 72

i. Strengths and Weaknesses of the Theses of Barnett and Bobbitt 89

ii. Terrorism in Contemporary Spain 95

iii. Counter-terrorism Policies in Contemporary Spain 104

Terrorist Organisations in France 109

i. Counter-terrorism Policies in Contemporary France 112

Challenges to Counter-terrorism Policies in France and Spain 115

Public Diplomacy as Counter-Terrorism Strategy 118

i. Spain’s Use of Public Diplomacy 122

Conclusion 124

Chapter Three: The Ethics and Practices of Internet and Social Media Research 128

Introduction 128

The Methodological Issues of Terrorism Research 130

Ethics and Practices of Online Research: Comparing Traditional and Contemporary Methodologies 132

i. A History and Definition of Social Media 132

ii. Privacy and Trust in Social Media Analysis 135

iii. Specific Internet Research Methodologies and Practices 141

a. Content Analysis 141

b. Network Analysis 145

c. Web Metrics 149

d. Web Analytics 151

e. Netnography 152

f. Mobile Research Methods 154

Measurement Approaches for Digital Public Diplomacy 163

i. Why Measure Public Diplomacy Programmes? 163

Approach Used for the Internet Research: Methods and Categories for Analysis 167

Semi-Structured Interviews 183

Conclusion 184

Chapter Four: Immigration, Technology, Terrorism and Counter-Terrorism in Spain 186

Introduction 186

Immigration in Contemporary Spain 192

Terrorist Attacks in Madrid on 11 March 2004 196

Spanish Immigration Policy and Technological Determinism 206

Limitations of the Confluence of Technology, Immigration and Terrorism 210

Internet Research on the 11-M Attacks: Key Narratives and Immigration (2004-2010) 215

i. Sentiment Analysis 219

ii. Key Narratives 220

Conclusion 224

Chapter Five: Influence, Technology, Terrorism and Counter-Terrorism in Spain: An Overview of Understandings, 2004-2010 227

Introduction 227

Terrorism in Spain and the Traditional Media 233

Terrorism and the Internet / World Wide Web in Spain 240

Internet Research on the 11-M Attacks: Key Narratives and Sentiment Analysis (2004-2010) 248

i. Overview of Results 249

a. Volume of Content Over Time (2004-2010) 249

b. Most Frequent Narratives, Sentiment Analysis and Narrative Source (2004-2010) 251

c. Results from 11 March 2004 to 11 August 2004 260

d. Results from 11 March 2005 to 11 August 2005 266

e. Results from 11 March 2006 to 11 August 2007 271

f. Results from 11 March 2008 to 11 August 2009 274

g. Results from 11 March 2010 to 11 August 2010 277

h. Network Analysis of Online Communities by Core Narratives (2004-2010) 278

Conclusion 281

Chapter Six: Cybercrime, Terrorism and Counter-Terrorism in Spain 284

Introduction 284

Defining Cybercrime 287

Cybercrime in Spain 296

The Development of Cybercrime vs. Cyberterrorism in Spain 307

Internet Research on the 11-M Attacks: Key Findings Related to the Topic of Cybercrime and Terrorism (2004-2010) 311

Conclusion 314

Chapter Seven: Community Engagement, Technology, Terrorism and Counter-Terrorism in Spain 318

Introduction 318

Engagement with Local Communities in Spain 323

Engagement with Online Communities 334

Public Diplomacy and Engagement with Communities 341

Internet Research on 11-M Attacks: Behaviour of Online Communities 342

i. Overview of Results 343

ii. Monitoring and Analysis of the Behaviour of Online Communities Over Time (2004-2010) 346

a. Results from 11 March 2004 to 11 August 2004 346

b. Results from 11 March 2005 to 11 August 2005 349

c. Results from 11 March 2006 to 11 August 2007 352

d. Results from 11 March 2008 to 11 August 2009 354

e. Results from 11 March 2010 to 11 August 2010 357

f. Analysis of Negative Sentiment Over Time (2004-2010) 359

Conclusion 365

Chapter Eight: Online Life Online Death: Terrorism 3.0, Recommendations and the Death of Osama Bin Laden 368

The Concept of Terrorism 3.0 368

Main Conclusions from the Thesis 377

Internet Research on the 11-M Attacks: Spanish Reaction to the Death of Osama Bin Laden 388

i. Volume of Content 390

ii. Key Narrative Analysis 391

iii. Narrative Source 392

iv. Sentiment Analysis 394

v. Key Narrative Analysis by Sentiment 397

vi. Network Analysis 400

Final Analysis 402

Appendix One: List of Interviewees 407

Appendix Two: Detailed Methodology for Semi-Structured Interviews 410

Questionnaires Used 410

i. Government 410

ii. Academia 411

iii. Business 411

Challenges to the Conduct of the Semi-structured Interviews 412

Appendix Three: Glossary of Terms 414

Bibliography 422

# **Figures and Tables**

## List of Figures

|  |  |
| --- | --- |
| **Figure One**: Top 10 Countries with the Highest Number of Fixed Broadband Connections in the OECD | **14** |
| **Figure Two**: Top 10 Countries with the Highest Number of Wireless Broadband Connections in the OECD | **15** |
| **Figure Three**: Structurational Model of Technology | **45** |
| **Figure Four**: Inflows of Immigrants to Spain and France from 1999 to 2008 | **74** |
| **Figure Five**: The Pentagon’s New Map | **76** |
| **Figure Six**: Number of National and International Terrorist Incidents in France from 1970 to 2008 | **113** |
| **Figure Seven**: Inflows of Foreign Migrants to France, Spain and the UK | **195** |
| **Figure Eight**: Line Chart Presenting the Total Volume of Immigration-related Commentary Over Time | **216** |
| **Figure Nine**: Stacked Column Chart Demonstrating the Sentiment of Immigration-related Commentary Over Time | **220** |
| **Figure Ten**: Stacked Bar Chart Demonstrating the Most-Frequent Narratives Involved in Immigration-related Commentary Over Time | **221** |
| **Figure Eleven**: Total Volume of Commentary Over Time Inclusive of All Media Types | **250** |
| **Figure Twelve**: Total Volume of Content by Core Narrative | **254** |
| **Figure Thirteen**: Total Volume of Content by Narrative Source Over Time | **255** |
| **Figure Fourteen**: Total Volume of Content by Sentiment Over Time | **260** |
| **Figure Fifteen**: Top Ten Narratives by Sentiment in 2004 | **261** |
| **Figure Sixteen**: Top Ten Most Frequent Narratives by Sentiment in 2005 | **267** |
| **Figure Seventeen**: Top Ten Narratives by Sentiment in 2006 and 2007 | **272** |
| **Figure Eighteen**: Top Ten Most Frequent Narratives by Sentiment in 2008 and 2009 | **275** |
| **Figure Nineteen**: Top Ten Most Frequent Narratives by Sentiment in 2010 | **277** |
| **Figure Twenty**: Network Map of Online Communities by Core Narrative Delivery | **279** |
| **Figure Twenty-One**: Crime – Terror Nexus Model | **308** |
| **Figure Twenty-Two**: Bar Chart of Online Communities by Sentiment in 2004 | **347** |
| **Figure Twenty-Three**: Bar Chart of Online Communities by Sentiment in 2005 | **350** |
| **Figure Twenty-Four**: Bar Chart of Online Communities by Sentiment in 2006 and 2007 | **352** |
| **Figure Twenty-Five**: Bar Chart of Online Communities by Sentiment in 2008 and 2009 | **355** |
| **Figure Twenty-Six**: Bar Chart of Online Communities by Sentiment in 2010 | **358** |
| **Figure Twenty-Seven**: Line Chart Presenting the Negative Sentiment by Key Narrative Over Time | **360** |
| **Figure Twenty-Eight**: Line Chart Showing the Principal Negative Commentary Associated with the ‘Government Lies About 11-M’ Narrative Over Time | **362** |
| **Figure Twenty-Nine**: Emergent Model of Terrorism 3.0 | **373** |
| **Figure Thirty**: Volume of Online Content Over Time | **390** |
| **Figure Thirty-One**: Total Volume of Content by Narrative Source | **393** |
| **Figure Thirty-Two**: Sentiment Over Time | **395** |
| **Figure Thirty-Three**: Most Frequent Narratives by Sentiment | **398** |
| **Figure Thirty-Four**: Network Analysis of Communities Involved in Discussion of the Death of Osama Bin Laden with Reference to 11-M | **401** |

## List of Tables

|  |  |
| --- | --- |
| **Table One**: The Psychosocial Principles of Terrorism | **158** |
| **Table Two**: List of Narratives and Keywords by Organisation Used for the Internet Research  **Table Three**: Flowchart of Methodological Process for the Internet Research | **175**  **182** |
| **Table Four**: Key Narratives Used for the Internet Research | **252** |
| **Table Five**: Bennett’s Patterns of Communication | **338** |
| **Table Six**: Online Communities Discussing the 11 March 2004 Attacks | **344** |
| **Table Seven**: Description of Segmentations Used for Empirical Analysis | **389** |
| **Table Eight**: Key Emergent Narratives on the Death of Osama Bin Laden with Reference to 11-M | **392** |

# **Acknowledgements**

This thesis represents the end of a journey. It is also the culmination of the dedication, patience and encouragement of those who have provided support along the way. Although it is impossible to thank all those who have supported me, I would like to acknowledge the efforts of the following people who deserve special mention.

I would like to express my appreciation to my supervisor Professor Ben O’Loughlin who, over four years, has tirelessly fostered my ideas, aspirations and energy towards the completion of this endeavour. I am extremely grateful to him and our colleagues in the New Political Communication Unit and Department of Politics and International Relations, such as Professor Andrew Chadwick, for creating a stimulating environment in which to pursue and realise my academic aspirations.

Thanks must also be extended to Professor Marie Gillespie who has provided much enthusiasm and encouragement during the thesis. Her help and support towards my continued professional advancement is something for which I am especially grateful.

Russell and Michael also deserve mention for their limitless patience and support over the past four years. It has contributed enormously to the development of my work and has made that endeavour significantly more pleasurable.

My deepest thanks also go to Luke and Sandrine who have been great friends during the course of this thesis, making sure I stayed healthy, motivated and focused.

Marilyn Ampofo is someone who deserves mention above all others for her contribution to the successful completion of this thesis. She has provided me with support, love and motivation during this journey. She continues to inspire me and her faith, encouragement and pride will help me reach new professional heights.

My heartfelt thanks go to Victoria Pounce who has influenced the conceptualisation, development and completion of this thesis immensely. During the most challenging periods, she has always inspired faith in the strength of my ideas and my abilities as a writer, an analyst and an academic. The successful completion of this thesis could not have been achieved without her, and for her support I will always be indebted.

This thesis is dedicated to Granny and Leigh who are always in my thoughts and have been steadfast sources of inspiration and strength during trying times.

# **Chapter One: The Socio-Technical Development of the Internet and the World Wide Web**

## Introduction

The social, cultural and political impacts of the internet[[1]](#footnote-1) and the World Wide Web (Web) permeate society as a whole and only a systematic understanding of these impacts will help to address the challenges faced by the global community in the 21st century.

As the percentage of the global population connected to the internet and World Wide Web via personal computers, mobile phones and tablet computers increases, so too does the range and depth of interactions in kind. These ever-evolving technologies, which connect people to the internet and the Web, capture numerous aspects of societal interactions. In addition, the development of these technologies to include new elements such as the Semantic Web, the “internet of things” and the “real-time Web”[[2]](#footnote-2) (conjointly defined as Web 3.0) will facilitate the introduction of millions of new users to these technologies and, by implication, billions of new interactions.

Individuals, therefore, use the internet and the Web to engage with issues and content of interest to them, forming communities that have the potential to influence the attitudes and behaviours of other users. It is this phenomenon that forms the inspiration for this thesis, as users engage with the issues of terrorism, counter-terrorism and technology in a fashion that is at once digital, collaborative and mediated by technologies that encourage mobile, ubiquitous and intelligent computing. The potential, therefore, for communities engaged with the issue of terrorism - counter-terrorist policymakers, journalists, terrorists themselves and potentially terror-ised publics - to influence the attitudes and behaviours of others, facilitated in large part by high technology, is significant.

Spain has one of the highest internet penetration rates in Western Europe as shown in Figures One and Two below.

Figure One: Top 10 Countries with the Highest Number of Fixed Broadband Connections in the OECD

Source: OECD Statistics N=289,463,581

Figure Two: Top 10 Countries with the Highest Number of Wireless Broadband Connections in the OECD

Source: OECD Statistics N=498,828,827

Spain also has a unique experience with terrorism. Having confronted Basque separatist terrorism since 1959, the country is today faced with a dual security concern with the additional issue of international terrorism. This particular phenomenon became most prominent following the Madrid bombings of 11 March 2004.

The hypothesis this thesis seeks to test is therefore the following: the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives. Although this hypothesis appears common-sensical, the research is designed to identify variations that exist within this relationship such as, when and how have terrorist and counter-terrorist actors capabilities been increased by their access to and use of new communications technologies? What explains these variations?

In order to provide a comprehensive analysis of the extent to which access to high technology increases overall capabilities to achieve communication objectives, the specific research question developed to test this hypothesis is: what understandings exist of the relationships between technology, terrorism and counter-terrorism in Spain? This will be analysed by conducting internet research into the responses of online users and communities to the Madrid terrorist attacks of 11 March 2004, in addition to semi-structured interviews and in-depth literature reviews. This particular event was elected as the focus of the empirical research as it offered an opportunity to monitor and analyse the behaviour of multiple online communities as they engaged around the same issue in Spain over time.

It is anticipated that the analysis of these questions will contribute to the literature on the internet and terrorism in Spain. The thesis, as a result, seeks to test the following ancillary questions:

* How are understandings in Spain of technology, terrorism and counter-terrorism explained?
* What interactions have emerged from these understandings?
* What are the implications for policy practitioners in the field of security and counter-terrorism?

This thesis adds an original contribution to the body of work relating to terrorism in Spain by testing whether the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives. Five themes within public discourse were examined closely: the relation of terrorism to migration, terrorism and narratives, terrorism and crime, terrorism and communities, and the death of Osama bin Laden. The main findings of the research were that the availability of technologies has not brought concomitant success for government or terrorist organisations, government narratives were not considered persuasive by online users, online communities wish to engage and may contain key influencers to be conduits or “gatekeepers” (Hoskins and O’Loughlin, 2010) for government or terrorist narratives, terrorist organisations do not have greater capacity to operationalise visibility and invisibility within their strategies and, partly independent phenomena have been commensurated into one nexus of concern.

In addition, the thesis seeks to explain this online behaviour from the perspective of a new emergent model of online behaviour called Terrorism 3.0 in which it proposes that understandings of terrorism in an online context within Spain are a socio-technical, emergent phenomenon enabled by the form and structure of the continually evolving structure of the Web. This understanding of online behaviour in relation to terrorism in Spain was derived from an amalgamation of elite interviews, analysis of policy documents and internet research methods adapted by the author of comments relating to the 11 March 2004 bombings in Madrid from 2004 to 2011.

This approach is different to other research conducted on Spanish terrorism. The combination of this approach, combined with scholarship previously conducted on Spanish terrorism, inspired this research. Prominent scholars such as Reinares (2006), Soriano (2008) and Jordán (2008) have argued that the Web enables terrorist organisations to undertake their activities such as recruitment, propaganda and reconnaissance. Other scholars, such as Curto et al. (2007) have contended that media technologies, especially television and newspapers, play a pivotal role in influencing the consciousness of the general public in relation to terrorism. The thesis argues that terrorist content, propaganda and engagement with the issue of terrorism occurs across the web over long periods of time and, as a result, it is imperative that counter-terrorism practitioners make strident efforts to understand the changing nature of online behaviour in order to counteract it in the future.

## Thesis Outline

The structure of this thesis has been designed to clearly reflect the findings of the research undertaken, contribute to understandings of the potential use of Web 3.0 in terrorism and counter-terrorism communication strategies and, ultimately, to advance the literature on online communication initiatives through the analysis of the changing nature of online behaviour.

Analysis of online behaviour in relation to the Madrid bombings on 11 March 2004 contributes to understandings of technology, terrorism and counter-terrorism in Spain by providing the contextual setting against which various issues were analysed. The following issues emerged from the semi-structured interviews and the internet research and they are presented chronologically in the thesis. Immigration is located in Chapter Four, narratives in Chapter Five, cybercrime in Chapter Six and communities in Chapter Seven. Internet research analysing the behaviour of Spanish language online users and communities reacting to the death of Osama bin Laden in May 2011 and in relation to the Madrid bombings on 11 March 2004 was also conducted. The principal reason for this particular analysis is that the death of Osama bin Laden was considered the ideal context in which to observe the saliency of the conclusions presented in Chapter Eight. In addition, it was correctly anticipated that online discussion of the death of Osama bin Laden in relation to 11-M would be analytically congruent with the findings from the internet research conducted in previous chapters. Such an analysis, as a result, provides relevant insight into the ways that the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives, particularly those which include the use of contemporary technologies such as social networking sites.

In addition, public diplomacy, as a central theme, is interwoven within the thesis as a means to explore ways in which political organisations communicate to domestic and overseas publics using digital campaigns and initiatives. For the purpose of this thesis, public diplomacy is defined as the engagement of target populations by a state or other entity seeking to convince audiences of the legitimacy of its core narratives (Hope, 2009). As such, public diplomacy is presented as a lens through which analysis of the nature of online behaviour in relation to terrorism in Spain can be conducted, in addition to supporting the introduction of the Terrorism 3.0 model.

Chapter One takes, as its theoretical starting point, the notion that the internet and the Web are social and cultural spaces where influential actors and communities assert “influence” over others. For the purpose of this thesis, influence refers to the definition of users attaining online influence as outlined by Baldwin, ‘[Influencers are] conduits for human based filtering and content discovery within their communities, as members of the community look to the person of influence to connect them to people and content they should trust, and fuel positive community growth’ (Baldwin, 2009: 1). It is in light of the socio-technical context introduced in this chapter that the thesis examines the extent to which the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives. The attainment of such understanding is of considerable importance, particularly as the transition to Web 3.0, outlined in detail in this chapter, assumes greater prominence in the future, and publics use these technologies to uncover new ways of engaging with the issue of terrorism. This chapter analyses the socio-technical development of the internet and the Web as a means of demonstrating Spanish society’s transition to “Terrorism 3.0”, a concept provided by the author as a result of the thesis findings, to describe a distinct form of engagement with the issue of terrorism online that is concurrently networked, mobile, ubiquitous and pervasive.

Chapter Two examines contemporary Spain’s experience of terrorism; first it situates the Spanish and French experiences within general trends of globalisation and terrorism, introducing the theories of Bobbitt and Barnett who outline these trends which are used as a theoretical framework throughout the thesis. The chapter draws upon original interviews as well as requisite scholarship. It juxtaposes this with an analysis of terrorism in France, which is used to provide greater context, illuminating the reasons for Spain’s particular experience with terrorism (during which, the two countries’ experiences, at times, overlap). The chapter, therefore, provides an ideal context within which to test the theoretical frameworks chosen to underpin explanations for terrorism in these regions, which come from theories on globalisation and violence. In addition, Chapter Two introduces and analyses key terms such as terrorism and Jihadism. Jihadism is defined as ‘the political culture promoting the goals, practices, and ideology of Al-Qaeda (as an idea and set of networks) rather than to broader forms of political Islam which may also advocate violence’ (Hoskins & O’Loughlin, 2010: 7). While the definition of terrorism is a vigorously contested term (Stampnitzky, 2011), this thesis has used the definition as provided by the Spanish State as encompassing both interior and exterior terrorism:

‘External Terrorism is that which is committed outside the borders of the state of origin or within countries of origin but against the interests of other countries…such as attacks, sabotage, assassinations and kidnappings…[t]here are other aspects, which are linked in respect to international terrorism which should be taken into account. The existence of mercenaries and dangerous material that is very sophisticated as well as the possibilities that new technologies offer to obtain information about material that could be involved in international terrorism adds another factor to the terrorism phenomenon.

Interior Terrorism is that which is born inside a state and is conducted against a specific state…This terrorism could maintain international links of support between groups, maintain administration camps or take refuge in sanctuaries’[[3]](#footnote-3) (*Revisión Estratégica de la Defensa*, 2003: 127).

Chapter Three sets out the overarching methodological framework used to comprehensively analyse understandings of various actors and communities towards technology, terrorism and counter-terrorism in Spain. This framework emerges from literature reviews and semi-structured interviews of both counter-terrorism practitioners and other academic and commercial experts. Secondly, the author developed an internet research methodology to systematically analyse the behaviour and commentary of online users in relation to discussions of the 11 March 2004 Madrid terrorist attacks. For the purpose of this thesis, the author utilises the definition of “internet research” as provided by the scholar Anette Markham, who outlined that the discipline can be described as ‘*[t]he study of sociocultural phenomena that are mediated by, interwoven with, or rely on the internet for their composition or function’* (Markham, 2010: 2, cited in Silverman (ed.) 2010, emphasis in original). In this description, Markham asserts that internet research is related to the study of the ways people experience cultural interactions and artefacts that occur on the internet and that a wide range of methodologies can be used to study such interactions (Markham, 2010, cited in Silverman (ed.), 2010). In order to understand the emergence of Terrorism 3.0 in Spain and how the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives, Chapter Three provides a comprehensive overview of methodological approaches and tools through which to analyse the nature of online behaviour in this emerging context, and explains why certain methodologies were chosen over others for the purpose of this thesis.

Chapter Four analyses the relationship of the issue of immigration to technology, terrorism, and counter-terrorism, maintaining that understandings of this relationship should be perceived within the theoretical framework of commensuration as a social process. The issue of immigration emerged as a central theme during the course of the interviews, and, in addition, the internet research revealed that online users referenced the issue of immigration and terrorism most prevalently during the two years following the attack in comparison with other issues. Commensuration and the securitisation of discourse relating to immigration, terrorism and counter-terrorism are key terms examined in the analysis of online behaviour and discussions related to the terrorist attacks in Madrid on 11 March 2004. Commensuration refers to the process of the conflation of independent variables or issues, to create one dependent variable, when certain information is discarded and the remains are formed into something new (Espeland & Stevens, 1998). Commensuration and the securitisation of discourse relating to immigration, terrorism and counter-terrorism are key terms examined in the analysis of online behaviour and discussions related to the terrorist attacks in Madrid on 11 March 2004. Commensuration as a social process refers to the measurement of features that are usually represented by differing units merged into one unified metric. As a result, independent variables, or issues, are combined to create one dependent variable, as certain information is discarded and the remains are formed into an entirely new metric (Espeland & Stevens, 1998). Commensuration as a social process is similar to the notion of conflation, which the Oxford English Dictionary defines as the combination of ‘(two or more sets of information, texts, ideas, etc.) into one’ (Oxford Dictionaries, 2012).

However, Espeland and Stevens note that the main difference between commensuration as a social process and conflation is that it is possible to conceive of commensuration as a device of social thought and a mode of power. The authors wrote of the topic that ‘Commensuration transforms qualities into quantities, difference into magnitude. It is a way to reduce and simplify disparate information into numbers that can easily be compared. This transformation allows people to quickly grasp, represent, and compare differences. One virtue of commensuration is that it offers standardized ways of constructing proxies for uncertain and elusive qualities. Another virtue is that it condenses and reduces the amount of information people have to process, which is useful for representing value and simplifying decision-making’ (Espeland and Stevens, 1998: 317).

The fact that the previous quote underscores commensuration’s propensity to expunge complexity means that certain aspects of social life that have value can become lost or rendered extraneous. However, Espeland and Stevens claim that the process is essential to understanding how people make sense of the world; ‘[w]e argue that commensuration is no mere technical process but a fundamental feature of social life. Commensuration as a practical task requires enormous organization and discipline that has become largely invisible to us…Commensuration changes the terms of what can be talked about, how we value, and how we treat what we value. It is symbolic, inherently interpretive, deeply political, and too important to be left implicit in sociological work’ (Espeland and Stevens, 1998: 315).

Commensuration is a particularly important concept in Chapter Four as the analysis uncovers instances where users of social media services conceptualise the issues of immigration and terrorism as one ostensible topic. This occurrence is curious when the official data and testimony from terrorism and immigration experts considers the issues as separate.

Securitisation, as outlined by Ole Wœver and Barry Buzan, is defined as ‘the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects’ (Buzan et al. 1998: 8). Chapter Four also includes a chronological outline of events surrounding the terrorist attacks on 11 March 2004 in Madrid and provides the reader with the appropriate context for subsequent analysis of the ways in which various issues, namely immigration and cybercrime, were conflated by different actors during, and in the aftermath, of the terrorist event.

Chapter Five focuses on communication and “influence” online within public debates concerning technology, terrorism and counter-terrorism. It examines the ways in which narratives from the Spanish Government and from terrorist organisations were interpreted by online users from 2004 to 2010, and how communication works online within identified theoretical frameworks. A comprehensive analysis of online behaviour and discussions related to the terrorist attacks in Madrid on 11 March 2004 provides insight into the flow of information and online user engagement, and sheds further light on commensuration and the securitisation of the issues introduced in Chapter Four. The findings indicate that the construction of effective narratives is of great importance to contemporary terrorist organisations, as media technologies, conceptualised as a force multiplier, have the potential to change terrorist organisations from agents of violence into agents of influence, capable of shaping the attitudes and behaviours of other online users. This emphasises the importance of creating and maintaining effective narratives in online communication and, additionally, for counter-terrorism organisations to become cognisant of shaping such narratives to meet their communication objectives.

Chapter Six argues that understandings of cybercrime, terrorism and counter-terrorism are intrinsically bound within understandings of immigration, technology and terrorism. The semi-structured interviews focused on the use of Web technologies to commit the Madrid attacks. However, the internet research indicated that this issue was not prevalent amongst general online users and that discussion of this was located primarily in epistemic and practitioner communities. This relates strongly to the findings in chapters Four and Five, indicating that certain issues become conflated using commensuration as a social process through the effective creation and maintenance of narratives.

Chapter Seven focuses on the myriad ways communities develop understandings of technology, terrorism and counter-terrorism and, especially, how online communities attempt to assert influence over a discussion in order to affect the resulting behaviour and affiliation of that group and its members. These informed amateurs, adroit in the use of new media for communication, have been termed the *new intellectuals* (Fisher, 2003). Analysis of the behaviour of online communities related to the Madrid bombings on 11 March 2004 highlights the complexity inherent within interactions between communities online, emphasising the utility of a multi-directional approach as opposed to a top-down approach. This is enhanced by further findings from the internet research which intimated that the focus of online users shifted to the role of communities, particularly in later years following the 11-M attacks, in 2009 and 2010. In particular, online users focused on the ways groups of people sought and provided sympathy, empathy and support to those affected by the attacks.

This thesis incorporates the Patterns of Communication model by Lance Bennett which was derived from research and observations based on protests directed towards trade and development organisations and corporations. According to Bennett, the research conducted ‘supports a number of generalizations about the Internet and activist politics, four of which are reported here. The intriguing feature of each generalization is that communication practices are hard to separate from organisational and political capabilities, suggesting personal digital communication is a foundation of…identity-driven subpolitics’ (Bennett, 2003: 12). Bennett’s Patterns of Communication were chosen as the framework within which to situate the analysis of online communities in Chapter Seven because, following the conclusion of the social media analysis relating to the terrorist attacks in Madrid in 2004, it was determined that the eventual composition of the online community groups was most similar to that outlined by Bennett’s Patterns of Communication. The nature of the communities analysed in the thesis, as outlined in greater detail in Chapter Seven, is described by Bennett himself; ‘Various uses of the Internet and other digital media facilitate the loosely structured networks, the weak identity ties, and the issue and demonstration campaign organizing that define a new global politics. In particular…[specific] configurations of digital networks facilitate: permanent campaigns, the growth of broad networks despite (or because of) relatively weak social identity and ideology ties, the transformation of both individual member organizations and the growth patterns of whole networks...[t]he same qualities that make these communication-based politics durable also make them vulnerable to problems of control, decision-making and collective identity’ (Bennett, 2003: 33).

Although Bennett’s Patterns of Communication is the framework employed throughout Chapter Seven of this thesis to understand the nature of online communities, it is not without limitations. There exist alternative patterns of communication, which describe the formation of online communities that have not been used in this work.

One model used to describe the nature and composition of online political discussion is the Liberal Individualist model of communication which encompasses four separate traits particular to online discussion, which are monologue; a trait in which the user exercises his or her own desire to express themselves at the expense of dialogue, personal revelation; the propensity for the disclosure of information about oneself in a public computer mediated forum, and similar to another trait seen in liberal individualist communication, which is personal showcasing, defined as the tendency for people to reveal details about themselves by using online portals as advertising platforms for self-created content and finally, Liberal Individualist communities are characterised by the presence of flaming which is defined as ‘hostile intentions characterised by words of profanity, obscenity and insults that inflict harm to a person or an organisation resulting from uninhibited behaviour’ (Freelon, 2010: 8).

Another communication model outlined by Freelon for the enhanced understanding of online communities is the Communitarian Model. The communitarian model refers to online public spaces ‘that are predominantly communitarian, uphold the cultivation of social cohesion and group identity above the fulfilment of individual desires. The communitarian model can be characterised by the following five traits which are ideological fragmentation, mobilization, community identification, in-group reciprocity and in-group questioning’ (Freelon, 2010: 9).

Ideological fragmentation refers to the extent to which online users organise themselves into online communities which are politically homogenous, as communitarian groups rarely, if ever, engage with others from outside. Mobilisation refers to the extent to which online users who more naturally fit into the communitarian model are most likely to mobilise for political action, either online or offline.

Another measure of the communitarian model is the extent to which members of that community envision themselves, as part of a community, or the propensity for intra-ideological response. Similarly, intra-ideological questioning is considered to denote one’s propensity to engage with other users within the community or group.

Chapter Eight presents the main conclusions of the thesis, including policy recommendations and suggestions for future research. Following the research conducted within the previous chapters, the author contends that the term Terrorism 3.0 should be introduced to conceptualise the nature of online behaviour in relation to the issue of terrorism and reflect the fact that society is currently in the transition towards Web 3.0, a transition that is already partly but unevenly realised. The analysis in this thesis, which has examined how different groups have engaged with Web 1.0 and Web 2.0 in the 2004-11 period, helps identify how online users are likely to understand and make use of Web 3.0. In order to demonstrate the saliency of the conclusions reached in the thesis, and the transition to Terrorism 3.0, an analysis of online behaviour and discussions in Spanish language related to the death of Osama bin Laden was carried out in real-time (1-5 May 2011). As a terrorism-related event that indirectly relates to Spain, and one, it was anticipated, that it would generate extensive interest and activity from online users, the findings reflect the expediency and complexity inherent within the conclusions outlined in the chapter. The chapter concludes by asserting that the emergence of Terrorism 3.0 requires that new internet research approaches are necessary in order to gain insight into the optimal ways of engaging with citizens to prevent another terrorist attack. If such knowledge is to be attained then it could lead to new ways of conducting counter-terrorism, which place socio-technical and influence-focused methods at its nucleus.

## The Internet, the Web and Society

This particular chapter maps the various determinants that explain the development of the internet and the World Wide Web, setting out the different ways in which each actor influences the eventual development of these technologies. As such, Chapter One - and the eventual thesis – will untangle what Latour calls the “sociotechnical mess” through a study of the understandings of the relationships between technology, terrorism and counter-terrorism in Spain.

It is also important to consider the role played by new Web technologies in affecting the extent to which the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives. This thesis, and Chapter One in particular, considers the ways in which technologies that comprise Web 3.0 will affect general online users’ perceptions of how terrorist or counter-terrorist organisations use communication technologies and investigates ways in which counter-terrorism practitioners can act upon this.

This chapter will also contend that national governments exert significant influence over the development of the internet and the Web, something that is exemplified by the raft of official legislation that has been implemented with the intent of wresting greater control over the social and technical development of the Web and the internet. These laws place controls on the unregulated development of the internet and the Web, particularly since the terrorist attacks on the United States of America (US) on 11 September 2001, the Madrid terrorist attacks on 11 March 2004 and the London bombings on 7 July 2005. Technology-focused legislation, such as the Regulation of Investigatory Powers Act and the *Ley de Economía Sostenible*, as will be elaborated upon further, has a palpable and direct effect on the nature of the underlying technical constructs inherent within the internet and the Web.

Chapter One will posit, therefore, that a social constructivist approach should be adopted when conceptualising the development of the internet and the Web, as socio-technical constructs where social and cultural artefacts are both embedded in their technical architecture, as well as the content that is subsequently created by their users. For the purpose of this thesis, the referent term “constructivism” or “constructivist” refers to that defined within the framework of the theories comprising the social construction of technology. Therefore, this thesis will utilise the definition offered by the scholar Langdon Winner (1993) as a framework in which ‘to look carefully at the inner workings of real technologies and their histories to see what is actually taking place. It recommends that rather than employ such broad-gauged notions as technological determinism or technological imperatives, scholars need to talk more precisely about the dynamics of technological change. Rather than try to explain things through such loosely conceived notions as the trajectory of a technical field or technical momentum, we need to look very closely at the artefacts and varieties of technical knowledge in question and at the social actors whose activities affect their development’ (Winner, 1993: 365). It is crucial that a definition of social constructivism, as it pertains to science and technology studies, be made in order to avoid misinterpretation between the social constructivist framework as it applies to International Relations (Wendt, 1992).

As such, it is analytically pertinent to consider these technologies as figurative and physical spaces where the attitudes and behaviours of users can and are influenced by the strategic objectives of other actors, since other actors not only communicate within these spaces, but can also impact how these spaces are made. For instance, the formation of the internet and the Web are shaped, in part, by regulation, monitoring and the actual adaption of information spaces by state counter-terrorism organisations and private sector actors in response to terrorist organisations’ use of these spaces. The internet does not emerge from a vacuum or technical exercise but through social and political interactions. In addition to this chapter outlining the ways in which various actors shape the development of the internet and the Web, the wider thesis will also demonstrate how these technologies are in turn used by certain groups and organisations to influence the attitudes and behaviours of online users to ensure the success of their own communication objectives. This will be investigated in greater depth in chapters Four, Five, Six and Seven.

It is the author’s intention in this chapter to demonstrate the notion that social, political, economic and civil society actors influence the development of the internet and the Web. It seeks to explain the nature of their influence using a number of complimentary theoretical frameworks.

The subsequent development of the internet and the Web brought about by the collective influence of the identified actors will highlight how these actors use the pre-determined technology to achieve their own objectives and, finally, contend that the advent of new technology such as Web 3.0 will be influential in shaping understandings on the relationships between technology, terrorism and counter-terrorism in Spain.

The ongoing commercial development of the World Wide Web and the internet has done much to encourage their widespread adoption by a great number of people. The facility to send and store electronic information quickly and safely has bequeathed innumerable benefits for billions of people. The demand for general access to a cost-effective, reliable internet connection has facilitated the adoption of these technologies in an increasing number of countries (Rice, 2008). It is clear, however, that some countries have greater access to this technology than others. Internet penetration[[4]](#footnote-4) as a percentage of regional populations is lowest in Africa and Asia at 11.4 per cent and 23.8 per cent respectively, in comparison to significantly higher measures in other regions such as Europe, which stands at 58.3 per cent (Internet World Stats, 2011). The strong increase in the number of internet users in the period 2000 to 2011 has led an expanding number of supranational organisations to proclaim that unrestricted internet access is an incontrovertible human right (Global Network Initiative, 2008, La Rue, 2011).

Societal-level changes have been enabled by the continued evolution and development of the internet and the Web. The path of this development, which will be documented in subsequent sections of this chapter in stages, has been denoted Web 1.0 and Web 2.0 for analytical clarity. Indeed, their development has progressed to the point of the emergence of a radically different iteration of the Web, controversially termed Web 3.0 (Markoff, 2006, Mitra, 2006, Anderson & Raine, 2006, Spivack, 2006, Bratt, 2006, Provost & Bornier 2009). The use of the title Web 3.0 has generated contention amongst information technology experts because, it is argued, the term is an oversimplification of the technologies, similar to the term ‘Web 2.0’, and there is in fact no new version of the Web. The influential information technology entrepreneur Tim O’Reilly argued; ‘[a]las, I find the Web 3.0 arguments as clear evidence that the proponents don’t understand Web 2.0 at all’ (O’Reilly, 2007: 1).

However, champions of Web 3.0 believe the term neatly encapsulates the emergence of a markedly different iteration of previous and current versions of the Web, most saliently in the various technological developments currently underway at the core level of the Web. These developments enable Web 3.0, amongst other things, to connect a greater number of people and devices to its architecture and simultaneously make available a vastly greater amount of data for individual users in a more intuitive fashion, based on a history of their online behaviour and other users displaying similar preferences. This development, an umbrella term for a number of different technological innovations, collectively comprises the Semantic Web and the internet of things[[5]](#footnote-5) (Berners-Lee, 1999), enabling the Web to effectively understand meaning and context after interacting with a particular user and fitting within the more macro-level conceptual definition of Web 3.0. Currently, the most effective way of sourcing relevant information on the Web for a general user is to utilise a proprietary search engine to retrieve previously indexed information and Web pages based on keywords inputted by individual users.

## Theoretical Framework Underpinning the Development of the Internet and the Web

‘There is an old rule of sociological method, unfortunately more honored in the breach than the observance, that if we want to understand social life then we need to follow the actors wherever they may lead us’ (Law & Callon, 1988: 284)

Scholars such as Jacques Ellul have opined that technology is developed in a vacuum, created and introduced to the market, subsequently ameliorating or deteriorating the function of a society. Ellul claimed ‘technology is produced for its own sake with no regard for human need’ (Kranzberg, 1986: 545). An ostensibly similar but more nuanced view on the relationship of technology to society is also evidenced in the writings of scholars such as Marx (2007). In his treatise, *Capital*, he claimed that the nature of man and society were closely bound by the state of productive forces or technology:

‘Technology discloses man’s mode of dealing with Nature, the process of production by which he sustains his life, and thereby also lays bare the mode of formation of his social relations, and the mental conceptions that flow from them’ (Marx, 2007:406).

Contemporary experts, such as *The Guardian*’s Spain Correspondent Giles Tremlett, also support Marx’s viewpoint that technology on its own has a direct and discernible effect on society. In commenting on the potential effects that technology has had on Spanish terrorism, Tremlett claimed that the increasing development of the internet and the Web had led to a commensurate decrease in the number of terrorist attacks committed:

“Well historically in Spain…[technological development has] coincided with a decrease in terrorism. You know, if you were going to do it statistically, you’d have to say that the effect was inverse”[[6]](#footnote-6).

Other scholars have commented on the notion that technological development occurs in a deterministic fashion, but that it should be conceptualised in a more nuanced way. Bruce Bimber, for example, argued that use of the term technological determinism is imprecise and contended that it should be theorised using three labels – Normative accounts, Logical Sequence accounts and Unintended Consequences accounts. Technological determinism is a reductionist theory, the proponents of which claim the existence of a causal relationship between technology and society. Chandler (1995) wrote of technological determinism: ‘[it is the] particular technical developments, communications technologies or media, or, most broadly, technology in general [as] the sole or prime antecedent causes of changes in society, and…as the fundamental condition underlying the pattern of social organization. Technological determinists interpret technology in general and communications technology in particular as the basis of society in the past, present and even the future. They say that technologies such as writing or print or television or the computer “changed society”. In its most extreme form, the entire form of society is seen as being determined by technology: new technologies transform society at every level, including institutions, social interaction and individuals’ (Chandler, 1995: 1).

Bimber’s Normative account can be conceptualised as technological development that is shaped by the goals and judgments of the people who develop technology as ‘their actions follow certain culturally accepted norms and are sanctioned by politically legitimized forms of power’ (Bimber, 1990: 3). In addition, we can see how Bimber’s normative account of technological determinism, as will be outlined later in this chapter, could be used to analyse how civil society and technical developers contribute both ideologically and physically to technological development. Bimber posits that the Normative Account should not be conceived as technological determinism because the approach does not focus on the effect of the technological artefact in shaping society. Rather, it is human agency that is given primacy over technological development, which, he claims, is neither technological nor deterministic (Bimber, 1990).

When discussing the Unintended Consequences account, Bimber outlines that it refers to the unplanned outcomes of technological development. He uses the example of the development of automobiles in which contemporary models are fitted with a host of environmental protection technologies such as catalytic converters. This type of technological development, Bimber argues, was not previously conceived by the original architects of the technology and can therefore be defined as a specific form of technological determinism (Bimber, 1990). According to Bimber, this also suggests that technological determinism occurs independently of human intervention and will, a completely different interpretation of technological development to that offered by Wanda Orlikowski, as will be outlined subsequently. Bimber claimed that Unintended Consequences could not be termed as technologically deterministic as it is impossible to overlay the unpredictability of human actions to technological development. He writes that ‘[u]nintended consequences are basic facets of social action rather than the special products of technology…These accounts are also neither technological nor deterministic’ (Bimber in Roe Smith & Marx (eds.) 1994: 89).

Finally, the Logical Sequence account refers to the type of technological development that occurs according to the laws of society and nature. As an example, Bimber claims that a society that built railways would have exhibited a natural tendency to build the telegraph and large-scale steel production (Bimber, 1990). This form of technological development, Bimber claims, is the truest form of technological determinism because it offers an explanation of technological development independent of human intervention, which means they can therefore be classified as strictly deterministic. He adds that Nomological Accounts are the most deserving of the title technological determinism because society evolves along a set path, independent of human interaction, a path set in motion by the technology itself ‘and it’s parent, science’ (Bimber in Roe Smith & Marx (eds.) 1994: 89).

However, for the purpose of this thesis, the notion that technology alone has a direct effect on society, otherwise known as technological determinism, is rejected. The causal theoretical framework underpinning technological determinism fails to incorporate the myriad other forces at work that manipulate the development of these technologies, such as political and economic influences as well as the roles played by other actors such as civil society organisations and multinational corporations. The scholar Bruno Latour, in particular, was critical of technological determinism as a theory providing an adequate understanding of technological development. He argued that, in order to accurately explain such developments, one must consider the aforementioned facets impinging upon the development of technology, such as technical, political, economic and scientific determinants, which together form the “sociotechnical” conception of technological innovation. At this point, it is worth quoting Latour at length:

‘[G]oals, scenarios, tactics for [the] constitution, mobilisation and juxtaposition and the obduracy of materials – these though they overlap and do not necessarily occur in a clear sequence, are the features that between them determine the character of technological innovation. Most important however, is the fact that they all have to do more or less indifferently with the technological, the scientific, the political, the economic and the social…If we wish to understand innovation, for most purposes we should not think of the social and the technological as being different in kind. In particular, we should not assume that it is necessarily the social that moulds the technological, nor indeed the converse. Rather, we should say that it is the sociotechnical, and note that the least malleable part of the system – that part which most affects the structure of the rest – varies from system to system. We have, therefore, to embrace the heterogeneity of sociotechnical systems if we are to understand the way in which artefacts are created’ (Latour, 1988: 22).

Here we see Latour’s interpretation of technological development explained as the resulting interactions of various social and technological influences, which can be analysed within contemporary political theory. For the purpose of this thesis, Latour’s socio-technical viewpoint will be used as the theoretical basis. The socio-technical foundation does much to help analyse the nature of the behaviour of online communities, how communication works online and, importantly, the understandings that exist of the relationships between the internet, terrorism and counter-terrorism in Spain. The development of the internet and the Web, it is proposed, is heterogeneous in nature due to the complexity of the factors involved in their creation. Instead of assuming technological changes will automatically produce changes in terrorist and counter-terrorist practices, from a socio-technical starting point, the goal rather is to explain *how* technology, terrorism and counter-terrorism interact, with analysis open to unforeseen relationships. Such an approach will also enable the generation of new hypotheses for research beyond this thesis.

Socio-technical explanations for the development of the internet and the Web highlight the range of elements involved in its evolution and the strong degree to which they overlap and influence each other. As a result of the cross-pollination of actors and influences dictating technological development, it is useful to consider the role of Actor-Network Theory in explaining the inter-relationship between the actors involved and the development of these technologies because; ‘different materials – people, machines, “ideas” and all the rest – …[are] interactional effects rather than primitive causes…and more importantly…[Actor Network Theory][[7]](#footnote-7) says that we should be exploring social effects, whatever their material form, if we want to answer the ‘how’ questions about structure, power and organisation’ (Law, 1992: 7).

Law’s argument, that an understanding of the social effects is critical in order to gain a more holistic understanding of the processes driving the development of technology is central to the focus of this chapter and the thesis more generally. Using Law’s proposition, it is possible to ascertain how the influence of dominant political ideologies, corporations, civil society actors and governments form a complex network which, when analysed as a whole, provides a more complete account of the technological advancement of the internet and the Web. Put differently, Actor-Network Theory highlights the interdependence of these elements in relation to the development of the internet and the Web.

In addition, Michel Callon claimed that techno-deterministic assumptions of technological development are insufficient, that they do not explain the uneven development of technological artefacts, nor the revolutionary impact that technology at times has on society. He therefore posited that there is a multitude of actors influencing the development of technology called the techno-economic network (TEN). This is defined as a ‘coordinated set of heterogeneous actors which interact more or less successfully to develop, produce, distribute and diffuse methods for generating goods and services’ (Callon in Law ed., 1991: 135).

Callon outlined that TENs are created around three distinct poles: the scientific pole, places such as research institutes and universities where scientific knowledge is created, the technical pole where technological artefacts are manipulated and developed, finally, there is the market pole, which refers to the group of users and consumers who use such technological artefacts.

Within these poles, Callon claimed that there are four intermediaries which facilitate relationships between the actors mentioned previously. They are texts, or literary inscriptions such as patents, books and reports, technical artefacts such as consumer goods and machinery, human beings (including the skill and knowledge they bring to the network), and, fourthly, Callon identified money as the final intermediary. In this way, Callon defined actors as ‘any entity able to associate texts, humans, non-humans and money’ (Callon in Law ed., 1991: 140).

There are, however, weaknesses associated with ANT. In his analysis of ANT and political power, the scholar Rolland Munro claimed that although a useful concept, ANT did not go far enough in fully explaining power relations. In particular, he claimed that ANT only paid attention to associations and links which seemed “strong” and did not focus on weaker links in networks. He wrote that ‘research in sociology and ANT has to open up to asymmetries in power that do not only nurture ephemeral, but rely on the intermittency of such links’ (Munro in Clegg ed., 2009: 135).

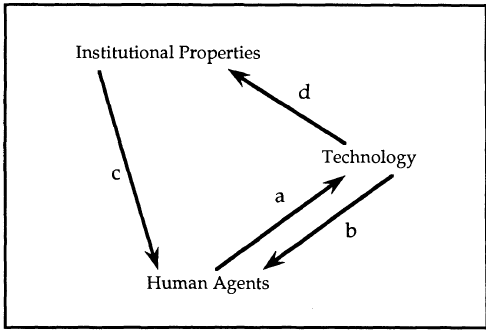
The concept of ANT also gives rise to another useful theory explaining the dominant forces influencing the development of these technologies, which emphasises that individual actors are simply the manifestation of another network of social, political and technological influences, Foucault’s theory of governmentality.

The philosopher Michel Foucault defined governmentality as a phenomenon that ‘views practices of government in their complex and variable relations to the different ways in which “truth” is produced in social, cultural and political practices’ (Dean, 1999: 18). This definition can be extrapolated, for the purpose of this chapter, to explain how government actors assert greater control of Web and internet development by passing specific legislation that has a palpable effect on the technical elements that can be incorporated into its development. Governmentality can be used to explain how corporations, for example, develop software and hardware that help governments achieve their strategic objectives. This can encompass, for example the monitoring of internet user online behaviour. In turn, as corporations develop this software, it can engender the notion that such online controls are indeed part of the normative structure of technological development, and that some users come to expect and feel comfortable in the presence of such monitoring and control.

What has become apparent is that the actors mentioned above are ‘products of power circulating through society in capillary fashion’ (Lipschutz in Berenskoetter & Williams (eds.), 2007: 230). They collectively influence each other and together shape the intrinsic features of the internet and the Web. It is this vision of technological development that represents a distinct change from the original vision held by engineers and scientists that causes consternation amongst influential scholars. Jonathan Zittrain is one such scholar who expressed concern at the current influences shaping the development of the Web, claiming that ‘[a] lockdown on…[the use of the internet] and a corresponding rise of tethered appliances[[8]](#footnote-8) will eliminate what today we take for granted: a world where mainstream technology can be influenced…Stopping this future depends on some wisely developed and implemented locks, along with new technologies and a community ethos that secures the keys to those locks among groups with shared norms and a sense of public purpose, rather than in the hands of a single gatekeeping entity, whether public or private’ (Zittrain, 2008: 5)*.* Although Zittrain laments the perceived negative effects of widespread governmentality, he also expresses confidence that communities of evangelists will come together to realign the ‘lock down’ of the Web and the internet. These communities are currently comprised of civil society organisations such as Human Rights Watch and the Open Source Software movement. Such entities, Zittrain claims, are essential if these technologies are to remain true to the aspirations of their creators and become the true repository of humanity’s knowledge available to all.

In addition, the scholar Wanda Olikowski (1992, 2000, 2006) linked her assessment of the development of technology to the social theorist Anthony Giddens’ theory of structuration (1984). Giddens claimed that social systems, such as technology, could be better understood as properties of social structures ‘which presumably have been built into the technology by designers during its development and which are then appropriated by users as they interact with this technology’ (Orlikowski, 2006: 29). Although Giddens’ theory of structuration was not specifically designed for technology, Orlikowski deemed it useful to adapt the theory to explain that technology, such as the development of the internet and the Web, is more complex than a one-dimensional technical explanation would provide. Socio-technical processes and the technologies produced do, in fact, have considerable human agency which can have unintended effects on the end user. Orlikowski built on Giddens’s work by offering a Structurational Model of Technology, which is illustrated in the diagram below:

Figure Three: Structurational Model of Technology



Source: Orlikowski (1992: 410)

In explaining the model, Orlikowski contended that technology is only created by humans as exemplified by arrow a. Using this model to explain the use of technology in organisations, Orlikowski added that technology mediates human action because ‘[a]nyone who has used a typewriter, telephone, computer, hammer, or pencil can attest that technology facilitates the performance of certain kinds of work’ (Orlikowski, 1992: 411).

Orlikowski’s structurational model of technology shows that the development of technology is more than the collection of technological components that comprise the collective artefact, similar to Latour’s concept of a “socio-technical mess”. A one-dimensional argument would yield an incomplete analysis, missing the interdependencies involved. This chapter will now seek to identify the different elements driving the development of the internet and the Web by charting the chronological development of these technologies, in order to provide the reader with a clearer definition and coherent understanding of the different elements influencing their development. It will also offer insight into the main technological components comprising future Web technologies such as the aforementioned Web 3.0. This analysis offers context for subsequent explorations of relations between the internet, Web and terrorism in Spain. Unpacking how these technologies operate (both as tools and infrastructures) is important for explaining the contemporary actions and understandings of terrorism and counter-terrorism organisations.

## Evolution of the Internet and the World Wide Web

### The Internet

The first physical iteration of the internet was realised in 1962 by the Massachusetts Institute of Technology (MIT) lecturer J.C.R. Licklider who conceived of the ‘Galaxy Network’, a collection of computers that could access electronic data from any computer terminal. At the same time, a different MIT researcher, Lawrence Roberts, developed the concept of packet switching, the transference of data in packets of information, replacing of the hitherto traditional circuits, which had been used as part of the telephone network. The United States Department of Defense, Defense Advanced Research Project Agency (DARPA) and Roberts funded the Advanced Research Projects Agency Network (ARPANET), the first packet switching communications system. By the late 1960s, ARPANET had been installed in four US universities, the University of California Los Angeles, Stanford University, the University of California Santa Barbara and the University of Utah. The contemporary internet used the original ARPANET as a template for sending packets of information quickly, cheaply and efficiently over long distances.

The most influential facet that eventually shaped the entire architecture of the internet was the implementation of the open-architecture network. The adoption of the open-architecture network, a system whereby internet service providers had the freedom to choose any network architecture to which they could connect without being penalised, by utilising a specific kind of technology, was crucial in fostering the internet as a global communications medium and embodiment of free and unhindered access to information. It was through this “Internetworking Architecture” (Leiner et al, 2003: 1) that widespread communication between computers became possible and not dictated by technical specifications set by a particular corporation or organisation such as the government.

The internet continued to be utilised in the academic realm until the development of the Transmission Control Protocol / Internet Protocol (TCP/IP), which facilitated the development of instant communications technologies such as email, and subsequently the general commercialisation of the personal computer.

### The World Wide Web

The Web was conceived by the former European Organisation for Nuclear Research (Organisation Européene pour la Recherche Nucléaire, CERN) researcher Tim Berners-Lee under similar motivations as that for the internet. At CERN, Berners-Lee also had the idea of devising a computer-based system which would sanction the easy retrieval and storage of scientific data amongst the various researchers. Perhaps the most salient aspect of the early iteration of the Web is Berners-Lee’s vision of a system facilitating the ‘decentralised, organic growth of ideas, technology and society…It is a vision that provides us with new freedom, and allows us to grow faster than we ever could when we were fettered by the hierarchical classification systems into which we bound ourselves’ (Berners-Lee, 1999: 2). Berners-Lee therefore ensured that his version of the Web would be extensively used by capitalising on the geographic proclivity of the internet in combination with the successful commercialisation of the personal computer. Since its initial conception, the Web has undergone a number of different iterations, leading to the widespread implementation of the forthcoming Web 3.0. A more detailed explanation of the different versions of the Web is given below.

### Iterations of the World Wide Web

Web 1.0 can be described as the development and implementation of a range of key software applications such as Hypertext Transfer Protocol (HTTP), Internet Message Access Protocol (IMAP) and Internet Protocol (IP) to name but a few. The development of these technologies allowed users to share information via networked computers facilitated by the internet. Crucially, these technologies, created during the initial development of the Web, saw the creation of Hypertext Markup Language (HTML) and Web pages, which could be navigated using Web browsers such as Netscape and Internet Explorer. This stage of development for the Web also saw the creation of key online portals for activities such as search and electronic commerce such as Google and Amazon, in addition to the implementation of numerous software platforms such as Java and Flash. Web 1.0 was a read-only platform, insofar as users were able to access information from a particular Web page but not contribute to the alteration of that data, or create and upload their own information unless they had prior technical expertise.

Web 2.0 is conceptually and technically different from Web 1.0 as it allows for enhanced participation from its users. Industry analysts and scholars have described Web 2.0 as ‘the read-write Web, where we started seeing “…all of these services that make it easy for us to contribute content and interact with others”’ (Wells, 2006: 1). In this fashion, the onset of Web 2.0 saw the development of front-end services including folksonomies, social bookmarking, media sharing and social collaboration[[9]](#footnote-9).

Web 3.0 is technically different to the other two iterations of the Web. The technical focus has been applied to back-end development by making Web protocols more interoperable and lowering the barriers that prohibited widespread internet access. Web 3.0 allows the development of new software platforms, which lie outside the scope of those defined as Web 2.0, such as Resource Description Frameworks, SPARQL and the Web Ontology Language (OWL). The development of these protocols, in particular, will eventually herald the implementation of one potentially influential technology, the Semantic Web, a term used to describe a Web where all knowledge and information is available and can be understood by the aforementioned protocols. If the Semantic Web allows knowledge to be more easily understood by new Web protocols then ‘software will essentially become able to understand knowledge, and create new knowledge. In other words, software will become more intelligent’ (Spivack, 2007: 1).

While Semantic Web technologies will signal the convergence of new software and hardware making the Web more intelligent and intuitive, the third generation of the Web will also signal the advancement of further technological trends. Perhaps the most significant of these is the increased penetration of mobile technologies such as cellular telephones, and tablet computers[[10]](#footnote-10). The increased uptake of mobile technologies with Web access, combined with the intuition of the Semantic Web, means that significantly greater numbers of people, particularly those from developing countries, will be able to access vast repositories of information. Web 3.0 will also see the maturity of other technologies which are currently operating principally within a Web 2.0 framework such as distributed computing and other open technologies such as open source software, cloud computing and the internet of things[[11]](#footnote-11). Again, these technologies will have the effect of unpacking the information stored on the Web, and that generated by other people, into a system, which encourages the free and open contribution and retrieval of information.

Some industry experts have attempted to define Web 3.0, claiming that it ‘implies a seamless integration of devices. Your data moves with you and knows where you are’ (Roberts, 2007: 1). Collectively, these different technologies are indicative of the new version of the Web where, according to the scientist Ray Kurzweil, ‘several major technology trends…are about to reach a new level of maturity at the same time. The simultaneous maturity of these trends is mutually reinforcing, and collectively they will drive the third-generation Web. From this broader perspective, Web 3.0 might be defined as a third-generation of the Web enabled by the convergence of several key emerging technology trends’ (Kurzweil, 2006: 1).

This chapter will now examine the roles played by different actors and contexts influencing the development of the internet and the Web. Its aim is to present a clearer landscape of the roles played and the reasons explaining this development. The socio-political forces that initially inspired the development of the Web and the internet continue to encourage its development today. This chapter also investigates how technical actors, responsible for the development of the Web, incorporated their own normative values into the fabric of these technologies, heavily influencing the ways in which people use them and, by association, interact with each other.

In addition to the pivotal role played by the actors responsible for the technical development of these technologies, this analysis also stresses the importance of civil society and non-state actors in the development of the internet and the Web. These elements, which together comprise the overall focus of this chapter, aim to provide the reader with a clear definition of the internet and the Web and a coherent understanding of the different elements influencing their development.

## What Inspires the Development of the internet and the World Wide Web?

The internet and the Web do not develop in a vacuum; rather there are a great many different actors with equally differing motivations that influence development. This section examines the nature of some of those shaping developments, including social and political contexts, governments, civil society organisations and corporations.

### Social and Political Contexts

One of the main factors involved in the development of the internet and the Web can be seen in the dominant social and political ideologies which originally encouraged the initial development of these technologies. The *realpolitik* that dominated the Cold War landscape of 1960s global politics made the possibility of a nuclear attack distinctly conceivable. In the event of such an attack, government departments and military officials from the US mandated that a communications system be developed that was impervious to nuclear attack in order to ensure the continuation of government. Manuel Castells argued that in order to withstand an attack from a nuclear device, this communications system would have to resemble a decentralised network, ensuring that an attack on one node would not result in the complete destruction of the entire structure. He also argued that the internet was originally designed as ‘a network architecture that, as its inventors wanted…[could not] be controlled from any centre, and is made up of thousands of autonomous computer networks that have innumerable ways to link up going around electronic barriers’ (Castells, 2000: 6).

The development of the Web was fashioned in a similar way. The Cold War still dominated strategic policymaking for world governments during the time of its development in the 1980s. Although not intended as a military application, Berners-Lee aimed to construct a communications system utilising computers to permit the easy storage and retrieval of electronic information. His overarching vision was for a system that would allow any user of the internet and the Web to access and contribute information to this system, which would eventually reflect the collective accumulation of the knowledge of humanity, something that was not in keeping with the ideology of containment and enlargement adhered to by the US and its allies during the Cold War (Berners-Lee, 1999).

It is especially important when considering the influence of the dominant social and political ideologies on the initial development of the internet and the Web that the reader understands some of the theoretical frameworks used to explain power in the political context. A clearer understanding of the theories of political power that informed the continuation of the Cold War will do much to shed light on one of the principal forces stimulating those involved in technological development. Realist international politics and neoliberal economics provided the backdrop to the initial development of the internet and the Web. Realist power politics provided the scope for the creation of the internet and neo-liberalism allowed for the commercialisation of both technologies on a global scale.

The race to develop and gain a competitive advantage in weapons and technology between the Soviet Union and the United States and their various allies represented the overriding concern during the Cold War. The Cold War was principally fought against the backdrop of realist power politics where military planners maintained the belief that military power determined overall security in the international arena. Political realism was most poignantly demonstrated in the race by the two superpowers and their primary allies to stockpile nuclear weapons as a means of guaranteeing state-survival from the 1950s to 1989. Realism was also the driving force behind the race for technological pre-eminence amongst the two superpowers, with both sides believing strongly that technological superiority directly correlated to military supremacy; realism ‘depicts international affairs as a struggle for power among self-interested states and is generally pessimistic about the prospects for eliminating conflict and war’ (Dunne & Schmidt in Baylis & Smith (eds.) 2001: 145). The demonstration of political realism translated to the practice of offensive realism in the pursuit of technological supremacy as both the United States and the Soviet Union sought to ensure security by becoming the most influential actor in international politics. It was, therefore, this scramble for technological dominance as a means of ensuring military security that gave rise to the perception of the necessity for an impregnable communications system to mitigate a possible attack from which the United States believed it was vulnerable (Layne, 2006).

A separate theoretical framework significantly influenced the early development of the internet and the Web by extending the use of these technologies by the military and academic institutions towards the private sector and the general public. Devolving responsibility for the development of these technologies to the private sector thus enabled neo-liberal free-market economics to bring their influence to bear and was an important step in developing the internet and the Web to their current iterations. The technologies were therefore allowed to develop in the 1970s according to the dictates of global supply and demand and ultimately become one of the core technological frameworks of contemporary global society. Indeed, the US Government actively promoted the involvement of the private sector in technological advancement as part of its post-Cold War programme of ensuring political and economic globalisation as a truly worldwide phenomenon. This intention was elucidated by international relations scholar Andrew Bacevich who commented on the government’s strategy of ensuring global economic, political and social openness; ‘robust and continuing economic growth is an imperative, absolute and unconditional’ (Bacevich, 2002: 79). Here, we can see how the US Government linked the development of technology, particularly communications technology, strongly to notions of national and global security, therefore applying the principle of neo-liberalism. This subsequently led, during the 1990s, to the creation of the first electronic commerce websites such as eBay and Amazon, the first search engines such as Google and Ask, and the provision of the first Web-based electronic mail services such as Hotmail and Yahoo! Mail. As will be outlined below, once the development of the Web and the internet were principally entrusted to the hands of private actors, it is clear that they did much to drastically alter the original purpose of the Web and the internet in the eyes of their creators (Couldry, 2004).

Although one of the important elements in the development of Web 3.0 is the increasing number of users connected to these technologies, principally via greater access to internet-enabled mobile devices[[12]](#footnote-12), these technologies are being used under the condition that influential actors retain the ability to control production of data generated by users of their particular network architectures (BBC News, 2010: 1). As a result, some governments have implemented legal measures to counteract terrorism such as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT) in the US (2001) and the United Kingdom Counterterrorism Bill (2008). These Acts seek to restrict the free and unfettered use of the Web by the citizenry by providing governments with the right to monitor online behaviour and access hitherto private information, such as the content of emails and telephone conversations. These measures demonstrate how the contemporary political backdrop has led some governments to reassert control over the development of the internet and the Web, and away from the original vision of a decentralised platform for information exchange. This indicates governments’ continued understanding of technological development through the prism of political realism at a time when citizens and interests are threatened by, what Philip Bobbitt calls ‘market state terror’[[13]](#footnote-13) (explored below) (Bobbitt, 2008).

It appears that technological development is understood as a zero-sum situation defined by the ability to exert political control over the internet and the Web. This is in contrast to the vision outlined by the early pioneers of the technologies who advocated the free and unfettered sharing of information. In this way, Langdon Winner’s assertion that ‘artefacts may, indeed, have politics’ (Winner, 1983: 16) becomes a distinct possibility.

### Government

Although government actors played a marginal role in the early development and commercialisation of the Web, it is clear that national governments are active participants in influencing contemporary developments of these technologies.

One of the major ways in which government directs the development of the internet and the Web is by implementing legislation that not only enhances but extends its control over the activities of its citizens. An example of this is the Communications Assistance for Law Enforcement Act (CALEA) (1994) in the US, which maintained the ability of law enforcement agencies to conduct online surveillance by mandating companies to modify their equipment and software to facilitate this. Another example of legislation that effectively exerts its influence over the development over the Web and the internet is the Regulation of Investigatory Powers act in the UK (RIPA) (2000). This Act also allows the UK Government to intercept communications if it deems its contents to be a threat to national security. It has been suggested that the UK Government initiated this act as a response to the growth in the use of the internet and the Web in the latter part of the 20th century, and the introduction of strong encryption of online content (The Register, 2008). In 2011, the Spanish Government approved the implementation of the Sustainable Economy Law (*Ley de Economía Sostenible*) in which it decreed that it had the power to close down any website that had peer-to-peer links to copyrighted material in order to cease illegal file sharing (La Moncloa, 2011).

The passing of legislation that compels internet users to act in concert with a government’s strategic objectives is particularly significant, as businesses that are responsible to their shareholders now also become responsible to the mandates of national governments. Commenting on internet neutrality and the CALEA legislation, the scholar Susan Crawford claimed that ‘[a]ll prudent businesses will want to run their services by law enforcement…service providers would be well advised to seek guidance early, preferably well before deployment of a service, if they believe that their service is not covered by CALEA…DOJ [US Department of Justice] would certainly consider a service provider’s failure to request such a guidance in any enforcement action’ (cited in Lessig, 2006: 63).

The examples given above of governments’ ability to pass legislation that reasserts influence on the development of the internet and the Web not only demonstrates how the original vision of the Web as a source of free information is being eroded, but also suggests that governments can influence the behaviour of citizens indirectly by controlling technological development directly.

This perspective of government influence over technological development was highlighted by Foucault who claimed that the use of forces such as language, politics and economics, embodied in such elements as nationwide legislation, would ‘normalise’ society, whilst having the will of government prevail on a given issue. Foucault called this process ‘governmentality’. Indeed, the process of governmentality shows governments’ ability to use structural power to impose rules on society and then productive power to inflict a set of normative edicts, which reinforce the notion that it is right that they have access to such information. Foucault describes the process by which influence is exerted indirectly by government actors, writing ‘the mechanisms of power [in] its capillary form of existence, the point where power reaches into the very grain of individuals, touches their bodies, and inserts into their actions and attitudes, their discourses, learning processes and everyday lives’ (Foucault, 1980: 28).

The notion of governmentality shaping the development of the Web was also highlighted by the internet scholar Lawrence Lessig who claimed that ‘government wants to regulate [behaviour], but…cannot regulate directly. [Hence,] the government thus regulates that behaviour indirectly by directly regulating technologies that affect behaviour. Those regulated technologies in turn influence or constrain the targeted behaviour differently’ (Lessig, 2006: 70).

That governments play an intrinsically important role in the development of the internet and the Web is clear. This role is brought to bear in the ability of governments to establish certain normative structures which influence other actors such as corporations, technical developers and civil society actors.

### Technical Developers

The continued development of the internet and the Web can also be explained by the efforts of various technical actors involved in the creation of these technologies. It is clear that the creators of both held particular viewpoints and ideals about the way in which these technologies should be constructed, and these ideals permeate the fabric of the internet and the Web to this day. The software and hardware engineers behind the development of the internet, for example, envisioned the technology as facilitating the free and unfettered sharing of information and communication, most clearly seen in the efforts to fashion the internet into a communications network facilitated by the Internetworked Architecture. In this sense, hardware and software designers can therefore be conceptualised as social and political as well as technical engineers.

In creating the Web, Tim Berners-Lee held a similar idea. He believed in the creation of an information storage and retrieval system that was at once free and easily accessible to everyone. It was this facility to contribute to the collation and evolution of the world’s knowledge that informed the overall vision of the Web:

‘[l]ike the Internet, the Semantic Web will be as decentralized as possible…Decentralization requires compromises: the Web had to throw away the ideal of total consistency of all of its interconnections, ushering in the infamous message “Error 404: Not Found” but allowing unchecked exponential growth…The real power of the Semantic Web will be realized when people create many programs that collect Web content from diverse sources, process the information and exchange the results with other programs. The effectiveness of such software agents will increase exponentially as more machine-readable Web content and automated services (including other agents) become available. The Semantic Web promotes this synergy: even agents that were not expressly designed to work together can transfer data among themselves when the data come with semantics’ (Berners-Lee, Hendler & Lassila, 2001: 1).

From this perspective, technology acquires its own capacities to do things: to connect content and user data to produce new patterns and knowledge, which in turn shape behaviour. The ideals of free, decentralised communication and collaboration envisioned in the initial iterations of the Web and the internet can also be seen in the values held by actors influencing the current Open Source Software movement[[14]](#footnote-14). Open Source Software, which has been developed with its source code freely available to all who wish to modify it, is unlike closed-source proprietary software development, during which engineers who do not have authorisation from the owner of a particular software patent are prohibited from freely modifying its source code. Companies such as Microsoft, Apple and Sun Microsystems have dominated the closed-source software market by protecting their source codes under national and international intellectual property law. However, certain organisations develop Web-based software under the auspices of the Open Source Software agreement, such as the Mozilla Foundation and Linux. The technologies developed by the companies – most notably Mozilla’s Firefox Web browser and the Linux operating system – are used extensively by major corporations and individual users alike, doing much to undercut the use of established software programs like Microsoft’s Windows Operating System and Apple’s Safari Web browser.

It is also clear that open source technologies, which utilise the efforts of disparate epistemic communities to develop robust, peer-reviewed software, adhering to the principles of the pioneers of the internet and the Web, are part of a collection of technologies that seek to undermine the influence of multinational corporations that develop software for the market place with the source codes for their products secured (Mozilla, 2011: 1). They collaborate in groups, using their collective expertise to produce software that people can download or modify free of charge. One can also see how in Hannah Arendt’s terms, influence in the realm of software development is creative, ‘something productive, as a phenomenon of empowerment emerging through togetherness exemplified in non-violent resistance movements’ (Berenskoetter 2007 in Berenskoetter & Williams eds., 2007: 4). The actors who sought to create a space that inspired unrestricted communication and the free sharing of information in the 1960s and 1980s, continued today by non-profit organisations, were, in the words of Arendt, ‘acting in concert, creat[ing] something new that has not been there before’ (Berenskoetter 2007 in Berenskoetter & Williams eds., 2007: 4). Through their willingness to collaborate in Web and internet development whilst defying the closed-source model of software development, these technical actors were collectively empowered to influence the development of these technologies.

The notion that technological artefacts have a direct impact on society is something that has long been propounded in the framework of technological determinism (Chandler, 1995, Shaw, 1979, Asimov, 1980). However, a closer examination shows that the social values built into these technologies influence the very way in which they are used and can do much to destabilise traditional loci of power, such as corporations or states. This is also a view shared by Manuel Castells, who argued ‘for years to come, nation states will struggle to control information circulating in globally interconnected telecommunications networks. I bet it is a lost battle. And with this eventual defeat will come the loss of a cornerstone of state power’ (Castells, 2000: 259).

The most important feature of the influence of developers of the Web and the internet is the notion that the ability to create such technology is itself a form of power:

‘[F]or citizens of cyberspace…code…is becoming a crucial focus of political contest. Who shall write that software that increasingly structures our daily lives? As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed. They are the ones who set its nature. Their decisions, now made in the interstices of how the Net is coded, define what the Net is’ (Lessig, 2006: 79).

Here we see how the internet studies scholar Lawrence Lessig frames his conception of software and hardware engineers as assuming power capacities, as their ability to write code directly impacts the behaviour of ordinary users of such technologies. Lessig’s interpretation, while compelling and salient for the purpose of this chapter, is also flawed. While he correctly attributes an increasing level of influence to engineers thanks to their ability to affect user behaviour, he pays little attention to the power structures influencing the software engineers in the same way that a Foucauldian/governmentality approach would. The fact that relatively little reference is made to the socio-technical influences on software and hardware engineers means that Lessig’s interpretation only relates to part of the full compliment of actors currently influencing the development of the Web and the internet.

### Civil Society

Although a definition of civil society could strictly consist of non-profit organisations such as the aforementioned Mozilla Foundation, this section of the analysis will focus on the role played by non-government organisations, non-state actors and activists.

The influence that civil society has brought to bear on the development of the internet and the Web can be seen in various ways. Influential non-governmental organisations have campaigned against the censorship of online information by governments. Since the widespread adoption of the internet and the Web, organisations such as Amnesty International and Human Rights Watch have, in their campaigns, propounded liberal, democratic values, that access to information is a human right and that governments should not restrict general access to technology or hinder freedom of speech. Such a declaration was offered by Amnesty International in its “Irrepressible Campaign” against global internet repression (2006). The organisation claimed that internet repression in countries such as China, Burma, North Korea and Zimbabwe was tantamount to a violation of human rights and that their governments should permit the free and unfettered flow of information to their citizens. A similar report was commissioned by Human Rights Watch entitled ‘False Freedom: Online Censorship in the Middle East and North Africa’ (Human Rights Watch, 2005). It claimed that Middle Eastern governments using software called SmartFilter purchased from a US computer security company were blocking numerous websites with political content.

These grassroots campaigns by civil society groups do much to influence the development of the internet and the Web because they exert pressure on governments’ top-down form of control over the technologies. Campaigns such as these, which attempt to wrest control of technological development and, in particular, freedom of information, away from corporations and governments and back into the hands of individuals, are proving to be champions of the ideals held by the original developers of the internet and the Web. Campaigns such as Irrepressible and the Global Network Initiative seek to ensure that a Web as decentralised as possible emerges, in place of a platform under the control of governments and corporations for the purpose of maximising the power and influence of a relatively low number of actors.

A second example of civil society actors seeking to influence the development of the internet and the Web is the creation of Psiphon and the Onion Network, Web proxy servers that provide access to sites which would be otherwise restricted in countries like Syria, China and Iran. Although its creators warn potential users that use of the technology could violate national and international law and incite the possibility of severe repercussions in certain countries, Amnesty International supported the release of the software, claiming that ‘an increasing number of brave activists are evading censorship and using the Internet to impart and receive information about human rights…We hope that the new Psiphon software will also help people express their peaceful political views online’ (Fiveash, 2006).

Another prominent example can be seen in the active online privacy movement which campaigns against the surveillance of online behaviour. The activities of No2ID and Privacy International in the UK focused on lobbying against the creation of surveillance technologies such as identity card systems or nationwide databases of personal information. The actions of these organisations highlight that collectively, civil society organisations have managed to challenge the power of influential actors such as central governments or multinational corporations (Berenskoetter & Williams, 2007), a notion that was supported by the scholar Lance Bennett who commented that the internet and the Web help civil society organisations fragment into groups and form networks, leaving them better placed to challenge hitherto powerful actors (Bennett, 2003).

A final example of a civil society group or non-state actors influencing the development of the internet and the Web is the presence of actors such as terrorist organisations. Contemporary terrorist organisations are more likely to organise themselves into small cells and form complex networks to launch attacks on states and their people (Bobbitt, 2008, Soriano, 2010). Although accounts of these groups using the Web to perpetrate their attacks are replete in counter-terrorism literature (Sageman, 2008, Conway, 2005, Prentice et al. 2010, Wilton Park, 2010), comparatively little has been written about their impact on the development of the Web. Much of the existing literature analyses the ways in which terrorist organisations utilise the Web as a tool to facilitate their organisational goals. As a result, scholars such as Gabriel Wiemann have written about the ways in which terrorist organisations use the Web to fulfil their strategic objectives such as recruitment, propaganda and reconnaissance (Wiemann, 2008). Certain internet and political violence scholars, on the other hand, analyse the impact that groups of hackers can have in propagating cybercrime and possibly cyberterrorism (Denning 2002). Other scholars focus on the ways in which contemporary terrorist organisations use the internet and the Web to facilitate their operational goals of working in small networked cells to instigate attacks (Bobbitt, 2008, Arquilla & Ronfeldt, 1999, Barnett, 2005). However, the activities of terrorist groups have consequently prompted a forthright reaction from civil society groups, who create Web-based software in order to circumvent more attacks. Examples of this include the University of Arizona’s Dark Web Terrorism Research project and the SOMA Terror Organization Portal (STOP) which attempt to ‘let experts query automatically learned rules on terrorist organization behavior, forecast potential behavior based on these rules and network with other analysts examining the same subjects’ (Networked World, 2008).

The emergence of such projects has created tension between organisations which would use internet technologies to terrorise publics, and those which attempt to counter such behaviour. This tension can be seen to have an impact on the development of the internet and the Web by the creation of software that monitors the nature of online behaviour of internet users. As such, Lessig’s assertion that the creation of code has social and political ramifications can be conceived in this case, as such software continually monitors and analyses the characteristics of terrorist websites and forces the creators of such content to find new places to express their ideas or to modify their behaviour altogether (CQ Researcher, 2009).

### Corporations

Corporations have had a strong influence on the development of the internet and the Web. For instance, corporations have conceded to the demands of governments and developed code or software which shapes the Web to fulfil the needs of such organisations (demonstrating that technology is not created in a vacuum). This is underscored in the alteration of Yahoo! and Google’s policies of freedom of information in China in 2006. These companies obeyed the wishes of the ruling government to restrict the amount of information available to Chinese citizens to a level it deemed suitable, curtailing Chinese citizens’ access to information on issues such as democracy, Tiananmen Square and the Dalai Lama. Google claimed that the move was necessary as ‘[f]or several years, we’ve debated whether entering the Chinese market at this point in history could be consistent with our mission and values…We ultimately reached our decision by asking ourselves which course would most effectively further Google’s mission to organize the world’s information and make it universally useful and accessible. Or, put simply: how can we provide the greatest access to information to the greatest number of people?’ (McLaughlin, 2006: 1). This case is a prime example of the way in which corporations are able to restrict internet users’ “information horizons” (Fisher, forthcoming) in the name of meeting the demands of free-market economics and the policies of a particular state.

Corporations can also influence the development of the internet and the Web by developing technologies which prioritise the maximisation of profit over the wellbeing of users. This is exemplified by the realisation that the Web is more useful to commercial activities if it is able to robustly recognise user identity. Corporations are, therefore, engaged in adding capabilities to Web content and services to ascertain the true identities of its users because, according to the scholar Lawrence Lessig, ‘with the original Internet: everyone was an invisible man. As cyberspace was originally architected, there was no simple way to know who someone was, where he was, or what he was doing. As the Internet was originally architected, then, there was no simple way to regulate behaviour there’ (Lessig, 2006: 38). An example of a corporation exerting its influence to obtain detailed user identity data can be seen in the commercial trial of behavioural advertising technology by British Telecommunications PLC in 2006 which monitored and analysed the browsing behaviour of its users to display advertisements related to the accrued information. Critics of the technology claimed that it violated people’s rights to privacy, while supporters claimed that it was simply serving the needs of the market and that it would help consumers make better-informed choices (Williams, 2008: 1).

Similarly, corporations have added geo-location authorisation code to Web content, making it more difficult for people to freely access data. This geo-location authorisation requires users to enter an identification code or display an internet protocol (IP) address related to a specific country before they are able to access information. Such an example can be seen in the access to certain sites such as Pandora.com from users outside the US. As a result of music copyright restrictions, Pandora.com will not grant full access to its site to users outside the US.

The influence exerted by corporations on the development of the internet and the Web can be considered pervasive, as seen in the variety of ways they are able to influence the behaviour of citizens by adhering to the demands of governments. This dovetails with Foucault’s definition of governmentality, as corporate influence in the development of the internet and the Web is shown to be a parameter forming and system-shaping sort. This is reflected in the way that corporations can create software that surreptitiously directs the behaviour of users.

## Conclusion

This chapter has presented Foucault’s notion of governmentality and Bruno Latour’s conception, from science and technology studies, of the socio-technical mess as theoretical constructs that help explain the development of the internet and the Web, constructs that are more analytically useful than techno-determinist approaches.

The development of both the Web and the internet has been more extensive since the end of the Cold War due to the globalisation of the internet and the fact that it has become essential to the functioning of nation states. This, according to Bobbitt (2008), has facilitated the rise of market states, which in turn has encouraged the evolution of what he terms market states of terror. These conceptions will be addressed in Chapter Two.

This introductory chapter has shown that the relationship of the internet with terrorism and counter-terrorism is a close one. This is seen in examples of actors who use the internet to intercept communications and also those who attempt to regulate what communications are possible and shape the development of the technology itself.

The objective of this thesis, as will be demonstrated in the conclusions presented in Chapter Eight, is to analyse understandings that exist of the relationships between technology, terrorism and counter-terrorism in Spain. The research question will be analysed using the ancillary theoretical questions described previously, namely: how are these understandings explained? What interactions have emerged as a result of these interactions? What is the effect or overall result of these interactions? What more could be done to positively influence these understandings? The thesis will then test these questions through the empirical analysis of data from publications, papers, policy decisions, interviews with experts in both English and Spanish languages and, original, unobtrusive research methodologies using Web-based content. The analysis of social media content will provide insight into the nature of discussions and behaviour of online communities. It is anticipated that collectively, this thesis will yield an original, systematic study of technology, terrorism and counter-terrorism in Spain and contribute to discussions on policymaking and strategy.

# **Chapter Two: Terrorism, Counter-terrorism and Public Diplomacy in Spain**

## Introduction

The complexity of Spain’s dual security problem has compelled the Government to adopt a ‘comprehensive approach’ to counter-terrorism. The adoption of a socio-technical solution is different to that of other nation states.

The overarching research question of *what* *understandings exist of the relationship between technology, terrorism and counter-terrorism* *in Spain* is examined in greater detail in this chapter. While Chapter One analysed the theoretical frameworks related to the development of the internet and the Web, this chapter explores the development of terrorism in Spain as it relates to theoretical frameworks offered by the scholars Thomas P.M. Barnett and Philip Bobbitt.

This chapter examines further the notion of complexity in social and technical systems. Chapter One focused on untangling the nature of power and influence as it relates to technological development, particularly that of the internet and Web. Chapter Two unpacks contemporary Spain’s official responses to terrorism and juxtaposes them with the official responses of the French Government by outlining the history of terrorism activity in both countries from 1980 to the present day.

France was chosen as the country with which to compare Spain’s official responses to terrorism due to the geographic proximity of the countries and their shared experiences of terrorism, the most prominent being ethno-nationalist terrorism. In spite of these similarities, however, Spain and France have responded to terrorism in very different ways as will be analysed subsequently.

The theoretical frameworks offered by both Bobbitt and Barnett will contribute to the analysis explaining the reasons for such differing official responses. In addition, this chapter examines further the context elected in which to test the hypothesis formulated in Chapter One; the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives.

This chapter analyses and outlines that while France has relied upon technological solutions to mitigate its terrorist threat, Spain has opted instead to tackle, in the words of Prime Minister Zapatero “the root causes of terrorism” (Alianza de Civilizaciones, 2011), favouring a mixture of technological and diplomatic responses. Extrapolating from the conclusions offered in Chapter One, the official responses demonstrate France’s preference towards prioritising a technological deterministic counter-terrorism policy: an understanding that access to high technology enhances its capabilities to counter terrorism. Spain, on the other hand, appears to have opted for a policy that refutes the main hypothesis, believing that technology-focused solutions alone will not solve the challenges of terrorism it faces and favouring a socio-technical response.

## Theoretical Approaches to Terrorism in Spain

Terrorism in Western Europe is not just a contemporary phenomenon. The Basque terrorist organisation Euskadi Ta Askatasuna (ETA), which operates principally between the borders of North-eastern Spain and South-western France, is one of the most readily identifiable terrorist organisations in the world, having been in existence in its present form for the past 40 years, and in that time perpetrating hundreds of attacks (Moore, 2005). Indeed, while the Spanish government focused on containing the threat of ETA both during and after the Franco dictatorship, France was simultaneously combatting ethno-nationalist terrorism by Corsican and Marxist separatists (Human Rights Watch, 2005). In recent years, however, the threat of terrorism has evolved from that posed by the aforementioned organisations to that of international terrorist organisations operating in both Spain and France (Chau, 2008).

Spain and France administer sophisticated counter-terrorist programmes specialising in multilingual intelligence gathering and analysis, military response and terrorism-specific jurisprudence (Gutiérrez, 2005). However, the cultivation of effective counter-terrorism programmes and organisations was in part, a pyrrhic victory, motivated in response to the deaths of hundreds of people resulting from attacks in both countries. Both countries justified the implementation of far-reaching, and at times violent, counter-terrorism measures in the 1980s and 1990s as necessary steps to decrease the threat of terrorism within their borders, and Europe at large, strongly identifying themselves to be part of the vanguard against the encroachment of contemporary terrorist organisations into Western states (Michavila & Guerra, 2005). This perception is held for a variety of reasons; the most salient of which concerns the perceptions of policymakers in Spain and France in their identification of an ‘Arc of Conflict’ (Présidence de la République, 2008), a group of states from the Maghreb to South Asia which together present a perceived threat to state interests. In addition, the close geographic proximity of Spain to the Maghreb region, including the location of the Spanish enclaves of Ceuta and Melilla, which lie close to Moroccan territory (Ministerio de Defensa, 2003), provides policymakers with cause for concern. The commensuration of the issue of high rates of immigration to Spain, as shown in Figure Four, with the threat of terrorism, and the subsequent securitisation of immigration, will be analysed in detail in Chapter Four.

Figure Four: Inflows of Immigrants to Spain and France from 1999 to 2008

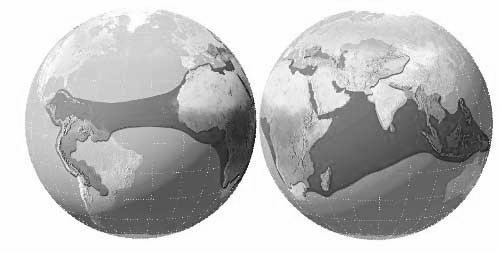
Source: OECD Statistics

It is intriguing to note that the aforementioned ETA, long considered a high priority terrorist threat to both the Spanish and French Governments by the security services, came into being in its present form at approximately the same time as the internet was created in 1959 (Jaruegi, 2006). The Cold War was dominant on the political landscape and the US Government was actively promoting its policy of containment and expansion. The notion that the Cold War was predicated on the ‘containment of Soviet territorial temptations through military and economic power [and] expansion through alliances, bases, investments and bribes’ (Ikenberry, 1999: 2) intimates strongly that territorial sovereignty during this time was of overriding importance for ethno-nationalist organisations and states alike. This tenet is affirmed when one considers that ETA’s motivation behind its campaign for independence of the Basque state lies in its perception that the Basque country is under occupation by the Spanish State (Jaruegi, 2006).

With the Cold War ending in 1989, and the US Government dispensing with the policy of containment and enlargement, openness of the global economic, political and security system, commonly termed “globalisation”, became the dominant paradigm in International Relations. It is clear, however, that in addition to globalisation providing the conditions for greater economic and political integration amongst states, principally via the use of electronic communications technologies, it had the secondary effect of globalising the terrorist threat facing nation states and Spain and France in particular.

A wealth of opinions have been offered by scholars who claim that globalisation has either changed or enhanced the terrorist threat faced by nation states, one of which was expounded by the political scientist Thomas P.M. Barnett. He claimed that terrorism, and particularly international terrorism, results from the failure of certain countries to adjust to globalising forces. He added that terrorism, particularly international terrorism, was especially likely to emanate from states which remained ostracised from the “Functioning Core” of economically, politically and militarily bound states. Countries in the “Non-Integrating Gap”, according to Barnett, include, amongst others, states in the Maghreb, the Middle East, South Asia and Africa and are noticeable by their high levels of poverty, civil unrest and rampant political instability (Barnett, 2005). The Non-Integrating Gap is marked in shade in Figure Five below:

Figure Five: The Pentagon’s New Map



Source: Thomas P.M. Barnett, 2005.

Barnett claimed that such political instability, increased migration from unstable regions and above all, failure to adhere to economic and political rules imposed by leading globalising states subsequently manifested into increased security threats to those states in the Functioning Core. As a result, he stipulated that it is incumbent upon those in the Functioning Core to incorporate into the process of globalisation those states residing in the non-Integrating Gap or face the possibility of further violence crossing over the borders into those in the Functioning Core. He put it that;

‘[I]n this century, it is disconnectedness that defines danger. Disconnectedness allows bad actors to flourish by keeping entire societies detached from the global community and under their control. Eradicating disconnectedness, therefore, becomes the defining security task of our age. Just as important, however, is the result that by expanding the connectivity of globalisation, we increase peace and prosperity planet-wide’ (Barnett, 2005: 8).

Barnett is not alone in his proclamation that globalisation is a potentially dangerous phenomenon unless participated in by all nation states. Other globalisation and terrorism scholars, such as Moisés Naím, claimed that the terrorist attacks on the US in 2001 underscored the need to better understand people and organisations residing outside globalisation’s “natural” borders or risk the influx of more violence. He argued that ‘[t]hanks to al Qaeda, everyone knows that globalization goes well beyond the links that bind corporations, traders, financiers, and central bankers. It provides a conduit not only for ideas but also for processes of coordination and cooperation used by terrorists, politicians, religious leaders, antiglobalization [sic] activists, and bureaucrats alike...[t]he terrorist attacks showed that political globalization is as powerful a phenomenon as the globalization of the economy’ (Naím, 2005: 1).

In addition to comments made by Naím, other authors such as Thomas Friedman in the ‘Lexus and the Olive Tree’ (Friedman, 2000), Samuel Huntingdon in the ‘Clash of Civilisations’ (Huntingdon, 2002) and Benjamin Barber in ‘Jihad Vs McWorld’ (Barber, 1992) have all penned in various discourses that international terrorism can be explained as a direct reaction to the states in the Functioning Core that have benefited from global economic, political and military integration while others in the non-Integrating Gap have not. Other scholars, such as Michael Mann, have extrapolated on Barnett’s argument by relating the upsurge in violence in the non-Integrating Gap to their wholesale neglect and virtual exclusion of the process of globalisation by the members of the Functioning Core (Mann, 2002).

This perception that international terrorism is the negative aspect of globalisation helps explain the nature of the terrorist threat faced by both Spain and France, though the presence of al-Qaeda-inspired terrorism inside and outside the core does problematise this conceptualisation (Hoskins & O’Loughlin, 2010). Nevertheless, Barnett writes that a policy of greater inclusion in the globalising process with countries in these regions would do much to decrease the possibility of further attacks and ensure greater security for states. However, there is another compelling interpretation of the increase in international terrorism that dovetails with the current situations in both Spain and France.

The US scholar Philip Bobbitt proposed in *Terror and Consent: Wars of the 21st Century* that the nation state, which he outlined exists to maximise the welfare of the population, is currently evolving into a market state, which, he argued, ‘does not see the state as more than a minimal provider or redistributor. Whereas the nation state justified itself as an instrument to serve the welfare of the people (the nation), the market state exists to maximise the opportunities [of its citizens]. Such a state depends on the international capital markets and, to a lesser degree, on the modern multinational business network [including the news media and NGOs]…in preference to management by national or transnational political bodies. Its political institutions are less representative (though in some ways more democratic) than those of the nation state’ (Bobbitt, 2008: 42). As nations morph into market states, he claimed that threats facing these states will change and terrorist threats will generally utilise internet-based technologies to organise themselves in accordance with (or as a reflection of) the state it directs its attacks against, and propagate attacks. Indeed, Bobbitt claimed that:

*‘Market state terrorists evade attempts to suppress them and enhance their power through the adroit use of modern communications technology, especially the Internet…*the Internet allows al Qaeda to communicate its strategy even while its leaders are in hiding…which once would have meant defeat and marginalization but is now easily overcome’(Bobbitt, 2008: 57, emphasis in original)*.*

Bobbitt’s assessment of the role of globalising forces such as technology in the propagation of international terrorism is particularly salient in evaluating the predicament facing both Spain and France. The hypothesis that globalisation of nation states, enabled by technologies such as the internet and the Web, will encourage new threats is also reconcilable with Barnett’s theory as both scholars hold similar sentiments that technology largely facilitates the operational strategies of terrorist organisations. However, the two theories become estranged at points, as Barnett argues that terrorism is caused by an absence of globalising forces in the non-integrating gap. Bobbitt, on the other hand, proposes that the evolution from nation states to market states will, by implication, spawn new market-style forms of violence, most prominently in the guise of international terrorism.

Bobbitt’s hypothesis above is similar to that posited by the scholar Audrey Kurth Cronin who claimed that contemporary terrorism is not only a reaction to globalisation but is also driven by it. She puts it that ‘the fact that so many people in so many nations are being left behind has given new ammunition to terrorist groups…and spurred Islamic radical movements to recruit, propagandize, and support terrorism throughout many parts of the Muslim world’ (Cronin, 2003: 55).

Other terrorism scholars have made attempts to explain the causes of terrorism in light of the widespread introduction of the internet and the Web. In outlining his investigation in the context of the history of the phenomenon, David Rapoport claimed that terrorism occurred in “waves”; ‘four successive, major waves of terror have washed over the world, each with its own special character, purposes and tactics’ (Rapoport, 2001: 420). He contended that ETA belongs to the third wave of terrorist organisation, which he claimed is characterised by international acts of terrorism in which the revolutionary ethos was comprised of international dimensions. However, this wave began to dissipate in the 1980s as concerted efforts by states to defeat these organisations became successful (Rapoport, 2001). Fourth Wave Terrorism, contended Rapoport, is characterised by its ability to transcend state boundaries, using religion as an ideological framework. He outlineed that this facet is important when referring to Jihadism in explaining how Fourth Wave Terrorism’s ability to transcend national boundaries can be facilitated by high technology such as the internet and the Web. Indeed, the 11 March 2004 terrorist attacks (11-M) television and documentary producer Justin Webster commented of al-Qaeda, ‘[t]he fourth wave’s parallel for the PLO’ (Rapoport, 2001: 427), that “it is impossible to imagine al-Qaeda without the internet”[[15]](#footnote-15)

The scholar Marc Sageman argues that the union of terrorism and the internet and the Web creates arrangements whereby terrorist organisations are no longer comprised of fixed hierarchical structures. Rather they are now comprised of groups of loosely connected individuals who are attracted to certain ideas from terrorist ideologies. The connection of such individuals, which he classifies as a third wave of Jihadism, is eminently facilitated by contemporary communications technologies ‘[terrorists] form fluid, informal, networks that are self-financed and self-trained. They have no physical headquarters or sanctuary, but the tolerant, virtual environment of the Internet offers them a semblance of unity and purpose. Theirs is a scattered, decentralized social structure – a leaderless jihad’ (Sageman, 2008: 2). Sageman’s viewpoint which places primacy on the role of the internet as a force multiplier is also emphasised by Post, Ruby & Shaw (2000) who argued for the presence of information terrorism, which is defined as the ‘definition of terrorism plus “through the exploitation of computerized systems deployed by the target”’ (Post, Ruby & Shaw, 2000: 99). In addition, as increasing numbers of people become increasingly acquainted with the internet and the Web, this will lead to specific online group dynamics whereby groups are less formal and people can share ideas more easily and connect with more people than they would be able to without the technology (Post, Ruby & Shaw, 2000).

However, it has also been predicated that contemporary terrorism that uses high technology is simply a product of modernity and that the use of such technology by terrorist organisations such as al-Qaeda was inevitable. Martha Crenshaw for example argued thirty years ago that modernisation was a significant permissive cause of terrorism increasing both the opportunities for and complexity of terrorist organisations, whilst enhancing the vulnerability for states (Crenshaw, 1981: 381). Crenshaw’s viewpoint is similar to that espoused by the political scientist Robert Imre today who claims that while technology is having a demonstrable effect on terrorist organisations, the impact of high technology is overstated and terrorism fundamentally has not changed: “I really think that the role of technology has been overplayed. I mean to me, and we can get into a much deeper question about what technology does…So perhaps we’ve increased the capacity for people to talk further distances, but I’m not sure how that influences particular types of terrorist activity.”[[16]](#footnote-16)

Imre’s notion that, although modernisation and technologies such as the internet and the Web have an impact, they are essentially force multipliers that should not be conflated with the intrinsic nature of terrorism, is highlighted again by Jamie Bartlett, Head of Violence and Extremism at the UK think tank DEMOS. He argued that terrorism is inherently more complex and difficult than consuming terrorist content online; “if you’re willing to blow yourself up or other people up, I think it takes more than spending time online, looking at images and talking to people online. You need the face-to-face interaction and more importantly you need the training, which is what you can’t get from the internet. Like I said, bomb making is harder than people think”.[[17]](#footnote-17)

This thesis’ central focus on *The Pentagon’s New Map:* *War and Peace in the Twenty First Century* by Thomas Barnett and *Terror and Consent: Wars for the Twenty First Century* by Philip Bobbitt as the dominant theoretical paradigms was maintained for a number of reasons that will be explained in this section.

As outlined previously, a close reading of Bobbitt’s *Terror and Consent: Wars for the 21st Century* brings into sharper focus some of the arguments put across by Bobbitt in his previous thesis *The Shield of Achilles: War, Peace and the Course of History* (2003). In it, one of Bobbitt’s principal arguments follow his contention that the intrinsic nature of the Nation State is in flux, following its evolution from various other constitutional orders throughout the course of history. The other constitutional orders identified within the book include the Princely States, Kingly States, Territorial States, State-nations and Nation States. Most noteworthy, however, is Bobbitt’s contention that the Nation State, whose basis for legitimacy is found in its stated mandate to maximise the welfare of its citizens, is developing inexorably into, what he defines, a Market State. Bobbitt claimed that ‘the legitimacy of the constitutional order we call the nation-state depended upon its claim to better the well-being of the nation’ (Bobbitt, 2003: 25). The principal *raison d’être* of the Market State, Bobbitt asserts, is to maximise the opportunities for its citizens, as defined previously in this chapter.

It was, therefore, the contention of the author that Bobbitt’s analysis of the changing nature of the state within his two major works, and particularly his analyses of the problems that are likely to emerge from such changes, were central to the policymaking trajectory of the Spanish Government at the time of the terrorist attacks in Madrid in 2004. This viewpoint is particularly well exemplified in the creation and deployment of certain elements of Spanish counter-terrorism policy after the terrorist attacks in Madrid in 2004, such as Zapatero’s counter-terrorism policy that emphasised integration and dialogue between Spain’s citizens and Muslim residents. It is for this reason that the author deemed that the focus of Bobbitt’s thesis in *Terror and Consent: The Wars of the Twenty First Century* dovetailed well with the policies of the Spanish Government at the time of the terrorist attacks and, therefore, serve as an apt theoretical paradigm within which to place the focus of the thesis.

It was also the assertion of the author that a close reading of Thomas Barnett’s *The Pentagon’s New Map: War and Peace in the Twenty-First Century* conveyed a suitably useful theoretical paradigm within which to situate the thesis. This contention is particularly well founded when applied to the nature of counter-terrorism policymaking in Spain before the terrorist attacks in Madrid in 2004. Barnett’s principal argument in his thesis contends that the world can be divided into a Functioning Core and a non-Integrating Gap (Barnett, 2005). This theory is extremely close to the security and counter-terrorism policymaking dictates of the Spanish Government both before the terrorist attacks and in their immediate aftermath. It was most notably evinced in the policy edicts that emanated from the Government, particularly the Strategic Defence Review of 2003 in which it announced its intention to segment its focus on the terrorist threat facing the country into national and foreign threats. This, in many ways, is similar to the Core and non-Integrating Gap theory of terrorism and strategic threats as outlined by Barnett. It is, therefore, the author’s contention that the two works by Barnett and Bobbitt were elected for their close theoretical and ideological positions to that of the Spanish Government both before, during and after the terrorist attacks.

The focus of this thesis on the works by Barnett (2005) and Bobbitt (2007) can be justified by their theoretically close accord with other academic research conducted in relation to terrorism in Spain, particularly that research which originates from Spain. For example, the prominent terrorism scholar Javier Jordán contends that the nature of Jihadism in Spain necessitates that those involved in the movement utilise globalisation to perform certain operational tasks such as logistics, recruitment and propaganda (Jordán, 2003). Jordán claims that those involved in Jihad use Spain as a European base for their operations. This perspective merges well with Bobbitt and Barnett’s perspective of the tensions and challenges faced by Market States and states in the Core.

In addition, Jordán contends that the growth in Jihadist activity in Spain is due to a pervasive undercurrent of discontent directed at Spain’s foreign policy by those sympathetic to the philosophy of Jihaidism (Jordán, 2003, 2006). The nature of this discontent is witnessed most starkly in the widespread protests against the invasions of Iraq and Afghanistan, announced by the Aznar and Zapatero administrations respectively. Above all, Jordán emphasises that Spain experiences significant concerns with national and international terrorism as it contends with Jihadist terrorism from abroad in addition to terrorist activity from ETA. It is clear, therefore, that Jordán’s perspective, while focused on a Spanish context, complements main arguments put forward by Barnett in in *The Pentagon’s New Map: War and Peace in the Twenty-First Century*.

Barnett’s thesis also corresponds strongly with the theoretical paradigms offered by another prominent Spanish terrorism academic, Fernando Reinares (2006, 2010). His research on the demographic make-up of Jihadist terrorism in Spain argued that those involved in such groups are generally not of Spanish descent and Muslim (2010). This perspective echoes the thesis by Barnett who emphasised the tensions that could arise as a result of flows from states in the non-Integrating Gap and the Core. In the case of the research by Reinares, the inherent problems brought forth by globalisation’s flows are focused entirely within a Spanish context.

In addition to the arguments proffered by leading Spanish academics, it is clear that other scholars align the theoretical paradigms of their work alongside that of other prominent academic works, thereby justifying this author’s reasoning for the focus on these particular works.

John Esposito, in his book *Who Speaks for Islam? What a Billion Muslims REALLY Think* (2008), stated that the increase in globalising forces can be perceived by some to directly affect Islam, such as certain actors like Osama Bin Laden and, by implication, the wider Al-Qaeda movement. Such globalising forces, as a result, place pressure on the citizens of the Arab world and wider adherents to the creed of Islam. It is this sentiment that Bobbitt and Barnett echo in their theoretical paradigms previously outlined when they claim that globalising economic and security ‘rule-sets’ (Barnett) and the rise of the ‘market state’, fostered by globalising forces (Bobbitt), will lead to unforeseen consequences such as terrorism if not adequately tempered.

In addition, it is wise at this stage to consider the work conducted by Stevens and Neumann (2009), in which they claimed that the increasing global reach of the internet and other related technologies has lowered the barrier to entry for engagement with radicalising content and terrorism. Their claim stems from research into the cessation of online radicalisation conducted for the Centre for the Study of Radicalisation and Political Violence. In their paper, they draw up a strategy to counter the occurrence of online radicalisation including deterring online users from creating such content, empowering online communities to counter online radicalisation, reducing the appeal of radicalising messages and finally promoting the appeal of positive messages (Stevens and Neumann, 2009: 49). The authors also argue that government measures to simply remove radicalising content are generally counter-productive. The UK Government should create an environment in which the creation of such content is at once unacceptable and less desirable, as well as technically difficult. This argument corresponds closely to that made in Bobbitt’s thesis in which he outlines the potential for the unfettered implementation of globalising forces, especially the internet, to cause extensive problems for the continued development of Market States of consent.

Similar claims were made by the prominent terrorism scholar Bruce Berkowitz (2002) who argued that governments and counter-terrorism agencies should make better use of technology for more accurate and, by implication, more effective intelligence analysis in order to prevent more major terrorism attacks.

One prominent voice supporting the viewpoints made by Bobbitt (2007), comes from Jarret Brachman (2006) who argued that Al-Qaeda has transformed itself from a terrorist organisation into a social movement as a result of their use of the internet and other related, widely available technologies. Brachman contended, therefore, that governments and counter-terrorism organisations should study the online statements and dialogue by Al-Qaeda members and ideologues as a priority, as these statements inevitably serve to empower groups of new recruits by influencing their overall worldview. He claims that websites such as the Al-Hesbah discussion forum and the Syrian Islamic Forum, serve as portals through which people can interact with terrorist ideologies. Again, it is possible to witness parallels in the arguments offered by Brachman and the theoretical frameworks offered by Barnett and Bobbitt, as the nature of globalising forces to enhance the appeal and reach of terrorist organisations is the overriding element between them.

The influential role of communications technologies to foster widespread discontent and discourses of radicalisation in the context of terrorism was also examined closely by O’Loughlin, Bordeau and Hoskins in their paper *Distancing the Extraordinary: Audience Understandings of Discourses of Radicalisation* (2011). The authors conducted discourse analysis of interviewees in France and the UK with the aim of analysing their responses to radicalising discourses in the media. The findings of the analyses contend that audiences and publics are ‘diffuse entities which exist by virtue of being regularly addressed, whose membership is uncertain, but through which understandings of common matters of concern are forged…[r]ather than understanding radicalisation as merely a diffuse threat, it can also be seen as a phenomenon embedded within tangible struggles involving identifiable actors such as government security agencies or journalists’ (O’Loughlin et al., 2011: 162).

Indeed, the tensions between globalisation and contemporary security threats outlined in Bobbitt and Barnett’s theses come into sharper focus when we consider the framework proposed by Hoskins and O’Loughlin of Diffused War (2010, 2011, 2010, 2010). Hoskins and O’Loughlin proposed that the nature of Diffused War is seen in the increasingly frequent conduct of war through media services with the aim of engaging larger audiences. The components of the Diffused War model are such that ‘(i) the mediatisation of war (ii) makes possible more diffuse causal relations between action and effect, (iii) creating greater uncertainty for policymakers in the conduct of war’ (Hoskins and O’Loughlin, 2010: 3). Therefore, the nature of Diffused War, particularly the notions of mediatisation and nonlinear causality, means that modern communications technologies, one of the embodiments of globalisation, can attract a larger audience to terrorist content, and thereby fortify the conceptual linkages between the works by Barnett and Bobbitt.

These linkages between globalising forces, such as the media and terrorism were explored by Brigitte Nacos who examined the extent to which the terrorist attacks on the US on 11 September 2001 achieved their media goals (Nacos, 2003). Nacos claimed that the attacks on that day were very aware that ‘the mass media of communication [was]…central to furthering their publicity goals and even their religious objectives. Without the frightening images and the shocking reportage, the impact on Americana and the rest of the world wouldn’t have been as immediate and intense as it was’ (Nacos, 2003: 30). The idea that the terrorist attacks on the US would not have had the same impact were it not for the extensive network of global media networks replaying the images to a worldwide audience is central to the theses of both Bobbitt and Barnett and is something, they claim, of which counter-terrorism agencies and government departments need to be cognisant when conceiving and implementing counter-terrorism strategies.

### Strengths and Weaknesses of the Theses of Barnett and Bobbitt

While the aforementioned academic works are outlined in order to justify the reasons for the influence of the focus of the theoretical paradigms stated in Thomas Barnett and Philip Bobbitt’s works, it is important to note at this stage that their perspectives should not be accepted uncritically. Indeed, there is a range of strengths and weaknesses associated with the works of Bobbitt and Barnett, which was considered before proceeding further with the thesis.

One of the shortcomings of *The Pentagon’s New Map: Wars for the Twenty First Century* is neglect of other forms of terrorism that could possibly emanate from the states, which comprise the Core, such as home-grown terrorism. This renders the book’s appreciation of the nature of new security threats, and terrorism in particular, incomplete. Another weakness of *The Pentagon’s New Map: Wars for the Twenty First Century* resides in its emphasis on the need for a protracted presence of military forces in an effort to close the non-Integrating Gap. This can be perceived as a weakness because Barnett does not readily acknowledge the role of other soft-power alternatives such as the influence of the media and control of narratives in closing the Gap. *The Pentagon’s New Map: Wars for the Twenty First Century,* in this sense never gets beyond the binary selections he presents and, therefore, does not acknowledge the complexity inherent in the twenty-first century global security environment. This issue was also addressed by Richard Jackson et al. (2007), who claimed that terrorism studies as a whole focus on a small range of issues to explain the phenomenon and fail to consider the wider picture. They contend that ‘[t]errorism studies has also been noted for its restricted research focus on a highly selective number of presumed topical subjects and its consequent failure to fully engage with a range of other important issues. For example, in recent years, literally hundreds of studies have been undertaken on Al Qaeda and related forms of ‘Islamic Terrorism’, Northern Ireland, the Middle East conflict and issues related to counter-terrorism in the US and UK, such as the role of the media, suicide terrorism, weapons of mass destruction (WMD) terrorism, cyber-terrorism and terrorist financing…[t]he cause and consequence of this restricted focus is a general failure to fully examine a range of other important issues, such as state terrorism, the impact of the war on terror on the global south, gender dimensions of terrorism, historical cases of terrorism, the cultural construction of terrorism, pathways out of terrorism, and the political causes of terrorism’ (Jackson, Gunning and Smyth, 2007: 6). As a result of Jackson’s perspective, it is important to bear in mind during the course of this thesis that, while Barnett’s perspective may align itself with the position of the Spanish Government, it might be improved by considering other factors for the inception of political violence from other states.

Another weakness inherent within Barnett’s work is evinced in his overreliance on the strength of markets to close the non-Integrating Gap. The Harvard economist Dani Rodrik (2008) claimed that certain economies have employed economic structures that are not liberal and have become extremely successful from them. Rodrik puts it that ‘the nature of industrial policies is that they complement – opponents would say “distort” – market forces: they reinforce or counteract the allocative effects that the market would otherwise produce’ (Rodrik, 2008: 100). Barnett’s prescription to close the Gap and, by implication, force the countries therein to align themselves with globalising forces and institutions such as the World Trade Organization and the International Monetary Fund, can be counter-productive as they might not benefit those new countries seeking to enter them. Rodrik also points out that other countries such as the US and the UK had established protectionist ‘rule sets’, in the words of Barnett, when establishing their economies, and, therefore, the countries in the Gap have very little incentive to join the forces and institutions of globalisation. Rodrik outlines the following; ‘every country that has had to do so by rigging its rules: extracting extra money from its people and steering money into industrialists’ hands’ (Rodrik, 2006).

There are, however, strengths to Barnett’s thesis. As written previously, Barnett’s thesis links very well with commentary emanating from other Spanish theorists. In addition, *The Pentagon’s New Map: Wars for the Twenty First Century* dovetails with pre-2004 government policy and, to an extent, post-2004 policy. This is because Barnett’s thesis was written in 2004-2005, following a period of close ideological and political alignment between the Aznar administration in Spain and the Bush administration in the US.

Barnett’s theoretical paradigm is also proximate to the vision of Ann-Marie Slaughter of a disaggregated state in which nation states work with other like-minded international organisations and states to simultaneously promote their sovereignty and secure their national interests (2004). This would be achieved, not by the establishment of more governmental networks, but by granting further horizontal and vertical exposure to their presence around the world. This perspective is a strength of Barnett’s because the Zapatero administration adopted a similar framework in its attempts to mitigate the terrorism threat faced by Spain.

Another strength in the *Pentagon’s new Map: Wars of the Twenty-First Century* is the admission that nation states are no longer the dominant actor in global geopolitics and that international community should unite to further integrate those countries situated in the Gap, because it is from this region that other threats will emerge, such as acts of terrorism.

One of the weaknesses evident in Bobbitt’s *Terror and Consent: The Wars of the Twenty First Century* is that his argument relates to the need to uphold international law in order to effectively combat market states of terror. This is flouted by certain states that act in their own self-interests. An example of this is seen in the United States, which has thus far declined to ratify the Geneva Convention, the Kyoto Process, and failed to recognise the jurisdiction of the International Criminal Court.

Bobbitt also advocates the use of data mining or identity profiling with the excuse of counter-balancing nefarious behaviour such as terrorism. However, it has been written elsewhere, particularly by the scholars David Betz and Anthony Cormack, that overreliance on technology to solve something as complex as terrorism is not a panacea to the phenomenon (Betz and Cormack, 2009). This sentiment is also an aspect in which Spain has direct experience, as its reliance on technological solutions with regard to its border controls, written about extensively in Chapter Four, nevertheless resulted in the propagation of terrorist attacks on its soil.

Finally, Bobbitt advocates the use of preventive war if the situation merits it; ‘States such as the U.S. and the U.K., which have global interests that are quite vulnerable to unconventional, terrorist assaults, will come to believe that they must intervene in order to take precautions against terrorists developing ever more lethal attacks…[t]herefore, the states threatened by terrorists may conclude that they must intervene against terrorists and their collaborators before they are attacked’ (Bobbitt, 2008: 10). This viewpoint contradicts his earlier point that states should adhere to international law if they intend to counter threats to the constitutional order, as pre-emptive war is illegal in the eyes of international law.

There are strengths to Bobbitt’s work, most notably his acknowledgement that non-state actors are becoming influential players on the world stage and that jurisprudence will be the most effective way to stop any problems that might arise from this. In addition, Bobbitt claims that terrorism is the result of cultural and religious clashes of poverty and underdevelopment. This not only resonates with the points of view from other scholars such as Barnett, Huntington, but also the Spanish Governments under Aznar and Zapatero.

In summary, Barnett and Bobbitt identify structural transformations in global politics and International Relations. Barnett points to dis-connectivities as a source of insecurity and violence, Bobbitt to a changing state form which terrorist groups mirror. For both, access to technologies has increased terrorists’ capacities. However, Crenshaw argues that terrorists have always used technologies to some extent and Bartlett and Imre argue that technologies are never the sole driver of radicalisation to violence. These perspectives show the complexities globally and generally which will be tested empirically in relation to Spain in this thesis.

In order to evaluate the official responses to terrorism in Spain, this chapter will now assess the history of terrorism in Spain and France from the 1980s to the present day. It will then analyse the past and present counter-terrorism policies adopted by both countries, simultaneously juxtaposing them within the theoretical frameworks offered by both Barnett and Bobbitt. Such an analysis will illuminate the complexity of the terrorism threats that confront both countries and, importantly, the role of technology within such policies. In addition, this chapter will consider general ways in which national governments respond to the threat of terrorism by implementing strategies aimed at influencing attitudes and behaviours using public diplomacy methods.

These analyses will explore how Spain’s historical and contemporary experiences of terrorism and counter-terrorism have incorporated understandings of the role of technology, and articulate the Bobbitt and Barnett frameworks to make sense of these accounts. The extent to which other governments have implemented socio-technical or technological deterministic responses to their experiences of terrorism will also be asked.

### Terrorism in Contemporary Spain

Spain has a long history of terrorism within its borders as terrorist attacks by ethno-nationalist separatist groups have proved a particularly egregious problem for the state. For the purpose of this chapter, the analysis will focus on terrorism in Spain from 1980 to the present day.

The most prominent and enduring symbol of the fight for regional independence in Spain is the ongoing campaign for self-determination in the Basque region. The campaign for full independence of the region that lies between North-eastern Spain and South-western France was assumed most prominently by ETA and their political affiliation Sozialista Abertzaleak Batasuna (Batasuna), and before that Herri Batasuna. The conceptualisation of ETA embodying Spain’s experience of terrorism is encapsulated by the 11-M television producer Justin Webster who put it that “[t]he uniquely Spanish characteristics [of terrorism in Spain] are to do with ETA and…the way in which the Spanish state is constructed…they [ETA] are specifically Spanish and…the way that ETA has behaved has Spanish characteristics. I’m thinking about the choice of targets, their campaigns, their justifications. You can’t really understand it properly outside of the Spanish context.”[[18]](#footnote-18)

Batasuna has been campaigning for Basque independence in different guises for over three decades, despite the fact that its popularity amongst the general Spanish populace has decreased sharply in recent times. It was banned from participating in national mainstream politics in 2003 by the Spanish Government, due to its strong financial and ideological links to ETA, which have been responsible for a large number of deaths in its pursuit of Basque independence. The scholar, Luis Moreno, considered ETA to be the most prominent terrorist threat currently facing Spain in 2004. He opined that it is certainly ‘one of the most long-lived terrorist organisations in the Western world, with more than forty years of existence, more than thirty years of personal attacks and about a thousand homicides’ (Moreno, 2004: 5). After a long series of attacks over many years, it is clear that the eradication of ETA was at the forefront of counter-terrorism policy for both Spanish and French policymakers.

ETA was borne from the energy of the populist Basque independence movement in 1952. The violent methods adopted by the organisation increased both in frequency and in terms of the level of violence in the years following the death of General Francisco Franco (Franco) in 1975. Batasuna and ETA believed that the political upheaval sparked by the death of the Spanish dictator would provide the opportunity to petition for complete independence, in spite of the fact that the Basque region was devolved a level of autonomy far in excess of that granted to other Spanish autonomous communities such as Catalonia, Galicia, Ceuta and Melilla (Human Rights Watch, 2005), during the Spanish Transition from a dictatorship to a constitutional democracy (1975-1978).

However, Madrid denied Basque demands for full independence in 1978, thereby compelling ETA to adopt violence as a means of forcibly persuading the Government into conceding to its demands. It used a variety of methods during the 1980s and 1990s to perpetrate violence on the Spanish populace and the national security services, including targeted assassinations, kidnappings, extortion and indiscriminate bombings. Indeed, ETA’s strategy subsequent to the denial of Basque autonomy consisted ‘of pressure on the State through committing hundreds of murders, especially the military and members of the security forces, but also civilian groups in order to force them to give in to their aims in a supposed negotiating table’ (Cosidó, 2002: 1). However, it soon became apparent that ETA’s bloody strategy was part of an all-encompassing model of escalating violence which it not only used to coerce political figures into capitulating to its demands, but as a mechanism of forcing widespread political destabilisation; ‘[f]irst of all, the one [aspect of ETA’s strategy] they call “Fight X” includes violent demonstrations and coercion and intimidation acts against those who oppose the terrorist group thesis. Secondly, “Fight Y” consists of acts of sabotage and organised street violence, which could be considered as low intensity terrorism. Finally, “Fight Z” is constituted by more serious terrorist acts such as murders or to plant explosive devices’ (Cosido, 2002: 1). These tactics resulted in a significant degree of success for the organisation insofar as the attacks maintained the visage of the group in the public consciousness and that of policymakers.

ETA’s tactics resonate strongly with Bobbitt’s assessment of nation state terrorists, which he claimed targeted professionals, such as teachers and mayors. He claimed that when such targets were assassinated, ‘local officers were replaced by military personnel, counter-atrocities occurred, increasing political support for the terrorists. Sympathy abroad generally favoured those who used the methods of asymmetric warfare because they were, almost by definition, the weaker party without realistic military alternatives’ (Bobbitt, 2008: 42).

However, ETA underestimated the determination of Spanish Government policy forbidding negotiation with terrorists, which was emphasised by introducing a counter-terrorism policy designed to decimate the organisation. One particularly austere tenet of this counter-terrorism policy was the introduction of the government Anti-Terrorist Liberation Groups (GAL) during the mid-1980s, which had a mandate to conduct assassinations of suspected ETA members clandestinely. The GAL was responsible for the deaths of many people wrongly suspected of being ETA members, and also incited a sharp increase in retaliatory ETA violence. When it became clear in 1988 that the GAL’s method was proving unsuccessful and unpopular amongst the general public, the Government, which had by now improved bilateral relations with France, employed the combined use of the Gendarmerie and the Guardia Civil during the 1990s to counter ETA, resulting in the arrest of a number of its senior members. The incarceration of a significant portion of ETA’s hierarchy forced the organisation to drastically reappraise its strategy and accept that a process of dialogue and negotiation would be the most effective option to successfully fulfil its demands (Human Rights Watch, 2005).

The creation of the Lizarra/Estella Pact or the Lizarrako Akordioa in 1998 involved the most prominent political parties in the Basque region implementing a diplomatic solution to the contention of Basque independence. ETA agreed to the conditions of the Pact and, most importantly, the cessation of violence for the duration of the negotiations between the government and the coalition of parties until the new conditions underlying Basque independence could be imposed. However, the right-wing Partido Popular(PP), under the leadership of José María Aznar, suspended negotiations with ETA and Batasuna in August 1999 as a result of its unwillingness to renounce the use of violence (Wood, 2007: 1) in the long term. The Government’s suspension of negotiation with ETA led to renewed vigour in its crackdown on domestic terrorist organisations, conducting a number of high-profile counter-terrorism operations which led to the incarceration of some of ETA’s senior members and the decimation of its logistics structure in December 2002. The success of this period of sustained pressure from the Government was, according to the Royal Elcano Institute, due to the judicial pressure in Spain and other countries, which increased their counter-terrorism measures and resulted in the arrest of increasing numbers of terrorist members. The number of arrests made in 2003 were 187 after ETA reorganised itself during the Estella Pact (Avilés, 2003).

In the immediate aftermath of the Madrid train bombings on 11 March 2004, the Aznar Government publicly blamed ETA. The widespread and categorical public rejection of terrorism following the 11 March bombings compelled ETA to declare a complete ceasefire in 2006, despite the fact that many of its senior figures were by this time incarcerated. However, this renunciation of the use of violence was revoked in 2006 as the organisation, ‘frustrated that the government had not been more forthcoming in negotiations…announced its members will “keep taking up arms.” The Zapatero government has stated that while it will negotiate for a peaceful dissolution of the group, it will not make any concessions toward Basque independence’ in September 2006 (Selway, 2007: 32).

While ETA and the Spanish Government have engaged in a long-running conflict, the simultaneous rise in international terrorist organisations has been prolific and, during the 1980s and 1990s, official campaigns against ETA were largely ignored by the Spanish Government. While ETA operated across the borders of both Spain and France and can be construed as an international terrorist organisation, for the purpose of this thesis, and in conjunction with the content of the interviews conducted, it will be considered a Spanish terrorist organisation.

International terrorism in Spain is a complex issue. It is generally conceived by scholars and subject-matter experts to emanate from al-Qaeda and al-Qaeda inspired groups operating within the country. The scholar John Postill said that “[t]here are two main types of terrorism…The terrorism of ETA, well, it isn’t unique as regional separatist terrorism is quite common around the world…In terms of Islamist terrorism…It’s a type of terrorism that we’ve seen in other parts of Europe.”[[19]](#footnote-19) In addition, the Spanish political scientist Javier Jordán argued that Jihadist terrorism had assumed prominence in Spain following the Madrid attacks in 2004 and the London bombings in 2005 (Jordán, 2005).

Immigration to Spain from neighbouring countries has increased steadily since the 1980s as demonstrated by the chart in Figure Four. Indeed, levels of illegal immigration of citizens from North African states had reached such proportions that the Spanish Government in 1998 erected ‘12-foot high fences to halt African immigration illegally entering Europe by way of Spain’s North African enclave territory in Melilla’ (Crain, 1999: 1). The conflation of immigration with terrorism was also identified by Javier Jordán who claimed that the threat of international terrorism in Spain had increased ‘since the mid-1990’s jihadist networks have started to direct their recruitment and propaganda to the growing immigrant Islamic community. Without falling foul of simplicity by criminalising immigration, it is undoubted that this fact has complicated the efforts of the police and intelligence services and has increased the number of potential candidates, within the ranks of immigrants, who could be radicalised or, once in Spain, who could be drawn into the orbit of Jihadism’ (Jordán, 2005: 3).[[20]](#footnote-20) Unchecked migration from North Africa is therefore perceived, to a certain extent, to be a problem for counter-terrorist organisations as it increases the number of people in Spain who might be attracted to Jihadist ideology. The author accepts that the term Jihad and Jihadist ideology are disputed terms with a distinct lack of agreement on the parameters of the term (Bunt, 2003, Al-Lami, 2009). However, for the purpose of this thesis, the definition of Jihad offered by Hoskins and O’Loughlin in their analysis of the nature of the remediation of speeches by Ayman Al-Zawahiri will be used. They contend that Jihad is ‘the political culture promoting the goals, practices and ideology of Al-Qaeda (as an idea and set of networks) rather than to broader forms of political Islam which may also advocate violence’ (Hoskins & O’Loughlin, 2010: 7).

Indeed, the number of people passing through Spain’s borders has increased to such a level that, according to counter-terrorism policymakers, international terrorism of Maghreb and South Asian descent is considered a distinct policy concern (Reínares, 2006, Colás, 2010).

The number of international terrorist organisations in Spain grew steadily from 1995 due to the desire of these groups to extend their bases of operations to Western Europe (Jordán, 2005, Reinares, 2006). The main stated motivation from international terrorist groups to operate in Spain and France was to reclaim both countries as part of a 21st century Caliphate (Celso, 2008). This stated desire has been proffered most prominently by al-Qaeda. Selway, (2007: 15) writes that its former figurehead, Osama bin Laden, referred to ‘“the tragedy of al-Andalus” when speaking about Spain…In October 2003, bin Laden promised “crusader Spain” repercussions for participation in the Afghan and Iraq wars. But the term “crusader”, besides referring to Spain’s current actions abroad, also refers to the Catholic monarchs who drove the Muslim population out of the country some 500 years ago after centuries of war. The network that executed the attacks referred to Spain as the “land of Tarek Ben Ziyad,” after the Arab leader who launched the Islamic conquest of the Iberian Peninsula in 711. Any land once in Muslim hands is considered fair game for global jihad’.

This ideology has subsequently resulted in a large number of groups operating in Spain involved in activities linked to the ideology propounded by Bin Laden and al-Qaeda, all of which have made use of internet and Web technologies (Jordán et al. 2006). The most prominent of these groups is the Grupo Islámico Armado (GIA), which was established in 1992. The group is closely linked with the extensive underground criminal network of drug and people trafficking from North Africa, which contributes prominently to the group’s financing. It has been noted, however, that the group experienced severe internal struggles and a number of its members subsequently joined the Grupo Salafista por la Predicación y el Combate (GSPC), which is purportedly better connected in Spain than al-Qaeda (Jordán, 2005).

The GIA is also closely linked with the Moroccan Islamic Combatant Group (Groupe Islamique Combattant Marocain(GICM)), another North African terrorist organisation that has extensive operational networks in Spain. The GICM has a major presence in Spain, exemplified by the fact that investigations into the culpability of the Madrid bombings focused on this group. Its operatives are known to conduct criminal activities and plan attacks together, leading the Government to designate the targeting and eradication of these groups as a priority (Marsaud, 2008).

There is, however, another prominent international terrorist organisation operating alongside both the GIA and GICM, the Abu Dahdah or Syrian network. This group, which first came to the country in the 1980s and has links with the Muslim Brotherhood, is strongly linked with the global Jihad and had three of its members arrested by the Spanish counter-terrorist squads between 2001 and 2003 (Jordán, 2005).

### Counter-terrorism Policies in Contemporary Spain

The Spanish Government formed its counter-terrorism policy and national security departments initially to respond to the threat posed by ETA under what it termed the “comprehensive approach”. This approach adopted by the Government in the 1990s was described by Ignacío Cosído; ‘[t]he new comprehensive approach to combat terrorism starts from the premise that ETA is not only its cells, but also a big network with political parties, social organisations, companies and propagandistic means…The government approach is, therefore, to fight against that network so as to hinder, on the one hand, the regeneration capacity the armed gang has enjoyed along its history and on the other the impunity most of the organisation has had [in] making use of democracy’ (Cosidó, 2002: 1).

The Spanish Government, therefore, cited cooperation with France as the cornerstone of its overall strategy against ETA in the 1990s, as a considerable number of individuals from the organisation’s hierarchy were based in France. It merged the national and local police, Guardia Civíl and the Policía, into a single unit, which had an extended mandate to work together to perform all manner of counter-terrorist operations. The alliance of the security services was important for a number of reasons, the most salient of which was that ‘it makes it an intermediate instrument that has kept the Spanish Armed Forces out of the fight against ETA, thus avoiding the disadvantages that an intervention of the Army in missions within national territory entails’ (Cosidó, 2002: 1).

Spain’s counter-terrorism policy in the 1990s demonstrably mirrored France’s revised policy following the failure and ultimate abandonment of the Sanctuary Doctrine in 1986 (Ballesteros, 2005), which will be analysed in the following section. However, one aspect of Spain’s counter-terrorism policy, the deployment of the Anti-Terrorist Liberation Groups or death squads (Grupos Antiterroristas de Liberación or GAL) from the *Guardia Civil*, proved to be similarly counter-productive. The deployment of the GAL became part of what was eventually termed the “Dirty War”, a move by the Spanish Government in 1983 ‘to punish the French government for its unwillingness to cooperate with Madrid by bringing the fight against terrorism across the border into France’ (Selway, 2006: 31). GAL members crossed the border into France to carry out summary executions of people suspected of being ETA members, resulting in the deaths of many people who were later exonerated of involvement with the organisation (Human Rights Watch, 2005). The Dirty War inadvertently escalated ETA’s violent campaign as the group entered into revenge killings, which ended in 1986 after France committed to cooperate with Madrid in its counter-terrorism efforts.

In addition to the widespread changes of the national security services, the Government took greater steps to forge stronger bilateral agreements with the French Government. As a result, Spain conducted considerably more surveillance missions into French territory. There were also a significantly higher number of extraditions of French nationals suspected of colluding with ETA, as well as a sharp increase in the number of arrests made by French officers of suspected ETA members in France.

After the terrorist attacks in Madrid on 11 March 2004, as outlined in Chapter Four, the Spanish Socialist Party (Partido Socialista Obrero Español or PSOE) was elected to power and immediately implemented a new phase of counter-terrorist policies. When it was revealed that the Madrid attacks had been perpetrated by international terrorist organisations, the Government advanced its new vision of counter-terrorism by promoting better coordination of resources and intelligence at the interstate level. Firstly, it established new guidelines under which its intelligence agencies were to work by creating the National Intelligence Centre (Centro Nacional de Inteligencia or CNI) in 2002 which was framed in order to better coordinate terrorist-related information (including digital data) between the Guardia Civil and the Policía. This new system of organising domestic intelligence has yielded success, not least in the foiling of an attempted attack by North African militants on the Barcelona Metro in 2007 (Goodman, 2008: 1).

In addition to this, Spain enhanced its strategic vision of a collaborative, state-based response to terrorism through its efforts to ameliorate bilateral relations with other Maghreb countries – most notably Morocco. Zapatero signed various agreements with King Mohammed VI promising to strengthen ties that better challenge the criminal networks that operate between the two countries and fund terrorist organisations. This strengthening of bilateral relations as part of a country’s counter-terrorism strategy is strongly reminiscent of Barnett’s declaration that the integration of countries from the non-Integrating Gap into the Functioning Core should be conducted in order to halt the spread of international terrorism.

The 11 March 2004 attacks caused the Spanish Government to sharply re-examine the efficacy of its counter-terrorist policy. The attacks demonstrated that the presence of international terrorist organisations was a completely distinct threat to that faced by Spain in the past. As a result of this altered understanding of the nature of the terrorist threat in Spain, the late terrorism scholar Paul Wilkinson commented that the Government adopted a hard-line approach that allowed it to effectively combat terrorism and other security threats by combining the use of ‘politics and diplomacy, the use of law enforcement and criminal justice systems, and the role of the military. Key elements…include emphasis on intelligence, all institutions involved in combating terrorism firmly accountable to the government and electorate, no special status for convicted terrorists, no major concessions for terrorists, and frequent review of any special emergency government measures taken to combat terrorism’ (cited in Selway, 2006: 12). Spain also adopted a public diplomacy strategy to influence opinion outside its borders, the overall efficacy of which will be addressed later in this chapter.

The moves to alter Spain’s counter-terrorist policy were considered timely by a number of counter-terrorism scholars who acknowledged that the propagation of the Madrid attacks demonstrated Spain’s failure to understand the changing nature of the threat facing the State. Support for this viewpoint came from the conclusions of the 11-M Commission, which claimed that international terrorist organisations operated freely in the country due to the Government’s attention to ETA. It concluded that ‘[t]errorism of radical Islamist groups was a “secondary concern.” Spanish intelligence had actually penetrated part of the 11-M terrorist network, and there were police informants who had contacts with the terrorists…Spain had numerous warnings and links to an impending attack, but simply did not give them the priority they deserved…ETA distracted the Spanish intelligence community from the Islamic threat’ (cited in Selway, 2006: 84). Bobbitt also noted that Spanish counter-terrorism officials could be accused of focusing on the threat posed by ETA and not of the more prescient threat that emanated from the changing nature of the global political, economic and civic systems:

‘Like generals, spies and policemen tend to fight the last war…Similarly…until the bombing of a Madrid commuter train by Moroccan radicals in March 2004 [Spain’s] focus was almost entirely on ETA, and its principal action the banning of the allegedly related Basque nationalist party Batasuna. Security services must learn to look forward to emerging threats, not backwards at Cold War and separatist ones’ (Bobbitt, 2008: 44).

Bobbitt’s comments, as well as those from the 11-M Commission, are indicative of the notion that threats facing the international community, of which Spain is a part, were changing. Globalisation was encouraging the flow of people, ideas, capital and with them threats, all hallmarks of an environment where market states of terror can thrive (Bobbitt, 2008).

As a result, Spain’s counter-terrorism policy since the Madrid attack has sought dialogue and negotiation with states it understood as constituting a threat to national security (Portero, 2005, Elorza, 2005). This strategy, as mentioned previously, supports Barnett’s hypothesis that greater moves are needed by those countries in the Functioning Core to integrate those in the non-Integrating Gap if further acts of terrorism are to cease.

This chapter will now outline France’s experience of terrorism and assess the extent to which either Barnett’s or Bobbitt’s hypotheses can be applied to this context. This contrast also helps clarify Spain’s experiences.

## Terrorist Organisations in France

The French response to terrorism is strikingly different to that which occurred in Spain. France was the first European country to experience international terrorism of Middle Eastern origin. The phenomenon came to the attention of the French Government in 1980 when a car bomb was detonated in the Paris *Rue de Copernic* on a Jewish target, motivated by ‘foreign terrorists whose purpose was to influence French foreign policy in the Middle East’ (Shapiro & Suzan, 2003: 67).

In the 1980s, France was considered by international policymakers and terrorist organisations to be a haven for international terrorist organisations, due largely to its adherence to the Sanctuary Doctrine adopted by the Government which was instituted ‘prior to the 1980s’ (Shapiro & Suzan 2003: 69). The main tenets of this doctrine centred on the belief that if terrorist organisations were given sanctuary within French borders, they would be less likely to pose a threat to French interests. While the Sanctuary Doctrine would eventually yield flaws, it was initially successful. Terrorist groups, such as the Palestinian Liberation Organisation (PLO) and the Factions Armées Révolutionnaires Libanaises, which had been a long-term problem in France, dramatically reduced their attacks on French interests (Garapon, 2005).

The fact that the decrease of terrorist attacks was not enforced but a situation agreed upon meant that small inconsistencies in French counter-terrorism policy eventually became deep fissures. The problems inherent within the Sanctuary Doctrine were considerable and ultimately positioned France as a pariah amongst members of the international community and detractors of the terrorist groups it sheltered. Numerous states and terrorist organisations also perceived the doctrine to be a sign of weakness, a perception not lost upon certain terrorist organisations which utilised violence against French interests when they became strategically important such as the terrorist attacks of the Paris subway, trains and public buildings in 1986 by the Committee for Solidarity with Near Eastern Political Prisoners (CSPPA) (Shapiro & Suzan, 2003).

Although the increase in international terrorism in France was in large part ascribed to the convergence of a burgeoning Middle Eastern and North African population in combination with a permissive counter-terrorism strategy (Human Rights Watch, 2005), scholars such as Jeremy Shapiro and Bénédicte Suzan noted that international terrorism was widely perceived in the French Government to be the result of the country’s “colonial hangover” in North Africa. International terrorism was therefore widely considered by the French Government to be more of a diplomatic and foreign policy problem than a law enforcement problem (Shapiro & Suzan, 2003).

The permissiveness of the French approach to counter-terrorism during this period attracted a host of terrorist organisations to the country. The Kurdish Workers Party (Parti Karkerani Kurdistan (PKK)), in particular, was active in the country in the 1980s. In addition to the organisation using France as a base to conduct its operational strategies, it was also the region where the PKK generated substantial funds. The organisation allegedly controls the drug and human trafficking market in Europe, a multi-billion pound industry, the profits of which were siphoned off to the operational base in Kurdistan, Northern Iraq (Laciner, 2006, Global Security, 2011).

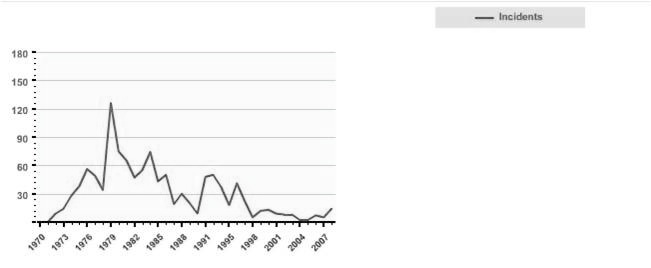
In addition to the PKK, Hezbollah also maintained a strong presence in France, even hosting the al-Manar television station in the region through which it broadcasted its *raison d’être* to the Middle East and other members of the Europe-based Palestinian diaspora. The presence of Hezbollah did nothing to appease the negative perception of France held by Israel, particularly after it was made clear that the Palestinian Liberation Organisation was operating within the country and yet perpetrating attacks on Israeli citizens (Shapiro & Suzan, 2003).

It should not be overlooked that France had to contend with a high level of ethno-nationalist terrorism. It was widely known that while ETA was conducting its campaign on Spanish territory against the Spanish Government, its base of operations was located in South-western France. The fact that ETA was allowed for a time to plan attacks in France with impunity and subsequently execute them in Spain enraged Spanish policymakers. France also had to counter the threat of ethno-nationalist terrorism from Corsica as rebel groups such as The Corsican People’s Army (APC) and the National Liberation Front of Corsica perpetrated numerous attacks on French infrastructure such as the assassination of the French Prefect Claude Erignac in 1998 in Corsica (Shapiro & Suzan, 2003). France also suffered from the threat of Marxist terrorism, most prominently in the form of Action Directe*,* which was active until 1987. Although the group was prolific at causing widespread damage and a number of deaths (BBC News, 1986), its mantle was superseded by the presence of international terrorist organisations.

### Counter-terrorism Policies in Contemporary France

The political and operational fragility of the Sanctuary Doctrine was eventually exposed following the 1986 Paris subway attacks. The attacks, which severely affected the subway, killed 11 people and injured more than 220, and spurred the French Government into a complete revision of its counter-terrorist policy, conceding that the Sanctuary Doctrine was in fact detrimental to French interests. To this end, it bestowed far-reaching powers upon its judicial system, granting it the authority to implement legislative changes quickly and without obstacle from central or local government (Shapiro & Suzan, 2003). In addition to this, the national police force, the Gendarmerie, and the military were given extra mandates that they were also to be used in counter-terrorism operations. In this way, the Gendarmerie was to be used in a similar manner to that of Spain’s Guardia Civil, to assist the efforts of the revamped judicial service and the newly created counter-terrorism departments (Ballesteros, 2005). It also sought to remedy the problem of miscommunication amongst the security services and as a result created the Unité deCoordination de la Lutte Anti-Terroriste (UCLAT), and the Service pour Coordination de la Lutte Anti-Terroriste (SCLAT), which eventually became the Direction de la Surveillance du Territoire (DST) in 2006, and then merged with the [Direction Centrale des Renseignements Généraux](http://en.wikipedia.org/wiki/Direction_centrale_des_renseignements_g%C3%A9n%C3%A9raux) to become the [Direction Centrale du Renseignement Intérieur](http://en.wikipedia.org/wiki/Direction_centrale_du_renseignement_int%C3%A9rieur) in 2008. As a result of this restructuring, France witnessed a significant decline in the number of terrorist incidents and terrorist organisations it had hitherto provided refuge as part of its Sanctuary Doctrine (Shapiro & Suzan, 2003). The effect of this policy is represented below:

Figure Six: Number of National and International Terrorist Incidents in France from 1970 to 2008



Source: Global Terrorism Database

From the perspective of Barnett’s theory, that global political, economic and military integration is a panacea for the cessation of political violence, the Sanctuary Doctrine demonstrated that in the long term it was abject at discouraging terrorist violence. The policy was myopic as it simply sought to preserve the interests and security of the French State, with no concern for that of other States. In addition, the Sanctuary Doctrine did little to include states from the non-Integrating Gap into global processes and therefore left France vulnerable to reprisal attacks by other rival terrorist organisations. From the perspective of Barnett’s theory, the Sanctuary Doctrine would only have invited violence upon French interests, as it did nothing to ensure region-wide security and prosperity by considering the interests of other states in its counter-terrorist policy. Rather it sought to maintain its own security, independent of other states, by indulging the demands of terrorist organisations.

The fact that the structure of France’s new counter-terrorism system was more akin to the network structure of the terrorist organisations it faced was an erudite posture to adopt for a number of reasons. The Government became strongly cognisant of the changing nature of terrorism as the country became more integrated in global political and economic structures. The drastic change in counter-terrorism policy is suggestive of an increase in awareness at the highest levels of Government that international terrorism in the region would not abate unless a more effective system was created that could mirror the organisations against which it was positioning itself. Such a significant change in outlook for combatting terrorism also validates Bobbitt’s theory that radical change in conventional counter-terrorist strategies is needed in order to mitigate contemporary political violence as nation states evolve into market states because; ‘Market state terrorism is global terrorism. Markets, unlike nations, are often global. Indeed, it is becoming increasingly apparent that al-Qaeda is not only a reaction to globalisation, but a manifestation and exploitation of globalisation. To see that is also to see that market state terrorism is an unintended side-effect of the globalisation of international communications (including travel), rapid computation, and radical weapons development of the late twentieth century, which is to say the very strategic developments that are bringing into being the constitutional innovations of the market state. This suggests that al-Qaeda will be copied by other globally networked infrastructures engendered by the emergence of market states’ (Bobbitt, 2008: 83).

It also appears that in the past the French Government thought it more useful to adopt a counter-terrorism system that allowed terrorist organisations to operate as long as French interests were not targeted. This decision closely follows Bobbitt’s assertion that in order to effectively combat market or networked forms of terrorism, emerging market states need to adopt market-style structures and solutions.

## Challenges to Counter-terrorism Policies in France and Spain

Analyses of the current domestic security strategies for both nations show that international terrorism, in particular, constitutes a pressing threat against national and supranational security in the minds of policymakers.

An investigation of France’s counter-terrorist strategy since 1980 has outlined its journey from providing sanctuary to terrorist organisations within its borders, to “suppression and prevention” (Starobin, 2003: 7), redistributing judicial and military power to counter threats through judiciary and law enforcement bodies. However, there are strong indications that France invests heavily in the use of technology as a central tenet of its future counter-terrorism strategy. The Government has invested a large amount of resources and funds into the development of surveillance technologies, in particular, to monitor conversations. In addition, the development of vast identity databases was undertaken, such as the identity card scheme (European Digital Rights, 2009). The implementation of identity cards significantly restricted the ability of those who, for example, attempted to enter the country illegally to open a bank account under a different alias for example. The 2008 French National Security Strategy also underscored the need to focus on the role of technology in the strategy to contain modern terrorism. To this end, France has constructed a national database named the Exploitation Documentaire et Valorisation de l’Information Générale (EDVIGE) which logs and makes available to the security services information on people it suspects of entering into nefarious activity from age 14 upwards (Tetu, 2008). The French White Paper on national security also highlights the new focus of the Government on monitoring nationwide internet behaviour to counter the threat of terrorism (Présidence de la République, 2008). This investment in technology shows that France understands the threat it faces in the age of globalisation and the need to employ a technology-based solution to fight it. It appears, therefore, that France is more supportive of Bobbitt’s argument that market states need to employ market-based strategies to defeat terrorism, such as the use of the private sector, because, as this perspective by Mary Kaldor attests, ‘new wars…[are] fought by networks of state and non-state actors, where battles are rare and violence is directed mainly against civilians’ (Kaldor, 2006: 9). A facet of France’s revised approach to terrorism is to advocate stronger bilateral transatlantic relationships with the US in particular. This emphasis on forging stronger counter-terrorism ties with the US suggests that it considers international terrorism to be a global problem and not simply a domestic or regional concern.

The stance taken by France, however, in its prescriptive conceptions of counter-terrorism policy is wholly different to that taken by Spain. The first main difference is that Prime Minister Zapatero prioritised greater political cooperation between states as the cornerstone of his counter-terrorist policy, strongly promoting the idea that the general prevention of terrorism is something that should be undertaken by all states, and not singularly. To this end, Zapatero has gone to great lengths, since the Madrid terrorist attacks in 2004, to enhance bilateral and trilateral relationships with Morocco and other Maghreb States. As a result, Spain and Morocco, in particular, have agreed to enhance border security and closely monitor entry to Spain from North Africa. To this end, Spain is seeking to further strengthen its ties with Morocco by considering the construction of a transnational tunnel between the two continents to further develop positive cultural ties between the peoples of the two countries (BBC News, 2003). The potential project to construct a tunnel, in conjunction with the implementation of enhanced border control, is indicative that Spain views the cessation of terrorism, by the means of good governance and public diplomacy, as opposed to the French model which actively securitised its counter-terrorism policy.

Since 2003, Zapatero has done much to emphasise the need for a multilateral solution to international terrorism, away from a strategy that pertains only to Spain or other European states. In the National Defence Strategy of 2003, (*Revisión Estratégica de Defensa*, RED), the case for a clearly defined UN counter-terrorism strategy was proposed in contrast to separate national security strategies. This is slightly different from the direction taken by the French Government, which specifically advocated a stronger alliance with the US to counteract the threat of international terrorism and foster a more coherent European response (Présidence de la République, 2008).

As mentioned previously, the Spanish Government’s stance on counter-terrorism has demonstrated a preference for the use of public diplomacy as the cornerstone of its strategy. However, a more in-depth explanation of public diplomacy is required to provide greater context of the depth and complexity of its counter-terrorism policy.

## Public Diplomacy as Counter-Terrorism Strategy

“[There] is more power in blue jeans and rock n’ roll than the entire Red Army”

(Debray cited in Sullivan, 2006: 216)

In his treatise on international politics and reputation, the scholar Jonathan Mercer highlighted the importance of cultivating a positive general perception of a country. He argued that national reputation ‘is unquestionably an instrument of power’ (Wang, 2005: 1) and an integral part of foreign policymaking. In his opinion, reputation should therefore be considered ‘a judgment of someone’s [or something’s] character (or disposition) that is then used to predict or explain future behaviour’ (Mercer, 1996: 6), which also applies in the context of states.

Public diplomacy is one tool that some non-state actors use to ameliorate that reputation. It is defined as the practice of diplomatic communication incorporating government-to-people contact, different to the more traditional government-to-government and diplomat-to-diplomat communication (Manheim, 1982). It is referenced in diplomacy literature as the engagement of target populations by a state or other entity seeking to influence that audience of the legitimacy of its core messages and narratives. According to the public diplomacy scholar Stacy Hope, the discipline or practice ‘contributes to a country’s national security by building the sustainable influence of one nation on the citizens of another’ (Hope, 2009: 60). This form of engagement is different to other forms of diplomacy, such as bilateral and multilateral diplomacy. Bilateral diplomacy, which is predicated on ‘the conduct of relations between two or more states’ and multilateral diplomacy, ‘the conduct of relations between three or more states’, are characterised by the maintenance and amelioration of formal relationships between nation states. The presence of a third dimension to diplomacy has also been promulgated by Geoffrey Wiseman who contended that diplomatic relations between states and non-state entities exist and should be denoted as polylateralism. He contended that polylateralism is conceptualised as ‘the conduct of relations between official entities…and at least one unofficial, non-state entity in which there is a reasonable expectation of systematic relationships, involving some form of reporting, communication, negotiation, and representation, but not involving mutual recognition as sovereign, equivalent entities’ (Wiseman, 2004: 41). It is Wiseman’s definition of polylateralism that emphasises the importance of government-to-people diplomacy.

Considering the nature of polylateralism in diplomatic literature, it can be conceived that other non-state actors, such as terrorist organisations, practise public diplomacy. The ability of contemporary terrorist organisations as well as nation and market states to forge and foster strong relationships with their target audiences will be analysed at length in subsequent chapters of this thesis. As the author has written elsewhere, ‘Al-Qaeda and Osama bin Laden (described by one observer as “the quintessential public diplomat”) are innovative communicators who have forged a single powerful narrative of oppression out of a range of grievances, taking advantage of modern forms of communication including the internet and satellite broadcasting. By contrast, traditional diplomacy has been poor at constructing coalitions based around a distinct set of values and ponderous in communicating effective branding’ (Ampofo, 2010: 4). Contemporary non-state actors, especially organisations such as terrorist groups, can therefore be as effective as States in constructing and propagating effective public diplomacy programmes that influence great numbers of foreign publics.

Like traditional diplomacy, public diplomacy is observed by prominent international relations scholars such as Anne Marie Slaughter and Joseph Nye as an element of soft power. In his thesis on the nature of soft power, Nye claimed that the techniques encompassed within public diplomacy for influencing the general public are an altogether different form of power than that of other forms of state influence such as kinetic warfare or what he termed “hard power”. Hard power, which, according to Nye, refers to the ability to influence an actor to comply with your way of thinking by military force, becomes increasingly costly and, by implication, less attractive as a means of coercion to governments. The interconnectedness of the contemporary globalised world also means that a military attack on one state would likely impact upon the strategic interests of the attacker.

The earlier quotation from Regis Debray neatly sums up Nye’s perception of the strength of US cultural influence and national reputation in relation to hard power. Nye supported Debray’s assertion that soft power tactics, such as public diplomacy, are as important to modern day politics and statecraft as traditional military power. Therefore, public diplomacy, which exists to influence foreign publics of the legitimacy of government policy, encapsulates all of the elements of a soft power technique, rendering it a core tactic of influence and power.

Although soft power is an overarching framework for the implementation of public diplomacy programmes, there are numerous other explanations for their inclusion in the application of foreign policy. One of the principal reasons for exerting influence over the people of a particular state is to ameliorate its reputation. The motivations driving states’ desires to maintain and improve their reputation were proffered by the researcher and creator of the Nation Brands Index, Simon Anholt. Together with the German market research company Gesellschaft für Konsumforschung (GfK), the Nation Brands Index conducts annual survey research of a sample of the global population and ranks the popularity of more than 200 countries based on the responses. In appraising the efficacy of the Nation Brands Index, Anholt argued that individual states guard and maintain their national reputations to the extent that they can be perceived as brands, ‘as important…as any other corporate brand. Every country in the world has to compete with more than 200 other countries for positive reputations’ (Ampofo, 2010: 4). Positive national reputation is a critically important strategic objective for all states as without it, key narratives, and by implication policy objectives, become more difficult to convey to the general public.

If the key to success in public diplomacy programmes is to ensure the delivery of core narratives in a way that enhances a state’s credibility and reputation, then it follows that emphasis has to be placed on the delivery of key narratives. Mark Leonard focused on this in his critique of post-September 11 public diplomacy, which he claimed ‘has failed to deliver information convincingly. The tone of many messages is declamatory, without any apparent intent to engage in dialogue or listen’ (Leonard, 2002: 53).

It would be unwise to take Leonard’s comments as sacrosanct however, as the linkages between public opinion and official policies are not always in evidence. However, it is clear that public opinion creates a climate in which official policies can be pursued, making national reputation and credibility (and by implication public diplomacy as a tool to advance these perceptions) central to national strategic objectives (Burstein, 2003: 32).

Public diplomacy can, therefore, be an effective way of influencing foreign publics in comparison to military action. Public diplomacy is also an extremely malleable tactic, able to dovetail with a range of programmes to achieve strategic objectives. Public diplomacy objectives and programmes can therefore be easily incorporated into the activities of a number of different sectors such as religion (International Center for Religion and Diplomacy, 2011), sport (World Paddle Sport Foundation, 2011), business (Watkins et al. 2000) and counter-terrorism (Alliance of Civilisations, 2011), thereby enhancing its reputation as an effective method of influencing large groups of people.

### Spain’s Use of Public Diplomacy

The Spanish Government has made extensive use of public diplomacy techniques to inform its broader counter-terrorism strategy since the 1800s. The use of public diplomacy techniques related to terrorism in the Zapatero administration are informed by the Prime Minister’s vision that terrorism should be defeated using the tools of soft power.

Spain, as a result, employs the use of a wide variety of public diplomacy techniques as part of its national and international counter-terrorism strategy, in addition to its traditional military-backed strategy. One of the most important initiatives for this is the Government’s commitment to interfaith dialogue using civil society.

The Spanish Government empowered civil society to play a key role in effectively delivering on this mandate. Organisations such as the UNESCO Centre of Catalonia (Unescocat) create and implement religious diversity programmes which seek to promote understanding and tolerance amongst the general Catalan population through inter-religious understanding. The use of Faith Diplomacy as part of a wider public diplomacy programme has been supported by prominent proponents such as Tim Livesey from the office of the Archbishop of Canterbury as an effective medium to achieve strategic objectives (Wilton Park, 2010).

The Spanish Government also launched a number of online diplomacy initiatives that support their real-world counter-terrorism programmes using public diplomacy. An example of this is the creation of the Alliance of Civilisations (Alianza de Civilizaciones). The initiative, launched in close cooperation with the United Nations and the Turkish Prime Minister, Recep Tayyip Erdogan, was designed as a subtle rebuke to Professor Samuel Huntington’s influential 1993 Clash of Civilisations thesis (Huntington 1993). It is a programme established with the United Nations designed to counter the spread of extremism and radicalisation through inter-cultural and inter-religious dialogue and cooperation. The organisation forms partnerships with other non-governmental organisations, corporations and governments on programmes that facilitate mutual understanding, and reconciliation amongst cultures; ‘and in particular, between “Muslim” and “Western” societies’ (Alianza de Civilizaciones, 2010).

In addition, the Government afforded considerable support to civil society groups who sought to join the fight against terrorism. One such organisation that uses its online profile to campaign against terrorism is the Victims Association of Terrorism (Asociación de Victimas de Terrorismo). This organisation was created by the mother of a victim of the Madrid 2004 bombings, through which she could gather a community of like-minded people to conduct counter-radicalisation work. Similarly, the organisation Basta! was created following ETA’s kidnap and eventual assassination of the Spanish politician Miguel Ángel Blanco in 1997. The organisation continues to attract people to the task of preventing future terrorist activity in Spain.

Spain has focused on public diplomacy strategies because it believes that effective counter-terrorism is not a technologically deterministic process. Rather, it is about identifying, establishing and maintaining good relationships with different actors using a variety of socio-technical means. As a result, Spain could better employ the use of the internet and the Web to fulfil its communication objectives as will be outlined in greater detail in Chapters Four, Five, Six and Seven.

## Conclusion

This chapter has focused its analysis of Government responses to terrorism operating in contemporary Spain. Ethno-nationalism continues to drive certain groups to perpetrate acts of violence against state infrastructure and citizens. However, policymakers consider the most pressing issue relating to terrorism and counter-terrorism to both Spain and France today to be the threat of international terrorism from organisations emanating from North Africa and South Asia.

As we have seen, during the 1980s the respective governments initially adopted very different tactics to counter-terrorism, one of sanctuary and the other, a hard-line, like-for-like exchange of killings. In the 1990s, however, both governments implemented similar strategies after becoming cognisant of the need to combine forces to counter domestic terrorism. Now, both states have come to appreciate the importance of countering international terrorism together as the increasingly borderless and globalised European Union (EU) leaves them potentially open to attacks from an enemy that is difficult to identify and even more difficult to stop. In addition, the War on Terror, like the Cold War before it, is an overarching political ideology which shaped the development and use of the internet and the Web in relation to terrorism and counter-terrorism in Spain.

The official policy of the Zapatero Government to increase cultural flows between Europe and the Maghreb, while maintaining and even enhancing border controls, recognises that a small group of people are responsible and that to isolate Spain from its neighbours would do much to foster resentment and ill-feeling amongst people in Maghreb countries.

France, on the other hand, has taken a different route and initially proposed to make Europe’s military forces more formidable should a more serious attack manifest in the future. France has also singled out the use of technology as a frontier in the fight against terrorism and, to this end, has created a database that monitors the online behaviour of the French people and underscores its renewed zeal to combat cyberterrorism over the next ten years when another security review is scheduled (Présidence de la République 2008).

These strategies suggest that both Spain and France have perceived the answer to the threat of terrorism to come from two different sources. Spain principally sees the need to address what it perceives to be the root causes of international terrorism, by withdrawing its troops from the Middle East in 2004 and fostering better multilateral solutions using supranational institutions. It is not only a solution that treats the source of the problem before it becomes a tangible issue to the state and the people, but also one that aligns itself closely with Barnett’s theory that greater integration of states in the non-Integrating Gap will deter violence. France, on the other hand, is cognisant of the need to protect itself and its allies from international terrorism. It sees the threat of terrorism as already present in society and that it should be dealt with by expansion of military forces and better surveillance of the people within its borders. To this end, France closely examines the trend of terrorists using technology to perpetrate attacks and implementing technologically deterministic measures to counter it.

Spain’s deployment of socio-technical responses to its terrorist threat is also encapsulated in its use of public diplomacy, particularly digital diplomacy, to influence domestic and foreign publics of the need to counter terrorism. This response is qualitatively different to that used by France, which has instead focused on technological solutions to decrease the threat of terrorism in the region.

Two understandings of terrorism have become clear; the globalisation of high technology and the evolution of the market state have led to market state terror in Spain (Bobbitt, 2008). The second is that effective responses to market state terror in Spain using communications technologies such as the internet should incorporate the use of effective online communications and engagement strategies to influence the attitudes and behaviours of online users. This could have the effect of convincing the general public of the nature of government counter-terrorism strategy, as well as dissuading people from accepting Jihadist ideologies. The process of engagement with communities, and creation of compelling narratives as part of counter-terrorism strategy, is investigated further in Chapters Five and Seven.

# **Chapter Three: The Ethics and Practices of Internet and Social Media Research**

## Introduction

Spain has one of the highest internet penetration rates in Western Europe[[21]](#footnote-21) and, using social media, users comment frequently on events and issues such as terrorism.

The increase in Web-based content makes the practice of internet research for terrorism more feasible as retrospective and real-time analyses can provide further insight on aspects of terrorism. However, the ability to aggregate and analyse such content raises questions about workable ethics guidelines, which, to date, have not been drafted.

The complexity surrounding the continued development of the Web and the internet, influenced by a range of actors from governments, to civil society to terrorist organisations, was analysed in Chapter One. This confluence of actors led to the conclusion that rather than conceptualising the internet and the Web from a technological deterministic perspective, it is preferable that they be conceived as social and cultural spaces where meaningful social interactions occur, or from a social constructivist perspective in Latour’s sense (1998). This conclusion led to the hypothesis that the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives.

The overarching research question was developed in Chapter One, which would permit the testing of the hypothesis: what understandings exist concerning the relationship between technology, terrorism and counter-terrorism in Spain? The following questions were posed to provide the overall thesis with greater richness and depth:

* How do we explain the understandings in Spain of technology, terrorism and counter-terrorism?
* What interactions have emerged from these understandings?
* What is the effect / result of these interactions?
* What are the implications for policy practitioners in the field of security and counter-terrorism?

In order to answer these questions, the context and the complexity of terrorist threats facing Spain were analysed in Chapter Two by comparing its official responses to terrorism with that of France. It concluded that, in spite of Spain and France’s close geographic proximity and shared terrorist threats, the two governments displayed very different understandings of terrorism, technology and counter-terrorism. France’s counter-terrorism strategy relies mainly on a technology-focused solution suggesting that the French Government adheres to the notion that the application of technology will have a direct effect on society and result in the reduction of terrorism in the region.

Spain, however, has adopted a more socio-technical approach to counter-terrorism by entering into bilateral agreements, developing a domestic counter-terrorism system and, crucially, by employing public diplomacy strategies aimed at contributing to counter-terrorism. Whether this latter day form of terrorism faced by Spain should be designated as “fourth wave” (Rapoport, 2004) or “market state terrorism” (Bobbit, 2008) was discussed in the previous chapter.

This chapter examines the numerous research methods used for the purpose of terrorism analysis and general social science research. It sets out an overarching methodological framework that will be used to comprehensively analyse the understandings of various actors and communities towards the internet, terrorism and counter-terrorism in Spain. This framework consists of semi-structured interviews of both counter-terrorism practitioners and other academic and commercial experts to provide insight on this issue. Secondly, the author created a methodology adapted from media analysis that systematically analyses the behaviour and commentary of online users and communities in relation to the research question.

A more complete account of the chronological details concerning the semi-structured interviews can be found in Appendix Two of this thesis.

## The Methodological Issues of Terrorism Research

Contemporary terrorist organisations have a clear understanding that a strong Web presence is an essential element in fulfilling a wide range of their strategic objectives. Weimann (2004) posited that the majority of prominent terrorist organisations, such as Hamas, ETA, the Liberation Tigers of Tamil Elam (LTTE) and al-Qaeda have prominent Web presences (Weimann, 2004). The fact that such a high number of terrorist organisations have Web presences should not be construed, as has been wont, as a threat to national security and an indicator of imminent attacks on government key strategic interests (Bendrath, 2001). In fact, that members of terrorist organisations, as well as members of the public who choose to engage in discussion on the topic, generate digital content presents an excellent opportunity to conduct more in-depth research on such organisations and the issue in general.

Rigorous research of terrorism has traditionally been beset by the problem that such organisations are notoriously difficult to gain valuable information from. Much of the information required is necessarily classified. The notion that ‘terrorists don’t fill in questionnaires’ has led to the charge that traditional research methods are inadequate to satisfactorily analyse terrorist behaviour, and that new approaches would be more useful (Davis et al. 2009). In his publication on the development of terrorism research, the terrorism scholar Andrew Silke supported this point, arguing that contemporary terrorism research is weak because it relies on mainly qualitative, journalistic methods to gain insights and data from actual terrorists. Silke adds that other methods are required as a matter of urgency and preferably those which are more quantitative than qualitative (Silke et al. 2004). The scholar Paul Davis supports this by claiming that another main source for information on terrorism – government files such as the court documents relied upon by other terrorism scholars to substantiate their research (Sageman, 2008, Reinares, 2009) – are not completely reliable as some governments have a vested interest in reporting lower incidents of terrorism, as this implies the success of their counter-terrorism strategies. New ways of presenting and interrogating data collected on terrorists are therefore imperative if the discipline is to progress (Davis et al. 2009).

Paradoxically, while there has been a call for more robust research methodologies by prominent terrorism researchers, traditional data-driven approaches of terrorism in the past were widely considered too complex and time consuming to be conducted by a team of human researchers. However, as mentioned previously, conducting research using the vast quantity of social media content available concerning the understandings of technology, terrorism and counter-terrorism would yield data that could be translated into usable research findings. It is this process of research that was elected and developed by the author to further interrogate the research question and test the hypothesis.

As new digital methodologies and tools emerge to analyse the nature of the behaviour of online users and the communities in which they congregate, this poses an important problem in the context of the research question, namely; of the array of methods available, which are the most adequate to investigate the range of understandings that exist concerning technology, terrorism and counter-terrorism in Spain, and the interactions that follow?

## Ethics and Practices of Online Research: Comparing Traditional and Contemporary Methodologies

### A History and Definition of Social Media

In order to fully understand the ethics and practices involved in internet research using social media content, it is critical to first establish a clear definition of social media so that the nature of the content being analysed is understood clearly. Any definition of social media should first include a description of Web 2.0 and user generated content. Such a definition assumes greater importance as the analytical distinction made between the internet and the Web in Chapter One, and throughout the thesis more generally, is not of investigative importance in the empirical research.

Web 2.0 is a term that was coined by the Web analyst Tim O’Reilly and was used to describe the collaborative use of Web technologies. Web 2.0 sites allow its users to create, collaborate, share and publish their own content such as video, text and audio files. Websites such as Dictionary.com and MSN.com were online spaces where the user simply consumed content without contributing to its creation, and are therefore technologically and ideologically different to Web 2.0 sites. These sites are ostensibly different to other websites, which actively seek user participation in order to create new content such as Wikipedia and the various blog platforms such as Wordpress and Blogger.

User generated content, which is produced using Web 2.0 as a technological platform, can be described as the creation of online content by the users of particular social media platforms. The Organisation for Economic Cooperation and Development (OECD) defined user generated content as digital content that could be placed on a website, to have demonstrated a degree of creativity and, finally, to not have been professionally created (OECD, 2007).

The first iterations of social media came in 1979 with the implementation of User Networks (Usenet), bulletin boards and Internet Relay Chat (IRC) portals, precursors to the more contemporary discussion forums and Instant Message clients. Discussions were hosted on distributed servers and anyone in the world could access them and contribute. Indeed, Usenets and bulletin boards have been described as the first internet peer-to-peer technology and global repositories of useful knowledge as ‘so many questions are asked and answered there. It is also particularly useful when looking for information about late-breaking or non-mainstream subjects likely to be part of the popular conversation’ (The Usenet Newsgroups, 2008: 1). Usenets and bulletin boards were the first incarnation of what would later become discussion forums in which users could participate in live online conversations. IRC portals were the first incarnation of modern-day instant message clients and chat rooms.

Contemporary discussion forums and instant messaging services subsequently displaced Usenets, bulletin boards and IRCs as widely used social media platforms. Sizeable communities coalesced around topics of discussion on bulletin boards and Usenets, in the same way as today’s discussion forums.

The premise and technology behind discussion forums is today incorporated in virtually all online social media such as blogs, video-sharing websites and social networks. Contemporary instant messaging services, such as Microsoft Network Messenger and Skype, permit their members to converse with each other in real-time whilst sharing a range of other content such as images, documents and video.

Social networking sites and blogs have become deeply influential elements of social media, attracting a great number of users. Over 130 million blogs are tracked by the influential blog search engine Technorati (Arrington, 2010), and one in four minutes spent by users online is dedicated to social networking sites (Nielsenwire, 2010).

In addition, contemporary social networking sites include a range of technologies that enable an array of real-time services, such as instant messaging, discussion forums and status update facilities, allowing users to update to their profile, and their larger network, details of what they are doing at any particular moment. The development of social media services and the ubiquity of these sites have been further enhanced by the continued development of mobile devices. Mobile devices now allow social network users to update their profiles wherever they are, without the use of a desktop computer.

The combination of Web 2.0 technologies, and the resulting emergence of user generated content, gives rise to an articulation of social media such as that given by Kaplan & Haenlein, ‘a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content’ as the most adequate description for the purpose of this thesis (Kaplan & Haenlein, 2010: 61).

### Privacy and Trust in Social Media Analysis

Privacy and trust in internet research is a contentious issue as online users are today constantly reminded of the need to protect their information from criminal actors by prominent media campaigns lobbying for greater public awareness. While it is possible to aggregate and analyse the information contained in social media portals, before research can commence, the question as to whether rigorous ethical standards can be maintained should be tackled. Before conducting internet research, one must consider whether the study conforms to the general ethical standards in Human Subject research. A variety of ethical guidelines have been written for numerous scientific disciplines based on the principle of Human Subject research. These guidelines refer to scientific experiments, which include human beings as active participants, including digital research programmes (Association of Internet Researchers, 2002). The Nuremberg Code (1947) is one of the earliest sets of ethical guidelines for scientific research in general, and was established following the Second World War to protect participants from questionable scientific studies. The first of its ten directives for human experimentation states:

‘The voluntary consent of the human subject is absolutely essential. This means that the person involved should have legal capacity to give consent; should be so situated as to be able to exercise free power of choice, without the intervention of any element of force, fraud, deceit, duress, over-reaching, or other ulterior form of constraint or coercion; and should have sufficient knowledge and comprehension of the elements of the subject matter involved as to enable him to make an understanding and enlightened decision…The duty and responsibility for ascertaining the quality of the consent rests upon each individual who initiates, directs or engages in the experiment. It is a personal duty and responsibility which may not be delegated to another with impunity’ (Office of Human Subjects Research: 1).

The principles outlined in the Human Subject model and subsequent Nuremberg Code guide the focus of ethical guidelines for other social scientific organisations where human behaviour is the focus of the research process (British Sociological Association, 2003, American Psychological Association, 2008, American Anthropological Association, 2010).

The human-centric nature of social media monitoring requires that any analysis project follow the principles of the Nuremberg Code and other social science research ethics. However, the computer-mediated nature of social media content mandates that a specially crafted set of guidelines outside the Human Subjects model is necessary for ethical digital research. Bassett and O’Riordan (2002) underscored this assertion, claiming that a new ethical framework for digital research should not be based on the current guidelines around the Human Subjects model because it could potentially limit the depth of analysis researchers are able to derive from digital content: ‘[t]o maintain a research model akin to the human subjects [sic] model would be to risk impeding and potentially eliminating promising research. It is not always possible, for example, to gain the consent of a large number of participants who may have changed their email address or ceased posting to a Web site [sic] on which the material under research is located’ (Bassett & O’Riordan, 2002: 1).

The issue of participant consent is central to any research programme that places the Human Subject model within the guidelines of other social scientific disciplines. The British Sociological Association guidelines for example state that: ‘*As far as possible* participation in sociological research should be based on the freely given informed consent of those studied. This implies a responsibility on the sociologist to explain in appropriate detail, and in terms meaningful to participants, what the research is about, who is undertaking and financing it, why it is being undertaken, and how it is to be disseminated and used’ (Bassett and O’Riordan, 2002: 1, emphasis added).

Bassett and O’Riordan’s argument (2002) is particularly compelling when conducting internet research. Online users are, in general, hostile to the notion that researchers might use their content for analysis purposes, risking the possibility that the researcher might be unable to use the content. In addition, soliciting permission for the use of social media content is often unfeasible due to the fact that the content creators might not be available. As a result, internet research programmes could become difficult to implement as any unauthorised use of social media content could go against the wishes of the original content creator. Commenting on the challenges of collecting data for internet ethnographic projects, the researcher Malin Sveningsson claimed that when looking at online discussion forums, ‘users would probably classify us as spammers, get annoyed and treat us the way spammers are generally treated, i.e. filter us out or harass us to leave. As a last resort, they might leave the chatroom themselves. Complicated studies often require that researchers give participants additional information, beyond the informed-consent statement. In practice, many studies are so complex that it is impossible to give participants a full explanation of the research before they participate, without running the risk of skewing the results’ (Sveningsson, 2003: 50).

The difficulties of soliciting permission for participant consent can be alleviated as scholars have argued that the conduct of research on the understanding that social media content is placed in a public place and considered available for public consumption, is acceptable. Johns, Chen, & Hall (2004) write: ‘[w]e view public discourse on Computer Mediated Communication as just that: public-analysis of such content, where individuals’, institutions’ and lists’ identities are shielded, is not subject to human subject restraints. Such study is more akin to the study of tombstone epitaphs, graffiti, or letters to the editor. Personal? Yes. Private? No…’ (Johns, Chen & Hall, 2004: 50).

Finally, data ownership and the extent to which researchers can aggregate social media content for their own purposes is another issue that should be considered before undertaking internet research. Ensconced within the user agreements of most social media portals is the condition that user generated content is owned by the company in question and third parties are not permitted to gather their content for their own purposes without authorisation.

In addition to the difficulty of gaining consent from content creators, internet researchers face the added problem of being unable to accurately verify the accuracy of the information contained in social media content. Online users actively protect their identities using a range of methods, one of which is the creation of alternate identities or *noms de guerre*: ‘[o]ne of the main subversive ways that users try to protect their social privacy is the use of an alias. Pablo, an [sic] newspaper editor, told me his boyfriend used “Awesome Andrew” as his Facebook name…The goal of this is to make it difficult for people to find them via search, or to attribute their Facebook activities to their “real” identities’ (Raynes-Goldie, 2010: 1).

The use of alternative identities has the effect of protecting a person from possible reprisals or any unwanted responses, while allowing them to express themselves more freely than with their personal identities. The ability of researchers to trust social media content rests, therefore, on a willingness of the original content creator to truthfully disclose their personal data, not their alternate identities (Kozinets, 2010).

The anonymity afforded by the internet and social media highlights one of the main differences between internet research and traditional research methods. Participants are generally required to devolve their real identifying information as part of the research (Kozinets, 2010). Social media users however are not bound by this and this, according to Beckmann & Langer, makes the job of internet research more difficult: ‘Cyberspace appears to be a dark hallway filled with fugitive egos seeking to entrap the vulnerable neophyte’ (Beckmann & Langer, 2005: 4).

However, the potential insight to be gained from the analysis of social media content, verified or not, enshrined within a workable ethical policy, is at once enticing and incalculable. One of the benefits of internet research is that the researcher has the opportunity of conducting unobtrusive research without disturbing the research environment, something that is not possible with other research methods (Kozinets, 2010). Johns et al (2004) underscored this point, claiming that a ‘benefit of virtual research is the extent to which it provides one with the ability to conduct research with virtually no “observer effects.”…Thus, virtual settings may provide the opportunity for “naturalistic research” in the extreme’ (Johns, Chen & Hall, 2004: 39). One of the main advantages of an undisturbed research environment is that the participants are free to express themselves in a more naturalistic way; ‘in which features such as one’s age, gender, ethnicity, and aesthetic appearance do not dominate social interaction...In such a setting, people are more likely to respond to the content of other’s interaction rather than their appearance or personality’ (Johns, Chen & Hall, 2004: 214). The issues presented above relating to ethics, privacy and consent in social media monitoring are some of the most prominent that the contemporary internet researchers have to consider. However, while it is possible within research programmes that utilise traditional methodologies to request the consent of participants, it is impractical and at times impossible in the case of contemporary research on large volumes of social media data.

It appears that the increasing volume of user generated content requires that internet research develops a wholly new set of guidelines based on the principles of the Human Subjects Model, and other ideas that can accommodate the complexity of the social and cultural content being analysed. Furthermore, these guidelines have to be able to protect the privacy of those people who produce the content in a way that does not compromise the efficacy of the research.

### Specific Internet Research Methodologies and Practices

For the purpose of the chapter, this section will discuss the uses of methodologies for the ethical conduct of retrospective and real-time monitoring and analysis of social media content. Firstly, it presents the range of internet research methodologies used as part of this thesis and explains the reasons for their inclusion. Secondly, it presents a range of other methodologies that can be used in the analysis of online terrorism and counter-terrorism communication but were ultimately not included as part of the thesis.

#### a. Content Analysis

Content analysis is a methodological approach that is used for internet research and, more specifically, was used to conduct analysis in this thesis. It uses a range of procedures for the systematic quantitative analysis of text, pictorial verbal and symbolic communications data (Krippendorff, 1980) and is used in communications research, particularly for ‘character-driven portrayals in TV commercials, films and novels, the computer-driven investigation of word usage...and so much more’ (Neuendorf, 2002).

A wide range of definitions of content analysis exists, posited by numerous experts. The influential US behavioural scientist, Bernhard Berelson (1952) described content analysis as a research technique for the objective, systematic and quantitative description of the manifest content of communication. Riffe, Lacy, & Fico (1998) define content analysis as ‘the systemic and replicable examination of symbols of communication, which have been assigned numeric values using statistical methods, in order to describe the communication, draw inferences about its meaning, or infer from the communication to its context, both of production and consumption’ (Riffe, Lacy & Fico 1998: 33). Content analysis is used frequently for internet research in order to capture the frequency, and, by implication, saliency of certain words, phrases and images.

Content analysis has been used to conduct terrorism research due to the increasing volume of online content in recent years and the extremely low barrier to entry in terms of its access. The inexpensive production of high quality online content such as video, text and audio content could make it far easier for terrorist organisations to propagate their *raison d’être* to an international audience. The result of this increase in online content from and about terrorist organisations has led to a great deal of information that can be subsequently analysed.

Some organisations exclusively examine large volumes of online terrorist content using content analysis such as the Search for International Terrorist Entities Intelligence Group (SITE), which searches the Web for terrorist websites and content in order to learn more about them. It claims to have developed several coding schemes ‘to analyze the contents of terrorist and extremist web sites [sic]. Content categories include: recruiting, training, sharing ideology, communication, propaganda, etc.’ (SITE Approach and Methodology, 2009: 1).

Content analysis was fundamental in investigating the semantic construction of online terrorist content to better identify the various persuasion strategies used by extremist organisations during the 2008 Gaza conflict. Following the creation of a coding scheme that categorised the strategies of online extremist content during the conflict, it was discovered that numerous instances of audience persuasion had taken place, especially that which sought to justify the actions of extremist organisations from a moral standpoint. It was subsequently recommended that future communications strategies could focus on communicating the messages of anti-extremist forces by constructing messages that have a strong moral component to them (Prentice et al. 2010).

There are, however, caveats to the exclusive use of content analysis for terrorism research, namely that a great deal of studies are limited to the study of English-language only content analyses. Content analysis therefore tends to rely almost entirely on the requisite linguistic skills of researchers to interpret the content they come across and can result in a vast corpus of content going unanalysed. This problem was experienced in Conway & McInerney’s exploratory study of auto-radicalisation from online video sources, and the researcher’s ability to analyse solely English language content and disregard potentially valuable Arabic language content (Conway & McInerney, 2009).

In addition to the above techniques, specialist software programs automate the content analysis process, which can be used in tandem with human researchers. However, the ability to conduct effective internet research has become increasingly difficult for a host of reasons. In the nascent stages of the development of social media platforms, access to the conversations hosted on discussion fora, IRCs and bulletin boards was widely permitted. Social media sites simply required potential users to create a profile, and access to all of the current and historical data was granted to them. Contemporary social media services, however, restrict widespread access to their data as part of their terms of service, restricting effective monitoring and analysis of social media content. The creator of the Web, Tim Berners-Lee, echoed this assertion by arguing that large social networks were, in effect, creating a two tiered Web because they effectively engage in ‘walling off information posted by their users from the rest of the Web’ (Berners-Lee, 2010: 1).

In addition, the use of both qualitative and quantitative social media monitoring tools provides a powerful mechanism through which to analyse social media content in real-time. However, the ability of these tools to fully analyse the wealth of information available is somewhat curtailed by the various access restrictions that companies have placed on their data. As part of their privacy policies, individual organisations, such as Facebook and Google stipulate that all content posted to their services remains their property. However, other services, such as Twitter, have less restrictive rules on their data where users can pay to access all the tweets generated or access a sample of content through Twitter’s application programming interface (API) (unless users specifically request that their tweets be restricted to people in their network). It is important that the reader is aware of this issue as it underscores how the issue of privacy can restrict the conduct of effective, unrestricted internet research.

Recently, natural language processing (NLP) technology has been applied to social media monitoring and is used as part of the internet research process within this thesis. It automatically analyses text-based digital content, speeding up the process of hitherto time-intensive analysis techniques such as content and discourse analyses. NLP technology provides the opportunity to examine a vast range of content in a number of languages and nuances.

Content posted on social media sites by users depicts their innermost feelings and daily activities, bestowing a unique opportunity to gain insight from people of the kind that has traditionally been available through polling and surveys. Content analysis and NLP technology were used as part of this thesis as both technologies and approaches were included on the content aggregation software used for the internet research process. In addition, the use of a manual content analysis allowed a more granular examination of the behaviour of the communities and online users.

#### b. Network Analysis

Social network analysis is a quantitative network analysis methodology that is used in contemporary terrorist research. It analyses the relationships between disparate items of information about terrorist organisations and maps them according to the results of statistical tests (Haythornwaite, 1996, Crossley et al., 2009). Social network analysis assumed prominence in social science research in the 1960s in tandem with the growth in use of the computer. In recent times, the technique has been used more widely in contemporary terrorism research following the distinct organisational change in terrorist organisations from hierarchical to more small scale, cellular structures (Ressler, 2006). A social network analysis performed on terrorist organisations would, therefore, present terrorist actors themselves or separate organisations for example as nodes, and the connecting links, or “edges”, in network analysis parlance, would denote the relationship between them. In addition, distances between the nodes can also represent the strength of the relationship calculated using various mathematical techniques. Contemporary terrorism research has made use of the technique as a method of identifying hitherto difficult to access information, such as individual or organisational information hubs within an apparently disparate group of cells.

Social network analysis has been applied in various examinations of violent political behaviour. In his analysis on the mapping of covert networks after the terrorist attacks of 11 September 2001 in the US, Valdis Krebs used social network analysis to map the relationships between the individuals responsible for the attacks. He concluded that, ‘[w]eak ties were almost non-existent between members of the hijacker network and outside contacts. It was often reported that the hijackers kept to themselves. They would rarely interact with outsiders, and then often one of them would speak for the whole group. A minimum of weak ties reduces the visibility into the network, and chance of leaks out of the network… The hijacker’s network had a hidden strength – massive redundancy through trusted prior contacts. The ties forged in school, through kinship, and training/fighting in Afghanistan made this network very resilient*.*’ (Krebs, 2002: 7).

Other studies have made use of social network analysis to map the relationships between various terrorist organisations. In their analysis of the topology of terrorist organisations on the Web, Xu et al. discovered that the networks are small worlds, that the in-degree and out-degree distributions follow a power-law degree and have a large amount of inter-site links (Xu et al, 2006).

In spite of the widespread use of social network analysis in contemporary terrorism and communications research, there is, however, criticism levelled at its use stemming from the notion that the cellular, fluid and interchanging nature of such organisations means that social network analysis can only analyse these organisations in a moment in time. By the time social network analysis has examined this information, the network might have already changed and its immediacy becoming all at once redundant (Borgatti, Date Unknown).

To circumvent this, some terrorism researchers have suggested the implementation of dynamic network analysis, a network analysis technique similar to social network analysis but its analyses comprise the methods of complex adaptive systems theory and can therefore map the composition of networks over time.

Dynamic network analysis is a technique derived from social network analysis and complex adaptive systems theory, allowing the researcher to map multiple relationships between data points over time. As detailed above, this technique is different to that offered by social network analysis, which permits the analysis of static datasets. Dynamic network analysis is, therefore, a potentially powerful analysis technique as it purports to be perfectly suited to the ever-changing terrorist networks that challenge nation states today. Indeed, one of the discipline’s prominent exponents, the scholar Kathleen Carley, claimed that employing dynamic network analysis allows researchers the opportunity to map changes in terrorist organisations over time and thereby reveal specific time periods and conditions during which change affected these organisations (Carley, 2002). She added that this type of analysis was imperative to include in terrorism research because, ‘terrorist organizations have network structures that are distinct from those in typical hierarchical organizations. Their structure is distinct from the organizations that most people in western culture are used to dealing with. In particular, they tend to be more cellular and distributed’ (Carley, 2003: 1).

In spite of the potential benefits that could be derived from dynamic network analysis, it is important to note the importance of detecting flows of incorrect data[[22]](#footnote-22) when using this methodology. Carley herself wrote of the potential pitfalls if incorrect information or “false alarms” are inserted into the network and subsequently, as there is no way of mitigating for this in a dynamic network.

Network analysis was used as a methodological approach for this thesis as it was considered the optimal approach to display the relationships between online communities and their requisite behaviour.

The following methodologies were not used as part of the internet research conducted in this thesis. However, it is important to outline their utility in conducting internet research of online behaviour in relation to terrorism in Spain.

#### c. Web Metrics

Web metrics (also described as Webometrics and cybermetrics) stem from the discipline of computer science and are employed in order to aggregate, extract and analyse pertinent online data to reveal information about online user behaviour. One of the most prominent exponents of this method, Michael Thelwall, described the discipline as ‘the study of web-based content with primarily quantitative methods for social science research goals that are not specific to one field of study’ (Thelwall, 2009: 6). The term was originally coined by the researchers Almind and Ingwersen (1997) in reference to the Web as an important source of user information and through which important metadata could be extracted. Thelwall claims that, in addition to web metric methods being capable of analysing important Web-based metadata, its use also allows the researcher to analyse old problems that have traditionally been considered to be real-world topics far more easily than in the past, such as public opinion and the spread of ideas (Thelwall, 2009).

Web metrics is an umbrella term used to describe the collective actions of a number of analyses, which examine qualitative Web data for the purposes of posthumous analysis. This particular type of analysis is particularly useful for analysing the online behaviour of content or online users: Web impact reports, for example, can reveal the online presence of a particular site or idea online. Other kinds of Web metric analyses, such as the analysis of Top Level Domains (TLDs) give the researcher insight into the geographic location of a site or content and are again important in determining the extent to which ideas and ideology have spread online.

Proponents of hyperlink analysis for example contend that websites are themselves actors, ‘linked by their hyperlinks…despite the Internet’s brief existence, its increasing role in communication has been made possible by the continual change in the structure of the network of hyperlinks’ (Thelwall, 2009: 22). Hyperlink analysis is increasingly used in political science research in response to the changing organisational structure of contemporary terrorist organisations, evolving from the more traditional hierarchical structure seen in the 1980s, to a more fluid, interchangeable cellular structure witnessed today. In addition, the scholar Park outlined the social constructivist notion that websites can be described as actors in their own right when he claimed that patterns of hyperlinks designed or modified by individuals or organisations who own websites ‘reflect the communicative choices, agendas, or ends…of the owners’ (Park, 2003: 53).

An analysis of the linkages and metadata contained within hyperlinks between websites can therefore be used to map relationships between terrorist organisations, where it was traditionally used to analyse the relationships between academic institutions in which UK institutions were ranked according to the number of hyperlinks linking to them (Thelwall, 2002). Such an analysis aligns itself with earlier work by Brin and Page who, when explaining the premise behind their PageRank algorithm, outlined that a Website’s influence could be ascertained by the number of other sites that link to it (Brin & Page, 1998).

Hyperlink analysis has subsequently been applied to a range of analyses of terrorist organisations, such as those by the Search for International Terrorist Entities Intelligence Group (SITE), which analyses the online activity of terrorist organisations by gathering online content from their websites with specialist content aggregators and spiders. Hyperlink analyses are then conducted to ascertain the relationships between established and newly found terrorist websites. In their study on the relationships between extremist websites, Reid and Chen concluded that the technique would be especially useful in demonstrating ‘both U.S. domestic and Middle Eastern extremist groups [having]…networked web clusters that appear to be organized based on ideologies and contain prominent websites…acting as nodes that link different clusters.’ (Reid & Chen, 2007: 51).

Other Web metric techniques are used to analyse the behaviour of online users and are especially useful in the analysis of online terrorist activity, namely behavioural tracking metrics. These metrics, which are otherwise known as web analytics or log file analysis, denotes the analysis of user behaviour from their interaction with the website itself, such as the number of page impressions, unique visitors and count of top level domains (TLDs) to determine the geographic location of users. Web analytic data has been used by researchers to investigate and measure the level of engagement and interactivity on a site, and is particularly useful in helping researchers identify the particular elements of content that resonate with people.

#### d. Web Analytics

The term Web analytics refers to the process of measuring, collecting, analysing and reporting internet data for the purpose of understanding and optimising Web usage (Web Analytics Association, 2010). There are two categories of Web analytics, which are on-site and off-site.

Off-site Web analytics refers to the measurement of general Web activity and includes the measurement of a Website’s potential audience, share of voice and overall volume of commentary in relation to general internet activity. They are macro-level tools which allow users to evaluate the performance of a website in relation to others. On-site Web analytics refers to the measurement of traffic to a particular Website. Such an analysis could include an examination of the landing pages that encourage people to make a purchase (Clifton, 2010).

The use of Web analytic data could, therefore, have the dual effect of indicating not only the popularity of a terrorist website, but also the behaviour of the users who access it, providing invaluable information that would help researchers understand the type of user that consumes online terrorist content, or which type of content resonates most strongly with online users.

#### e. Netnography

Netnography, or ethnographic studies mediated by the internet, is a technique used to analyse the behaviour and composition of online communities. Developed in 1995 by Robert Kozinets (2002), studies are conducted of online communities and cultures utilising publicly available information to identify the needs and desires of a particular online community.

Netnography is useful as a research approach as it ‘is capable of being conducted in a manner that is entirely unobtrusive. Compared to focus groups and personal interviews, “Netnography” is far less obtrusive, conducted using observations of consumers in a context that is not fabricated by the marketing researcher’ (Kozinets, 2002).

The methodology, described by Kozinets (2002) as ‘a new qualitative research methodology that adapts ethnographic research techniques to the study of cultures and communities emerging through computer-mediated communications’, analyses online content and discourse as real examples of social interaction, an embedded expression of meaning and cultural artefact (Kozinets, 2010: 5).

According to Kozinets (2010), netnography’s popularity amongst researchers is apparent because it is ‘*naturalistic*, following social expression to its online appearances. It is *immersive*, drawing the researcher into an engaged, deeper understanding. It is *descriptive*, seeking to convey the rich reality of contemporary consumers’ lives, with all of their hidden cultural meanings as well as their colorful graphics, drawings, symbols, sounds, photos, and videos. It is multi-method, combining well with other methods, both online and off, such as interviews and videography’ (Kozinets, 2010: 4, emphasis in original).

Kozinet’s description of the scope of netnography to interrogate the various social and cultural interactions from social media or computer mediated conversations represents one way in which internet research can be conducted to accurately analyse the underlying complexities of interactions on social media. This approach, therefore, implies that it is important to ascertain not only what people say online, but also why they might say it.

The internet scholar Annette Markham also discusses the use of other qualitative methods to conduct internet research such as email interviews, instant message interviews and interviewing via video conferencing. However, these approaches are not without their problems. Email interviews and instant messaging interviews allow the participant to retain a degree of anonymity and proximity from the interviewer, although, as Markham comments, this ‘may be inadequate for certain participants or research questions’. She adds that some participants, while preferring to conduct an interview via video conferencing, might provide more information if they were able to email or instant message the researcher during the process of the interview (Markham, 2011: 115).

#### f. Mobile Research Methods

Online research methods that have been specifically modified for mobile devices represent a new frontier. Mobile device is a collective term used to describe a range of Web-enabled mobile devices such as tablet computers, mobile phones and laptops. With experts predicting that people will increasingly connect to the internet via their mobile devices and not via personal computers, the opportunity to conduct research either using mobiles or social media optimised for such devices, is significant (Warah, 2009).

There is a range of mobile research methods applicable to the monitoring of social media in real-time, one of which is location-based research. The accumulation of real-time location data by such techniques as Global Positioning System tracking (GPS) has been used extensively by social media organisations to promote services such as crisis mapping (Coyle & Meier, 2010) and social networking. However, researchers must also be mindful of unwittingly encroaching on users’ privacy when accessing a person’s specific location: ‘privacy is an essential issue...and the subject is often addressed in terms of how sensitive information is kept secured in the application…Identity has several aspects to it and we consider a person’s position to be a specific attribute of identity, like full name and social security number. The major difference between location and most other attributes is that location changes continually and is mostly relevant to mobile computing’ (Barkuus & Dey, 2003: 3).

Although the development of methodologies for internet research has spawned a variety of methods, it is clear that the need to combine information from a range of different methods is of singular importance. Traditional research methods, therefore, remain a key element of any study on terrorist organisations, the testimonies of key audience groups with close relationships to such organisations provides the researcher with a degree of insight that is extremely useful and otherwise difficult to obtain (Richardson, 2006). Interview-based research has traditionally required the researcher to physically present questions to the participant. However, researchers are increasingly utilising online tools to more easily question and analyse a greater number of participants across a larger geographical distance than it has been possible to do hitherto. Examples of the use of online surveys are less well known in terrorism research and are more widely used in general political science research such as research undertaken by Best & Krueger who investigated public perceptions of government surveillance online (Best & Krueger 2008). A survey was created by the Center for Survey Research and Analysis, which surveyed the opinions of 670 people. The results were then analysed using multivariate and descriptive statistics to determine patterns between the responses. Best & Krueger found that non-violent political phrases critical of the executive government influenced perceptions of internet surveillance and had implications on the debate about whether the internet will become a means of citizen empowerment.

The primary research derived from interviews and questionnaires is of great benefit to terrorism researchers. Members of terrorist organisations are extremely difficult to access for research purposes, which would otherwise yield extremely valuable results. This difficulty has been overcome in research by terrorism scholars such as Louise Richardson (2007), John Horgan (2010) and Fernando Reinares (2009) who have conducted face-to-face interviews with those suspected and convicted of terrorism-related offences. However, it has been proffered that interview research only provides an image of the interviewee at a specific place in time, ‘and growing levels of non-response are crumbling its scientific foundation’ according to the scholars King et al. (2009). They argued that interview research on political behaviour is being increasingly supplemented by research with various forms of electronic data ‘based on text sources (via automated information extraction from blogs, emails, speeches, government reports, and other web sources), electoral activity (via ballot images, precinct-level results, and individual-level registration primary participation, and campaign contribution data), commercial activity (through every credit card and real estate transaction and via product RFIDs), geographic location (by carrying cell phones or passing through toll booths with Fastlane or EZPass transponders), health information (through digital medical records, hospital admittances, and accelerometers and other devices being included in cell phones), and others’ (King, G., Schlozman & Nie, N.H., 2009: 92).

In spite of the persuasive criticisms made by Silke in his arguments over the utility of the current state of terrorism research, it is apparent that his contentions do have some limitations. Indeed, alternative approaches to the conduct of terrorism research, such as the psychosocial approach offered by the scholar John Horgan, for example, do much to complement the socio-technical explanation for the development of the Web and the internet outlined in Chapter One. It can, for example, be shown that terrorist organisations attempt to influence the perceptions of the general public by utilising the entire range of media technologies such as the radio, television and the internet. The process of influencing people can be said to have a strong psychosocial element to it.

The psychosocial approach to terrorism research can be defined as the study of the various ways political acts can be interpreted as acts designed to influence people as opposed to inflicting physical harm (Papastamou et al. 2008). It can be conceived as the environment in which people’s behaviours are conditioned and influenced by the socio-structural frameworks in which they live, in addition to their psychological predispositions. It is different to a macrosocial interpretation of terrorism, which is defined as ‘a reflection of various social dysfunctions or conflictive trends in the social system’ (De La Corte, 2007: 1). De La Corte adds that it is also different from psychopathological approaches to terrorism, which attempts to understand the terrorist through their propensity for violence and perceived inability to control their violent urges.

The scholar De La Corte sought to explain the nature of terrorism using a psychosocial approach, in which he created a model of the psychosocial development of terrorism that he segmented into seven separate sections.

**Table One: The Psychosocial Principles of Terrorism**

|  |
| --- |
| **Psychosocial Principles of Terrorism** |
| * Terrorism is not a syndrome but a tool of social and political influence |
| * The attributes of terrorists are shaped by processes of social interaction |
| * Terrorist organisations can be analysed by analogy with other social movements |
| * Terrorism is only possible when terrorists have access to certain resources |
| * The decision to begin and sustain a terrorist campaign is always legitimised by an extreme ideology |
| * Every terrorist campaign involves strategic goals but the rationality that terrorists apply to their violence is imperfect |
| * The activity of terrorists partly reflects the internal features of their organisations |

Of primary utility for the purpose of this chapter, is De La Corte’s first point in the list of Principles as he argues that terrorism should be perceived as a tool of social and political influence and not as a syndrome that afflicts a small minority of people. He contended that terrorist actions should be interpreted as those which incorporate several interactive processes that take place in both inter and intra-group environments. He added that these processes take place in a strategic way as, often, terrorist organisations utilise an advertising technique similar to propaganda campaigns when promoting their cause (De La Corte, 2007). These campaigns and interactions can take various forms such as discussions on various social media platforms or other internet discussion services. De La Corte also put forward that the most important element in the psychosocial development of terrorism is that the minority group (terrorist organisation) effectively influences the opinions and beliefs of the majority group (the general public), as ‘the spreading of fear or terror through violence has a communicative dimension’, making it akin to public relations campaigns (De La Corte, 2007: 1).

De La Porte’s second principle of the psychosocial composition of terrorism is that the attributes of terrorists are shaped by processes of social interaction. By this, De La Porte argues that, while certain social interactions with respect to terrorism, can take place physically, there are many other cases in which social interactions can take place in computer mediated environments such as the internet and social media. With regard to the focus of this thesis, the examination of people’s responses to terrorist behaviour in Spain using social media and other Web-based discussion services, serves as an original and complementary method through which to examine such behaviour and, indeed, one element of the psychosocial nature of terrorism in Spain, to other studies that have been conducted hitherto.

A prominent example of the ways in which psychosocial tactics have been interwoven into the interpretation of terrorism can be seen in research by Mythen and Walklate (2006) in which they examined the way British government departments communicated the threat of terrorism to the public. They claim that the post 9/11 construction of a new global terrorism threat has been exploited by the British Government with the aim of garnering increased public support for international military activity and changes to the law. Moreover, Silverman and Thomas (2011), in their analysis of the role of psychosocial tactics used by the media to influence the perceptions of the general public in relation to terrorism, argued that the fragmenting media landscape in the UK was largely responsible for enabling politicians to alter the public’s perception of terrorism to their own ends, something the scholar Barry Richards termed emotional governance to describe the ‘deliberate attention paid by politicians to the emotional “dynamics” of the public’ (Silverman and Thomas, 2011: 10).

Indeed, the psychosocial role of the media to influence the general public to radicalisation is tackled in research by the scholars Andrew Hoskins and Ben O’Loughlin in which they conducted semi-structured interviews with British Muslims, aiming to demonstrate that the mainstream media plays a prominent and influential role in terrorism and security studies. They claimed that ‘a pervasive and continuously present medial underlayer relating [to] the suffering of persecuted groups (for example, Palestinians), and the weakness of western administrations’ responses to that suffering, that the mainstream is viewed and understood by those seen as potentially ‘vulnerable’ to violent extremist messages’ (Hoskins and O’Loughlin, 2010: 903). Indeed, their findings revealed that when groups of British Muslims were shown radical material, they could understand and sympathise with the motives of some Jihadist actors without supporting their actions because the media content reinforced and justified *a priori* narratives of Muslim grievance.

Indeed, Hoskins and O’Loughlin contended that news reporting, which takes the form of security journalism, has delivered regular representations of the perceived terrorist threats on a nationwide basis ‘showing “us” the threat “we” face by offering coverage of Al-Qaeda leaders’ speeches, bomb attempts, criminal trials and “radical” protestors in Britain…By repackaging and remediating jihadist media productions from one context and language into another, reporters offer to British audiences “messages” presumed to be radicalising to would-be jihadist recruits’ (Hoskins and O’Loughlin, 2010: 905). Hoskins and O’Loughlin also exclaimed that British security journalism regularly reduces complex Jihadi texts ‘to short clips of angry, gesticulating men’ (Hoskins and O’Loughlin, 2010: 905), which has the effect of impeding understanding of the apparent threat because some of the content of the texts could be persuasive to Muslim audiences.

Another prominent scholar who has published influential research focusing on the psychosocial nature of terrorism is John Horgan who argued that terrorism is a psychosocial process. Horgan conducted a series of interviews with individuals from 2006-2008 on the topic of disengagement from terrorist organisations. He claims that while all the interviewees could be termed as dis-engaged from the practice of terrorism, ‘not a single one of them could be said to be “de-radicalised”. In fact, even the process of disengagement was highly idiosyncratic for those interviewed. For some, leaving the movement was temporary, with some members opting to come back to the movement at some later stage. Sometimes, this was to a different role, otherwise it was a return to the same role or function held before the initial departure’ (Horgan, 2008: 1). In particular, Horgan argued that there are various psychological and emotional issues that lead to disengagement from terrorism and terrorist organisations such as a change in personal priorities, the development of negative sentiments or a sense of growing disillusionment with the avenues being pursued.

While it is imperative to consider the role of psychosocial processes in respect to terrorism, it is the focus of this thesis to analyse the nature of online behaviour and conversation of online users on social media in relation to the topic. It is the contention of this author that adopting a multidimensional, cross-disciplinary work incorporating the psychosocial analytic processes into the nature of terrorism in Spain would be beneficial. However, for the purpose of this thesis, it is beyond the scope of work.

## Measurement Approaches for Digital Public Diplomacy

### Why Measure Public Diplomacy Programmes?

* As previously outlined in Chapter Two, public diplomacy programmes have been used by the Spanish Government as part of its counter-terrorism strategy, however there is a lack of information concerning the measurement of the effectiveness of such programmes. The measurement of public diplomacy programmes for counter-terrorism can provide understanding on the efficacy of engagement and influence strategies, something that was outlined at a public diplomacy conference at Wilton Park in which it was mentioned that ‘[e]valuating the impact and value of Public Diplomacy campaigns is as essential as the overall campaign in difficult economic conditions. If we cannot robustly prove the effect and return on investment of campaigns then we cannot improve them in the future’ (Ampofo, 2010: 1). Such measurement techniques are strongly linked to the internet research conducted in this thesis as digital public diplomacy programmes seek to elicit responses from online users and communities in relation to terrorism and counter-terrorism.

The ability to accurately evaluate the success of a digital public diplomacy programme is much easier now that software and methodological processes exist that allow practitioners to examine online behaviour. This, coupled with the analysis of external data, such as information and data from a specific initiative, can generate insights into the effectiveness of the programmes in achieving strategic objectives. Although the Spanish Government is yet to attempt this, the thesis will offer such an analysis of the online behaviour of Spanish language Web users in response to the 11 March 2004 terrorist attacks in Madrid.

As such, this thesis is of practical relevance to public diplomacy practitioners who are themselves under pressure to measure the impact of their initiatives. The public diplomacy measurement scholar Ali Fisher argued that ongoing measurement and evaluation of public diplomacy is critical because ‘it underpins evidence-based evaluation, prioritisation, policy planning and spending. This is highly challenging particularly amidst changing priorities and threats, but not uniquely so’ (Wilton Park, 2011: 1). As practitioners are under increasing pressure to deliver successful programmes, it is possible to provide evidence-based analysis of the strengths and weaknesses of specific programmes and for the practitioner to act upon this information quickly and effectively. Indeed, measurement techniques have been employed to a number of counter-terrorism programmes with differing measures of success or key performance indicators (KPI).

The effectiveness of digital diplomacy programmes can be assessed by implementing network analysis to examine the differing relationships between data in order to arrive at new insights. Ali Fisher commented that network analysis of digital diplomacy initiatives could yield significant insights, thereby improving the efficacy of such programmes. He argued that ‘[t]o understand online actors and conversations, it is important to recognise the links between them. A network approach, focusing not on the “points” (users of forums) but on the connections between them, reveals both the wider context of jihad online, and the “information horizons”…of the vulnerable or radicalised individuals who are of concern. Self-association between individuals or between individuals and different web forums reveals complex networks, in multi-hub, multi-directional systems...This approach, although apparently theoretical, allows analysts [sic] to move past lists and see connections. With further work this may illustrate the dynamics of online conversations and association – for instance, showing when sites reappear, how users migrate between Jihadi sites (and to and from non-jihadi sites), and the growing or weakening influence of particular individuals or messengers’ (Wilton Park, 2011: 4). However, at this juncture there is inherent difficulty in securing online content for analysis and evaluation. Online content is characteristically ephemeral and subject to deletion or alteration by the site administrator. This poses challenges to practitioners and researchers wishing to analyse the content. This problem can be overcome if regular content aggregation and storage is conducted, although this solution is costly and requires considerable data storage space and security facilities. Indeed, the author had to overcome similar challenges when conducting the internet research for this thesis as outlined in Appendix Two.

If, however, relevant volumes of online content can be accessed, sentiment analysis is a useful method of analysing the general disposition of the public towards a particular public diplomacy programme. Items of content are analysed by software programs or human analysts who then assign the item a sentiment ranking from strongly negative to strongly positive. While a more detailed description of the sentiment analysis used for the purpose of this thesis is given in the methodology section for the internet research below, such analysis is not without its problems as the analysis of volumes of content is time consuming and prone to error for both machine and human analysts (Kanayama et al. 2004, Read et al., 2007, O’Connor et al., 2010).

It is also possible to conduct attribution analysis of online content by aggregating specific content related to a public diplomacy campaign. This can be achieved using specific online content aggregators such as Sysomos, Alterian or Radian6, which gather online content specifically related to a particular programme or campaign. The content derived from such a search would reveal the number of conversations online that referred to the programme or initiative in question. This kind of analysis is also known as citation analysis and has been used extensively in information science research, during which the importance of academic articles was measured by the number of times they were referenced (Thelwall, 2004). Conducting this kind of analysis will present to the researcher insight on the share of voice a particular programme has in relation to others. This technique will be used in Chapters Four to Eight. In addition, traditional research methods are also used to measure the effectiveness of public programmes or campaigns. Interview research has been used to derive insight of the perceptions of key audience groups of particular campaigns or programmes.

Finally, real-time data capture and analysis methodologies can be used to analyse the impact of public diplomacy programmes. Real-time data capture and analysis methodologies describe the implementation of a range of techniques and software tools that allow the researcher and practitioner the ability to aggregate and analyse relevant information as it is created in relation to a particular initiative. This helps the project coordinator react to critical information as it arises and quickly formulate appropriate responses. These techniques, which are in their nascent stages, have demonstrated potential in their ability to provide insight and effective evaluation of public diplomacy programmes and complex emergencies (Coyle & Meier, 2010). This will be employed in Chapter Eight, where real-time data is aggregated and analysed following the death of Osama bin Laden.

## Approach Used for the Internet Research: Methods and Categories for Analysis

The internet research conducted to empirically test the main hypothesis of this thesis examined online content generated in relation to the terrorist attacks of 11 March 2004 in Madrid. The study aggregated and examined online content each year during a six month period (11 March – 11 August) over a period of seven years (2004 – 2010), in order to conduct a longitudinal analysis of online behaviour occurring during that time. The study aggregated and examined online discourse in Spanish language.

Aggregating content retrospectively is a challenging task due to the ephemeral nature of the availability of online commentary. It is almost certain that a number of posts that were available in 2004, and would have contributed to the subsequent analysis, have been deleted or altered by website administrators. The scarcity of historical online content is further compounded by the distinct reduction of online media portals available in 2004 compared to those publicly available today. Facebook, which was launched in 2004, was made available to the general public in 2007, Twitter in 2006 and YouTube in 2005. To this end, the author elected to focus the analysis on a manual and automated retrospective examination of online media channels that yielded relevant content in 2004 (and in all years since), namely web logs (blogs), discussion forums and websites. The analysis of these specific online media channels was conducted over a seven year time period in order to retain consistency of the media types examined.

There are, however, advantages and disadvantages involved in omitting certain social media channels such as social networking sites and micromedia, which shall be considered subsequently.

One of the disadvantages of omitting the aforementioned social media channels is that they are prominent destinations for online users. In order to illustrate this, it is pertinent to consider the statistics from the multinational advertising and market research corporation Nielsen Ratings in 2010 that online users spent one minute in every four on social networking sites. This, according to Nielsen, ‘equates to 22 percent [sic] of all time online or one in every four and a half minutes. For the first time ever, social network or blog sites are visited by three quarters of global consumers who go online, after the numbers of people visiting these sites increased by 24% last year’ (Nielsen, 2010: 1). Nielsen’s analysis underscores the fact that the popularity of social networks is high and coverage of this 22 per cent of internet use would yield a considerable amount of relevant content about the behaviour of online users and communities useful for this thesis. However, there are numerous reasons that provide justification for the author’s decision to focus on the social media channels that generated relevant content in 2004.

One of the main benefits of focusing on specific social media channels is that it ensures the consistency of the analysis of media types throughout the dataset. This assertion is ostensibly difficult to put into practice, as it is clear that websites, discussion forums and blogs conflate a number of media types into one posting. An article on a website or blog post can normally include video, audio, text and images, making analysis of such online content problematic. However, it was decided that for the purpose of this thesis, it was analytically more useful to conduct research on the four aforementioned media types, although the author has outlined in Chapter Eight the potential benefits to be gleaned in conducting longitudinal analysis of social media content evaluating a range of digital media channels.

In addition, it is important to consider the notion that the barrier to entry for creating an article on a website or blog post is high. The inherent complexity and difficulty in creating influential content on these media channels is illustrated by Drake (2010) in which she outlines that it is a common perception that blogging and creating lengthy, accurate social media content is ‘hard and time-consuming’ (Drake, 2010: 1). The high barrier to entry in creating accurate content therefore results in fewer people creating content and much less “noise”[[23]](#footnote-23), or irrelevant content for the researcher to sift through. The introduction of new social media channels such as status updates and microblogging, which emphasise brevity and immediacy and provide a “stream” of information to users, can also result in a high level of “noise” (Loayza, 2010). In addition, the proclivity of some online communities, of the kind witnessed in discussion forums, to require a rigorous authentication process before trust is conferred on new participants entering online communities can result in more relevant content (Friedman, Kahn, & Howe, 2000).

The date range of the internet research was selected at six months from 11 March to 11 August, over a period of seven years (2004 to 2010). This particular date range was elected in order to analyse the evolution of discussion and user perception at six-month intervals over a period of seven years. It was decided that a retrospective longitudinal analysis incorporating these dates would gain access to content directly related to the Madrid attacks and people’s reaction to it. This approach, although problematic because of the potential lack of access to data, is preferable over and above a static analysis of content relating to the attacks from a particular search in 2011. An analysis of this kind would simply provide a snapshot of discussion concerning the event from indeterminate points in time. It was instead concluded that there is far more utility in obtaining a sense of the discussion over time by conducting a structured annual analysis that allows us to compare and contrast opinions and understandings over time.

Upon electing the optimal research approach, it was determined that the automated content aggregation would be conducted using proprietary software, namely the online media content aggregation software Techrigy by Alterian. This software was chosen primarily because online content stored *en masse* in the company’s data warehouses since 2007 offers researchers the opportunity to conduct in-depth retrospective analyses of online content. For the purposes of this research, it was deemed useful to combine Alterian’s historical archive while simultaneously conducting manual searches for content.

In order to manually accumulate content from 2004 to 2006 in the public domain, a range of free search engines were employed by the author including Google Blog Search and Group Search, Board Reader, IceRocket, Big Boards and Blogdigger. Online content was aggregated in this fashion for the years 2004 to 2006 because it is unavailable in Techrigy’s data warehouses, and is difficult to aggregate because of its relative scarcity.

Online content was aggregated using a range of carefully selected keywords associated with the Madrid 2004 terrorist attacks. Suitable keywords were chosen based on contextual research that allowed the author to analyse the variety of key narratives delivered and the different types of community that delivered them. As a result, key narratives from terrorist organisations and government departments were analysed as the most effective way to ascertain which narratives from the organisations were discussed online, how, and which communities were responsible for propagating them.

The lexicon of key narratives was gathered from academic papers that had conducted analyses on media content in traditional media channels previously. Manuel Torres Soriano’s (2008) study on the mentions of Spain in Jihadist propaganda (Soriano, 2008), during the Madrid bombings provided the author with a comprehensive list of terrorist narratives delivered during 2004 related to Spain. These narratives were subsequently inputted into the content aggregator as keywords to gather material used to conduct the online research for the thesis. The selection of keywords for this thesis has been used in similar studies of terrorism research conducted by other scholars and practitioners using online content. One study in particular, employed a similar process to that employed in this thesis. Bunt (2003) conducted an analysis of the reaction of online users identified as Muslims to the content contained within terrorist websites. Bunt employed qualitative analysis of messages from al-Qaeda and Taliban websites and analysed the response of Muslim users. However, it is pertinent to note at this stage the assertion made by Qin et al. (2007) in which the inherent failings of employing purely manual analyses of messages in social media were outlined. Qin et al. asserted that the majority of online terrorism researchers do not use automated methodologies for aggregating and analysing content on websites due to ‘the enormous size and dynamic nature of the Web, the manual collection and analysis approaches have limited the comprehensiveness of their analyses’ (Qin et al., 2007: 73). In addition, Gerstenfeld et al. (2003) conducted a content analysis of extremist websites in which they analysed 157 websites to ascertain how extremist groups use the Web. Through this analysis, they determined that the internet and the Web are effective tools in allowing extremists the opportunity to reach a broad international audience, conduct recruitment and maintain their public image. Such conclusions resonate strongly with analyses of the ways in which the Web is used by terrorist organisations, as mentioned in previous chapters such as Wiemann (2005), Conway, (2005) and Bobbitt, (2008).

Finally, Yang and Ng (2007) used content analysis and social network analysis to analyse terrorism and crime related blogs. The content analysis was used to analyse similar blog messages to view any relationships and to aid the subsequent social network analysis. The content analysis was conducted by segmenting the requisite post into logical units for the analysis. However, Yang and Ng acknowledge one of the principal difficulties with content analysis of social media data, similar to that encountered by the author; namely that narratives and social media data may not be written in correct grammar or sentence structure (Tand & Ng, 2007: 4). In order to overcome this difficulty, and for the purpose of this thesis, the author did not rely on automated text analysis, as there existed the propensity for relevant data to be overlooked and irrelevant data to be included into the overall datasheet. Rather a combination of NLP text analysis software and human analysis was used to analyse social media content.

In order to collate the Spanish Government’s narrative after the attack, a preliminary analysis was conducted of print media content using the Lexis Nexis database. The key narratives used by the Government to convey their most critical narratives during the crisis focused on content contained in prominent Spanish newspapers *El País, El Mundo* and *La Vanguardia*. In addition, an analysis of Government press releases situated on the official website La Moncloa also helped collate Government narratives.

As a result, it was decided to focus on a small corpus of narratives. Ten narratives were chosen; five from Government departments and five from terrorist organisations. This decision was made in order to render the subsequent aggregation and analysis of content more focused. It should also be noted that every keyword was preceded with the fixed words “11-M OR 11 Marzo” AND “terrorismo OR atententado” in the Boolean format. Table Two below details the range of key narratives chosen for both Government and terrorist organisations, in addition to the range of keywords selected for the content aggregator. Additionally, it should be noted at this juncture that the search engines used to seek for variations on certain words compensated for the possibility that various words will be used to describe the event over time. This is important because investigating a static set of words would exclude the evolving wide range of vocabulary used by different users and communities over time.

It is important to acknowledge at this juncture that it is problematic to utilise one set of keywords applicable to a dataset that comprises content over an extended period of time. It is challenging because it presupposes that the terms used by online users in 2004 would continue to be used in 2010. As a result, there was the potential to miss certain relevant content that might have arisen in a different time period as a result of the changing nature of online discussion. The author overcame this problem by ensuring that the search engines and content aggregators used natural language processing technology that automatically searched for various iterations and permutations of words. For example, by inputting the word “Jihad”, the content aggregators were able to gather content featuring other permutations of the word such as “Jihadist”, “Jihadism” and “Jihadi”. The internet research completed in Chapter Eight overcame the aforementioned eventualities by conducting real-time research and analysis of online reaction to the death of al-Qaeda leader Osama bin Laden.

A list of the narratives and keywords used as part of the 11-M online analysis is detailed below:

**Table Two: List of Narratives and Keywords by Organisation Used for the Internet Research**

|  |  |
| --- | --- |
| **Terrorist Narratives** | **Keywords** |
| * Jihad will reclaim land that was once part of the Caliphate | * Al-Ándalus, Liberación, Ceuta, Melilla, Tierra Islámica, Reconquista, Limpia las tierras del Maghreb, recobra Al-Ándalus, Liberar Al-Ándalus |
| * Al-Qaeda will launch repeat attacks if necessary | * Repetir, recurrimos la lenguaje del sangre |
| * Spain’s participation in Afghanistan and Iraq invasions has made it a target | * Presencia militar de España en Afganistán, retirada de Irak, tropas en Irak, muertos en Irak |
| * Spain’s general elections are an opportunity to strike | * Eleccion General, Al-Qaeda en Europa, Politica gubernamental |
| * Al-Qaeda was responsible for the attacks | * Culpabilidad, Al-Qaeda en España, Abu Dadah, Yihadista, Responsabilidad, Islamista, Ninguna duda, Lo que ocurrió en Madrid. |

|  |  |
| --- | --- |
| **Government Narratives** | **Keywords** |
| * The Government will obliterate terrorism in Spain | * No es posible ni deseable negociar, derrota completa y total, defender la constitución, logramos acabar con la banda terrorista. |
| * ETA is responsible for the attacks | * Responsable, acto de ETA, cometido, culpabilidad, autoría del atentado, dinamitar la democracia |
| * Terrorism must be defeated with dialogue | * Colaboración internacional, reforma del código penal, acuerdo contra el terrorismo, merece la pena |
| * Compassion must be shown to the victims of the Madrid attacks and all victims of terrorism | * Respeto a las víctimas, homenaje, recuerdos a las victimas |
| * Spain and the international community must remain united in the fight against terrorism | * Estamos en una guerra, alianza de civilisaciones, estamos en peligro, cultura de unidad, combate de las ideas, contra el terrorismo |

Source: Lawrence Ampofo

After the identification and definition of the keywords, content was aggregated and a content analysis then conducted. The content analysis allowed the data to be segmented into the following categories:

**Communities**: Online content was categorised by community group based on the principal issue focus of the online portal from which the content was sourced, based on a description of the source by the website’s owner. For example, online portals that demonstrated a principal focus on the 11 March bombings were categorised as 11-M, while those which focused fully on general political issues were categorised as Political, those online portals that had an indeterminate issue focus were categorised as the General Public. As discussed extensively in this chapter, it is not always possible or reliable to ascertain the true identity of those people who maintain the websites in questions or those who choose to make comments or other forms of user generated content.

**Most Frequent Narrative**: The most frequent narrative segmentation refers to the principal narrative contained within a specific post. This categorisation was completed in order to fully ascertain the main impetus for the post in question. It was critical to include this category to investigate how the principal motivations of online users evolved over time. For the purpose of this thesis, the most frequent narrative refers to the narratives which were iterated by online users most regularly.

It is important at this juncture to define exactly the nature of a narrative before commencing with the presentation of the findings of the empirical research. Narratives are complex linguistic structures that allow humans to make sense of complex and occasionally unconnected phenomena. Antoniades et al. (2010) analysed the various ways in which nation states use “strategic” narratives to achieve their stated aims and objectives. They defined narratives as semantic structure that ‘entails an initial situation or order, a problem that disrupts the order and a resolution that re-establishes order, though that order may be slightly altered from the initial situation. Narrative therefore is distinguished by a particular structure through which sense is achieved’ (Antoniades et al., 2010: 4). Here we see that the aforementioned definition is appropriate for analysis of the empirical evidence as a phrase such as ‘Jihad will reclaim land that was once part of the Caliphate’ fulfils all of the criteria of a narrative. First of all, the sentence contains reference to a past order, which is the Caliphate, in addition to reference to something that has disrupted the order in the mention that lands have to be reclaimed for Jihad. The sentence also suggests a resolution to the problem that, once the lands of the Caliphate are reclaimed for Jihad, then order will be restored. For this reason, the argument by Antoniades et al. that narratives ‘are politically efficacious, since an overall heroic or inspiring national or personal plot may mask episodes that contradict the plot’ (Antoniades et al. 2010: 4) is effective because it is possible to appreciate that certain narratives can be constructed for particular actors in order to influence a particular audience.

**Narrative Source**: The narrative source refers to the community that originated the narrative that occurred most frequently.

**Sentiment Analysis**: The sentiment was analysed in order to ascertain the opinion or the polarity of discussion amongst online users or communities. The measurement of online sentiment is intellectually challenging because of its inherent subjectivity and complexity. Various academic scholars have offered varying definitions of sentiment from the field of psychology, computational linguistics, computer science and linguistics, amongst others. The task of assigning a sentiment marker to a particular item of content is termed sentiment classification and can be used, according to Eguchi & Lavrenko (2006), to summarise content relating to ‘opinionated text units on a topic, whether they be positive or negative, or for only retrieving items of a given sentiment orientation (say positive)’ (Pang & Lee, 2008: 20). To this end, this thesis will take as its point of reference, the definition of sentiment analysis offered by the scholar Yelena Mejova who argued that sentiment analysis is the study of ‘“subjective elements”…These are usually single words, phrases or sentences. Sometimes whole documents are studied as a sentiment unit…but it is generally agreed that sentiment resides in smaller linguistic units’ (Mejova, 2009: 5).

Firstly, the sentiment analysis component of the Alterian content aggregator was used to analyse sentiment based on ‘word parsing, weighting, proximity and Natural Language Processing’ (Alterian, 2011). Following this, a five-point sentiment measurement scale was created that reflected the polarity of online content. The scale was comprised of strongly negative, slightly negative, neutral, slightly positive and strongly positive measures. The author then utilised the analytical process of developing an annotation scheme, following on from the work of Wilson, Wiebe & Hoffmann (2005) who conducted semi-automated sentiment analyses for the development of machine learning protocols. In order to maintain inter-coder reliability, a separate coder was instructed to analyse a sample of content and tag the sentiment polarity of the social media content within. Strongly positive was denoted for positive emotions, evaluations, and stances. The negative sentiment was attributed to negative emotions, evaluations and stances. Slightly positive sentiment was attributed to content that was both positive and negative but had a higher quantity of positivity. Likewise, slightly negative sentiment was attributed to content that contained both positive and negative sentiment but with a higher quantity of negativity. Although this method is not a direct extrapolation of that offered by Wilson, Wiebe & Hoffmann (2005), the author has developed the methodology for the purpose of this thesis as a means of presenting the complexity of online behaviour in relation to terrorism, counter-terrorism and technology. Although it would have been simpler for the author to classify the social media content as either positive or negative, it was felt that a finer grained analysis was required to depict understandings of technology, terrorism and counter-terrorism. This type of analysis was selected in order to demonstrate to the reader the complexity of opinions ensconced within discussions of 11 March 2004 amongst Spanish language online users. In order to limit the propensity for bias, each post was analysed in individual context units in line with sentiment analyses conducted by Mejova (2009), Pang & Lee (2008) and Qin et al. (2003). Each context unit, usually a paragraph, was isolated and analysed individually before being assigned a sentiment rating. The totality of the sentiment ratings for a particular post was then tallied up at the end of the analysis to give the researcher a final sentiment score.

Below are examples of the sentiment classification used as part of this thesis:

* **Strongly positive**: I strongly believe that Zapatero is the right man for the job
* **Slightly positive**: I strongly believe that Zapatero is the right man for the job but worry about the possibility of another imminent attack
* **Neutral**: A series of explosions was carried out in Madrid this morning.
* **Slightly negative**: Zapatero is elected but still has much to do to prevent more terrorist attacks from occurring
* **Strongly negative**: Zapatero is not the right man for the job and I am terrified that ETA or al-Qaeda will mount another attack

**Media Type**: Each online portal was assigned a specific media type which helped the researcher gain insight into the most popular media platform for specific discussion topics. The media types were categorised as forums, blogs or websites.

**Issue**: The issue category refers to the principal focus of a particular post or discussion thread.

Finally, a network analysis was conducted on the dataset that allowed the author to examine the relationships between the named categories above. The data were analysed using the open source network visualisation software Cytoscape and its Organic Layout Algorithm to appropriately situate the nodes in an analysable format. According to Cytoscape, the Organic Layout Algorithm ‘is a kind of spring-embedded algorithm that combines elements of other algorithms to show a clustered structure of a graph’ (Cytoscape, 2011: 1). Put more simply, this particular layout algorithm was elected because it uses a combination of other layouts to present groups or clusters of information more clearly. Examples of the types of relationship that can be revealed include the type of community with the most frequent narrative and media type with sentiment.

A total of 879 individual items of content were analysed for the internet research. Although this amount may appear small in comparison to the high number of Spanish-language online users who might have commented on 11 March 2004 attacks, it is worth considering the comment made by the scholar Shafer (2002) in his content analysis of extremist websites that ‘content analyses of web sites [sic] is problematic because it is impossible to determine the true size and nature of the population. The internet is in constant flux, and there exists no comprehensive directory of web sites [sic]. Therefore a purposive sampling must be used’ (Shafer, 2002 in Gerstenfeld, Grant & Chiang, 2003: 31). In this case, the representative sampling used for the purpose of this thesis is the total volume of content that contained reference to government and terrorist narratives as a result of the searches performed in the social media content aggregator and other search engines.

**Table Three: Flowchart of Methodological Process for the Internet Research**

Source: Lawrence Ampofo

The findings of the internet research into the 11-M attacks are presented throughout the thesis to focus and contribute insight, in a more in-depth way, on specific chapter topics. Therefore, Chapter Four focuses on the findings in relation to the issue of immigration, Chapter Five on narratives, Chapter Six on cybercrime and Chapter Seven on communities. Chapter Eight contains separate internet research into reactions to the death of Osama bin Laden referencing the 11-M attacks.

The methodology described above enables an assessment of the behaviour of online communities in relation to the Madrid attacks in 2004, the results of which will be described in later chapters. There are a number of possibilities for future research using this internet research methodology, as will be described more fully in Chapter Eight.

## Semi-Structured Interviews

Semi-structured interviews[[24]](#footnote-24) were conducted throughout 2009 – 2010 during fieldwork carried out in Spain between May 2010 and January 2011. They complement the internet research by providing contextualisation to the findings. Academics and commercial and public sector subject-matter experts were interviewed. It was decided that semi-structured interviews would provide the interviewer with the flexibility to obtain insight from a range of experts in different areas of expertise. To this end, experts from the Spanish and UK IT industries, UK security services, Spanish and British think tanks and members of the Spanish Government were interviewed.

A more detailed account of the semi-structured interviews, including the collection of questions posed, is included in Appendix Two. In addition, a list of the interviewees can also be found in Appendix One.

## Conclusion

Effective, ethical and well-designed internet research that systematically analyses understandings of the relationships between the internet, terrorism and counter-terrorism in Spain requires a mixture of qualitative and quantitative methodologies. Network analyses such as social and dynamic network analysis can be useful for providing insights into the structure of terrorist organisations and how information flows within such networks. In the midst of these quantitative advances, qualitative measures, such as survey research, continue to provide valuable understanding into audience understandings and opinions.

The increasing adoption of internet research methodologies is dovetailed by the ongoing development of computer processing power and specialist analysis tools, making the analysis of large data sets possible in a way that would not previously have been possible. To this end, political scientists are experimenting with new theories such as Bayesian econometrics and Monte Carlo modelling as ways of analysing complex adaptive systems.

These methodologies are gaining in popularity as a result of the increasingly vigorous debate amongst academics that research methods in political science need to be updated and made more robust to accommodate the new challenges it faces. Commenting on the possible new insights to be found in a robust analysis of Web data, King et al. argued ‘instead of studying the effects of context and interactions among people by asking respondents to recall their frequency and nature of social contacts, we now have the ability to obtain a continuous record of all phone calls, emails, text messages, and in-person contacts among a much larger group. In place of dubious or nonexistent [sic] governmental statistics to study economic development or population spread in Africa, we can use satellite pictures of human-generated light at night or networks of roads and other infrastructure measured from space during the day. The number, extent, and variety of questions we can address are considerable and increasing fast’ (King, G., Lehman Schlozman, K., & Nie, N.H., 2009: 93).

In light of these challenges, this thesis seeks to study the context and interactions in Spain of citizens, media, government and terrorist groups through mixed methodologies that capture naturally occurring communication data that allows for the tracing of changing patterns of communication. These patterns will be analysed to construct explanations of key shifts in the years 2004 to 2010. This is done through an examination of four themes, immigration to Spain, narratives during and after the 11-M, cybercrime in Spain and communities in Spain, which constitute the following chapters.

Ultimately, it is imperative that the advantages and disadvantages of internet research methodologies when conducting an analysis of a terrorism data set are understood. A mixed methods approach will encourage researchers to interrogate data in ways that have seldom been conducted and make greater inroads into understanding contemporary terrorism. A unified approach combining both data with theory and qualitative with quantitative methods will yield the most insightful conclusions.

# **Chapter Four: Immigration, Technology, Terrorism and Counter-Terrorism in Spain**

## Introduction

Understandings of immigration, technology, terrorism and counter-terrorism in Spain are emotive and involve many actors. Using the theoretical framework of commensuration as a social process is an analytically useful way of understanding such complexities.

This chapter has two aims. First, it sets out key developments in Spanish immigration policy since the 1990s, analysing their relation to terrorism and security policies. A tension emerges between technology-led and political/diplomatic approaches to immigration, terrorism and security. Second, it presents analysis of internet research of social media content from 2004 to 2010 based on the mixed methodology introduced in Chapter Three in order to illuminate understandings of these phenomena.

Previous chapters have explored the complex nature of technological development and terrorism in Spain. Chapter Three, in particular, outlined ways in which such complexity could be systematically analysed using a combination of traditional and internet research methodologies in addition to semi-structured interviews with subject matter experts. This chapter investigates immigration as one of the issues that emerged through the research processes and how these topics relate to understandings of technology, terrorism and counter-terrorism in Spain. As in subsequent chapters, internet research has been carried out into the 11 March 2004 bombings in Madrid and discussions and attitudes towards the event to gain insight into the issue of immigration in relation to this event and how it has changed over time (2004-2010).

This chapter, therefore, focuses on the nature of the relationships between the three independent variables – immigration, terrorism and counter-terrorism - arguing that it is analytically adroit to consider understandings of these relationships within the theoretical framework of commensuration as a social process. The utility of commensuration as a theoretical framework emerges as the result of a range of factors, one of which is the securitisation of the discourse pertaining to immigration and, secondly, the notion that Spain is becoming, as argued by Ulrich Beck, a risk society (1999).

Other elements support the notion that commensuration is a useful theoretical framework in which to conceptualise understandings of technology, immigration, terrorism and counter-terrorism. Notions of commensuration and securitisation of discourse relating to immigration, terrorism and counter-terrorism will be outlined in a systematic analysis of online discourse and behaviour. The research processes, therefore, attempt to highlight the complexity inherent within conceptualisations of the relationships between immigration, technology, terrorism and counter-terrorism amongst online users in Spain.

The issue of immigration in relation to technology, terrorism and counter-terrorism became a central area of analysis in Spain following the high volume of mainstream media attention paid to the topic in the wake of the terrorist attacks in Madrid on 11 March 2004. The terrorist attacks, as will be analysed in greater detail in Chapter Five, were, according to Elena Sánchez[[25]](#footnote-25), the driving factor linking terrorism, counter-terrorism, technology and immigration.

Understandings of immigration, technology, terrorism and counter-terrorism in Spain are complex and highly emotive. Increases in the numbers of immigrants entering the country, coupled with attacks by al-Qaeda-inspired groups in the Madrid bombings of 2004, have been interpreted by Government policymakers as signalling the need to enhance the security of immigration flows as a method of mitigating terrorist threats (Cesari, 2009).

This chapter will examine immigration flows into Spain and, subsequently, the official response to the ways in which such flows affect incidents of terrorism. In particular, this chapter will outline the ways in which the Government has conflated the issue of immigration and terrorism in the region. The conflation of these independent variables is a strong example of commensuration that, it will be argued, has been implemented with the intention of maintaining the existence of the state over and above that of the strategic objectives of non-state actors. This theoretical framework is useful in understanding the prevalence of related discussions during the research processes. In addition, it will be shown in the internet research within this chapter that commensuration is helpful in explaining the nature of the behaviour of online communities when engaging with other actors concerning the issues of immigration and terrorism / counter-terrorism in Spain.

Furthermore, this chapter will investigate the securitisation of official responses to immigration following terrorist attacks on Madrid in 2004 and London in 2005. This is evidenced most starkly in the deployment of socio-technological solutions as a means for policing both immigration and terrorism in Spain. This chapter will conclude, therefore, that technological solutions to counter-terrorism and immigration reduce the complexity of understandings of immigration, technology, terrorism and counter-terrorism to numerical dimensions and might, as a consequence, contribute to the creation of a wider surveillance society.

In spite of the importance of the role played by commensuration in forging understandings of the relationships between immigration, technology and terrorism, it is clear that this issue plays a central role in the formulation of the theoretical frameworks by both Barnett (2005) and Bobbitt (2008), analysed in detail in Chapter Two. These conceptual frameworks are useful in helping to explain some of the Government’s actions in this chapter and help to formulate suggestions for future Government actions.

In his thesis entitled the *Pentagon’s New Map*, Barnett’s (2005) central hypothesis emphasised the notion that immigration, technology and terrorism are indelibly linked, therefore offering scholarly legitimation to the conflation or commensuration of the three phenomena, within a securitisation rationale. The element of his thesis, which pertains most strongly to the scope of this chapter, is the assertion that acts of terrorism and political violence are more likely to be caused by groups emanating from countries outside the Functioning Core of states than by those within the non-Integrating Gap[[26]](#footnote-26). Attacks from these groups, he claimed, as well as other macro or system-level threats, would manifest themselves as a result of the flows enabled by globalisation such as the free movement of capital, ideas and, most importantly, people. Barnett hypothesised that international migratory flows were one of the main enablers of international terrorism if left unchecked. He argued such threats could be averted if those states in the Functioning Core actively integrated those countries, which remain part of the non-Integrating Gap (Barnett, 2005).

The active assimilation, or connection, of countries and their peoples into the Functioning Core is, according to Barnett, a security imperative as a means of lowering the threat of international terrorism. Similarly, the US scholar Philip Bobbitt outlined in his thesis, *Terror and Consent: The Wars for the Twenty-First Century* that nation states are changing into market states.[[27]](#footnote-27) To this end, as states become more organised in a structure that resembles ‘VISA or MasterCard organisation charts than they do the centralized, hierarchical structures of nation state governmental organizations, including nation state terrorist groups (or, for that matter, the twentieth century corporate business structures of the nation state)’, the nature of the threats facing that particular state become simultaneously networked and cellular in nature. Bobbitt argued that international terrorism was a direct response to globalisation and, in a similar vein to the argument enunciated by Barnett, that international flows that characterise globalisation, such as immigration, are critical in shaping this new threat. He put it that;

‘Terrorism appeared as part of the underside of globalisation. It was already becoming apparent that the consequence of the openness in the international system, economically, as much as politically, was taking certain things out of control. The resulting globalisation was the reduced power of control. The result of globalisation was the reduced power of states, the movement of capital and people around the world as governments opened up their borders. This created new opportunities for those who wished to inflict harm on the established order’ (Bobbitt, 2008: 62).

Similarly, the terrorism scholar Audrey Curth Cronin argued that the growth of globalisation was facilitating the emergence of new threats that states had to confront in a different way, ‘[t]he current wave of international terrorism, characterized by unpredictable and unprecedented threats from nonstate [sic] actors, not only is a reaction to globalization but is facilitated by it…The increasing threat of globalized terrorism must be met with flexible, multifaceted responses that deliberately and effectively exploit avenues of globalization in return’ (Cronin, 2005: 6). Indeed, one of the ways in which Spain has actively developed its counter-terrorism strategy and adapted to the threats posed by international terrorism and market states of terror is by implementing public diplomacy strategies. In this way, it appears as if the Zapatero Government has heeded the advice from Cronin by implementing a ‘flexible, multifaceted response that…exploit[s] avenues of globalization’ (Cronin, 2005), through the creation of multilateral agreements with Morocco and the United Nations. Although the nature of these strategies is discussed in Chapter Two, recommendations for enhancing digital public diplomacy emerge from the findings of the empirical research. However, this chapter addresses Spain’s immigration policies and what they indicate about understandings of immigration’s relation to counter-terrorism.

## Immigration in Contemporary Spain

Spain is a country of many cultures and languages. With its 17 different autonomous communities (*comunidades autónomas*), it comprises a range of different languages such as Aranese, Basque, Catalan and Galician. Located near North Africa, it is a key conduit to Western Europe. Indeed, its enclaves of Ceuta and Melilla border Morocco and are considered by the Spanish Government and European Union to be gateways for illegal immigration and places that foster radicalisation and potential terrorism (Tansey, 2009: 54, Witt, 2005: 5).

The establishment of a constitutional democracy in 1978 and accession to the European Union in 1985 signalled the onset of a significant escalation in the level of immigration to Spain that has been both lauded and criticised in equal measure by its citizens. From one perspective, the increase in migratory flows to Spain is considered an effective safeguard against the country’s labour shortages, an aging population and rising levels of international trade for the world’s ninth largest economy. From another perspective, however, the increase in immigrant numbers has left people feeling uneasy. Indeed, immigration in Spain is a complex and passionate topic because ‘[s]ince 2000, the number of non-EU foreigners in Spain has *skyrocketed*. In 1999, the total number of foreigners living in Spain stood at about 719,600. By 2005, this number had increased by almost 200 percent [sic], to just over 2 million…concentrated in five of Spain’s seventeen autonomous communities: Catalonia (22.93%); Madrid (20.63%); Andalusia (11.70%); Valencia (11.56%); and the Canary Islands (6.40%). As of January 2006, the number of foreign residents (including EU residents) had increased to roughly 4.1 million or 10.22%’ (Tansey, 2009: 45, emphasis in original).

One of the first to recognise the importance of opening Spain’s national borders was Franco who actively encouraged Spain to become a world leader in tourism in a policy document entitled the *Anteproyecto de Plan Nacional de Turismo* in 1952. This was evidenced in his decision to authorise the construction of Benidorm as a tourist haven as well as permitting widespread use of the bikini, which in 1959 was against the dictates of the clergy. Franco understood that tourism was not only a powerful public diplomacy tool used to generate favourable foreign public perception of the country, but also extremely useful in attracting financial wealth (Tremlett, 2007, Rosendorf, 2006).

During the 1980s, immigration control was not considered an issue important for serious discussion by the Government as the fledgling democracy was more concerned with establishing itself as an influential part of the European Community than focusing on its immigration flows (Ross, 2003: 3). Spain’s policymakers, as a consequence, paid little attention to the significant demographic shift that was taking place during this time as it rapidly went from an immigrant-sending country to an immigrant-receiving country (Celaya, 2009).

One of the first efforts to control immigration into Spain while simultaneously reaping the benefits of immigrant labour was the adoption of legislation that controlled immigration. When Spain joined the European Community in 1985, it implemented the *Ley Orgánica de Extranjera*, which significantly affected public perceptions of citizenship by classing all immigrants as temporary visitors and not as true immigrants. In doing this, the Government attempted to limit the time spent by foreigners within Spanish borders and to restrict the opportunities to become a permanent resident[[28]](#footnote-28) (Calavita, 2006: 3). However, between 1990 and 1995, the volume of legal immigration increased significantly from the European Union, in particular, as Spanish society came to have increased contact with immigrants (Calavita, 2006), ‘Between 1995 and 2001, for instance, the resident immigration population increased from 499,773 to 1,109,060, more than a 110% increase in six years according to the Spanish Ministry of Home Affairs. Importantly, the proportion of resident immigrants from non-EU countries increased substantially during the period, from 53.59% in 1996 to 70.55% in 2001’ (Ross, 2003: 7).

Statistics from the European Union and the OECD, however, reveal that Spain has experienced one of the largest increases in immigration in recent times, receiving ‘three - quarters more immigrants in 2006 than in 2002. In absolute numbers, Spain had the biggest increase [in] immigrants…in 2006 than five years earlier’ (Herm, 2008: 2). While the pressures of official immigration have been widely discussed in Spain, illegal immigration has grown to be a significant problem as the actual number of unknown immigrants in Spain is quite possibly much higher than the official statistics proclaim (Crain, 1999).

Figure Seven: Inflows of Foreign Migrants to France, Spain and the UK

Source: OECD Statistics

Immigration to Spain became the focus of mainstream media attention at the beginning of the 21st century, becoming a key element of public debate and the political agenda as ‘immigration had finally come of age in Spain, even as constructive public policy and open attitudes to address[ing] immigration issues continued to lag behind. Then came modern Spain’s day of infamy: 11 March 2004’ (Ross, 2004: 5). The issue of immigration became securitised and linked with terrorism on 11 March 2004, three days before the Spanish General Election when terrorist attacks were carried out on Madrid commuter trains in Atocha, El Pozo del Tío Raimundo*,* Santa Eugenia stations and the *Calle Téllez* street.

## Terrorist Attacks in Madrid on 11 March 2004

The terrorist attack which took place in Madrid on 11 March 2004 is second to the bombing of Pan AM Flight 103 over Lockerbie in Scotland, otherwise known as the Lockerbie Bombing, with respect to the loss of life caused by international terrorism in Europe. Due to the proximity of the General Election to be held three days after the attacks on Sunday 14 March 2004, 11-M, as it is termed by Spanish commentators, was not simply a bombing by international terrorists, but instead had considerable political and social ramifications on Spanish society over four days in March 2004. It was perceived by many scholars to have influenced the course of the elections (Baird, 2009, Moreno, 2004, Michavila, 2005).

At 07:00 on 11 March 2004, four trains departed within 15 minutes of each other from Alcalá de Henares and Guadalajara, en route to Chamartin. At 07:37, three bombs exploded on one of the busy commuter trains at El Pozo del Tío Raimundo station on a commuter train full of office-workers, students and schoolchildren in the third, fourth and sixth carriages (BBC News, 2004). A minute later, at 07:38, four bombs exploded on trains 500 metres outside the largest railway station in Madrid, Atocha, killing at least 59 people (BBC News, 2004, *El Mundo*, 2004). At 07:41 two bombs were detonated on a train as it passed through Calle Téllez train station with, according to investigators, 10 kilograms of explosives on board in the first, fourth and sixth carriages, killing 65 people. At 07:42 a bomb exploded in the fourth carriage of the train arriving at Santa Eugenia station, killing 17 people and wounding many more (*El Mundo*, 2004).

Over the hours and days that followed, in addition to the national demonstration of sympathy, anger and empathy by the Spanish populace (a nationwide march for peace was attended by approximately 11.4 million people on 12 March at 19:00 at the behest of Prime Minister Aznar after both the PP and the PSOE suspended campaigning for three days), there was vociferous debate about the ways in which the attacks could potentially affect the outcome of the General Election on Sunday 14 March. Wider debate amongst the Spanish public focused on a range of questions related to the attacks, asking themselves why it had happened; who had perpetrated the attacks? Was it related to the terrorist attacks in the US on September 11 2001? Was it a response to Spain’s involvement in the invasions of Afghanistan and Iraq? (Moreno, 2004)

With investigations by the security services and the police taking place into the occurrence of events of the day, mainstream media simultaneously reported on findings such as the discovery after the explosions of a white van with copies of the Qur’an and other Islamic verses on audiotape. Such reports were in direct contravention with details of the reports delivered by the Government (Celso, 2005: 91). In addition, it was reported on 12 March that unexploded bombs had been recovered and that the security services deduced that mobile phones had been used to detonate the devices in rucksacks (Baird, 2009). This discovery led to reports concerning the extent to which technology had been used to carry out the attacks and provided leads to apprehending those responsible for the attacks. Additionally, on 13 March 2004, counter-terrorist services located a video near a mosque in Madrid on which a person claiming to represent al-Qaeda admitted culpability for the attacks, explaining that they were an act of revenge for Spanish military involvement in Iraq and Afghanistan. The security services subsequently began arresting those suspected of involvement with the attack including a man who had sold pre-paid subscriber identity module cards (SIM) used in the mobile detonators (*The Guardian*, 2007). Mainstream media reports that detailed that Moroccan and Pakistani nationals were being arrested and questioned by the security services directly contradicted reports from high-ranking Government officials that ETA was the principal protagonist of the attacks (Michavila, 2005).

From 11-13 March, as part of the response by the Government, Prime Minister Aznar and Minister of Justice Ángel Acebes, in addition to other senior Government spokespeople, outlined to journalists in numerous press conferences that the attacks had been caused by the Basque terrorist organisation, ETA, although they were not ignoring other possible perpetrators (Baird, 2009). Indeed, scholars have maintained that Aznar was in constant contact with the principal mainstream media organisations in Spain, such as *El País*, *El Mundo* and *La Vanguardia*, to ensure that they produced media content proclaiming that ETA was responsible for the attacks (Curto et al. 2007). While the Government was making its case that ETA was responsible for the attacks, the spokesperson for the Basque nationalist political party Batasuna, Arnaldo Ortegi, had emphatically denied ETA’s involvement in the attack in a media response made on 11 March. He had instead argued that the attacks should be blamed on “Arab resistance”. However, over 11-13 March, prominent media organisations continued with the assertion that ETA was responsible, claiming that ‘[t]his series of attacks is the bloodiest yet committed by the terrorist organisation’ (*El Mundo*, 2004: 1).[[29]](#footnote-29) The justification for ETA’s involvement in the attacks stemmed from initial investigations into the type of explosive used to perpetrate the attacks which were GOMA 2 ECO, the type of explosive normally utilised by ETA (*El Mundo* 2006).

In contrast to public opinion polls before the 11-M attacks, which predicted that the PP would win, on 14 March large numbers of the Spanish electorate appeared in the largest turnout since 1977, and the death of Franco, to elect a change in Government from the PP (which won 148 seats) to the PSOE (which won 164 seats) (Moreno, 2004).

The misinformation concerning the authorship of the Madrid terrorist attacks, as well as the eventual admission of culpability by al-Qaeda, increased negative sentiments towards immigrant communities in Spain. This occurrence was detailed by the former Head of Communications for the Congreso de los Diputatados Maria Llorach who argued that the general Spanish population is wary of the immigrant South East Asian population in districts such as the Raval in Barcelona, which are environments for Islamic terrorism in Spain.[[30]](#footnote-30)

The Zapatero Government, and subsequently the mainstream media, established a link between immigration and terrorism when it emerged that the terrorist group responsible for the bombings on the Madrid train stations were illegal immigrants and Moroccan nationals. By 11 April 2006, 29 people in total had been arrested in connection with the attacks, including 15 Moroccans, nine Spaniards, two Syrians, one Egyptian, one Lebanese and one Algerian. From this point onwards, the discourse on immigration and terrorism in Spain became securitised.

The term “securitisation” originated from a group of scholars including Barry Buzan and Ole Wæver in what is denoted as the Copenhagen School. Wæver argued that securitisation is conceptualised as the following:

‘[S]ecuritization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects…A discourse that takes the form of presenting something as an existential threat to a referent object does not by itself create securitization – this is a *securitizing* move, but the issue is securitized only if and when the audience accepts it as such’ (Buzan et al. 1998: 25, emphasis in original).

For the Copenhagen School, security is not in itself an object. Rather, it is something that is socially constructed by analysing “speech acts”. Issues therefore become “securitized” as certain “speech acts” convert a specific issue into a security concern. Conceiving of security as an act of speech is useful because it allows for the expansion or contraction of security issues. As a result, the Copenhagen School has argued that the concept of security should be compartmentalised into five sectors; in the military sector the focus is the territorial integrity of the state and threats are typically exogenous to the state in question, in the political sector the survival of the governmental body is at stake and threats to this sector are generally sub-state actors. The societal sector refers to ‘the ability of a society to persist in its essential character under changing conditions and possible or actual threats’ (Hansen & Nissenbaum, 2009: 5). The economic sector refers to security of the economic structure of society and the environmental sector the environment. However, for any issue to become conceptualised as a threat to any of these sectors, it has to contain ‘existential threats, emergency action and effects on interunit relations’ (Buzan et al. 1996: 26).

One of the main criticisms of securitisation is its inherent intangibility. If security issues are nothing more than a specific framing of an issue, then it follows that any issue could be termed a security issue. In addition, it is questionable whether this theoretical framework, which relies on the specific construct of speech or text, is capable of addressing the complexities of security in the world. This is particularly the case with the use of images in the framing of security and war (Hoskins & O’Loughlin, 2010).

Another criticism of securitisation offered by Rita Floyd claimed that the very act of choosing a speech act to analyse inadvertently helps the analyst to reinforce the security issue and dichotomies of security and insecurity (Floyd, 2007). Floyd added that securitisation contains a major flaw with regards to its normative utility. Normative utility in this case is defined as the security analyst’s ability ‘to influence the securitization process in a deliberate and thought-out fashion and – though this ultimately depends on capabilities – to a desired effect’ (Floyd, 2007: 7).

However, while there are limitations to the use of securitisation to analyse security issues, it is ostensibly useful in the analysis of text-based content, particularly social media content and newspaper reports, part of the analytical focus of this thesis. Therefore, if we accept the above definition of securitisation offered by Wæver, Buzan and the Copenhagen School, it is possible to appreciate that the term is appropriate for the Government’s conflation of terrorism, counter-terrorism, technology and terrorism that will be analysed in greater detail subsequently. This is due to the fact that an existential threat is perceived to occur to the Spanish State in discourses concerning immigration, terrorism and counter-terrorism from the potential deleterious effects of unchecked immigration following 11-M. However, the findings from the internet research will assess the extent to which target audiences accepted the issues as securitised.

As the Spanish public elected a change in Government from the PP to the PSOE on the 14 March 2004, it became clear that the terrorist attacks in Madrid had played a significant role in compelling both the Zapatero Government and mainstream media organisations to focus on immigration as one of the main causes of terrorism. The attacks caused Spain, and the wider European Union, to focus on restricting access to the region for those without documentation as a national security issue (Witt, 2005: 2).

However, unlike their British, French and American counterparts, the new Zapatero Government did not draft new counter-terrorism policies following the terrorist attacks in Madrid. Rather, it kept in place the previous strategies and policies when deterring threats from the likes of ETA. The reluctance of the Spanish Government to overhaul its counter-terrorism structure stemmed from the belief that terrorism in Spain is ‘not a conjunctural phenomenon but a structural one, and as a result, it cannot be confronted militarily (as in the US) or with exceptional and extraordinary norms (as in the UK), but through ordinary legislation in compliance of the rule of law’ (Celaya, 2009: 5). As a result, Spain’s security and intelligence services have found ‘in the criminalization of terrorism a successful tool to counter the homegrown [sic] as well as the international terrorist threat’ (Celaya, 2009: 5). The evidence for Celaya’s assertion is located in extensive research conducted by the scholars Enrique Álvarez Conde and Hortensia González (2006) in which they compared the content of Spanish counter-terrorism legislation both before and after the US terrorist attacks on 11 September 2001 (Conde & González, 2006).

There is evidence that by 2004, the Spanish Government had already implemented the enhancement of the security of its borders in an effort to stem illegal immigration. For example, the Government constructed 12 feet high fences running ten kilometres along the borders of the enclave of Melilla and Morocco in 1999 (Crain, 1999). These fences were created specifically to halt the flow of African citizens to the country, as Morocco was perceived to be a Transit Country[[31]](#footnote-31) that exacerbated the problem of illegal immigration. Monitored by the Guardia Civil, the fences incorporated the latest in surveillance technology such as ‘cameras, sensors and armed guards stationed in lookout towers. These rigorous new border controls are required by the European Union’s adoption of stricter measures to regulate the inflow of individuals from non-EU nations. The coasts of southern Spain, as well as those of Spain’s two North African enclave territories (Melilla and Ceuta), have become key transit points into Europe for thousands of illegal migrants from across Africa’ (Crain, 1999: 24). The Spanish Government also installed a wide range of other security measures to enhance border security, which will be outlined in subsequent sections of this chapter.

The securitisation of Spain’s borders against illegal immigration can be conceived as part of a wider trend amongst European countries of using information technologies to obtain knowledge of people entering and leaving the continent. This can be seen in the adoption of a number of multilateral agreements by the US and the EU to increase border security as a means of preventing security risks, including terrorism. One such agreement is the creation of the Schengen Information System in 2001, following on from the signing of the original Schengen Agreement in 1985. The Schengen Information System (SIS) allows states involved in the agreement to share certain personal information about citizens entering their countries[[32]](#footnote-32). Indeed, it has been argued that Spain, and Europe at large, has adopted a ‘war or readiness model against terrorism which involves the strengthening of anti-terrorism legislation and/or the hardening of security measures…which emphasise the rule of law and policing models, rather than derogation and military models’ (Walker & Akdeniz (2003) in Levi & Wall, 2004: 3).

The securitisation of border controls, however, has been emphatically criticised for contravening humanitarian rights and being overly punitive in regards to the encroachment on civil liberties (Goldschmidt, 2010). Such criticisms were exacerbated by ‘the terrible pictures [of] sub-Saharan Africans trying to climb the barbed-wired fences around the Spanish enclave Melilla in Morocco’ (Witt, 2005: 3). Indeed, these images did much to reinforce the idea that Spain had not yet made the distinction between an effective and humane security policy for legal and illegal immigration (Crain, 1999).

As examined in Chapter Two, Spain’s experience of terrorism in the 1980s principally involved countering ETA. Indeed, border control was one of the central issues that formed the Government’s counter-terrorism strategy as ETA members had established operational bases both in Spain and in South-western France as a means of evading arrest and further conflict with Spanish authorities. However, bilateral agreements with France, which included specific counter-terrorism legislation on extradition, international movement of finance and border control, were put in place which dramatically restricted ETA’s ability to operate. Yet, as Bobbitt (2008) noted, as Spain entered the 21st century, its security services focused more on the threat posed by ETA as opposed to the new threats the country faced from international terrorism; ‘Like generals, spies and policemen tend to fight the last war…Similarly…until the bombing of a Madrid commuter train by Moroccan radicals in March 2004 [Spain’s] focus was almost entirely on ETA, and its principal action the banning of the allegedly related Basque nationalist party Batasuna. Security services must learn to look forward to emerging threats, not backwards at Cold War and separatist ones’ (Bobbitt, 2008: 44).

This notion was given greater credence as national statistics revealed ‘the rising number of immigrants coming [into Spain] from developing countries. The ratio of resident immigrants coming from developing and developed countries has shifted from virtual parity in 1999 to 63.04% in 2001 by factoring in the Human Development Index (HDI) of the sending countries. Significant, however, is the fact that among the non-EU developing countries, Morocco has “by far” the greatest number of resident immigrants living in Spain, with almost a quarter of a million in 2001’ (Ross, 2004: 5).

The Madrid terrorist attack motivated the Government’s decision to securitise immigration and was championed by the mainstream media, the Government itself and the general public (Colás 2010). The securitisation of immigration in Spain resulted in the implementation of a number of technological solutions to police the situation, analysed below.

## Spanish Immigration Policy and Technological Determinism

One of the major elements of Spain’s immigration policy following the Madrid attacks, and a prominent example of reliance on technology, suggestive of technological determinism, was the improvement of its border citizen surveillance capability as part of the Schengen Agreement and Schengen Information System, to cultivate a ‘more systematic entry of persons considered undesirable aliens in the Schengen Information System’ (Guild, 2001: 233 in Carr & Massey, 2006). Alongside this, another Europe-wide initiative was launched in order to better monitor the flow of asylum-seekers in the region. The EU created and implemented a fingerprint database called EURODAC, which ‘enables Member States to identify asylum applicants and persons who have been apprehended while unlawfully crossing an external frontier of the Community’ (Europa, 2010: 1).

Other initiatives were launched at the Member State level of the European Union that focused on a digital response to the securitisation of immigration in the region. The ‘rules on destruction of data regarding asylum seekers after their use have been relaxed. Foreigners, and in particular asylum seekers, no longer have the benefit of removal of their data from the databases once their files are completed. All the time periods for retention of data have been substantially extended’ (Guild, 2001: 243 in Carr & Massey, 2006). Finally, another initiative that the Spanish Government agreed to partake in, along with other EU Member States, was the Passenger Name Record Agreement whereby travellers to the US from the EU are required to share their details with the US Government. The information is then stored on a database in order to cross-reference with information stored in other crime-related databases.

These initiatives highlight the extent to which nation states believed that illegal immigration could be adequately dealt with using technological solutions, in effect, resonant of technological determinism. The limitations of this stance have been highlighted by scholars, such as Robert Imre, who commented that the implementation of technology to solve the problem of illegal immigration is counter-productive:

“I think that as these things shift and change, governments initially never get it right, governments initially jump in and try to stoke the flames of fear as it were and I think that where we see technology actually influencing things is where we see the sort of securitisation of people today.”[[33]](#footnote-33)

Imre’s comment demonstrates the notion that governments’ attempts to protect their borders using technology create an environment of securitisation and result in greater unrest amongst populations than illegal immigration.

The post-11-M security environment in which Spain’s immigration policies were drawn up demonstrates the ways in which the Government relied on the analysis of digital data as a means of profiling people and groups. Digital data comprising personal travel information, biometric information and financial transactions, amongst others, were regularly analysed in order to make operational decisions on whether a particular person or group constituted a potential security risk. The Deputy Head of Spain’s Centro Nacional de Inteligencia, Elena Sánchez-Blanco, buttressed this point when she commented that in the post-11 September and 11 March world, no one country had the ability to protect itself in isolation and that ‘new technology to modernize the CNI and enhance its performance [was]…needed’ (cited in Celaya, 2009: 28).

The Government’s reliance on technological solutions to enforce new laws on immigration and terrorism stemmed from the belief that technologies can reveal the level of risk posed by a particular person or community. In this sense, the belief that technological solutions are a panacea for immigration problems corresponds very closely to the central hypothesis of this thesis, that the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives.

However, the strategy of reliance upon technological solutions has been criticised by experts as indicative of ‘planned actuarial strategies that rely upon the analysis of secondary data obtained through the convergence of technologies and databases to survey individuals and suspect groups who have previously been identified as a potential risk’. The use of technology in tandem with border control and counter-terrorism has been referred by Roger Clark as “Dataveillance”, which describes the ‘systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons’ (Clarke, 1987: 2). Clarke’s assertion is reminiscent of that put forward by Imre, that overreliance on technology for complex issues such as immigration and terrorism can be problematic. It also suggests that counter-terrorism strategies should be social constructivist endeavours rather than techno-determinist ones.

However, the aggregation and analysis of personal data to collectively police migratory flows and terrorism have been called into question. The ability of biometric data, for example, to provide an effective deterrent against terrorist activity has been questioned by a range of scholars. The first problem is that individuals classified as security risks would already be visible to border control agents and anyone that potentially presented a danger would not be recognised by biometric information. Another is that the entire premise of illegal immigration and terrorism is to circumvent the systems used to police it. Widgren et al. argued ‘improved entry controls will be met with improved circumvention methods, be it with newly forged travel documents or in wholly clandestine ways’ and instead penalise honest citizens (Widgren et al., 2005: 3).

One of the main problems with technological responses to the securitisation of immigration is that the encroachment of technology into security strategy raises fears amongst Spain’s migrant communities that the use of databases in policing migration leads to the unfair treatment of migrants (Celaya, 2009: 26). Such fears have been given further credence by the range of new legal initiatives to combat the new style of terrorism it faces such as the fact that terrorism suspects can be held *incommunicado* for a maximum of thirteen days (Amnesty International, 2009). Such measures, inspired by the collection and analysis of personal digital data from databases and other technology suggest that the terrorist threat in Spain is being fought quantitatively and ‘materially and normatively shaped and framed to suit the interests of actors interested in “policing at a distance”’ (Celaya, 2009: 26).

To summarise, Spain has securitised its immigration policy, along with the European Union and the US in an effort to curb potential security threats that come with the free movement of people. However, the measures taken by Spain, particularly its reliance on technological solutions to underpin this new policy, have limitations. The next section of this chapter will analyse how the securitisation of immigration has limited Spain from access to potential increases in immigrants, and how technological solutions incubate the notion that Spain is a fortress. In addition, it will discuss how the securitisation of immigration could be used for political gain and suggests alternative methods of contending with this issue.

## Limitations of the Confluence of Technology, Immigration and Terrorism

As the Spanish Government simultaneously responded to the terrorist threats facing the country and the rising levels of immigration from outside the European Union, information and communications technologies played an increasingly important part in its response. However, responding to the three independent variables (or processes) outlined above, one particular issue is problematic. The relationship created by these three elements is ill-fitting, calling into question the possibility, relevance and utility of conflating such seemingly disparate variables.

The consequences of bringing together such diverse elements to make one measurable outcome have been outlined by Elspeland and Stevens (1998) in what they term commensuration as a social process. Commensuration is a process of conceptualising unrelated qualities as a single common measurement and, as has been illustrated in this chapter, is a central part to the Spanish approach to immigration control. Simply put, ‘it is a system for discarding information and organizing what remains into new forms. In abstracting and reducing in-formation, the link between what is represented and the empirical world is obscured and uncertainty is absorbed. Everyday experience, practical reasoning, and empathetic identification become increasingly irrelevant bases for judgment as context is stripped away and relationships become more abstractly represented by numbers’ (Espeland & Stevens, 1998: 6). Here it is possible to see how the fusion of terrorism and immigration, facilitated by technological solutions, is neatly applied to the process of commensuration.

Espeland and Stevens’s (1998) conceptual framework is useful as a way of unpacking understandings of immigration, technology and terrorism. It argues that the conflation of seemingly disparate topics, such as immigration and security, is problematic as it reduces the collection of complex topics to statistical figures and probability, meaning that a number of different elements within these issues are rendered irrelevant or invisible, similar to the issues raised in support of Dataveillance. In this case, immigration and terrorism have been brought together to create an entirely new discourse in Spain in which terrorism is thought to be made more probable by immigration and migratory flows and therefore becomes securitised as the perceived corollary becomes the notion that immigration flows are a gateway to violent attacks on mainland Europe (Colás, 2010). In a more unfavourable way, commensuration can be perceived as a ‘tactic [which] is embraced by some law-makers, environmentalists, and bureaucrats…who wish to expand what is considered relevant in bureaucratic decisions…by women advocating comparable worth as a means for redressing pay inequity…or by economists grappling with problems of externalities’ (Espeland & Stevens, 1998: 3).

The argument that immigration and terrorism are commensurable, thereby becoming a singular security issue is compelling. This is due to the notion that the securitisation of immigration goes a long way to upholding realist notions of the primacy of the state in the face of increasing numbers of foreign nationals from developing countries arriving on Spanish borders. Indeed, it is perhaps the very idea of the survival of traditional notions of the state against the threat of unseen, non-state actors, that has drawn the two issues of immigration and security together and perhaps prevents policymakers and technology companies from tackling the two issues as effectively as they might. Ross writes, ‘[f]itting borders into emerging understandings of transnational networks associated with a global level of analysis, non-state actors and the spread of extreme Islamist terrorism, policymakers need to revise traditional understandings of borders as fixed, static entities that merely define the bounds of state sovereignty. Another approach is to recognize the global processes that territorial borders help produce in the first place, such as international migration, and the risks pertinent to those processes that highly restrictive border practices and exclusionary policies are not going to alleviate’ (Ross, 2004: 2). This suggests that commensuration by the Spanish State (and the EU more generally) could produce risks and threats too.

The argument from Ross is provocative as it challenges states to conceive of national borders as entities in their own right that perpetuate violent international incidents such as terrorist attacks. This supports Barnett’s thesis that the boundary of the Functioning Core and Non-Integrating Gap must be overcome through intensified connections. If Ross’s argument is taken seriously then nation states could collaborate and find mutually beneficial solutions to issues such as illegal immigration and international terrorism. One such solution can be found in Spain’s leadership of multilateral agreements as a means of gaining international consensus on the best methods of securing national borders. The the Barcelona Process, the EuroMediterranean Summit of 2005 and the Mediterranean Union are three examples of Spain’s active leadership of multilateral agreements designed to ensure effective, humanitarian border control. In addition, these international agreements are examples of Spain’s willingness to adopt solutions that are not technological in nature, but rather focus on the utility of dialogue and human interaction.

These examples of multilateral agreements highlight an important facet about Spain that merits mention. In spite of Spain’s short experience of immigration (since the 1980s) in comparison to France and the UK, which have both experienced immigration flows since the 1960s (Figure Seven), Spain continues to emphasise the use of its soft power as well as other techno-centric solutions to the securitisation of immigration. The country has retained its historical proclivity to use diplomacy and mediation as a means of halting the threat posed by terrorism which highlights Spain’s ‘emphasis on multiculturalism and its growing acceptance of diversity’ (Tansey, 2009: 29). The inclination towards diplomacy and soft power to tackle terrorism and illegal immigration, previously outlined in Chapter Two, was supported by Elena Sánchez when she asserted that, from the perspective of the general public, there is no tangible link between terrorism, technology, counter-terrorism and immigration;

“[The Government] has linked more things with terrorism such as security and the immigrant population. It occurred in the first weeks after what happened in Madrid, but since then the link has been strong indeed. This is probably because the [majority] of the immigrant population is from Latin America although we say that the Moroccan is the second population with the most immigrants in Spain. It is also clear that regarding the problem of immigration and terrorism in Spain, it is my opinion that public opinion polls reveal that the things that most scare the Spanish population are unemployment…Definitely amongst the Spanish population, questions which focus on immigration are linked with employment and not so much terrorism.”[[34]](#footnote-34)

Sánchez’s comment is indicative of the disjuncture demonstrated in the internet research presented in this chapter of understandings of the relationship between technology, terrorism, counter-terrorism and immigration by the Government and general public. This chapter will now analyse the extent to which this phenomenon was evidenced amongst Web users commenting on the 11 March 2004 Madrid terrorist attacks. This understanding will be analysed using a mixed-method online analysis technique that was explained in Chapter Three.

## Internet Research on the 11-M Attacks: Key Narratives and Immigration (2004-2010)

The author created a methodological process from media analysis to analyse online discussion related to the Madrid terrorist attacks of 2004 to support the primary research conducted. The insight provided in this analysis is intended to enrich the points made during the course of the chapter and provide secondary data in addition to that provided by the semi-structured interviews. The date range of the analysis was six months from 11 March to 11 August each year over a period of seven years (2004 to 2010).

The internet research contained within this chapter is a version of that developed in Chapters Five, which focuses on the nature of narratives in online discussion, Chapter Six which focuses on cybercrime and Chapter Seven, which focuses on the nature of the behaviour of online communities in response to the 11 March terrorist attacks in Madrid in 2004. An explanation of the methodology used to conduct the internet research process was provided in Chapter Three.

In this chapter, the internet research provides an indicative assessment of the nature of behaviour of online communities in response to the 11 March 2004 terrorist attacks. It focuses on narratives relating to the bombings and the issue of immigration. Of the 879 individual data points analysed, comprised of content emanating from blogs, discussion forums and websites, 177 were directly related to the topic of immigration.

It is noticeable that, in spite of the discussion concerning immigration, technology and terrorism, the volume of discussion did not remain constant during the different time periods from 2004 to 2010. While the volume of discussion did taper off, it is not the opinion of the author that overall discussion on immigration, technology and terrorism fell. In fact, there is evidence to suggest that the focus of discussion related to the topic of immigration changed from relating discussion to 11-M to other more focused elements of terrorism such as *Operación NOVA I & II* and *Operación Sello I & II* outlined in greater detail in Chapter Five.

Figure Eight: Line Chart Presenting the Total Volume of Immigration-related Commentary Over Time

N=177

Source: Lawrence Ampofo

The line chart in Figure Eight demonstrates that the rate of commentary pertaining to immigration, technology and terrorism peaked in 2004-2005 in the immediate aftermath of the bombing and subsequently for the first anniversary of 11-M. Commentary at this time focused primarily on the commensuration of the independent variables and the securitisation of immigration as a result of al-Qaeda admitting culpability for the attacks. An example of this is seen in an article in the *Diario Córdoba* in which it claimed that vulnerable members of Spain’s Moroccan population were at risk of being recruited by the wider al-Qaeda organisation. It claimed that while Egyptians and Saudi Arabians were responsible for planning and strategy within al-Qaeda, the organisation had studied population migratory patterns to Spain and decided upon using Moroccan and Algerian groups to carry out the individual attacks, leaving Spain vulnerable to future attacks.[[35]](#footnote-35) This comment underscores the role that securitisation played in enabling the commensuration of the issues of terrorism and immigration, affording justification to the enhanced protection of Spanish borders by the Government.

In addition, other individual commentators claimed that the occurrence of 11-M had demonstrated that immigration and multiculturalism had failed in Spain because Moroccan nationals had perpetrated the attack. A participant in the newsgroup *es.charla.politica.misc*, for instance, claimed that if a person says that they are not in favour of the mixing of the races then they are classed as a neo-Nazi. He continued that he loves Spain and does not desire to share it with people who do not feel the same way about it as him.[[36]](#footnote-36)

The fear and resultant anger and frustration demonstrated between 2004 and 2005 are predictable in light of the magnitude of the attacks and the lack of a clear public diplomacy strategy. One of the main reasons for the commensuration of the issues of immigration and terrorism was the revelation that Moroccan nationals had admitted culpability for the attack. It is interesting that discussion pertaining to the topic fell markedly from 2006 to 2010, rising slightly in 2007 and 2009. 2007 saw more politicised comments as online users claimed that the terrorist attacks were the result of the Aznar Government’s decision to join the US-led coalition into Iraq. This, it was claimed, compelled people to engage in illegal immigration to perpetrate violent actions against the state.[[37]](#footnote-37)

The fifth anniversary of the 11 March attacks in 2009 encouraged an increase of commentary, in a similar vein to that seen previously in 2004 and 2005, as commentators claimed that immigration from North Africa was problematic to the security of Spain and that Jihadist terrorism had been actively perpetuated long before 11-M. An example of this is the blogger who commented on a tributary post to the *Que!* blog, claiming that Jihadist terrorist attacks had been occurring in Spain for decades and the main place for recruitment in the region is Catalonia.[[38]](#footnote-38)

The overall corpus of online content highlights the extent to which Spanish social media users and the mainstream media demonstrated a proclivity to commensurate immigration with terrorism. The reasons for this alternate between an understanding that illegal Moroccan immigrants were responsible for the attacks, and the notion that the attacks were retribution from immigrant Muslims to former Spanish Government foreign policy. The following chart (Figure Nine) shows the way in which such discussion was framed through a sentiment analysis of the content, which was largely negative in nature. This demonstrates that the majority of online users felt that the issues of immigration and terrorism were inextricably linked and subsequently (Figure Ten) having a deleterious effect on national security.

### Sentiment Analysis

Figure Nine shows the way in which discussion of immigration, technology, terrorism and counter-terrorism was framed through a sentiment analysis of the content, which was largely negative in nature. This finding, combined with the data on Figure Ten, showing the range of narratives most frequently mentioned, suggests that online users commensurated the issues of immigration and terrorism, subsequently provoking a harmful effect on national security.

Figure Nine: Stacked Column Chart Demonstrating the Sentiment of Immigration-related Commentary Over Time

Source: Lawrence Ampofo N=177

### Key Narratives

Figure Nine demonstrated the high proportion of strongly negative commentary featuring significantly in each year from 2004 to 2010. Figure Ten, in addition, demonstrates the range of the most frequent narratives comprising each year of commentary related to the topics.

Figure Ten: Stacked Bar Chart Demonstrating the Most-Frequent Narratives Involved in Immigration-related Commentary Over Time

Source: Lawrence Ampofo N=177

While strongly negative commentary was present, the main narrative it referred to was ‘Spain is still an object of terrorism’. An example of this is seen in a discussion thread on the *BBC Mundo* website following an article analysing the first anniversary of the 11-M attacks in 2005. One commentator claimed that Muslim communities in Spain were economically and socially deprived, which provided the conditions for the terrorist attacks witnessed in Madrid in 2004. The commentator added that the issue of non-integration is problematic for the Muslim and Spanish populations in Spain as it generates resentment, which feeds radicalised religious ideologies and gives credence to terrorist organisations, which might exploit an opportunity to for them to capitalise on.[[39]](#footnote-39) The sentiment that economic factors were responsible for the Madrid attacks was supported by Elena Sánchez at the Centre d’Informació i Documentació Internacionals a Barcelona(CIDOB) who claimed that the negative economic situation currently faced by Spain was largely responsible for creating entire neighbourhoods of immigrants, which in turn was fostering fear amongst the greater Spanish population.

This comment demonstrates the degree to which Spanish language online commentators emphasised integration of the immigrant population as an integral element to preventing future attacks. It also emphasises the extent to which religious discourses, such as the notion that al-Qaeda will continue the Jihad in the name of Islam, are also linked with immigration, technology and terrorism online following the 11-M attacks. The use of religious discourse, in addition to that of ethnic separatism, was a common feature explaining the propensity for strongly negative commentary online. The prevalence of such strong sentiment in online discussion also indicates that core narratives of tolerance and diversity from the Government were not being perceived by the general public.

Despite Spanish Government narratives of tolerance and diversity, delivered through its various public diplomacy strategies, and its efforts in creating multilateral agreements in the framework of the EUROMED, the findings of the internet research indicate that such messages are not being interpreted online in the same way. Another example of this is seen in a post to the blog *Labranza de Dios* about the Government’s sponsorship of a local Muslim political party called Renacimiento y Unión that was given public funds to represent the issues of immigrants. The author claimed that the establishment of this party signalled that Spanish society was facing significant danger from the perceived increment in political, social and economic power of migrants in the country.[[40]](#footnote-40)

The internet research indicates strongly that understandings of immigration, technology and terrorism in Spain exist amongst a wide range of actors. It has shown that the volume of content related to the topic of immigration increased significantly during the first and fifth year anniversaries of the 11-M attacks, while there was also an increase in coverage that related strongly to successes in national counter-terrorism programmes. The fact that the majority of the content was strongly negative in sentiment reveals that online commentators were prone to commensurating issues to support their arguments and align with their personal or group beliefs. Examples of this include conflating issues such as immigration, religion, integration and poverty with technology and terrorism to create one stand-alone issue of concern.

The findings suggest that while the Spanish Government is working to propagate a popular discourse that promotes diversity and tolerance through its international political activities and public diplomacy programmes, many online users are not interpreting events in the Government’s terms and thus the core narratives positively. It also suggests that in spite of the Government’s access to high technology as a means of influencing understandings of immigration, technology and terrorism, general perceptions of these issues (and this issue) are not positive.

## Conclusion

Understandings of immigration, technology and terrorism in Spain are inherently complex in nature. The impact of Francoism on understandings of these independent variables in Spain should not be underestimated. Spain’s transition from a dictatorship to becoming a constitutional democracy in 1978 encouraged widespread hope that the cultural homogeneity, which characterised Francoist Spain, would change to permit the blossoming of hitherto prohibited national cultures such as Catalan, Basque and Galician. In addition, it was hoped that Spain’s political elite would enshrine this notion of diversity in policy, as was seen in the adoption of the *Ley Orgánica Extranjería*, and the country’s accession to the European Community in 1985.

In spite of the fact that ETA maintained operations in France as well as in Spain, counter-terrorist policies that focused on controlling migratory flows were not considered in the same way before the 1980s. It was at this point, during the 1980s and 1990s, that greater efforts were made to secure Spain’s borders from rising numbers of illegal immigrants and to better police the French/Spanish border preventing the facilitation of ETA’s logistical operations. However, it was in the wake of the terrorist attacks by an al-Qaeda-inspired group of Moroccan nationals in 2004 that the commensuration of immigration, technology, terrorism and counter-terrorism was made to such an extent both in Spain and Europe at large. The commensuration of these independent variables was seen most prominently in the implementation of a range of policies and initiatives such as the Schengen Information System and the Passenger Data Agreement, which stored personal information and was used in counter-terrorism operations.

This fusion of the concepts of immigration and terrorism has resulted in a new reliance on technological solutions to mitigate against further terrorist attacks. To an extent, this has simultaneously reduced the complexity of terrorism, counter-terrorism, technology and immigration to numerical representations, while alienating entire communities of people, and increasing feelings of fear and resentment as witnessed in the behaviour of online communities.

Spain’s efforts to fortify and securitise its national borders using technological means suggests, certainly in part, a technological determinism belief is maintained, that technology will provide solutions to the country’s terrorism problem. However, the internet research conducted within this chapter highlights that understandings of immigration, technology and terrorism are strongly negative in Spain and some users believe that immigrant communities represent danger for Spanish communities, a view propagated in certain narratives from the mainstream media.

This finding suggests that it is not just technology that is responsible for the creation of capabilities in terrorism and counter-terrorism in Spain, and that the ability to positively communicate narratives is paramount. The following chapter examines in greater detail the role played by narratives in understandings of technology, terrorism and counter-terrorism in Spain.

# **Chapter Five: Influence, Technology, Terrorism and Counter-Terrorism in Spain: An Overview of Understandings, 2004-2010**

## Introduction

Terrorism is, above all, a communicative act, with the aim of delivering core messages and narratives to specialist target audiences. Terrorist and counter-terrorist strategies in Spain are, therefore, shaped by the contest for attitudes and behaviours. Ayman Al-Zawarhiri exemplified this by arguing in 2009 that “[w]e believe that the battle of the pen is no less important than the battle of the sword” (cited in SITE Intelligence Group, 2009: 1).

This chapter explores in greater detail the extent to which optimal delivery of core narratives impacts upon understandings of technology, terrorism and counter-terrorism in Spain. It investigates relationships between the media, technology and terrorism and, in particular, examines the various ways key narratives from Government actors and terrorist organisations are interpreted by the general public. In addition, it uses the theoretical frameworks introduced previously to examine the nature of the communication of core narratives online. It is intended that this analysis will contribute to discussions on recommendations for the amelioration of general communications strategies that focus on counter-terrorism in Spain.

This chapter will take as its starting point the assumption advanced within the central hypothesis outlined in Chapter One of this thesis, that the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives. As a result, the analytical process set out in this chapter tests the precept that as the sophistication of internet and Web technologies develop, terrorist organisations cultivate relationships with the general public, thereby increasing the public’s understandings of the relationships between the independent variables.

As outlined in detail in Chapter Two, the thesis focuses extensively on the theses by Bobbitt and Barnett. In his book ‘*Terror and Consent: The Wars for the Twenty-First Century’*, Bobbitt argues in support of the centrality of the internet and the Web in empowering market terrorist organisations to achieve their strategic objectives. Bobbitt claims that internet and Web technologies are an enabler for market state terrorists, helping them to augment their reach and influence in ways that they were not able to accomplish until the latter part of the 20th century. He argued:

‘Doctrine and strategy are debated in online discussion groups and chat rooms…the internet is responsible for 80 percent of the recruitment of youths for the jihad [in Saudi Arabia]. Photographs are shared – the Abu Ghraib prison pictures were instantaneously provided worldwide – and responsibility for attacks may be claimed. Most of all, perhaps, the diverse rage of many hundreds of thousands is channelled rather than dissipated. Often overlooked is the participatory dimension of the Web; it’s not just that the internet allows remote leaders to reach thousands or hundreds of thousands of otherwise inaccessible persons, it’s that it allows these alienated, often isolated people to speak back, to receive encouragement and reassurance as they separate themselves from society…it is the internet that allows Al Qaeda to communicate its strategy even while its leaders are in hiding, and despite the loss of its territorial base, which once would have meant defeat and marginalization but is now easily overcome’ (Bobbitt, 2008: 56).

Bobbitt’s above assertion illustrates his focus on the internet and the Web as tools that fulfil the strategic objectives of international terrorist organisations and help them, amongst other things, communicate with communities of people across national borders, even when their leaders are in hiding. In this way, Bobbitt’s argument champions the causal relationship between technology, terrorism and counter-terrorism and that access to these technologies results in their increased capabilities to fulfil their strategic objectives. This argument is, therefore, representative of a technological determinist assertion that technology itself has direct agency over human contexts.

Similarities can also be perceived between the theoretical framework propounded by Bobbitt and that provided by Barnett (2005) in *The Pentagon’s New Map: War and Peace in the Twenty-First Century*. In this work, Barnett argues that disconnectedness from the globalising systems created and maintained by countries within the Functioning Core, would inevitably encourage the development of threats to these countries such as international terrorism. The solution to this, he claims, is to “connect” the countries that reside in the non-Integrating Gap to those in the Functioning Core by using technologies such as the internet and the Web:

‘[E]xpanding the connectivity of globalisation, we increase peace and prosperity planet-wide…Simply put, when we see countries moving toward the acceptance of globalisation’s economic rule sets, we should expect to see commensurate acceptance of an emerging global security rule set – in effect, the agreement on why, and under what conditions, war makes sense. Where this global security rule set spreads and finds mass acceptance, the threat – by definition – will diminish.’ (Barnett, 2005: 26).

Barnett’s thesis closely resembles that espoused by Bobbitt. Barnett posits a close relationship between technology, terrorism and counter-terrorism, claiming it is global communications high technology that connects states in the non-Integrating Gap to those in the Functioning Core that will diminish international threats. In this way, Barnett argues that the internet and the Web are tools with which to promote peaceful coexistence between states.

Understandings of the internet and the Web as tools that promote the achievement of the strategic objectives of terrorist organisations are widespread in academic literature from internet and terrorism scholars. Gabriel Wiemann claimed that ‘Islamist, Marxist, nationalist, separatist, racist [groups] have learned many of the same lessons about how to make the most of the Internet. The great virtues of the Internet—ease of access, lack of regulation, vast potential audiences, fast flow of information, and so forth—have been turned to the advantage of groups committed to terrorizing societies to achieve their goals’ (Wiemann, 2004: 11). He added that terrorist organisations principally use the internet as a tool for data mining, propaganda, recruitment, fundraising, planning and coordination, sharing information, networking and psychological warfare. This conclusion is shared by a number of other academic authors on the topic (Thomas, 2003, Conway, 2005, Kaldor, 2007, Wilton Park, 2011).

This chapter will analyse the extent to which terrorist organisations focus more towards the employment of specialist communication skills to engage in relationship-building at the micro, macro and supranational level. As a result of the internet research findings developed in the previous chapter, it is anticipated that core Government narratives will not be interpreted or perceived well by their target audiences. There is also concern that those of terrorist organisations will be. The argument persists that governments are losing the war of ideas precisely because the decentralised market state terrorist organisations that Bobbitt described are manifestly more skilled at building strong relationships with a wide range of target audiences using both the traditional media and other communications technologies. The scholar Felix Arteaga of the Real Instituto Elcano epitomised this argument when he underscored the importance of narratives in counter-terrorism strategies, as he claims that the Spanish Government is being strategically outmanoeuvred by contemporary terrorist organisations:

“[Terrorism is] more about perception and this perception is shaped by the internet, by the message, by the way in which terrorists present their intentions, their goals and their narratives. I really do agree with Manuel Torres and others who say that we are losing the war of narratives because they are presenting their own war of Jihad or the terrorist actions in a better way than we do, we are just starting to learn how we counter these propaganda techniques, we have learned very much from the Afghanistan war and many other terrorist actions and this is something very difficult for us because they can prepare the message because they don’t have any moral or legal rules and they can present the story they want because they know how they are going to attack, for example how public opinion reacts to the information they give and this gives them a good advantage in their fight…we have to go to a more proactive mode somehow we have to create a state in which those potential readers and watchers of the messages have a previous filter and this is what we don’t have at the moment.”[[41]](#footnote-41)

One of the effects of the increasing adroitness exhibited by terrorist organisations in the realm of communications presented by both Bobbitt and Arteaga could be, according to the scholar Manuel Torres Soriano (2006), that “in the future, [the terrorists’] capacity to continue perpetrating terrorist acts could be greatly increased due to the perception of insecurity by the populace by the intelligent use of communication” (Soriano, 2010: 5).[[42]](#footnote-42) Soriano concludes, therefore, that the narratives of terrorist organisations could succeed if the general public becomes convinced of the possibility of future attacks, in effect becoming terrorised.

In this context, the chapter also analyses the use of digital public diplomacy in Spain to convey certain counter-terrorism narratives. The analysis of online behaviour and discussions related to the terrorist attacks contained within this chapter will be carried out using the context of the Madrid terrorist attacks on 11 March 2004. The online discussions and behaviour of communities generated as a result of this event will be used to analyse the extent to which bottom-up narratives from localised publics were more effective than top-down processes in conveying core narratives.

## Terrorism in Spain and the Traditional Media

Terrorism is a tactic that is necessarily communicative in nature, designed to convey a range of messages to target audiences. The terrorism scholar Brian Jenkins argued in the mid-1970s that the act of terrorism is an example of “choreographed violence”. In his paper investigating new forms of terrorism, he argued that:

‘Terrorism aims at creating an atmosphere of fear and alarm – of terror…Terrorist attacks are often carefully choreographed to attract the attention of the electronic media and the international press. Holding hostages increases the drama…Terrorism is aimed at the people watching, not at the actual victims. Terrorism is theatre’ (Jenkins, 1974: 6).

The conception of acts of terrorism as communication or theatre led Jenkins to assert that terrorists, therefore, want a lot of people watching and not necessarily a lot of people dead (Jenkins, 1975). Traditional media channels have historically played a pivotal role in the strategic objectives of terrorist organisations globally, and especially so in Spain. In fact, the late terrorism scholar Paul Wilkinson strongly supported the pre-eminence of the media in analyses of contemporary terrorism, claiming that the media is largely responsible for the development and continued prevalence of terrorism:

‘It would be foolish to deny that many modern terrorists and certain sections of the mass media can appear to become locked in a relationship of considerable mutual benefit. The former want to appear on prime time TV to obtain not only massive, possibly world-wide, publicity but also the aura of legitimisation that such media attention gains for them in the eyes of their own followers and sympathisers. For the mass media organisations the coverage of terrorism, especially prolonged incidents such as hijackings and hostage situations, provides an endless source of sensational and visually compelling news stories capable of boosting audience/readership figures’ (Wilkinson, 1997: 2).

The term ‘traditional media channel’ is an umbrella term that defines a wide range of media formats. Broadly speaking, the term refers to the class of media used predominantly before the introduction of the Web in 1990 and includes formats such as television, radio, newspapers, magazines and pamphlets. Media, therefore, not classified as traditional media for the purpose of this thesis include Web-based and internet-based media such as online videos, weblogs, discussion forums and voice-over-internet-protocol services, amongst others. The author is aware, however, that this definition is problematic given that the traditional media channels previously mentioned have their digital equivalents such as radio programmes, which are available online as well as television programmes. However, for the purpose of this thesis, the demarcation will suffice. This phenomenon is similar to the concept of renewal of old media outlined by Andrew Hoskins and Ben O’Loughlin in which old media forms come to develop digital equivalents (Hoskins & O’Loughlin, 2009).

It is important at this stage to elucidate further on the definition and contextualisation of the term Mainstream Media as it is used throughout the internet research. Mainstream Media refers to the category of media publications and other sources which have a nationwide remit. Such media organisations within this category can include newspapers such as *El País*, *La Vanguardia* and *El Mundo*, national television channels such as TV5 and newswires such as the *Associated Press* and *Reuters*. However, media organisations that have a distinctly local or regional remit are not classified in this thesis as mainstream media. Media organisations included in this category include local radio stations and local newspapers such as *Diario Independiente de Asturias*. In addition, the term mainstream media narrative refers to specific narratives emanating from these sources.

However, that while a fuller justification for the reasons as to the focus on the internet research was provided in Chapter Three, the conduct of a comparative study with the inclusion of other media formats, such as television or radio, was beyond the scope of work in this thesis.

The phenomenon of traditional or mainstream media content manifesting itself with a digital equivalent is termed as media renewal. The scholars Hoskins and O’Loughlin elucidated further on the concept of renewal in their research on the extent to which Jihadist media was subject to a process of “gatekeeping” or curation for Western news audiences, or the ‘“remediation”, translation and “trans-editing” by mainstream news organizations of the translation of often long, complex and highly multimodal texts initially published online by jihadists or Islamic extremists’ (Hoskins and O’Loughlin, 2010: 7). They argue that ‘mainstream media organisations have adapted to renew their models of news production and dissemination, harnessing user-generated content for instance’ (Hoskins and O’Loughlin, 2010: 6). In this sense, it is useful to conceptualise the transformation or renewal of media formats for the purpose of this thesis, as publications such as *El País* are present in the aggregated data set of social media content from 2004 to 2011. However, it is also extremely problematic to term content from El País as a digital newspaper, if we accept the concept of renewal. This is due to the fact that representations of these media forms on websites, for example, are very different to their physical format. The physical format of *El País* for instance does not accept comments in real-time from its audience, whereas the website version does have this utility. It was, therefore, decided that, for this particular work, it was prudent to focus on digital media and to incorporate other media channels such as television, in a separate study.

ETA, one of the preponderant domestic terrorist organisations in Spain, initially relied on print media to disseminate news of specific attacks, and their key political objectives, to the Spanish public. These *communiqués* took the form of pamphlets, such as *Insurrection in the Basque Country* in 1964, which were published in the Basque Country and disseminated within southern France and northern Spain. The content of these pamphlets detailed the motives for Basque independence, which claimed that the region was similar to a Spanish colony and used a range of metaphors to describe itself, such as the title of the book from Martiniquais Marxist author Franz Fanon; *The Wretched of the Earth* (Douglass & Zulaika, 1990: 8). The content of these pamphlets was reported by prominent national mainstream newspapers such as *El Mundo*, *El País* and *La Vanguardia* and the content analysed in great detail in the form of numerous articles and opinion pieces dedicated to them.

ETA also targeted television as a means of disseminating their messages to reach wider audiences. Increasingly, as noted by Jenkins (1974), the organisation designed their attacks to be theatrical, public spectacles to be broadcast to both Spanish and global audiences. One of the first ETA events to attract a national television audience was the organisation’s assassination of the Prime Minister Admiral Luís Carrero Blanco on 20 December 1973. The Naval Admiral Carrero Blanco was the person expected to be identified by General Francisco Franco as his successor. ETA carried out the assassination, which was codenamed Operation Ogre (*Operación Ogro*) in which a powerful car bomb was detonated in the street *Claudio Coello* inMadrid. Carrero Blanco was considered, more than any Government member in the Franco Administration, to be the epitome of Francoism and one of the main architects of the maintenance of the equilibrium of Francoism within the Government. The assassination, which was the most high-profile act carried out by the group in the Franco era, was reported by all of the major Spanish television channels. However, most importantly for the organisation, details of ETA’s manifesto, which justified the attack, were also broadcast. According to Douglass & Zulaika (1990), the attack was perceived by large sections of the general public in a positive manner as a result of its media coverage ‘not only across much of the Basque political spectrum but also within certain sectors of Spanish and even international public opinion’ (Douglass & Zulaika, 1990: 15).

While traditional media did much to disseminate news of ETA’s action in a positive fashion, the following example highlights how blanket coverage of ETA’s actions generated negative sentiments towards the organisation. The kidnapping and eventual assassination of the politician Miguel Ángel Blanco on 13 July 1997 was widely broadcast by all of Spain’s national television channels. Members of ETA kidnapped Blanco, a 29-year-old Councillor for the PP in Ermua, a town located in the Basque Country, on 11 July. The members of the group demanded a ransom from the Government, the transfer of ETA prisoners to other less secure prisons located in the Basque Country within 48 hours, a demand to which the Government refused. Within 48 hours, ETA group members had executed Ángel Blanco. In response, more than two million (Nash, 1997) Spanish citizens took to the streets in protest at ETA’s continued violence, which was in turn captured on national television and other traditional media channels. Television stations were instrumental in broadcasting the grief of the public and that of the family and, according to the scholars Sabucedo et al. (2000), the wider Spanish public in near real-time:

‘The public followed minute by minute the reactions of the rest of Spain and the rest of the world. The action by ETA is practically the only topic of discussion in informative announcements and citizen discussion. Through these announcements, the notion that ETA’s acts were inhuman were consolidated and reinforced, as well as solidarity with the victim, the need to do something to stop the assassination and the public indignation against those responsible’ (Sabucedo, Rodríguez & López, 2000: 11).

This supports the point made by Garcia et al. (2009) that the widespread television coverage of the Blanco assassination and the subsequent public demonstrations did much to erode ailing public support for the organisation (Garcia et al. 2009).

ETA, however, is not the only Spain-based terrorist organisation to have targeted television and other traditional media as a means of achieving their stated aims. al-Qaeda too has made prominent use of the medium to publicise their acts in reference to Spain, most notably in the form of the 11 March 2004 bombings of the mainline train services in Madrid. As outlined in detail in Chapter Four, the days subsequent to the attacks saw extensive coverage afforded to the event including interviews with eyewitnesses, victims, survivors and the subsequent court proceedings of the suspects.

In addition, the point made in Chapter Four should also be reiterated, that much of the output from traditional media 24 hours subsequent to the detonation of the bombs was inaccurate as the PP Government announced that ETA was responsible for the 2004 Madrid attacks. The inaccuracy of reporting, it was argued by Michavila (2005), was beneficial to the PP because it supported their previous policies on counter-terrorism. However, when traditional media channels began reporting that the attacks had been committed by al-Qaeda, they were instrumental in causing much of the Spanish electorate to vote for the PSOE and change of government (Michavila, 2005, Garcia, Rueda & Ruiz, 2009, Selway, 2006). In this sense, we can see how, in a reversal of Chomsky and Herman’s (1994) manufacturing consent thesis, which will be presented in detail later in this chapter, the Spanish Government, in this case, is perceived to have actively manufactured dissent by engaging directly with the mainstream media.

A body of academic research investigating television coverage of the 11 March attacks has explored whether certain channels displayed biases towards particular political candidates, framing their coverage accordingly (Blanco et al. Date Unknown, Baena, 2005, Galera & Pascal, 2005, Muñoz, 2005, Avendaño, 2010). In their study of the issue, Curto et al. (2007) concluded that *TeleMadrid*, known for its support of the PP, focused its broadcasts on the assertion that ETA was responsible for the attacks and not, as was being advanced by Government security staff when the information became more widely known, that they were perpetrated by an international terrorist group originating from Morocco. They argue that the 11-M bombings are a good example of the ideological narrative established by the channel which, according to Alfonso García, the Director of Broadcasting at *Telemadrid*, all programmes susceptible to manipulation are manipulated (Curto et al., 2007).

Traditional media represents one method of transmitting core narratives related to terrorism and counter-terrorism. However, the internet and the Web, as mentioned by both Bobbitt and Barnett previously, represent new technologies that connect billions of people. This chapter will now examine how the internet and the Web have been used to influence the general public of key narratives and strategic objectives.

## Terrorism and the Internet / World Wide Web in Spain

The use of the internet and the Web as critical elements used to achieve strategic organisational objectives has been widely adopted by contemporary terrorist organisations. The Spanish terrorism and internet scholar Javier Jordán (2008) claims that contemporary terrorist organisations would not be able to operate effectively without them. Indeed, Justin Webster argued “without the internet it is difficult to imagine al-Qaeda”.[[43]](#footnote-43)

In addition, according to the scholar Dorothy Denning, a major reason explaining the widespread adoption of the internet and the Web as the dominant media channel for their operations, is that traditional media channels are comparatively expensive and subject to editorial control, while online communication is cheaper, has a very low barrier to entry and can be viewed by anyone with an internet connection. She puts it that:

‘One reason the Internet is popular among activists is its cost advantage over traditional mass media. It is easier and cheaper to post a message to a public forum or put up a Web site [sic] than it is to operate a radio or television station or print a newspaper. Practically anyone can afford to be a Web publisher. In addition, the reach of the Internet is global. A message can potentially reach millions of people at no additional cost to the originator. Further, activists can control their presentation to the world. They decide what is said and how. They do not have to rely on the mass media to take notice and tell their story “right”’ (Denning, 2001: 8).

The notion that the internet and the Web have lowered the costs associated with the attainment of strategic objectives for terrorist organisations is significant because it argues that the fulfilment of such actions is at once more affordable and less difficult. Curto et al. (2007) underscored this point by claiming that the internet has facilitated the opportunity to maintain the cohesion of terrorist groups while simultaneously publicising the acts they have committed. They claim that the internet has allowed terrorist organisations to live a double life with strategic centrality and tactical de-centrality (Curto et al, 2007).

The previous assertion can be applied to the case of ETA. The organisation maintains an active Web presence with a website and pro-Basque independence presences in a number of online forums. Al-Qaeda in the Maghreb (AQIM) too regularly posts anti-Spanish commentary on its website and various other Web portals (Wiemann, 2008, Soriano, 2010). Soriano (2010) demonstrated this in his analysis of Jihadi online propaganda in Spain, claiming that the use of the internet has produced a qualitative and quantitative increase in communication activity within the group. Al-Qaeda in the Maghreb is now an actor capable of understanding the requirements of the information society (Soriano, 2010).

Terrorism and internet scholars, as outlined earlier in this chapter, have documented the ways in which terrorist organisations use digital media sources for a wide range of operations, enabling them to better collaborate and conduct certain operations across national borders, such as the indoctrination and recruitment of potential supporters. The indoctrination (Jordán, 2008) of potential supporters is achieved through the posting of multimedia content depicting images and videos of atrocities committed against Muslim civilians, beheadings and the final demands of suicide bombers (Davis, 2006). In addition, the inculcation of potential supporters is conducted by engaging with people on online discussion forums and websites with the aim of influencing users’ perceptions (Rogan, 2006). However, the ultimate aim of indoctrination techniques for Jihadist groups is not always clear. Taboul’s (2008) analysis of Jihadist francophone forums revealed that online users were concerned with being part of a community rather than committing violent acts, especially for those who do not reside in the Middle East. The overall aims and objectives of terrorist groups are therefore being achieved by exploiting online users’ need for ‘religious, moral, emotional and material support and it seems that social solidarity within this virtual community…reflecting the sense of being a minority in Europe’ (Rogan, 2006).

In addition, the internet has been used as a method for financing terrorist operations through the illegal activities of underground criminal networks. Terrorist organisations operating in Spain have been known to make use of online criminal methods to generate funds, such as identification theft, phishing and credit card fraud (Fragoso, 2010)[[44]](#footnote-44). The relationship between cybercrime and terrorist organisations in Spain will be investigated in more detail in the following chapter.

Terrorist organisations operating within Spanish borders are also known to use the internet as a means of obtaining information about specific targets (Soriano, 2010). Paz (2004), for example, documented the ways in which the perpetrators of the Madrid attacks downloaded and followed the instructions from a publication uploaded to the Global Islamic Media and The Information Commission in Support of the Iraqi People entitled *Message to the Spanish People*, in which Jihadists are encouraged to perpetrate attacks against Spain (Paz, 2004).

It is apparent that terrorist organisations engage with diverse and growing audiences using social media services (Conway, 2005). As outlined in detail in Chapters One and Three, the development of social media technologies enables people to engage in discussion on events both retrospectively and in real-time, hitherto difficult via traditional media channels. People affected by terrorist attacks in Spain use a variety of online platforms through which to express their views about the events, such as discussion forums, social networks and microblogs. While the use of these technologies enables people to debate the rationale behind the terrorists’ motives, the internet and the Web have in turn given terrorist organisations the opportunity to address audiences of millions and the opportunity to counter the occurrence of misinformation in online forums (Soriano, 2010). Used in this way, the internet can help terrorist organisations influence public opinion and debate in real-time across national borders; ‘[i]n other words, the Web has been a timely, efficient and effective tool for conducting information warfare’ (Burton, 2006: 8).

In addition, terrorist organisations further disperse their narratives using the internet and the online multimedia platforms created by traditional mainstream media corporations. Weimann (2006) claimed that the confluence of multimedia online platforms from traditional media corporations, in tandem with online terrorist rhetoric, resulted in the two-step flow of information from terrorists to journalists, the internet to the public, demonstrating how terrorist organisations are becoming more adroit at strategically using information and communication technologies. However, the apparent openness of this “flow” is contested by Hoskins and O’Loughlin who claim that Western mainstream media organisations exhibit a propensity to overlook online media channels, such as ‘terrorist monitoring sites, Arabic media, and jihadist websites’ own self-monitoring and feedback services’ as sources of information and, in the process, fail to present alternative perspectives on how terrorist content might be palatable to some audiences (Hoskins & O’Loughlin, 2010: 1).

It is at this point that it is pertinent to elucidate some of the theoretical frameworks that help examine the nature of communication explored in this thesis. This analysis begins by introducing the concept of Herman and Chomsky’s Manufacturing Consent theory (1988) that seeks to explain the nature of communication by studying the political economy of such communications methods. Secondly, it examines the media culture theory, where communication and narratives are transmitted through cultural norms and relationships, a multifaceted method where narratives are not communicated through one particular channel. Finally, the contest model from Cottle (2006) is explored in which it is determined that communication and the construction of certain narratives are given form through the writer’s antagonism with government policy.

Edward Herman and Noam Chomsky (1988), as mentioned previously, focused on constructing a theory explaining the nature of communication in the media by explaining the political economy of its production. They argued that because the media is an industry, just like any other, and relies on financial contributions to maintain its existence, the content and nature of its output is determined to a lesser or greater degree to the dictates of market forces. Several factors contribute to this according to Herman and Chomsky, the first of which concerns media organisations’ dependence on multinational news organisations for news content. Such multinational organisations can include governments and other corporations who produce newsworthy content. If media organisations are openly critical of such organisations then they are subsequently denied access to them and, by implication, a source of revenue (Herman & Chomsky, 1988). In addition, they claim that contemporary media organisations are extremely financially powerful as they are able to place their content across a range of media and distribution channels. The corollary of this is that space for alternative media is decreased and only wealthy media organisations are able to attract readers, something that is underscored by analyses of online traffic to the most popular news websites (ComScore, 2010).

Finally, Herman & Chomsky argue that media organisations are restricted in the range of news they can offer because of the necessity of attracting funds from advertisers. Advertisers are essentially the ‘patrons who provide media subsidy. As such, the media compete for their patronage, developing specialized staff to solicit advertisers and necessarily having to explain how their programs serve advertisers’ needs’ (Herman & Chomsky, 1988: 8).

This theory is useful because it can be applied to understandings of the nature of communication following the 11 March 2004 Madrid attacks when media organisations were instructed by Aznar to publish content blaming ETA, in spite of the mounting evidence to the contrary (Moreno, 2004). However, as will be presented subsequently, this led to discontent amongst the Spanish public. It is also pertinent to consider the limitations of the manufacturing consent theory, not least the argument put forward by Antoniades et al. (2010) that different media and strategic narratives are ‘projected across media systems, re-mediated and translated and responded to differently’ (Antoniades, Miskimmon & O’Loughlin, 2010: 9). If this is the case, then it is arguable that consent may be one element that is interpreted from media content and that Herman & Chomsky’s argument needs to be expanded to accommodate the various ways in which target audiences respond to media content and narratives.

The media contest model was advanced by the scholar Simon Cottle who maintained that the relationship between media organisations and the government or other influential institution cannot be known beforehand. Rather, it is only possible to determine whether consent has been granted by conducting a retrospective analysis and this, therefore, leaves space for other elements such as dissent and contestation to occur (Cottle, 2001 in Bromley ed., 2001). This theory is useful in that it demonstrates that other forces were instrumental in explaining the nature of communication following the 11 March 2004 Madrid attacks. It provides an explanation for the high volume of negative media coverage directed towards the Aznar Government after it emerged that ETA was not responsible for the attacks, that Aznar had provided newspaper editors with erroneous information and that an al-Qaeda-inspired group had admitted culpability for the attack.

Finally, media culture theory contends that media content is created according to the normative values and representations in society and culture (Cottle, 1998). Simon Cottle argued in his analysis of the application of Ulrich Beck’s (1999) risk society theory to the structure and practice of contemporary media that the creation of media content is shaped by ‘“value conservatism” or the value of preservation that seeks to check uninhabited industrialism’ (Cottle, 1998: 11). In order to illustrate this, Cottle makes the case that media coverage concerning the environment or ‘ecological journalism taps into a surrounding typification of the environment as a cultural good, and thereby enjoys increased media coverage and interest’ (Cottle, 1998: 12).

Cottle’s argument concerning the validity of the media culture theory has utility in explaining the reason why certain narratives continued to be discussed within certain media channels. This can be observed in the narrative condemning the Aznar Government’s provision of erroneous information to the mainstream media concerning the authorship of the Madrid terrorist attacks in their immediate aftermath, when evidence from the security services contradicted the story. This is a cultural process because the emergence of this particular narrative reflected the normative values of Spanish culture in relation to this event; namely, that Spanish citizens were entitled to know the truth of the events that occurred on 11 March 2004 in Madrid.

The use of digital media was widespread following the terrorist attacks on 11 March 2004, during which, communities of online users came to user-generated-content sites to comment on the events and discuss news perpetrated by the mainstream media. This use of social media is analysed further in this chapter.

## Internet Research on the 11-M Attacks: Key Narratives and Sentiment Analysis (2004-2010)

As previously described in Chapter Three, the author created a methodological process from media analysis to analyse online behaviour related to the Madrid terrorist attacks of 2004 to support the primary research conducted. The date range of the analysis was six months from 11 March to 11 August each year over a period of seven years (2004 to 2010). This chapter focuses on key narratives relating to the bombings and analyses the sentiment and narrative source. Further findings from the internet research are presented in relevant chapters of this thesis.

879 individual data points were analysed comprised of content emanating from blogs, discussion forums and websites. This section presents an overview of the results followed by an analysis into specific date ranges (2004, 2005, 2006-2007, 2008-2009 and 2010).

### Overview of Results

#### a. Volume of Content Over Time (2004-2010)

The internet research revealed that far more people were engaged in discussion on the Madrid bombings in 2004 and 2005 than in later years. Figure Eleven below demonstrates this overall decrease in the volume of activity over time. The reasons for this occurrence are unclear and could be ascribed to numerous factors such as declining mainstream media interest in the event or emotional fatigue on the part of the general public. By 2008 and 2009, the intense media coverage of the terrorist attacks that had been visible initially had diminished significantly leaving in its place a profound sense of loss among general online users that will be developed further below.

Figure Eleven: Total Volume of Commentary Over Time Inclusive of All Media Types

Source: Lawrence Ampofo N=879

In addition to the content presented above, the aggregation process gathered content that was outside the date range of the present internet research in order to indicatively assess the nature of commentary and content. This content underscored that the issue of Spanish terrorism was discussed widely amongst online users before the 11-M attacks took place in 2004 as an issue of concern. In 2003 for instance, blogger Lola Mateo advised readers to become members of the Victims’ Association of Terrorism (Asociación Víctimas del Terrorismo) because it helps those people affected by terrorism when the state will not (Mateo, 2003). There are a number of reasons for the long-standing focus on terrorism by online users; one is that the principal General Election candidates, José María Aznar of the PP and José Luis Rodriguez Zapatero of the PSOE, placed counter-terrorism measures against ETA at the centre of their election pledges, which in turn garnered widespread online discussion. Another reason can be seen in the numerous online users writing about terrorism in the Spanish-language blogosphere, inspired by activity from ETA and the impact of the terrorist attacks in the US on 11 September 2001. Examples are seen in the blogs *Bye Bye Spain*[[45]](#footnote-45) and *Matrix 666*[[46]](#footnote-46) in which the authors commented regularly on ETA and the problems they have caused Spanish society.

#### b. Most Frequent Narratives, Sentiment Analysis and Narrative Source (2004-2010)

For the purpose of this analysis, ten key narratives were elected; five from Government sources and five from terrorist organisations as described previously in Chapter Three. These narratives are presented in the following table:

**Table Four: Key Narratives Used for the Internet Research**

Source: Lawrence Ampofo

The development of the key narratives from online users over time in conjunction with other salient parameters (narrative source and sentiment) uncovers a number of significant points. The most striking of these is the distinct lack of key narratives from Government and terrorist organisations’ narratives overall, specifically in the visible Web.[[47]](#footnote-47) This is a curious phenomenon as it was hypothesised previously that core narratives from these influential groups would constitute the majority of the narrative corpus due to the resources available to them to conduct successful online communications campaigns. However, analysis of Spanish-language online content highlighted that the key narratives emanated from general online users who, in their discussions of the Madrid bombings, created their own key narratives, independent of key Government and terrorist narratives. This finding indicates that both the Government and terrorist organisations are not as influential in their online activity on the visible Web as hypothesised, and that general online users in turn are not necessarily receptive to narratives from these organisations. This example of bottom-up narrative construction also underscores the limitations of Foucault’s notion of Governmentality, as outlined in Chapter One, when related to online discussion of the 11-M.

These findings are valuable in providing insight into core narrative uptake in crisis situations and complex emergencies. The core narratives of large organisations during complex emergencies delivered via the mainstream media are often mistrusted unless they are supported with a comprehensive engagement strategy. An article in the *New York Times* (Mackey, 2009) concerning widespread rejection of the Iranian Government’s core narratives during the disputed presidential election of 2009 provides a helpful example of this. Despite narratives from Ayatollah Ali Khamenei and President Mahmoud Ahmadinejad that the elections were “real and free”, numerous online commentators roundly condemned the Government and quickly formed groups on social networks to voice their dissent. One such group called “Ahmadinejad is NOT my president” was especially active and to date has attracted almost 20,000 members.[[48]](#footnote-48)

The high volume of content from general online users highlighted that the Government and terrorist narratives did not influence the discussions and opinions of general online users. However, it also underscores the opportunity the Government has to attain influence online and to seek to positively engage people and foster long term support for its strategic objectives. This phenomenon also underscores that public spheres in Spain do not operate through top-down communications strategies. Rather, it suggests that the general public gathers media content from a range of sources.

The following table in Figure Twelve outlines the range of dominant narratives that emerged during the internet research. In addition, the message source, which details the main community responsible for each key narrative, is listed. The line chart in Figure Thirteen reveals a general lack of key narratives from Government and terrorist organisations and demonstrates, furthermore, that these organisations either connected infrequently with the online users they intended to reach or users rejected these narratives. However, it is inconclusive why this form of behaviour occurred from the data collected.

Figure Twelve: Total Volume of Content by Core Narrative

Source: Lawrence Ampofo. N=879

Figure Thirteen: Total Volume of Content by Narrative Source Over Time

Source: Lawrence Ampofo N=879

Some online users attempted to engage in discussion supporting the notion that immigration controls should be placed on immigrants entering Spain and that the Islamic religion was the main inspiration for the Madrid attacks in 2004. An example of this is seen in a Reuters article from 08 July 2005, published in the mainstream media publication *20 Minutos*. It documented that the Spanish Home Office (Ministerio del Interior) would send terrorism experts to London to assist the UK Government with the investigation into the London terrorist attacks on 07 July 2005. The news item claimed that Spain’s experience of Islamic terrorism, gained largely during the Madrid attacks in 2004, would be invaluable to the ongoing investigation. In the ensuing discussion, various online users took the opportunity to engage in anti-Islamic rhetoric claiming ‘ALL Islamists should get out of Europe. Problem solved. It’s a little radical yes, but effective. It is what the Catholic Kings did over 5 centuries and we did not have a problem. It is since this massive immigration of Moors into Spain that we have had problems. I know that not all Arabs are bad but it is better to be safe than sorry.’[[49]](#footnote-49) This comment emphasises the idea that some online users engaged in xenophobic commentary as a means of expressing their confusion and anger in the immediate aftermath of the attacks. It also demonstrates how some general online users displayed a proclivity to commensurate religion with terrorism after it emerged that the perpetrators of the attack did so using al-Qaeda ideology as justification for the act.

Another narrative that attained prominence was the notion that the attacks had directly influenced the decisions of voters participating in the General Election of March 2004. An example of this is seen in an article from *La Voz de Asturias* publication in which the journalist Mario Schwartz wrote an article outlining comments from the former Minister of the Interior Ángel Acebes who claimed that ‘the attacks had caused 200 deaths and a change in government.’[[50]](#footnote-50) This comment emphasises the notion also advanced by scholars (Moreno, 2004) that the terrorist attacks played a prominent role in influencing the decisions of voters in the 2004 General Election. Moreno (2004) analysed the possible effects that the terrorist attacks may have had on the outcome of the election by examining public opinion polls by Gallup and official election data from the Government. He contended, like the commentator above, that the high voter turnout and unforeseen victory by the PSOE was influenced significantly by the Madrid terrorist attacks (Moreno, 2004).

With respect to the analysis of sentiment, certain narratives simultaneously generated both strongly positive and strongly negative viewpoints from online users. One narrative that exhibited this nature was the ‘Remembrance for the victims’ narrative. An example of this is seen in the blog *El Blog que nos Acerca* in which the user outlined their experiences of the Madrid bombings and how their lives had changed irrevocably since the attacks; ‘4 years have passed since the 11 of March. My life has changed, I have different employment, I live in a different country, I have the luck to do what I like, I travel, I know admirable people here and there and today I think that, on the other hand, the lives of the 192 people stopped this morning of March, marking forever the lives of their friends and families. For them the remembrance is not a question of anniversaries and annual ceremonies. It is like Pilar Manjón told me this morning, for them, from then on, “there are good days and bad days”. From here, I will make my own personal homage.’[[51]](#footnote-51) This phenomenon provides strong support to Cottle’s media culture theory, as it is indicative of the notion that the creation of online media content related to this particular narrative was founded on the strong public sense of anger and frustration at the nature of the attacks. Online media was, therefore, created to support this sentiment and, considering the user-generated nature of this particular medium, provide a sense of catharsis, which is demonstrated prominently below in the strongly negative commentary made online.

Strongly negative entries referring to the ‘Remembrance for the victims’ narrative generally focused on online users outlining their personal experiences of the event and creating an online homage to the victims, such as the entry above. However, strongly positive comments were also replete. In a post to the web log *Palabras Retorcidas*, a discussion thread focused on general online users sharing their experiences of the day in a positive fashion. One user remarked that ‘This is more than a beautiful song, it talks about a life that was ended on the train that exploded on 11 March, it reflects the dreams completed in the event of death. When I heard it I felt it in my heart. It really reflects the support for the victims of terrorism. For the free voices, everyone, let us never be silent!’[[52]](#footnote-52) This phenomenon emphasises the utility of Cottle’s media culture theory as it is apparent that social media content was created as a result of the widespread feelings of people who consider themselves to have been affected by the attacks. The previous quotation also highlights how the creation of such content allows the users to exhibit other utilities, such as the creation of communities around a topic or viewpoint of shared interest, which in this case refers to the reinforcement of the victims against terrorism narrative.

These two discussions above underscore an important finding concerning online discussions; the more directly a person is affected by an event, the more negative their commentary online becomes. The commentary from *El Blog Que Nos Acerca* was inspired by Pílar Manjón, a woman whose son was killed in the attacks and who subsequently established the Asociación 11M de Afectados Terrorismo[[53]](#footnote-53). The user employed the strongly emotive language from Manjón’s declaration of the emotional pain she and the other victims feel daily to emphasise that she feels a strong affiliation with the victims, particularly now that she has moved to Holland. The second type of post from *Saulatino*, however, comes from users who were indirectly affected by the attack and posted more empathetic, and by extension, more positive posts, claiming that they can only imagine the pain of the victims.

Figure Fourteen: Total Volume of Content by Sentiment Over Time

Source: Lawrence Ampofo N=879

#### c. Results from 11 March 2004 to 11 August 2004

The narratives present a distinct pattern in 2004, whereby comments that expressed anger, retribution and frustration on the part of the online users were the most frequently occurring sentiments. The graph below shows the top ten most frequent narratives in 2004 by sentiment.

Figure Fifteen: Top Ten Narratives by Sentiment in 2004

Source: Lawrence Ampofo N=146

The narratives created in 2004 were demonstrative of a distinct emotional and impulsive reaction to the shock of the bombings and subsequent Government response. 146 items of social media content were analysed for 2004, of which 138 included emotional responses from online users who were directly affected by the attacks, those whose relatives or friends were in the attacks, people who intended to travel to Madrid and those who simply wished to express support and sympathy for others directly involved in the attacks.

An interesting finding from the 2004 data is the prominence of the terrorist narrative ‘Al-Qaeda to continue Jihad’. The popularity of this narrative was driven by the discovery of a video in which the attackers claimed that Jihad would continue on 13 March 2004. The newspaper *El Mundo* published a number of articles in which it claimed that the police had reconstructed a video from the attackers especially for the incumbent Zapatero administration which demanded that Spanish troops be withdrawn from Afghanistan and Iraq. If not, then Spain would face the strong possibility of further attacks.[[54]](#footnote-54) The vast majority of content that delivered this message was strongly negative in sentiment as online users expressed trepidation and fear that a similar attack on the country might be imminent. It is also a strong example of the way in which terrorist organisations engage with publics and subsequently create fear.

Other dominant narratives contained in online commentary in 2004 focused on the misinformation presented to the public by the Aznar administration in the immediate aftermath of the bombings. Influential members of the Aznar Government claimed that ETA had perpetrated the attacks and was the sole organisation involved. This narrative was present in 25 per cent of commentary featuring the Government, and events from 11 March to 15 March 2004 when the General Elections took place, in spite of compelling evidence from the security services that Jihadist-inspired organisations were instrumental in perpetrating the attacks. José Maria Aznar took great measures to inform key mainstream media organisations of this hypothesis, advising them that they should emphasise ETA’s culpability for the attack (Curto et al., 2007, Moreno, 2004).

To this end, the narrative that the Government had lied in its release of information to the public were predominant in online discussion of the 11 March bombings. The sentiment analysis showed that online users expressed negativity towards the Government’s actions in the days following the attack. This negative sentiment was demonstrated in a comment by the former Head of Communications for the Congreso de los Diputados, Maria Llorach, in which she described that ‘many politicians from the PP lied and apart from this, the Aznar Government knew from the beginning that [the terrorist attacks] were not committed by ETA but that story did not suit them politically…we were not prepared for this and everybody thought how could Aznar and Ácebes lie to us so much? But they lie to because it is useful to them and the people feel fooled.’[[55]](#footnote-55)

The negative sentiment felt by online users is, however, a complex phenomenon, expressed in a multitude of ways. It is clear that online users felt a strong sense of injustice, aggrieved, as they were, that the Government had lied to them about the true identity of the attackers. To online users in general, it appeared that the Government had a long-standing objective to eradicate ETA and that culpability for the attack on the organisation was employed for political gain at the expense of the general public (*3 Dias de Marzo*, 2004). If ETA was generally accepted as the perpetrator of the attacks then the Aznar administration believed that it would have strengthened its pre-election claim of providing a strong approach to Basque terrorism. However, only ten per cent of online users commented that evidence of Islamic terrorism in the attacks would have been indicative of a direct response to Spain’s involvement in the Afghanistan and Iraq invasions (Waldmann, 2006).

In addition, online users used the fact that the Aznar administration had lied about responsibility for the attacks to argue that it was not fit to govern Spain. This sentiment is expressed in a post to the blog *Minuto Digital* in which the original post discussed the Partido Popular’s seeming inclination towards acceptance of Basque nationalism. One commentator opined, ‘[f]rom the PP of Rajoy and all his troops of voters, you cannot expect anything good, neither better nor worse than from the PSOE. They are united until death they do part…and they keep negotiating with ETA and still negotiating agreements!’[[56]](#footnote-56)

Commentary in 2004 also showed that online users believed that the attacks profoundly influenced the decisions of voters to elect the PSOE into power. This was evidenced most strikingly in a discussion thread on the *es.charla.actualidad* newsgroup in which it was claimed that ‘The ‘Mirror of Madrid’ reflected in the days of 11-M a deformed image of Spanish society with an opposition that had the dogs set on it in the form of the citizens against the Government for their electoral interest, with their militants taking the headquarters of the Government hostage, with some media outlets playing the part of agitators in the confusion and signalling to the president of the nation that he is culpable.’ More disconcertingly, it was suggested that the eventual change in government had achieved the terrorists’ principal aim: ‘[i]n addition to provoking a change of government, they have achieved the destruction of Spanish unity against terror. This division has been prolonged due to ETA terrorism.’[[57]](#footnote-57) The collective negative sentiment focusing on the Aznar Government was expressed by content creators who emphasised the inability of the Government to effectively govern the country, as well as the frustration felt by those who believed that the Aznar Government had deliberately withheld information surrounding the culpability of the attacks. The creation of such content is also indicative of the focus of the media contest model in which it is outlined that media content is created in instances where content creators are willing to be openly critical of policy.

The events in 2004 also inspired a range of other less-prominent messages particularly those criticising Spain’s relations with Morocco. Discussion on this issue rapidly became xenophobic and Islamophobic in nature as commentators sought to link Moroccan citizens and the Islamic religion with the Madrid attacks and international terrorism more generally. Some online users also espoused the notion that Islamophobia in Spain was on the increase in the immediate aftermath of the attacks, ostensibly driven by both inflammatory stories in mainstream media, particular figureheads within the government and extreme groups appearing in the activist community.

#### d. Results from 11 March 2005 to 11 August 2005

2005 generated the highest volume of commentary concerning the 2004 Madrid bombings in the dataset with 305 analysed posts. Figure Sixteen below presents the top ten most frequent narratives in 2005 by sentiment.

Online commentators expressed a deep level of mistrust and malcontent towards the Government as they continued to enunciate their dissatisfaction with official explanations for culpability for the attacks. This dissatisfaction with the Government is witnessed in Figure Fourteen showing sentiment over time in which the volumes of strongly and slightly negative content reach their apogee in 2005 with 196 and 72 posts respectively. However, it was not exhibited in general public opinion polls as Angus Reid Consultants declared that support for the Zapatero Government was high in 2004/2005 (Angus Reid, 2004). This high level of discontent and negative sentiment was generated by the widely held assertion that the Aznar administration had lied about the identity of the perpetrators of the attacks. Furthermore, according to the data used in this analysis, the public did not believe that the Zapatero administration was close to revealing the truth about the event. The erroneous information initially communicated by the Aznar administration did much to undermine public trust, and the key narratives delivered in 2005 suggest that this trust had not been repaired in the year following the attack.

The composition of narratives delivered during 2005 was slightly different to those generated in 2004 (Figure Sixteen below). The key narratives in 2004 expressed online users’ disbelief, anger and frustration at the situation, whereas the most prominent key narratives in 2005 were ‘Attacks influenced voter decisions’, ‘Unity is the most important message to get over the attacks’ and ‘Government lies about 11-M’. The collection of key narratives in 2005 demonstrated on the previous chart is reflective of the fact that online users had time to reflect and analyse the far-reaching impact of the bombings, concluding that it was therefore important to demonstrate compassion to the victims, and demonstrate indignation at the Government’s reaction to the event.

Figure Sixteen: Top Ten Most Frequent Narratives by Sentiment in 2005

Source: Lawrence Ampofo N=305

The most frequent narrative to emerge during 2005 was the strongly held sentiment that the Government had inaccurately informed the public on the day of the attacks and *continued* to do so one year later. The prominence of this particular narrative indicates that online users, including prominent mainstream media outlets, were outraged at the Government’s handling of the event one year on, a sentiment more important to Spanish language commentators than any other aspect of the attacks in 2005. The negative sentiment associated with the emergence of this key narrative stemmed largely from online users who discussed the Government’s potential reasons for providing such erroneous information, evidenced in a discussion on the blog *3 Dias de Marzo*, considered to be a highly influential portal of information on the attacks[[58]](#footnote-58). The original post commented on the release of a documentary entitled *Tras la Masacre*, published by the Aznar headed foundation Fundación para el Ánalisis y los Estudios Sociales*[[59]](#footnote-59).* It claimed that the documentary was another example of the former Government attempting to obscure the truth of the event. Other commentators agreed to this argument, such as this user here who claimed that:

‘Between confidants, ETA connections, the Secret Service, Asturian Guardia Civil, Spies and the Islamic press and videos from FAES and TeleMadrid, they want to intoxicate us so we forget what happened during those three days and the absolute lack of political foresight from the previous government. This is not a replica of FAES, it’s a slap to the PP’s thesis and similar media.’[[60]](#footnote-60)

However, as demonstrated in the chart showing key narrative delivery in Figure Sixteen, there is a range of other narratives competing for prominence after the ‘Government lies about 11-M’ narrative. The most numerous of these secondary narratives is the ‘Government’s call for unity amongst the Spanish populace’ against the terrorist threat. The Zapatero Government underscored the importance of the Spanish public remaining united in order to combat international terrorist organisations (Giménez, 2010). Examples of discussions referring to this narrative were replete online, such as this *BBC Mundo* Have Your Say discussion thread entitled *¿Cómo es España después del 11-M?* One user called for unity after the attacks when they stated that;

‘In remembrance of the victims of 11-m and for the rest of the innocents assassinated by the terrorists that are used as tools by the incompetent politicians that dominate the world that is inundated with injustices’[[61]](#footnote-61)

In the case above, it is evident that the user has made a clear demarcation between the role of the Government in the terrorist attacks and the presence of victims, suggesting that the terrorist attacks were directly enabled by Government policies. The presence of anti-Government rhetoric amongst online users demonstrates the utility of considering the media contest theoretical model as a theoretical framework to trace the presence and development of such rhetoric. In addition, however, such content also indicates that Spanish-language online users do not consume media content in a top-down manner, that they are not passive recipients of information, which originated from elsewhere. Rather, this emphasises that online users source information and narratives from a range of different sources which, overall, contribute to their understandings of this issue.

There were other prominent narratives in the dataset for this particular period in which overall culpability for the 11-M attacks was deemed to be a more complex and nuanced affair than the simple narrative published by the mainstream media outlets that an al-Qaeda-inspired group was responsible. The narrative that 11-M culpability is complex expressed the idea amongst online users that exercising patience and tolerance until the full body of evidence is collated, analysed and presented before the 11-M Commission is the best course of action for all parties concerned.

Another key narrative prominent in 2005 is the comparison between the 11 March 2004 attacks with the London Bombings of 07 July 2005. Online commentators such as discussants on the activist blog *Escolar* claimed that Spain now shared many similarities with the UK in respect to international terrorist attacks (Escolar.net, 2005). However, other commentators were far more parochial, claiming that Spain, and subsequently the UK, had suffered these attacks because of their perceived favourable immigration policies. Now the two countries had to take responsibility for the high numbers of immigrants that had taken residence and the possibility that a number of them could have been radicalised. Arguments of this sort were seen in a number of lengthy discussions, such as the *BBC Mundo* discussion in which one participant claimed that ‘Muslim immigration is not of cultural quality and it is not integration, that is always difficult between both worlds, it generates resentment that is fed by religious ideologues of a fundamentalist nature and it gives space for groups of this character.’[[62]](#footnote-62)

The commensuration of immigration and terrorism was analysed in detail in Chapter Four. The presence of this type of discussion emphasises that in the year following the attacks, some online users linked the two independent variables to make one dependent variable, largely informed by the identity and motivations of the people responsible for the attacks.

#### e. Results from 11 March 2006 to 11 August 2007

Online commentary fell to its lowest level in 2006 and 2007, to 154 posts. Figure Seventeen below presents the top ten most frequent narratives by sentiment in 2006 and 2007.

Figure Seventeen: Top Ten Narratives by Sentiment in 2006 and 2007

Source: Lawrence Ampofo n=154

In 2006 and 2007, there was a sharp decrease in volumes of content in comparison to that produced in 2004 and 2005 as demonstrated in the bar chart above. It is arguable that the lower volume of coverage can be attributed to high volumes of media coverage on other aspects of the Government’s counter-terrorism activities. Such activities include *Operación Tigris* and *Operación Nova I* & *II,* and the development of Zapatero’s Alliance of Nations (Alianza de Civilizaciones), which attracted high volumes of both online and offline media attention as described above. In addition, mainstream media attention was directed to the Government’s on-going negotiations with ETA over the possibility of a permanent ceasefire. This meant that while online discussion concerning terrorism as an issue continued unabated, specific discussion about the 11 March attacks fell.

The narrative that the Government had intentionally misinformed the general public in the aftermath of the attacks remained prominent in 2006 and 2007. However, a broader range of narratives assumed prominence in this period, including the notion that Spain is still an object of terrorism three years after the Madrid attacks. This particular narrative stemmed from online users who claimed that the threat of international terrorism had not dwindled and that, in spite of Government rhetoric, people should still remain aware of this threat. In a post to the *Stirpes Forum*, it was outlined that the Centro Nacional de Inteligencia (CNI) had warned the Government that a new Jihadist group named the Grupo para la Liberación de Al-Andalus was becoming more influential in Spain. In response to this article, commentators to the discussion thread commented that Zapatero’s counter-terrorism efforts since the Madrid attacks, such as the Alliance of Civilisations, were too accommodating to known terrorist organisations. One user even went as far as to suggest that the Madrid attacks were only the beginning of a much larger and prolonged campaign against the Spanish state, ‘I don’t know if this will happen but when the Muslims do suicide bombings to conquer Ceuta and Melilla and we surrender without throwing a punch, this will be the beginning of the end.’[[63]](#footnote-63) This conflation of terrorism in Spain with other issues such as religion is an example of commensuration as was outlined in depth in Chapters One and Four. It is noteworthy that this occurrence continues to take place in 2006 and 2007 as it demonstrates that the debate concerning the presence of foreigners, religion, terrorism and counter-terrorism had not developed since the occurrence of the bombings in 2004.

#### f. Results from 11 March 2008 to 11 August 2009

Online commentary increased steadily in 2008 and 2009, featuring increased levels of activity from general online users. In tandem with this increased activity, 2008 and 2009 also registered the highest level of strongly positive sentiment[[64]](#footnote-64) in the entire dataset. Increased levels of online commentary can largely be attributed to the fifth anniversary of the attacks and the General Election of 2008, during which the 11 March 2004 attacks were discussed widely. The graph below details the top ten most frequent narratives in 2008 and 2009 by sentiment.

Figure Eighteen: Top Ten Most Frequent Narratives by Sentiment in 2008 and 2009

Source: Lawrence Ampofo n=171

The volume of discussion during 2008 and 2009 rose significantly after falling during 2006 and 2007. This period saw the predominance of the frequency of the narrative that the Government misinformed the Spanish public about the group(s) responsible for the Madrid attacks. The prevalence of this particular narrative is indicative of the fact that online users continued to feel aggrieved by the inability of the Government to provide them with clear responses to the true passage of events in March 2004.

Aside from the Government misinformation emphasised by the ‘Government lies about 11-M’ narrative, it was clear that the focus of the key narratives shifted away from the anger and frustration, emotions that characterised the collection of narratives from 2004 to 2005. Online commentary in 2008 and 2009, as a result, saw the emergence of narratives that encouraged online users to be more compassionate towards the victims of the bombings and to provide support for other members of their particular communities. The ‘Remembrance for the victims’ narrative was frequently occurring during this period after the ‘Government lies about 11-M’ narrative. This particular narrative was delivered by individual users who frequently posted accounts of their personal experiences of the attacks while simultaneously paying their respects to those who had died. An example is seen in a post to a discussion thread on the web log *Palabras Retorcidas* in which online users gathered to pay homage to the victims of the attack. One user noted that, in addition, she too desired to extend her support to Spanish society in general; ‘[t]his song has left me frozen. It made my hairs stand on end when I think of the fatal day of 11 March. It is incredible that at this time terrorism still exists without reason, as if we were beasts. Kisses to Spain.’[[65]](#footnote-65) This cathartic exercise compelled a range of other users to post their own stories and contribute to the emerging community, simultaneously allowing the author to track the evolution of the community as is exemplified in Chapter Seven.

Online users again expressed a heightened sense of trepidation, particularly in 2009, that another terrorist attack could occur at some point in the near future with the narrative that ‘Spain is still an object of terrorism’. This narrative, which originally emanated from a terrorist organisation as a threat (Soriano, 2010), is one of the few to have been delivered more frequently than Government narratives in the dataset. However, it is important to underscore that general online users are largely responsible for engaging in discussion delivering this narrative.

#### g. Results from 11 March 2010 to 11 August 2010

2010 saw a continuation of the trend that witnessed widespread commentary from general online users and a preponderance of strongly positive content. Figure Nineteen below details the top ten narratives in 2010 by sentiment.

Figure Nineteen: Top Ten Most Frequent Narratives by Sentiment in 2010

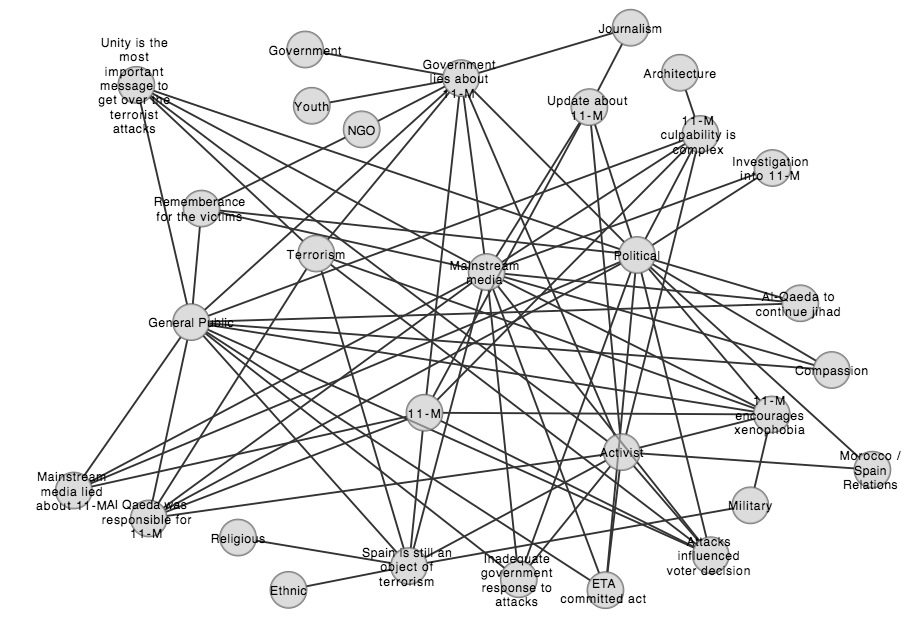
Source: Lawrence Ampofo n=103

2010 saw an increase in the trend that online users were more predisposed towards compassion and support than anger and frustration when discussing the 11 March 2004 attacks. The most frequently occurring narrative during 2010 was the ‘Remembrance for the victims’ narrative which strongly outranked the previously most frequent narrative of ‘Government lies about 11-M’ by generating 52 per cent of the total volume of content for this period. The rise in more compassionate narratives also generated significantly higher volumes of strongly positive content, which had been largely absent from the dataset until this point. This further emphasises that, while the majority of the online commentary was comprised of user-generated content and not from Government or terrorist organisations, there was a distinct inclination for online users to seek and provide emotional support for one another.

#### h. Network Analysis of Online Communities by Core Narratives (2004-2010)

The network map below demonstrates how the various narratives from Government and terrorist actors were largely ignored by other online users, who instead formulated their own narratives and discussed 11-M related issues amongst themselves, emphasising the fact that top-down explanations for the creation and assimilation of narratives are insufficient for this particular dataset. While the terrorist narratives ‘Spain is still an object of terrorism’ and ‘Al Qaeda was responsible for 11-M’ were central narratives in the dataset, it is clear that a wide range of other narratives were created by the communities for use in their own discussions. This phenomenon is symptomatic of the autonomous nature of online communities and how they often create their own narratives and content for use in their own communities, away from any mainstream media influence (Bennett, 2003).

Figure Twenty: Network Map of Online Communities by Core Narrative Delivery

 N=879

Source: Lawrence Ampofo

Although the nature and role of online communities is investigated in greater detail in Chapter Seven, it is pertinent to examine the nature and relationship of key narrative assimilation in tandem with individual communities to understand how such content is perceived. A detailed description of the method used to develop the network map is located in Chapter Three, but to summarise, Figure Twenty maps the various actors and their narratives. It is worth noting at this juncture that the Mainstream Media, Political General Public and Activist communities are extremely central within the network, exhibiting a great deal of activity and links to adjacent narratives. This demonstrates that these communities were extensively involved in all aspects of the discussion related to terrorism in Spain. It is also possible to witness communities such as Government located at the edge of the network and linked only to discussion of one particular narrative. This underscores that those involved in the governmental community did not participate widely in the array of conversations that took place concerning terrorism in Spain online.

Of the key narratives that were created by Government and terrorist organisations, very few were adopted by online communities. The Activist community, for example, delivered few Government narratives, and were instead more predisposed to emphasising the importance of cooperation to defeat terrorism in the country. An example of this is seen when the journalist Enric Sopena wrote in the online publication *El Plural* that cooperation from all political parties was necessary to defeat terrorism and that all methods should be employed to defeat it, including dialogue.[[66]](#footnote-66) However, the Activist community included comparatively more narratives from terrorist organisations such as those advocating responsibility for the attack and that proclaiming that the country continues to be a target of international terrorism.

In addition, it is noteworthy that there is a high rate of interdependence between the range of core narratives and the various online communities engaging in discussion of the 11 March 2004 terrorist attacks. The Political, Mainstream Media, 11-M, Activist and General Public communities are situated closely and, in turn, share links to a range of narratives.

This network analysis is useful because it pictorially demonstrates that online users, and online communities more generally, receive information and narratives from a range of sources, emphasising the multidirectional nature of communication in relation to the 11 March 2004 attacks. Therefore, while no one theoretical framework explaining the nature of communication outlined previously in this chapter would accurately explain the occurrences within this dataset, they collectively explain various elements of the nature of online discussion.

## Conclusion

The traditional media, as well as internet and Web technologies, play a central role in the activities of contemporary terrorist organisations. From the use of broadcast television and radio to disseminate news of attacks and statements, to the creation of sophisticated online multimedia content, to purpose-built digital portals and discussion forums, it is clear that 21st century terrorist organisations are extremely dependent on media technologies to remain effective (Bobbitt, 2008).

However, this chapter has also shown that media corporations in turn can be perceived to use terrorist attacks as a means of furthering their own political agendas. The relationship between the media and terrorist organisations is and always has been abundantly clear (Jenkins, 1974). However, what is less comprehensible is the relationship between the development of media technologies and the communication strategies of terrorist organisations. Traditional terrorist acts are communicative and part of a wider strategy, broadcasted using traditional media channels (Jenkins, 1974, 1975). Nevertheless, the development of information and communication technologies, particularly the internet and Web 2.0, has seen terrorist organisations build closer relationships with their target audiences. There is potential for terrorists to build stronger relationships with their target audiences across national borders, and it is possible that the organisations will decide to use less violence and more persuasion to advance their goals, something that was argued strongly by the scholar Jonathan Githens-Mazer who claimed that “with the increase in technology, you’re not seeing a commensurate decrease in attacks which I think is quite telling in and of itself in some ways.”[[67]](#footnote-67) What is suggested is that the Spanish Government is rapidly losing the battle for ideas online as flat, networked, interconnected organisations such as terrorist groups use electronic communications more adroitly than vertical, hierarchical government actors, insofar as the mere continued circulation of their narratives produced terror.[[68]](#footnote-68)

Ultimately, media technologies, as a force-multiplier of terrorist organisations, have the potential to change terrorist organisations from agents of violence to agents of influence, defined as those people who have the ability to affect the attitudes and behaviours of other online users, through the effective use of narratives and engagement. While the prospect of less violence might seem appealing to governments, the fact that some people find the ideas of terrorist organisations more palatable gives great cause for concern. Evidence for this is seen in the emergence of narratives such as ‘Attacks influenced voter decision’, which was the sixth most frequently mentioned narrative in the dataset. As a result, scholars have come to the realisation that the Government is losing the battle for ideas with terrorist organisations and should re-assess its counter-terrorism strategy (Soriano, 2010, Waldmann, 2006).

# **Chapter Six: Cybercrime, Terrorism and Counter-Terrorism in Spain**

## Introduction

The commensuration of cybercrime, terrorism and counter-terrorism in Spain as a social process is an increasingly prescient issue that is of concern in certain epistemic communities. The European Commission writes:

‘The rapid development of Internet and other information systems has given rise to a completely new economic sector…This has opened many new possibilities for criminals. A pattern of new criminal activities against the Internet, or with the use of information systems as a criminal tool, is clearly discernible. These criminal activities are in permanent evolution, and legislation and operational law enforcement have obvious difficulties in keeping pace’ (Europa, 2007: 1).

The proclivity for terrorist organisations to use the internet and the Web in specific ways to help them achieve their strategic objectives was outlined in greater detail in Chapters Four and Five in which it was supported by scholars such as Conway, (2005, 2008), Wiemann (2007, 2008), Denning, (2003), Arquilla and Rondfeldt (1999, 2003) and Colin (2003), amongst others. Examples include the tendency to use the internet for recruitment, propaganda, fund raising, data mining and information gathering (Wilton Park, 2011).

In addition, the conclusions derived from the research process and semi-structured interviews conducted indicated that cybercrime is a significant concern for the Spanish security services and private cybersecurity companies in equal measure. This phenomenon was outlined by the Spanish cybercrime expert Carles Fragoso who argued that terrorist organisations utilise cybercrime techniques to achieve their strategic objectives, thereby posing particular problems to the Government and private companies alike:

“It is a fear that technology is being used ever more by terrorists to conduct their operations. The positive points of technology in the real world in reality also benefit the criminal world or the world of cyberterrorism in aspects such as flexibility and location. Technology also permits in particular an exchange of information that is more fluid and convenient with access from remote devices that occurs instantly”. [[69]](#footnote-69)

As outlined above by Fragoso, the use of internet and Web technologies to facilitate the activities of terrorist organisations is problematic for Government and private organisations involved in countering them. Indeed, as will be analysed in this chapter, a similar sentiment has been outlined by the scholars Philip Bobbitt (2008) and Thomas P.M. Barnett (2005) in their analyses on the nature of contemporary terrorist organisations, the relevance of which is described in detail in Chapter Two.

This chapter offers the first analysis of the relationship between cybercrime, terrorism and counter-terrorism in Spain. It uses the theoretical framework of commensuration as a social process as a lens. Through the findings of the semi-structured interviews and analysis of the nature of online behaviour and discussion concerning cybercrime and the 11 March 2004 terrorist attacks in Madrid, it becomes apparent that understandings of cybercrime, terrorism and counter-terrorism are intrinsically bound within understandings of immigration, technology and terrorism.

This chapter seeks to examine the dualism between terrorist organisations and criminal organisations in the 21st century and the ways in which the two types of organisation use similar tactics to reach their stated goals.

It also explores the extent to which understandings exist between cybercrime, technology, terrorism and counter-terrorism in Spain. An analysis of this topic will shed light on the extent to which the issue of cybercrime is linked with terrorism and counter-terrorism in the region and whether the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives. This chapter will also explore the extent to which new internet and Web technologies such as Web 3.0 will ameliorate or deteriorate the ability of terrorist organisations to achieve their strategic objectives using cybercrime.

In addition, this chapter will elucidate how, in the 21st century, the two issues of cybercrime and terrorism form a close-knit, intricate relationship. It will conclude that the conflation of terrorist organisations utilising criminal methods via information and communications technology has had the effect of enhancing their online influence, becoming in the process an increasingly problematic entity for the Spanish Government to counter, thereby justifying the use of commensuration as a social process to more easily conceptualise the issues.

## Defining Cybercrime

The tendency to utilise the internet and the Web for illegal purposes is a broad definition of cybercrime, a loaded phrase that is full of uncertain, speculative, imprecise and complex definitions and terminology. The complexity of arriving at a universal definition of cybercrime is illustrated in the approaches taken by different public and private organisations. Private cybersecurity corporations such as Symantec provide their own definitions, such as the example below:

‘Symantec defines cybercrime as any crime that is committed using a computer, network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations’ (Fossi et al., 2008: 4).

However, supranational political organisations such as the International Telecommunications Union define the term as:

‘An activity that is carried out using a computer that is illicit or some parties consider illicit and which can be carried out across global electronic networks’ (ITU, 2009: 19).[[70]](#footnote-70)

The discord over a universal definition of cybercrime can also lead to instances of commensuration, where certain independent variables are conflated to constitute one overarching dependent variable, such as terrorism and cybercrime.

In the absence of a universal definition of cybercrime, it is useful to re-examine the theoretical frameworks offered by Barnett (2005) and Bobbitt (2008) who outline how internet and Web technologies support the activities of contemporary terrorist organisations. It is clear that in the theoretical frameworks offered by Bobbitt and Barnett, the internet and the Web are perceived as tools which help terrorist organisations more easily achieve their strategic objectives. In their estimation, the internet and the Web are force multipliers which help terrorist organisations generate more money, extend their geographical reach to conduct their activities across the world, and conduct more targeted propaganda, amongst other things. However, the complexity and difficulty of commensurating the two issues of terrorism and cybercrime is again demonstrated in discussions concerning cyberterrorism as currently, it remains only a theoretical possibility (Denning, 2003, Zunzunegui, 2008).

Barnett argued that internet and Web technologies would make the task of conducting international terrorism fundamentally easier as it gave organisations with a previously national purview, global reach (Barnett, 2005). Bobbitt on the other hand claimed, as will be outlined in greater detail in this chapter, that the internet-enabled market state terrorist organisation could commit eminently more dangerous attacks than they had done previously. He put it that:

‘Market state terrorists evade attempts to suppress them and enhance their power through the adroit use of modern communications technology, especially the internet. Paradoxically, the very decentralised network of communication that the US security services created out of fear of the Soviet Union now serves the interests of the greatest foe of the West’s security services since the end of the Cold War: international terror’ (Bobbitt, 2008: 55).

The notion that the internet and the Web are force multipliers, allowing international terrorist organisations to flourish in a veritable “underbelly of globalisation” (Owens, 2004) is something that underpins the arguments of both Bobbitt and Barnett.

Indeed, it was demonstrated in Chapter Five that the adroit use of new communications technologies, in tandem with an understanding of the demands and behaviour of their target audiences whilst using the medium, could provide terrorist organisations with the potential to exert greater control and manipulate the interpretation and uptake of their core narratives. An example of this is seen in the widespread use of the terrorist narrative ‘Al-Qaeda to continue Jihad’ following the discovery of a video in which the attackers pledged more attacks if Spanish troops were not withdrawn from Afghanistan. This ability to develop relationships with influential online audience groups suggests that terrorist organisations can develop an increasingly effective understanding of digital communication strategy in the same way that their government counterparts do.

The democratisation of internet and Web technologies, and the considerable opportunity for innovation they afford to all organisations including terrorist organisations, should not mean that these technologies be jettisoned, or that the medium should become a more securitised space, with net neutrality[[71]](#footnote-71) becoming an element of the past as a result. Rather, it is critical that security services and other relevant actors develop a similar understanding of the nature of online behaviour globally and how they can go about generating and exerting compelling online behaviour and narratives to positively affect the attitudes and behaviours of online users.

The technologically deterministic proclivity of some internet and terrorism scholars to argue that technologies would directly augment the abilities of terrorist organisations to carry out their operations has been refuted by others. The think tank analyst Jamie Bartlett claimed that technology in actuality has nothing to do with either augmenting or decreasing the capabilities of terrorist organisations because terrorism is still fundamentally about meeting with like-minded people face-to-face in communities:

“[Technology makes] [r]ecruitment…easier, radicalisation is easier because you can get like-minded people together who become more bold when they’re online and not face to face…Then you’ve got ease of access to bomb-making material and radical literature that you didn’t have access to before on YouTube, the Anarchists Cookbook, the al-Qaeda training manual, and this makes it much more difficult for government as well as if it spreads all over the place then its difficult to know what to do. But I do think, and it’s the point I keep reiterating, it’s hard to meet people, it’s hard to make bombs, I’ve only seen…one case…of someone completely self-radicalising online and going on to commit an action. You normally train overseas, 70% of people train overseas, and they normally have to meet their co-conspirators in person because it’s a big commitment”.[[72]](#footnote-72)

Although it is beyond the scope of this thesis to analyse Bartlett’s assertion of the correlation between the rate of technology penetration and frequency of terrorist attack, he nonetheless makes a noteworthy point that technology on its own does not have a direct effect on terrorist organisations. This argument dovetails well with the socio-technical theory outlined in Chapter One that it is both social interactions and technological development which together have a direct effect on the activities of human beings.

Spain has over 29 million internet users, representing a penetration rate of more than 60 per cent of the population, one of the highest in the OECD, as seen in Figures One and Two. The notion that the internet traverses geographic boundaries easily and quickly and offers its users economic, social and political opportunities has been outlined in detail during the course of this thesis, particularly through analysis of the theoretical frameworks offered by Philip Bobbitt and Thomas Barnett.

However, it has been discussed in this thesis that the converse of this vision of a global digital utopia is developing just as quickly, if not quicker (Council Of Europe, 2004). Cybercrime is a significant problem in Spain with the country having the highest level of copyright piracy in Western Europe (Intellectual Property Alliance, 2010). Reliance on such assertions is, however, problematic for a number of reasons, one being the notion that an agreed upon definition of the types of crime that constitute cybercrime has not yet been fulfilled. In addition, many people or organisations that might have been victims of cybercrime do not report it (Europa, 2007).

Different ministerial departments have created specific cyber security legislation such as the *Esquema Nacional de Seguridad* which regulates secure access to electronic mediums such as the internet and the Web, the Civil Guard’s Telematic Crime Group (Grupo de Delitos Telemáticos de la Guardia Civil) which combats online crime and the Spanish Data Protection Agency (Agencia Española de Protección de Datos) which enforces data protection regulations. However, the Spanish Government as a unit has not as yet created and implemented a national, overarching cyber security strategy in the same fashion as the UK (Chamorro &Villalba, 2010). Nevertheless, the approval of the Sustainable Economy Law which attempts to counter cybercrime in the country (*Ley Economía Sostenible* or *Ley Sinde*) was announced in February 2011 and will discussed later in this chapter.

The absence of a Spanish cybersecurity strategy highlights the importance of analysing the extent to which terrorist organisations utilise cybercriminal techniques as a method of increasing their influence and achieving their strategic objectives. It has been speculated that techniques such as identity theft, credit card fraud, phishing and copyright piracy[[73]](#footnote-73) are used by terrorist organisations, blurring the lines of common definition between terrorist organisations and organised crime syndicates (Bobbitt, 2008, Shelley, 2003, Wiemann, 2007). It has also been posited that the widespread proliferation of internet and Web technologies has played a major role in helping terrorist organisations and organised criminal syndicates to operate alike and indeed learn from each other. In the 2005 United Nations Congress for the Prevention of Crime and Penal Justice, the United Nations Office against Drugs and Crime outlined the findings of research conducted into data submitted by member states into the possible relationship between organised crime, drug trafficking and terrorism. It outlined that such a relationship does in fact exist:

‘[T]he nexus between terrorism and organised crime is intense. There are many crime-related stories that have become clear in the 11th United Nations Congress about Penal Justice and the Prevention of Crime. In the doctrine, there are studies related to the transformation of terrorists into criminals although it can happen the other way round. For this reason, terrorists and criminals learn reciprocally from one another, especially when they have to establish illicit avenues for their criminal activities’ (Úbeda-Portugués, 2009: 3).[[74]](#footnote-74)

Úbeda-Portugués’ argument above adds an extra dimension to the assertion offered by other terrorism, internet and globalisation scholars, that terrorist organisations’ use of internet and Web technologies has broadened to include cybercrime amongst other things (Conway, 2005, *Revisión Estratégica de Defensa*, 2003, Napoleoni, 2004).

At this juncture, it is worth reiterating the point made in Chapter Two concerning the complexity involved in adequately defining the term terrorism, in order to provide conceptual clarity for the reader. A universally accepted definition of the term terrorism is widely noted by terrorism scholars, sociologists and practitioners as extremely problematic (Stampnitzky, 2010). The problem of definition was identified by the terrorism scholar Bruce Hoffman in his analysis on the nature of global terrorism: ‘one can find such disparate acts as the bombing of a building, the assassination of a head of state, the massacre of civilians by a military unit, the poisoning of produce on supermarket shelves, or the deliberate contamination of over-the-counter medication in a drugstore, all described as acts of terrorism’ (Hoffmann, 2005: 1). The very ambiguity of the nature of terrorism can lead to confusion between the kinds of acts that can be denoted as such and those which are otherwise criminal activities.

As a result of the inherent complexity in defining terrorist acts, this thesis will utilise the definitions of terrorism (*terrorismo exterior*, *terrorismo interior*) as offered by the Spanish Government:

‘External Terrorism is that which is committed outside the borders of the state of origin or within countries of origin but against the interests of other countries…such as attacks, sabotage, assassinations and kidnappings…[t]here are other aspects, which are linked in respect to international terrorism which should be taken into account. The existence of mercenaries and dangerous material that is very sophisticated…as well as the possibilities that new technologies offer to obtain information about material that could be involved in international terrorism adds another factor to the terrorism phenomenon.

Interior Terrorism is that which is born inside a state and is conducted against a specific state…This terrorism can maintain international links of support between groups, use training camps or take refuge in sanctuaries’[[75]](#footnote-75) (*Revisión Estratégica de Defensa*, 2003: 127).

This definition of terrorism provided by the Spanish Government also emphasises its dual terrorism problem with both national and international terrorism (Celso, 2006). Philip Bobbitt argued that the Spanish security services were focused on countering the threat posed by ETA and disregarded the threat posed by international terrorist organisations before 2004 (Bobbitt, 2008). However, the above definition is more closely aligned with the assertion from the scholar Anthony Celso who claimed that Spain currently faces a dual security threat that relies on the availability of high technology (Celso, 2006).

One encounters similar definitional problems when attempting to arrive at a universally agreed upon explanation for the nature of crime or criminal actions, as they comprise a wealth of actions and interpretations. The difficulty of this endeavour is compounded by the assertion of crime experts, particularly criminologists, who claim that the definition of crime is not given by scientists but has rather been subsumed by governments, ‘[t]he state, not the scientist, determines the nature or the definition of crime’ (Gottfredson & Hirsch, 1990: 3). Therefore, for the purpose of this thesis, crime will be defined along the lines of the politico-criminal definition as provided by the Spanish Government and from the theory of crime causation as: ‘illicit or anti-juridical acts that threaten public order, territory or the state’ (Witker, date unknown: 3).

## Cybercrime in Spain

Cybercrime, which broadly describes the conflation of criminal activities and the internet, is an extensive problem in Europe and, in particular, Spain. The European Commission, in outlining the case for interstate cooperation on cybercrime legislation, declared that cybercrime has grown into a significant Europe-wide issue and is in a ‘permanent [state of] evolution, and legislation and operational law enforcement have obvious difficulties in keeping pace’ (Europa, 2007: 1). Indeed, as outlined briefly above, Bobbitt underscored the assertion made by the European Commission when he argued that internet and Web technologies enable criminal and terrorist organisations to conduct their activities utilising techniques such as phishing, identity theft and the creation of malicious software:

‘The internet has become an important tool for perpetuating terrorist groups, both openly and clandestinely. Many of them employ elaborate list serves, collect money from witting or unwitting donors, and distribute savvy political messages to a broad audience online...Clandestine methods include passing encrypted messages, embedding invisible graphic codes using steganography, employing the internet to send death threats and hiring hackers to collect intelligence such as the names and addresses of law enforcement officers from online databases…For example, higher casualties are brought about by simultaneous attacks, a diffusion in terrorist locations is made possible by internet communications, and extremist religious ideologies are spread through websites and videotapes accessible throughout the world’ (Bobbitt, 2008: 56).

Bobbitt’s argument above, that the increase in global flows, particularly the burgeoning use of internet and Web technologies, has been employed by terrorist organisations as a means of generating an increase in funds, is one that has been applied to terrorist organisations operating in Spain (Framis, 2007, Buesa, 2011, Wiemann, 2007). One of the principal means by which this has been achieved is through the use of internet and Web technologies for criminal purposes. The European Commission, in its Convention on Cybercrime (2001), defined cybercrime as a term that encompasses a range of nefarious computer-based activities:

‘[T]he term cyber crime is applied to three categories of criminal activities. The first covers traditional forms of crime such as fraud or forgery, though in a cyber crime [sic] context relates specifically to crimes committed over electronic communication networks and information systems (hereafter: electronic networks). The second concerns the publication of illegal content over electronic media (i.e. child sexual abuse material or incitement to racial hatred). The third includes crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking’ (Europa, 2007: 1).

The complexity of the term cybercrime is indelibly apparent in the definition offered by the European Commission. For example, identity theft, the first category of cybercrime, is a complex issue that has many nuances: ‘Most people associate identity theft with money because most reported cases involve criminals using the identity for activities such as obtaining credit cards, applying for loans, obtaining expensive medical or pharmaceutical treatments, or even stealing house titles. However, financial identity theft is only one of the many types of identity theft that exists. The Identity Theft Resource Center (ITRC) categorises identity theft into five major types: financial (the identity is used to obtain goods and services); criminal (the identity is used during a criminal investigation or arrest); commercial (the identity of a business is used to obtain credit); governmental (the identity is used to obtain government-issued documents such as a passport or driver’s license); and cloning (the identity is assumed by another and used on a daily basis)’ (Fossi et al. 2008: 24). The evidence for Fossi’s claim comes from the internet security corporation Symantec’s analysis of the goods and services offered for sale online by organisations conducting cybercrime. In addition, he references data stemming from the Identity Theft Resource Center’s 2007 annual report, which conducts qualitative and quantitative analysis of consumer experiences of identity theft. The quote above outlines the inherent complexity involved in defining identity theft and the differences in approach by both the public and private sectors. Such ontological difficulties make more difficult the challenge of opposing terrorism and cybercrime in Spain.

As mentioned previously, Spain currently experiences a significant cybercrime problem that is largely controlled by prominent organised crime groups (International Intellectual Property Alliance, 2010). Piracy and file-sharing of copyrighted material present a significant challenge with large, highly organised groups including the visible *mochileros* and *manteros[[76]](#footnote-76)* selling copyrighted DVDs and CDs, for example. This problem is compounded by permissive legislation which effectively permits users to download content that is copyrighted free of charge without fear of legal punishment. According to the International Intellectual Property Association:

‘Spain is among the worst-performing markets in the world, and has suffered greatly from an online piracy problem that is spiraling out of control. Contributing to Spain’s high piracy levels are the government’s policies that decriminalize illegal downloading of content distributed via peer-to-peer (P2P) file-sharing (as reflected in the 2006 Circular issued by the Attorney General), and its failure to meet the minimum EU-level requirements regarding liability for Internet service providers (ISPs) under the E-Commerce Directive. As a result of the legal uncertainties, the police refuse to take Internet enforcement actions, and the Attorney General’s circular instruction dismissal of current criminal cases against illegal portal and link sites remains in force’ (International Intellectual Property Alliance, 2010: 1).

Spain’s increase in incidents of cybercrime as outlined above were addressed in February 2011 as the Spanish Government approved the launch of the Sustainable Economy Law (*Ley de Economía Sostenible* or *Ley Sinde*) which focused on implementing a national set of changes that are designed to re-energise the economy, create employment and transform the national mode of production (La Moncloa, 2011). With respect to internet governance in Spain, the wide-ranging law proposed to outlaw illegal downloads of copyrighted material through peer-to-peer websites, something that was openly permitted in the past (Slashdot, 2010). The Government declared that it would close any Spain-based site that was suspected of providing illegal access to copyrighted material as a means of making the economy more productive and competitive (Navarro, 2011, *Ley de Economía Sostenible*, 2011). However, the sharp shift in focus by the Government has been met with widespread popular protests against the new law with some online users and communities claiming that the law does much to limit net neutrality and limit freedom of expression (*No al Cierre de Webs*, 2011).

While terrorists’ use of criminal techniques is one of the ways in which such organisations have been described as using the online space to further the aims of their agenda (Bobbitt, 2008, Barnett, 2005), much has also been written on the potential for real-world terrorist acts being committed using the internet or the Web as a tool (Denning, 2003, Pollitt, 2007, Nelson, et al., 1999). The internet and terrorism scholar Dorothy Denning defined cyberterrorism as:

‘[T]he convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not’ (Denning, 2000: 1).

While scholars and practitioners (Salellas, 2005, Post, Ruby & Shaw, 2000, Zunzunegui, 2008) have also written about the phenomenon of cyberterrorism as it relates to Spain, it should be remembered that cyberterrorism, as defined above, has never been witnessed as part of a terrorist attack. Terrorist organisations have not, until now, used the internet and the Web to directly attack physical objects, leading industry experts to declare that cybercrime is conceptually fantastical (while it can be argued that the 9/11 and 11-M attackers used web-based email to coordinate their attacks, internet and Web technologies have not been used to directly perpetrate violent acts). Indeed, the internet security expert Luciano Salellas makes the point that the networks of many high-value targets are not even on the internet: ‘Nuclear installations and their communications strategies are not available on the internet; less than one percent of hackers have the requisite knowledge to cause widespread damage’ (Salellas, 2005: 12).[[77]](#footnote-77)

While cyberterrorism as defined above has, therefore, never openly been committed by terrorist organisations, some nation states have deemed it appropriate to extend the parameters of the term to encapsulate more facets such as the conduct of behaviour that actively supports the objectives of terrorist organisations. This widening of the definition therefore could include all digital activity carried out by terrorist organisations in the furtherance of their cause, and cyberterrorism, therefore, becomes an eminently more prevalent online phenomenon. Bobbitt alluded to this new conception of cyberterrorism when he argued that:

‘As well as propaganda and ideological material, jihadist sites seem to be heavily used for practical training…since the loss of the Afghan training camps. Sites like Al Battar contain hugely detailed information on how to [conduct kidnappings and] surveillance [and how to fire] rocket propelled grenades. Careful instructions were…posted on one jihadist website on how to use mobile phones as detonators for explosives, as was [done] in Madrid’ (Bobbitt, 2008: 56).

Based on Bobbitt’s above assertion, it could be construed that the possession of a Web presence by a terrorist organisation, or Web content that supports or enshrines the objectives of a terrorist organisation is a form of cyberterrorism. Indeed, this very interpretation of terrorism is enshrined in current counter-terrorism legislation, such as that of the United Kingdom:

*‘All terrorist groups have an ideology. Promoting that ideology, often through the Internet, facilitates radicalisation and recruitment. Challenging ideology and disrupting the ability of terrorists to promote it is a fundamental part of Prevent…Challenge may mean simply debate about extremist ideas which form a part of terrorist narrative. But where propagandists break the law in encouraging or approving terrorism it must also mean arrest and law enforcement action. And where people seek to enter this country from overseas to engage in activity in support of extremist and terrorist groups we will also use the Home Secretary’s power to exclude them’* (UK Home Office, 2011, emphasis in original).

The legislation from the UK Government above highlights that terrorism and the internet is a far more complex and widespread phenomenon than simply committing attacks using internet and Web technologies as tools. Such a conception underscores adherence to the social constructivist understanding of technological development and approach to counter-terrorism. The Spanish Government, however, has not undertaken such measures to incorporate such a definition into law as part of its counter-terrorism strategy. The reason for this might reside in the fact that the national security services already monitor a wide range of internet activity related to terrorist activity (Jordán, 2005), in much the same way as does the UK and France (Garapon, 2005). It can be perceived, if we take Bobbitt’s argument as our starting point, that ETA undertakes cyberterrorist activities as it possesses a strong web presence that details its principal arguments, images and video (ETA Website, 2011). In addition, al-Qaeda has an extensive Web presence that hosts content related to Spain. Al-Qaeda in the Maghreb (AQIM) generates a variety of content relating to Spain and according to the prior definition of cyberterrorism, could be conceived as engaging in this action (Filiu, 2009).

Indeed, there is evidence to assert that the al-Qaeda-inspired perpetrators of the 11 March bombings in Madrid used a range of information and communications technologies to carry out their attacks. Web-based electronic mail was used by the attackers to coordinate and synchronise the attacks, as well as mobile phones. Given the above extension of the definition of cyberterrorism, the al-Qaeda cell did indeed engage in cyberterrorism for the purposes of communication, information gathering and reconnaissance. Justin Webster supported this assertion in his analysis of the role played by technology in the perpetration of the 11 March 2004 terrorist attacks in Madrid:

“There are many more stories along the timeline which demonstrate just how important the internet was. One early one would be Sahan al Touibithan [who]…as he kept changing groups, and steadily getting into more radical and extremist groups, well, he started off as not very extremist and then ended up being very extremist, but the one point is that he started hanging out with people in the mosques, with more and more closed Muslim groups, and he would take them to use the internet in the university and that was one of the best things he had access to, was to be able to go into an office as a PhD student, sit down at a computer and surf the net and he used to come in the afternoons when the PhD common room was empty, he’d bring his friends there to surf the internet. This was in 1998 when Al-Qaeda made a declaration of war against the United States and the declaration of the Crusade. It was also the year of the bombings in Kenya and Tanzania.”[[78]](#footnote-78)

Although Webster’s analysis demonstrates the importance of such technologies in the perpetration of the Madrid 2004 terrorist attacks, it is difficult to ascertain whether terrorist organisations have used internet and communications technologies to cause damage in the physical world. One reason for this is that cyber attacks against physical objects are normally carried out anonymously in order to protect the identities of the attacker(s) until such time that the organisation chooses to lay claim to a particular attack. This means that attacks to the electrical systems of certain organisations, for the most part, are indistinguishable from everyday malfunctions.[[79]](#footnote-79) The similarity of potential cyberterrorist attacks with general technical malfunction only serves to dilute the terrorists’ main narrative that an act of terror will be perpetrated in order to achieve a specific political goal. In addition, it detracts from the claim by Brian Jenkins which argued that modern terrorism is like theatre (Jenkins, 1974).

This postulation, that the internet is an unsatisfactory tool for real-world attacks, was underscored by the VeriSign cybersecurity analyst Stewart Bertram who argued that the internet and the Web are nothing more than a communications node:

“[Y]es you could [commit terrorist attacks] over IP but why bother?...it is just a communications node it’s not actually an attack vector…Terrorism on the web is all about people watching and even with Al Qaeda, even though they want lots of people dead, they still want a lot of people watching. So terrorists are not artists, they’re not looking for the most technically convoluted way to do it. They’re just looking for something effective and asymmetric warfare is exactly that you know, improvised explosive devices made of wood and plastic, you know, fertilizer, because you can’t mitigate against that – so that’s counter-intuitive to cyberterrorism.”[[80]](#footnote-80)

Bertram’s assertion that it is nearly impossible for terrorists to inflict real-world damage using the internet, and is generally used more for pre and post attack uses such as communication, finance, recruitment and information gathering, is also highlighted by Gabriel Weimann at the University of Haifa (2008) as support for the notion that contemporary terrorism is a socio-technological endeavour – a complex entanglement of human social relation technologies - rather than a technologically-determined one.

## The Development of Cybercrime vs. Cyberterrorism in Spain

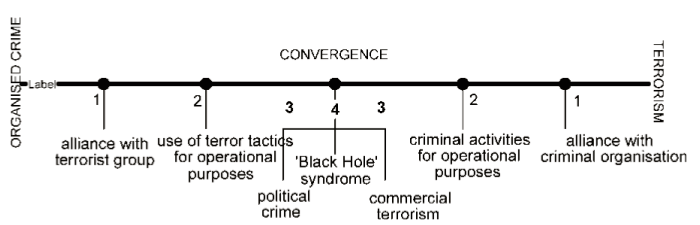
While the general stated *raison d'être* of terrorist organisations is to achieve political change, the problem of financing high-risk and expensive operations, compounded with the obvious need to ensure the continuation of the organisation at large, are ever-present concerns. The main aim of the *Euskadi Ta Askatasuna* or Basque Homeland and Freedom organisation (ETA) is for a fully independent state, separate from Spain.

During the Cold War era, terrorist organisations in Spain generated funds in a number of ways. From 1950 to 1990, ETA was adroit at carrying out such actions as extortion, kidnappings and assassinations as part of its collection of tactics designed to terrorise the Spanish Government and its people into accepting an independent Basque state (Buesa, 2011). With the ending of the Cold War, the onset of globalisation greatly facilitated ETA’s access to global flows of information, ideas, and capital, impacting the terrorist organisation profoundly. Ready access to high technology, the opportunity to trade and share information globally and the freedom to travel between national borders, particularly the European Union, meant that ETA could obtain other sources of funding which they had hitherto been unable to access. As a result, ETA operated heavily in areas such as the drug trade and arms trading in Spain as well as training other terrorist organisations in other parts of the world such as Colombia (Buesa, 2011, Shapiro & Suzan, 2003).

Similarly, groups related to al-Qaeda in Spain became adept at taking advantage of the opportunities afforded by globalisation to generate further funds. For example, the organisation became involved in the cannabis trade that operated in Ceuta, Melilla and other southern Spanish regions (Úbeda-Portugués, 2010).

It has been argued that, since the 1990s, terrorist organisations have engaged in activities that were normally the reserve of organised crime syndicates as a source of revenue. Tamara Makarenko contended that the 1990s saw the development of a crime-terror nexus in which there was a proclivity for terrorist organisations to engage in activities that were normally the reserve of organised crime syndicates and vice versa. Makarenko outlined this argument in a crime-terror continuum model, which depicted the relationships that exist between contemporary terrorist organisations and organised crime syndicates.

Figure Twenty-One: Crime – Terror Nexus Model



Source: Tamara Makarenko, 2004

Makarenko claimed that the relationships between the two organisations, as presented in Figure Twenty-One above, could be depicted along the same plane, on which organised crime is at one end and terrorist organisations are at the other. Using statistical evidence on rates of terrorism and incidents of crime from governments, in addition to media content and reviews of scholarly literature, Makarenko outlined that a point exists on the crime-terror continuum in which the two entities converge, or individual organisations adopt the characteristics of both elements i.e. the ‘Black Hole syndrome’ (Makarenko, 2004). Hence, she argued:

‘[T]he 1990s can be described as the decade in which the crime–terror nexus was consolidated [in a similar way to commensuration]: the rise of transnational organised crime and the changing nature of terrorism mean that two traditionally separate phenomena have begun to reveal many operational and organisational similarities. Indeed, criminal and terrorist groups appear to be learning from one another, and adapting to each other’s successes and failures, meaning that it is necessary to acknowledge, and to understand the crime–terror continuum to formulate effective state responses to these evolving, and periodically converging, threats’ (Makarenko, 2004: 42).

The argument that terrorist organisations and organised crime syndicates operate in a similar fashion and, indeed learn from each other, is indicative of an apparent shift in strategic thinking from terrorist organisations; that economic power has become a more powerful lever of political change than violence. The onset of globalisation had an effect on terrorist organisations operating in Spain as it allowed them to use international markets to attract greater levels of finance.

Philip Bobbitt posited this assertion again in *Terror and Consent: Wars for the 21st Century* in which he claimed that market state terrorists are much better funded than nation state terrorists. This is because they can rely ‘on a wider variety of sources for funding...terrorist organisations are broadening their reach in gathering financial resources to fund their operations…Websites are also important vehicles for raising funds’ (Bobbitt, 2008: 49).

Makarenko added to Bobbitt’s argument that globalisation had significantly altered the dynamic of the traditional terrorist organisation, making them much more of a threat to governments:

‘Growing reliance on cross-border criminal activities—facilitated by open borders, weak states, immigration flows, financial technology, and a highly intricate and accessible global transportation infrastructure—and an associated interest in establishing political control in order to consolidate and secure future operations, have all contributed to the rise of the crime–terror nexus…The realisation that economic and political power enhance one another, suggests that more and more groups will become hybrid organisations by nature. This is enhanced by the fact that criminal and terrorist groups appear to be learning from one another, and adapting to each other’s successes and failures’ (Makarenko, 2004: 141).

Following on from Makarenko’s argument above, Xavier Raufer was more synoptic in his appraisal of the globalisation, crime and terrorism nexus, claiming that ‘[g]rabbing control of financial institutions can both bring home the cash and advance political ambitions. Many groups, of course, will retain narrow portfolios of objectives, targets, and methods; others are becoming conglomerates of causes’ (Makarenko, 2004: 134).

As the widespread adoption of increasingly sophisticated internet and Web technologies were adopted into the strategic operations of terrorist organisations, it became increasingly apparent that cybercrime emerged as an excellent method of generating funds (Palicio, 2010). Spain, as has been outlined, has become a “breeding ground” for cybercrime and, as a result, terrorist organisations and organised crime syndicates have flourished[[81]](#footnote-81). This chapter will now analyse the range of understandings that existed in online discussion concerning cybercrime, technology, terrorism and counter-terrorism related to the 11 March 2004 attacks, in order to provide a greater degree of richness to the conclusions from the semi-structured interviews conducted on the topic; it will now explore whether citizens, journalists and others understood the two as one nexus.

## Internet Research on the 11-M Attacks: Key Findings Related to the Topic of Cybercrime and Terrorism (2004-2010)

As previously described in Chapter Three, the author developed a methodological process to analyse online discussion related to the Madrid terrorist attacks of 2004 to support the primary research of semi-structured interviews conducted previously. The date range of the analysis was six months from 11 March to 11 August each year over a period of seven years (2004 to 2010). In this chapter, the internet research focuses on the 11 March 2004 terrorist attacks and the prevalence of online discussion related to cybercrime, technology, terrorism and counter-terrorism.

The internet research concluded that very few discussions were generated in relation to cybercrime. Out of 879 items of content analysed, only four made specific reference to the topic.

One post came from the blog *Periodistas 21,* in which the author outlined that the people accused of perpetrating the attack were in possession of a video that was uploaded onto the internet by al-Qaeda and included a confession by Osama bin Laden detailing his culpability for the attacks. However, the majority of the post focused on the way in which SMS and other internet technologies were used to protest against the Government’s handling of the event and how this had subsequently resulted in the change of government:

‘The youth and groups that were loosely organised have utilised technology to communicate, arrange meetups and mobilise citizens. A loop of SMS and emails has been the medium and nucleus of the mobilisation’ (*Periodistas 21*, 2004).[[82]](#footnote-82)

Such a comment alludes to the perception of internet and Web technologies as tools or force multipliers in the activities of online users and communities involved in discussions of terrorism and counter-terrorism. This was underscored in a post to the newsgroup *es.charla.politica.misc,* which outlined how al-Qaeda terrorists who attacked the London transport system in 2005 used information found on Jihadist websites that they used to construct their bombs. The user continued that the Web was used because terrorists do not want to expose themselves to risks unnecessarily and jeopardise the mission[[83]](#footnote-83) (*es.charla.politica.misc*, 2005).

It is possible to deduce, however, that discussion concerning cybercrime, technology, terrorism and counter-terrorism in Spain is conspicuous by its absence. It appears that online users do not immediately commensurate the issues of cybercrime with terrorism and counter-terrorism. If such a link appears in online discussion, it is related to a wider discussion of the Government’s response to terrorism or conceptual discussions of terrorism as a political phenomenon. Such discussion, therefore, manifests itself in the notion that the internet and the Web are tools that enable terrorist organisations to publicise propaganda or for information retrieval concerning their mission. This technologically deterministic argument follows the theoretical framework outlined by Bobbitt in the beginning of the article that these technologies would act as a force multiplier for market state terrorists.

In spite of the numerous academic studies, media and government reports outlining evidence that cybercrime was involved at some stage of the Madrid bombings, it has barely been discussed amongst online users. This lack of discussion suggests that general online users demonstrate a lack of knowledge when it comes to understandings of cybercrime, technology, terrorism and counter-terrorism and that these understandings appear to reside only within epistemic communities, practitioners and industry experts.

## Conclusion

An examination of the intricacy inherent in understandings of cybercrime, terrorism, counter-terrorism and technology has shown that complexity, confusion and imprecision pervade understandings of these independent variables as one collective issue or nexus.

Historically, the Cold War encouraged terrorist organisations to resort to traditional forms of financial extortion such as kidnapping, political assassinations and drug trafficking. There is evidence that the onset of globalisation in the 1990s, however, had a profound effect on terrorist organisations, encouraging them to take advantage of globalising processes and gather vast sums of money for their operations. As terrorist organisations began to direct their attention towards economic influence, they became involved in activities, which had traditionally been the preserve of organised crime organisations.

The increasing proliferation of information and communications technologies provided terrorist organisations with the means to utilise cybercrime to earn yet more revenue. Phishing, credit card fraud and copyright piracy created a *de facto* Underground Economy (Fossi et al., 2008) and provided terrorist organisations with significant increases in funds.

The shift in focus by terrorist organisations to cybercrime techniques and tools demonstrates the extent to which communications technologies have afforded them the opportunity to gain a greater degree of influence to fulfil their stated communication aims and objectives. Internet and Web technologies have been highlighted as a potential enabler for terrorists to carry out their operations, which will increase their influence and resources if the situation is not dealt with effectively by national governments, supranational organisations and corporations. As has been discussed, legislation is still a long way behind the potential methods used by terrorist organisations to use these tools. As a result, the ability for the security services to counter the threat as effectively as they ought is being curtailed. This notion was outlined by a member of the UK security service who claimed that the UK Government is able to analyse in detail information about a small group of people, but not what the general public is saying online. The future of counter-terrorism intelligence will be in open source intelligence and finding out what people are saying online.[[84]](#footnote-84)

Certainly, the Spanish Government could do more from an organisational and legislative perspective if the terrorist threat is to be effectively countered (Fragoso, 2010), which will be outlined in more detail in Chapter Eight.

In addition, the onset of more sophisticated internet and Web technologies such as Web 3.0 will augment the challenges currently faced by the security services. The fact that a significantly higher number of people will be connected to the internet and the Web, coupled with their ability to create, consume and publish their own content means that terrorist organisations will have a greater opportunity to attain their strategic communication objectives. This could be achieved by terrorist organisations creating compelling narratives that engage with individual users, as witnessed previously in Chapter Five, and communities as will be outlined in greater detail in Chapter Seven.

However, the introduction of such technology also presents the security services with a significant opportunity to learn the underlying nature of online behaviour. The onset of Web 3.0 will mean, above all, an exponential increase in the amount of data available concerning all facets of online behaviour. There exists an opportunity for Government organisations to conduct research to develop their understandings of this phenomenon and designing strategies that exploit this evolving space. This type of action would help government organisations to remain ahead of terrorist organisations in generating understandings of the nature of power and influence in this space and their ability to convey core strategic narratives to the right people at the right time.

It follows that if Government organisations are able to understand the nature of online influence and power then they will also be able to incorporate more sophisticated strategies into their counter-terrorism programmes. It will also be able to support the efficacy of the notion, as proposed by Giles Tremlett and the scholar Jonathan Githens-Mazer, that terrorist organisations are more concerned with the potential ability of government actors, when in reality their capabilities are not as far-reaching. This notion lends weight to the credence that influence and power in the digital age are more concerned with the influence of attitudes and behaviours, complimenting the use of the more traditional hijackings, bombings and assassinations.

The subtle changes in the nature of influence in relation to terrorism highlight the theoretical and jurisprudential cleavage in understandings of this phenomenon, suggesting that more scholarship on this topic is needed. However, it also highlights that, in the case of terrorism in the digital age, the creation and maintenance of myths or narratives may be the source of real influence as was investigated in Chapter Five and will be explored in Chapter Seven.

# **Chapter Seven: Community Engagement, Technology, Terrorism and Counter-Terrorism in Spain**

## Introduction

Increasingly, the creation and maintenance of myths, particularly with the proliferation of new internet and Web technologies is becoming a key counter-terrorism strategy in Spain. A thorough understanding of the nature of online and real-world communities can provide counter-terrorism organisations with a strategic advantage.

The complexity and importance of the delivery of core narratives from a range of actors and their positive interpretation by target audiences was analysed and discussed in Chapter Five. It was concluded that, while target audiences are exposed to narratives from a range of sources in a multi-directional fashion, the effective delivery of core narratives is of utmost importance to actors involved in the nexus of technology, terrorism and counter-terrorism.

This chapter focuses on analysing understandings that exist of the relationship between technology, terrorism and counter-terrorism from the perspective of online and real-world communities. In particular, it will examine whether online groups are generally influenced by discussions from very active communities and the extent to which they take information as writ from influential organisations such as the Government and other prominent counter-terrorism organisations. It will also analyse the extent to which online communities in general attempt to gather and assert influence online by informed amateurs who are adroit in the use of media technologies for communication. These groups of informed amateurs, who influence discussion online, have been termed the “new intellectuals” *(*Fisher, 2003*)*, and it is predicted that these audiences will have greater sway in the influence of attitudes and behaviours online.

The issues of better integrating Islamic minority communities into Western societies, eradicating radicalisation and engaging local communities have been at the forefront of global counter-terrorism discourse and policy planning since the attacks in the US on 11 September 2001 by al-Qaeda. The terrorist attacks on the Madrid and London transport systems in March 2004 and July 2005, respectively, did much to shift the focus of Spain’s counter-terrorism and national defence strategy to emphasise less the historic domestic terrorism threat from ETA, and direct more resources towards the threat posed by international terrorism (Sageman, 2008).

As evinced in Chapter Four, in order to counter the threat of home-grown and international terrorism, the Spanish Government focused significant resources on positive engagement with the immigrant Muslim community as the principal means of averting future attacks after the Madrid terrorist attacks on 11 March 2004. Maintaining open and constructive dialogue and cooperation with local immigrant communities to prevent radicalisation, and future attacks, is an essential element of Spain’s counter-terrorism strategy.

For this reason, the Spanish Government has implemented a wide range of real-world policies that encourage dialogue and cooperation with its immigrant Muslim population in the hope it can ‘deny terror groups an environment in which to recruit more members’ (Celso, 2006: 136). However, it is important to note at this juncture that although Spain’s counter-terrorism strategy has focused on communities in the real world, it has not, to date, highlighted the importance of engagement with online communities.

The scholars Thomas Barnett and Philip Bobbitt supported the notion of the importance of engagement and attaining knowledge of communities in order to mitigate any risks against international terrorism, especially in the age of globalisation. The relevance of the theoretical frameworks within their theses are discussed in detail in Chapter Two. Barnett outlined the importance of allowing flows of migrants to move freely as it is an important step in integrating countries residing in the non-Integrating Gap into the Functioning Core (Barnett, 2005). Philip Bobbitt, in turn, argued that it is important to engage with other communities, because in the age of internet and Web technologies, greater numbers of people from communities all over the world would become vulnerable to radicalising discourse. He argued:

‘[B]y “moving from the physical sanctuaries of the 1990s to virtual sanctuaries on the internet, the terrorists reduce[d] their risk. No longer does recruiting occur only in the physical locations like mosques and jails. Instead, alienated individuals in isolated national niches can make contact with a new imagined community of fellow believers around the world”’ (Bobbitt, 2008: 58).

As analysed in Chapter One, the internet and the Web can be conceived as socio-technical spaces where social and cultural artefacts are created (Markham, 2008) and communities of people exert significant influence on the development of the technologies as well as on each other. In this context, online communities are influential entities, able to sway events both online and in the real world. Examples of this are seen in the organisation of the largest anti-terrorist demonstrations in the world against the Revolutionary Armed Forces of Colombia (Fuerzas Armadas Revolucionarias de Colombia (FARC)) in February 2008 as a Colombian engineer, Oscar Morales, organised more than 12 million people in 190 countries to demonstrate against the organisation using social networking sites such as Facebook (where he created a page entitled *Un Millón de Voces Contra Las FARC*). The effect of these demonstrations was seen in the fact that FARC ‘saw more demobilizations and desertions than it had during a decade of military action’ (Ross, 2010: 3). In addition, the influence of communities was seen in the violence that occurred as a result of the disputed Kenyan Presidential Elections in 2007 as bloggers and general online users posted information on the violence that the Kenyan Government was reluctant to publish. The event gave rise to the prominent crisis-mapping website, Ushahidi, which allowed individual people to form real-time communities by posting information about an event or topic and be able to witness the collective effect of such information production in real-time (Meier, 2009).

The development and eventual propagation of Web 3.0 technologies will ensure that people will be constantly connected to the Web. Online users will be able to connect to other like-minded people and form communities for any number of issues from wherever they happen to be, not just from a desktop computer. In addition, online communities will be able to gain access to data, thereby making an increasing number of elements that comprise society to be more transparent, open and accessible. This will help online users access new services to make more informed decisions about where they place their attention and, in particular, it will increase the opportunity for certain organisations and influential persons to affect the attitudes and behaviours of other users (Bell & Dourish, 2009).

This vision of Web 3.0 and in particular the real-time Web, Semantic Web, ambient computing and big data, predicts that the physical and online worlds will combine until the possibility emerges that in order to fully understand behaviour, and by implication obtain a strategic advantage, in one realm, it will be essential to understand the other.

Web 3.0 will lead to further opportunities for terrorist organisations to achieve their strategic objectives, as outlined in Chapter Six. The openness of information flows will lead to the development of new knowledge, as well as innovative ways of disseminating knowledge, information and narratives that terrorist organisations could capitalise upon. This is problematic for governments as terrorist organisations are finding that a wide range of communities can assimilate their narratives from multiple sources, particularly those who find the need to express their grievances online, as witnessed in Chapter Five.

The need to achieve a thorough understanding of influence as part of an effective counter-terrorism strategy is reflected in a study by the Spanish terrorism scholar Fernando Reinares. He constructed a sociological profile of a typical Jihadi terrorist by interviewing 188 men incarcerated in a Spanish prison. From this he deduced that incidents of international terrorism in Spain could be avoided if the Government constructed more compelling messages for its citizens and set about constructing stronger relationships with both the Spanish and immigrant communities. This type of strategy, he contended, would have a strong chance of success as al-Qaeda itself is an ideological entity whose ideas and strategies are used by both well-organised and well-financed North African terror organisations, or by disaffected, isolated people in Spain. Al-Qaeda’s influence is all the more powerful as a result of its prominent digital profile (Wilton Park, 2011). Reinares’s case study above supports the assertion from the Judge responsible for prosecuting those responsible for the 11 March attacks, Juan del Olmo, that the Madrid bombers were influenced by online content from al-Qaeda (Sageman, 2005, 2008). More, therefore, needs to be done to attain influence online by the Government to effectively counter the narratives filtering down to Muslims online (Reinares, 2006). By extension, such understanding of online behaviour could also lead to an enhanced understanding of the Spanish population in general to better serve it.

## Engagement with Local Communities in Spain

In order to understand the motivation for the Spanish Government’s attempts to engage with local communities as part of its counter-terrorism strategy after 11-M, it is first necessary to provide a contextual background of the rise to prominence of international terrorism for Spanish policymakers. While a more in-depth discussion of the development of terrorism in Spain is outlined in Chapter Two, it is felt that this section will provide a framework of understanding for the eventual insights that are derived in this chapter.

The terrorist attacks perpetrated against the US on 11 September 2001 had global ramifications. National security strategies and political acts (e.g. PATRIOT Act 2004, Présidence de la République 2008) were established by a range of states with the mandate of protecting their publics against a new type of adversary in the form of ‘violent extremists claiming to act in the name of Islam…the threat is greater in scale and ambition than terrorist threats [faced] in the past’ (UK Cabinet Office, 2008: 1). National governments immediately and emphatically fixated the focus of their counter-terrorism strategies on the roles played by immigrant religious and cultural communities, especially Muslim communities. The principal motivation for the focus on the link between Muslim communities and terrorism came from public announcements of culpability by the former leader of al-Qaeda, Osama bin Laden, for the 2001 US terrorist attacks and threats of further violent actions. Commenting in 2004 on his role in the terrorist attacks on the US, Bin Laden stated:

‘God knows it did not cross our minds to attack the towers but after the situation became unbearable and we witnessed the injustice and tyranny of the American-Israeli alliance against our people in Palestine and Lebanon, I thought about it…Your security is not in the hands of [Democratic presidential candidate John] Kerry or Bush or al-Qaida. Your security is in your own hands and each state which does not harm our security will remain safe’ (*The Guardian*, 2004: 1).

In this statement, Bin Laden highlighted that US-led military involvement in the Middle East was the overriding reason for acts of terrorism committed by al-Qaeda. It is for this reason that Bin Laden declared *fatwa*s against the US and its allies in which he emphasised that defending the Islamic religion was the motivating force for the use of terrorist acts for the al-Qaeda organisation. In 1996, Bin Laden declared:

*‘The people of Islam have suffered from aggression, iniquity and injustice imposed by the Zionist-Crusader alliance and their collaborators . . .It is the duty now on every tribe in the Arabian peninsula to fight jihad and cleanse the land from these Crusader occupiers. Their wealth is booty to those who kill them. My Muslim brothers: your brothers in Palestine and in the land of the two Holy Places* [Saudi Arabia] *are calling upon your help and asking you to take part in fighting against the enemy – the Americans and the Israelis. They are asking you to do whatever you can to expel the enemies out of the sanctities of Islam’* (National Archives, 2003: 1, emphasis in original).

In 1998, he had similarly announced:

*‘the killing of Americans and their civilian and military allies is a religious duty for each and every Muslim to be carried out in whichever country they are until Al Aqsa mosque has been liberated from their grasp and until their armies have left Muslim lands…We – with God’s help – call on every Muslim who believes in God and wishes to be rewarded to comply with God’s order to kill Americans and plunder their money whenever and wherever they find it. We also call on Muslims…to launch the raid on Satan’s US troops and the devil’s supporters allying with them, and to displace those who are behind them’* (National Archives, 2003: 1, emphasis in original).

The 11 September 2001 attacks represented a significant shift in the perceived threats faced by the US and its allies, including Spain. Terrorist acts had been committed by foreign persons within Western borders in the name of Islam, forcing governments and supranational agencies alike to significantly alter their counter-terrorism strategies to mitigate the threat. Osama bin Laden’s comments above indicated his belief that the US and its allies had illegally occupied what he considered to be Muslim territory, and that violence perpetrated against the US, its allies and interests by all Muslims was, as a result, permissible. His declaration of culpability following the 11 September attacks on the US, in addition to in-depth investigations by global intelligence services (*Revisión Estratégica de Defensa*, 2003), led governments to the conclusion that loosely connected terrorist groups, committed to enacting political violence in the name of Islam, constituted their principal terrorist threat.

Following the 2001 attacks, a number of countries quickly revised their counter-terrorism strategies (Présidence de la République 2008, UK Cabinet Office, 2008). The Spanish Government, however, decided to forego drafting a national security strategy that focused on the threat of international terrorism committed in the name of Islam at this time. Instead, as discussed in Chapter Two, it elected to focus the majority of its counter-terrorism resources on dismantling ETA (Bobbitt, 2008, Jordán, 2005).

From 2001 to 2003, the conservative Government led by José María Aznar succeeded in reducing the frequency of ETA attacks by severely disrupting their logistical capability and arresting high-profile ETA members. In addition, Aznar prohibited the Basque political party Batasuna from practicing mainstream Spanish politics, as it had been accused by the Government of maintaining high-level links to ETA. As the frequency of ETA attacks decreased and there appeared to be no discernible threat emanating from al-Qaeda, Aznar convincingly demonstrated that his decision to focus on Spain’s Basque terrorism situation was vindicated (Celso, 2006).

However, the threat to Spain from al-Qaeda and other North African organisations had been increasing steadily and surreptitiously since the mid-1990s. The conflation of the Algerian and Moroccan armed organisation Group for Preaching and Combat (GSPC, Groupe Salafiste pour la Prédication el le Combat) and the Armed Islamic Group (GIA) into the Al-Qaeda Organisation in the Maghreb (AQIM) in 1998 presented Spain with a significant terrorist concern. The organisation’s networks extended from North Africa into Spain and Western Europe, aided by criminal organisations, to the extent that they were fully capable of perpetrating violent attacks (Beutel 2007). Bezunartea et al. (2009) argued, that in addition to pronouncements from AQIM that Spain is a target for violent attacks, the real reason for the organisation’s presence in the country is for use as a logistics hub; ‘fundraising and the recruitment of persons willing to fight in Iraq and Afghanistan. Their operations revolve around phone centres but they have no roots or relationships with the religious communities’ (Bezunartea et al., 2009: 19).

In spite of AQIM’s growing presence in Spain from the mid-1990s, the Spanish Government focused the vast majority of its counter-terrorist resources on ETA (Bobbitt, 2008). However, the terrorist attacks on 11 March 2004 in Madrid indelibly changed the focus of national security in Spain. 11-M indicated a new type of al-Qaeda attack in which operations were not only carried out by direct members of the organisation, but also outsourced to loosely connected individuals and groups inspired by the ideologies purported by the group. At this point, Spain recognised that al-Qaeda was more than a traditional terrorist organisation with a classical hierarchical structure. It had, in fact evolved into a far more dangerous organisation; ‘a hardcore network of co-opted groups and an ideology’ (Burke, 2004: 25), capable of affecting people from the mountains of Peshawar to the digital portals of online discussion forums and video-sharing sites (Burke, 2005, Celso, 2008). The 11 March attacks led the Government to realise that the emerging terrorist threat facing Spain, and Europe at large, emanated from elements within the immigrant Muslim community and that measures had to be taken to actively engage with them (Celso, 2005, *El Mundo*, 2006, Jordán, 2003, 2009).

When the incumbent Prime Minister José Luis Rodríguez Zapatero assumed office directly after the 11 March attacks on 17 April 2004, he drafted his counter-terrorism strategy on the understanding that terrorism was borne from social injustice and that the situation could be ameliorated by relieving the conditions which, in his perception, led to radicalisation and terrorism within communities (Celso, 2009).

The investigation into the 11 March attacks by the 11-M Commission (Administración de Justicia, 2004), revealed that they were perpetrated by a group of men who, according to the prominent judge, Juan del Olmo, were not part of the al-Qaeda organisation (Brótons & Espósito, 2002). Rather, they were inspired by al-Qaeda propaganda located online and had formed a group to perform the attacks in the name of al-Qaeda. The Madrid attacks, therefore, represented a “home-grown phenomenon”, in which second generation Spanish citizens of Moroccan descent had detonated bombs, killing 191 people. This was similar to the terrorist attacks committed in London on 7 July 2005 by second generation UK nationals of Muslim descent, which killed 52 people. Collectively, the 11-M and 7/7 attacks collectively compelled Zapatero to adopt a radically different strategy to that in place, one that focused on engagement with local and foreign communities in Spain.

Zapatero, therefore, proposed the creation of a counter-terrorism strategy that provided incentives to members of Spain’s Muslim community to engage more in Spanish society. As discussed in Chapter Two, this approach led the Government to implement a wide range of counter-terrorism programmes and policies to better engage with Muslim communities. One of these measures was a bilateral agreement with Morocco to help counter illegal immigration to Spain (*BBC News*, 2005).

The Government also launched, in close cooperation with the United Nations and the Turkish Prime Minister, Recep Tayyip Erdogan, the Alianza de Civilizaciones (Alliance of Civilisations). This initiative was created to foster global understanding and cooperation through an online portal and offline events. Zapatero, who introduced this idea through the United Nations, believed that the threat of radicalisation could be significantly assuaged through the use of online tools to engage young people around the world.

Intelligence from the security services also gave weight to Zapatero’s belief that the environments that foster radicalisation and sympathy for terrorism, such as poverty and lack of access to education, needed to be eliminated for the successful integration of the Muslim community (Celso, 2009). Following the 11 March 2004 attacks, the Spanish security services investigated the Jihadist terrorist groups operating in the country and reported that the terror infrastructure relied on criminal organisations, community centres and groups that focus on unassimilated neighbourhoods (Celso 2006). In addition, some community centres and mosques emerged as complicit in providing the financial support for terrorist groups such as the ‘Algerian Armed Islamic Group, Abu Hafs al Masri Brigade, and the Moroccan Salfist Group for Preaching and Combat’ (Celso, 2006: 125). This evidence supported the importance of the Government’s focus on community engagement.

The strong linkage of Islam and the Muslim community to international and 21st century “home-grown terrorism” in Spain was based on comments from Osama bin Laden and from the revealed identities of the suicide bombers in the US and Madrid. However, in addition, terrorism scholars have sought to analyse the Muslim community and terrorism link through other perspectives, most notably the demographic of people involved in Jihadist terrorism offences in the country. As mentioned previously, Fernando Reinares conducted a small-scale study on the population of those incarcerated in Spain on suspicion of involvement in Jihadist terrorism in the hope of creating a ‘tentative sociological profile of those linked (in Spain) to cells, groups and organisations associated or aligned with al-Qaeda’ (Reinares, 2006: 1). Reinares based his study on a total sample of 188 people arrested in connection with Jihadist terrorism. He concluded, amongst other things, that 69 people involved in Jihadist terrorism (37%) were of Moroccan descent, and 66 of them were legally registered to reside in Spain (Reinares, 2006).

Spain’s experience of immigration, analysed in Chapter Four, is a relatively new phenomenon occurring mainly over the past ten years.[[85]](#footnote-85) Its effect on the country has been significant with the Spanish National Statistics Institute claiming that immigration increased GDP by 50% between 2001 and 2006. In 2009, the immigrant Muslim community in Spain numbered approximately one million, lower than the Latin American community at 2,273,324 (Bezunartea et al., 2009, Instituto Nacional de Estadística*,* 2010). According to the Spanish National Institute of Statistics in 2008, the largest immigrant community in Spain is from Morocco (676,405), with the Algerian community ranking second (55,042). Senegalese and Nigerian communities complete Africa’s largest migrant populations in Spain. In addition, immigrants from Pakistan, India and Bangladesh form a sizeable community in Spain (Bezunartea et al., 2009, Instituto Nacional de Estadística, 2010).

Concerns that discord between and amongst Spain’s communities could be a sign of the long-term potential for difficulties was evinced in concerns that, since the 11 September 2001 attacks, the Muslim community in Spain finds it difficult to fully integrate into the wider Spanish society. Elena Sánchez from the Spain-based think tank Centre d’Informació i Documentació Internacionals a Barcelona(CIDOB) claimed that certain communities have integrated well into Spanish societies, such as the Sub-Saharan African and Chinese communities, but that the Muslim community, for a wide variety of reasons, had not integrated as well as others. In his analysis of Spain’s dual security dilemma, the scholar Anthony Celso commented that while Muslim communities have been attracted to Europe because of the post-Cold War economic boom, Government concerns about integration have been on the increase, especially since 9/11. A number of new immigrants to Spain ‘have pronounced Islamic identities that have deepened as a result of their exposure to European society’. According to Celso, these profound Islamic identities form immigrants who were susceptible to the advances of Jihadist extremist communities, which had been extremely active in Europe, facilitating the development of terrorist organisations on the continent; providing ‘money, [recruitment, indoctrination, and training of] potential terrorists’ (Celso, 2004: 5).

In May 2005, the Spanish Government awarded residency status to almost 700,000 illegal immigrants. This was designed to help illegal immigrants, who could not attain legal employment or enter into the education system. Without residency status, Zapatero believed, marginalised immigrant communities were potentially at risk of becoming susceptible to radical indoctrination from some elements of their communities (Tremlett, 2005 cited in *Yale Global*, 2005).

In addition, the Government elected to negotiate a peaceful settlement with ETA in 2005, in the hope that such talks indicated to ETA that the Zapatero administration represented a true departure from the approach to counter-terrorism employed by Aznar (Selway, 2006). It was believed that bringing about the end of ETA’s violent campaign would lessen the risk to other Spanish communities of the threat of violence and also further exposure to ETA’s propaganda and rhetoric (Veres, 2004).

The approach taken by Zapatero to counter terrorism was dispelled when a breakdown in negotiations with ETA led to the organisation bombing Madrid’s Barajas Airport in December 2006, killing two people. In addition, *Operación Nova*, which incorporated the Spanish and Moroccan security services, averted major terrorist attacks on the National Court in Madrid in November 2005, and on Barcelona’s Twin Towers and underground transport system in 2008. The focus of the counter-terrorism operations on immigrants once again shifted the focus of policymakers and the general public back on Muslim communities. Hitherto seeking reconciliation and dialogue with terrorist organisations and immigrant communities alike, Zapatero added to this a more realist undercurrent. Arrests of prominent ETA members and people suspected of involvement in Jihadist terrorism increased sharply following the failed terrorist attacks.

In addition, as discussed in Chapter Two, Spain has employed a variety of public diplomacy techniques as part of its national and international counter-terrorism programmes, which are designed to engage communities and dissuade them from radicalising discourse. One of the most important initiatives for this is the Government’s commitment to interfaith dialogue through civil society. The use of interfaith dialogue is seen as a critical pillar of counter-radicalisation programmes and, by implication, counter-terrorism. This stems from the country’s experience of international Jihadi-inspired terrorism, and the Government assertion that faith diplomacy can positively engage the country’s large Muslim population away from radicalising discourse.

The use of Faith Diplomacy as part of a wider public diplomacy programme, has been supported by prominent proponents, such as Tim Livesey from the office of the Archbishop of Canterbury, as an effective medium to achieve strategic objectives (Wilton Park, 2010). The Spanish Government empowers civil society organisations to play a key role in effectively delivering on this mandate. Organisations such as the UNESCO Centre of Catalonia (Unescocat) create and deliver religious diversity programmes which seek to promote understanding and tolerance amongst the general population through inter-religious understanding.

This section has surveyed the different motivations of Spain’s counter-terrorism policies towards communities. The success of community-focused strategies is crucial if radical elements of the immigrant Muslim communities are to integrate successfully into Spanish society. The terrorism scholar Marc Sageman supported this by arguing that a deep sense of belonging needs to be cultivated in immigrant Muslim communities because if a person does not have a clear identity in relation to the society in which they live, this identity may be sought in “virtual Islam” (Sageman, 2004: 191).

Virtual Islam is the term given by Sageman to describe communities of Muslims meeting online. He writes: ‘the Internet creates a seemingly concrete bond between the individual and a virtual Muslim community. This virtual community plays the same role that “imagined communities” played in the development of the feeling of nationalism, which made people love and die for their nations as well as hate and kill for them…Because of its virtual nature, the Internet community has no earthly counterpart and becomes idealised in the mind of surfers. This community is just, egalitarian, full of opportunity, unified in Islam purged of national peculiarities, and devoid of corruption, and persecution’ (Sageman, 2004: 191).

Sageman’s argument concerning “virtual Islam” is important as the internet has emerged as a prominent space for people to express themselves. This chapter will now focus on the role of online communities in engaging with terrorist-inspired messages both implicitly and explicitly.

## Engagement with Online Communities

The Web, with its billions of pages and trillions of connections between users, provides a platform for users to engage with boundless numbers of issues and organisations to form communities. This vast collection of information offers online users the opportunity to either form or join communities on any number of topics. The Web reduces the barriers to entry for becoming part of a community, making online communities somewhat more ephemeral than their offline counterparts.

There is no one universally accepted definition of an online or virtual community, making accurate descriptions problematic. Online communities are complex entities and, as will be shown during the course of this chapter, have a palpable influence on the behaviour of groups both online and in the real world. A review of the literature on online communities reveals a composite of different attributes; for example, Wenger (1998) characterised them as displaying shared repertoires and resources, while Robert Kozinets (2002) claimed that the dominant characteristic of online communities is social activity and interaction. Rotman & Preece (2010), in a study into the nature of communities on YouTube, defined online communities as ‘*a group (or various subgroups) of people, brought together by a shared interest, using a virtual platform, to interact and create user-generated content that is accessible to all community members, while cultivating communal culture and adhering to specific norms*’ (Rotman & Preece, 2010: 4, emphasis in original).

Rotman & Preece’s definition of online communities is useful for the purpose of this chapter as it is flexible enough to be applied to a wide range of online community structures. For example, the more common expression of a community structure is the formal community in which members have to go through a structured registration process before they are permitted entry into the group and potentially becoming an accepted member. Communities of this kind exist on websites in which prospective members are required to undergo an *a priori* registration process such as the *Financial Times* or the *New Scientist*. Formal online communities exist on other digital platforms such as discussion forums and social networks that require specific user registration, such as the Association of Internet Researchers (Pharmaceutical Discussion Group, 2010).

Other communities demand significantly less formal means of attaining membership. If users simply contribute to discussions or demonstrate allegiance to a group then they become part of the community. This occurs when, in a specific posting, a particular user declares their support or opposition for a specific idea, organisation or issue. Online communities of this sort have been in existence since the development of Internet Relay Chat and discussion forum technologies in the 1960s. The most prominent example of this type of online community is the Whole Earth ‘Lectronic Link (WELL), which is considered to be one of the oldest and most influential online communities.[[86]](#footnote-86) Established in 1985, and founded by Larry Brilliant and Stewart Brand, the WELL allows its members to participate in a wide range of discussions, many of which do not require a password.

One of the results of this type of “push-button” community formation (Bishop 2003) is that online communities can quickly become enormous complex entities with the propensity to coalesce and dissipate quickly. The ephemeral nature of some online communities means it is possible to join and leave at will. It has been argued that many online communities are emotive, knee-jerk entities that form as a result of the immediate whims and desires of its users (Bishop, 2006). However, it can also be argued that large, quick-forming online communities are extremely useful when responding to events that require immediate action, such as the use of crisis mapping in natural disasters.[[87]](#footnote-87)

The ephemerality of online communities was emphasised by the scholar Lance Bennett who argued that the presence of internet and Web technologies enabled its users to scatter their allegiances to ideologies and causes across a wider spectrum of choice than hitherto, and without the need for a formal institution. He argued that citizens ‘born into these late modern societies display a greater tendency to organize political meaning, identity, and activity around what…I have called lifestyle politics’ (Bennett, 2002: 6). The conception of lifestyle politics is significant when interpreting the nature of online communities because it explains the ease with which online users can affiliate themselves with certain causes or ideologies, or, indeed, part of such causes and ideologies. Bennett argues that the characteristics of ephemeral online communities result in low confidence in government as comments highlight perceptions of the inadequacies in the performance of government. This will be examined in greater detail in the presentation of the empirical evidence in this chapter.

To this end, Bennett proposes that online activism can be characterised in certain ways that ‘are hard to separate from organizational capabilities as activists increasingly operate in networks without walls, conventional leadership or membership, geographical or issue boundaries, or other aspects of conventional hierarchical organisations or formal coalitions’ (Bennett, 2002: 7). These characterisations are useful structures within which to explain the nature of the behaviour of online communities when reacting to discussion concerning the 11 March 2004 terrorist attacks.

Table Five: Bennett’s Patterns of Communication

|  |  |
| --- | --- |
| **Pattern of Communication** | **Description** |
| * Permanent Campaigns | * Global activism is characterised by long-running campaigns that organise protests and publicise issues. This stems from online users’ proclivity to migrate from centralised political organisations to informal communities facilitated by internet and Web technologies |
| * Diverse Networks are Ideologically Thin | * The range of campaigns and ideologies renders it difficult to generate one coherent idea. This results in little depth to online activism. |
| * Disruption of Organization due to Internet Use | * The low barriers to entry facilitated by internet and Web technologies can result in low commitment to online communities. |
| * Alteration of Information Flows through Mass Media by New Media | * Global activism and the formation of strong online communities struggle to achieve prominence as a result of the multitude of networks and issues that comprise them. |

Source: Lance Bennett, 2002

While Bennett’s model above was created in order to analyse global activism, it is possible to conceive the utility of such a model for examining the general formation and maintenance of communities when analysing responses to the 11 March 2004 terrorist attacks, as numerous people engaged either individually or in groups to express their feelings with like-minded people.

Another characteristic of online communities is the relative lack of geographical limitation to membership of a particular group. This notion demonstrates how the Web lowers barriers to entry in forming and participating in groups; online communities are, to a large extent, dependent on linguistic and ideological congruence, not geographic proximity.

One of the central tenets of online communities is the potential they have to influence both online and real-world events. Although the link between the behaviour of online communities finding expression offline and vice versa is unproven, recent events in international politics provide evidence to the contrary. The example of the disputed elections in Iran in 2009 is particularly apt as protestors for the disputed candidate Mir-Hossein Mousavi used tools such as microblogs, blogs and discussion forums as a means of expressing their support and communicating with like-minded people (Bray, 2009).

While online communities can be grand in scale and influential in shaping the course of real-world events, it is prescient at this juncture to discuss what online influence actually is. In a similar vein to deriving a neat definition for online communities, online influence is equally difficult to define because of its intangibility. A review of the literature concerning online influence defines the concept in terms of users able to impact the behaviour and opinions of other users (Bertola 2010), or as ‘conduits for human based filtering and content discovery within their communities, as members of the community look to the person of influence to connect them to people and content they should trust, and fuel positive community growth’ (Baldwin, 2009: 1). Influential online users are, therefore, able to disseminate information to their network, which is then assimilated and subsequently passed to others within their respective networks; thereby creating a network effect (Katona et al., 2010).

Online influence can, as a result, be defined and measured in a number of different ways. One way of measuring online influence measurement is quantitatively, generally by counting the number of links or citations a user has aggregated, or the number of designated followers a user or organisation has. The amount of links accumulated, or professed followers a person has, is thought to be a strong indicator of the level of influence wielded online (Huberman et al., 2009, Skala 2010). This argument fits with the definition of online influence by Baldwin (2009); that an influential person within a community is perceived to be a conduit for human-based filtering and content discovery, and will be cited more often online and accumulate more followers. In addition, the level of influence for a particular user can be either augmented or degraded by the level of support or admonishment from other users (Kozinets 2002).

However, influence in online communities does not always reside in the networks of individual users. Influential users still rely on their networks to send recommended content to other members of their extended network. This means that the collective number of online users who are less active can collectively wield a significant degree of influence, as they are responsible for disseminating content from the influential users. In his analysis on the linkages between micro and macro-level sociological interactions, Granovetter (1973) commented that the less active members of communities or groups were “weak ties”. Granovetter claimed that an analysis of the behaviour of “weak ties” reveals much about the ‘interactions *between* groups and…analysis of segments of social structure not easily defined in terms of primary groups’ (Granovetter, 1973: 1360, emphasis in original) “Weak ties” therefore diffuse content from influential users to other groups of “weak ties” ensuring that the content is at once endorsed and dispersed widely online. This phenomenon of “weak ties” demonstrates the symbiosis between users with irregular activity in online communities collectively, and those more visible influential users.

The following section incorporates an analysis of ways in which public diplomacy strategies can be incorporated into counter-terrorism strategies as techniques to better engage with communities of people online and offline.

## Public Diplomacy and Engagement with Communities

The wider discipline and role of engaging with and influencing both foreign and domestic publics, known as public diplomacy, particularly online through digital diplomacy, plays a critical role in a country’s relationship with terrorism.

Well-crafted public diplomacy programmes help shape the opinions of target populations (La Porte, 2011, Szondi, 2008, Fisher, 2008). Although different to traditional diplomacy strategies, public diplomacy engages groups of people in an effort to positively increase the reputation of a state or government. The use of this type of “soft power” is not new to the Spanish state; it has been used extensively in the form of Expositions, sporting events, and education institutes as outlined in Chapter Two.

The introduction of digital communications technologies has had a significant impact on the practice of public diplomacy, in particular, accelerating the rate at which feedback on the responses of the target populations to specific programmes can directly affect a specific public diplomacy programme. Web-based communications platforms and the ubiquity of devices with Web connectivity, such as computers, mobile phones and tablet devices, have resulted in the general public being able to exert a far greater influence on public diplomacy programmes. The importance of effectively monitoring and analysing public diplomacy programmes was highlighted in a conference on the topic at Wilton Park in which it was argued ‘[i]t is also vital that the overall impact of public diplomacy campaigns is evaluated in order to improve them and continue building successful, long-term relationships’ (Ampofo, 2010: 14).

However, enhanced programme-specific data and opportunities to engage target populations should not detract from the need to craft influential programmes that are, above all, credible in the perception of the target population. The delivery of key narratives in a credible fashion does not always lie with the Government, however. If online groups, or communities, organised around a variety of interests, issues and demographics, are engaged in a credible fashion, then the potential for them to deliver key government narratives to a wider group of the target population is significant. Indeed, the potential for communities, such as the “new intellectuals” (Fisher, 2003), to play an integral role in public diplomacy was outlined in the Wilton Park conference on online Jihad in which it was claimed that communities ‘are not the problem but core to the solution, with a unique ability to organically generate compelling and self-sustaining counter-narratives and alternatives to radicalisation.’ (Wilton Park, 2011: 7).

The above comment highlights the opportunity that digital communications platforms have to provide a forum from which to counter negative narratives, to those which the Government is attempting to create. In the same way, online users and communities can help create new, positive narratives that support public diplomacy objectives in a credible way that enhances national reputation.

## Internet Research on 11-M Attacks: Behaviour of Online Communities

As previously described in Chapter Three, the author created a methodological process to analyse online discussion related to the Madrid terrorist attacks of 2004 to support the primary research conducted. The date range of the analysis was six months from 11 March to 11 August each year over a period of seven years (2004 to 2010). In this chapter, the internet research assesses the behaviour of online communities and analyses sentiment and, in particular, negative sentiment and grievances amongst communities. Further findings from the online analysis are presented in relevant chapters of this thesis.

879 individual data points were analysed which comprised of content emanating from blogs, discussion forums and websites. This section presents an overview of the results followed by an analysis into specific date ranges (2004, 2005, 2006-2007, 2008-2009, 2010), and an analysis of the high level of negative sentiment that emerged through research (739 data points or 84 per cent of the total volume of content).

### Overview of Results

The online community analysis highlighted a number of salient elements, the first of which is that the activity within the communities related to the 11-M is a strong example of online reaction to crisis events. Narratives from sources such as the Spanish Government and terrorist organisations were propagated by the mainstream media and were not well received by the online communities. As a result, the organisations in question suffered a decline in their influence online, evident as online users in general expressed mistrust at these institutional narratives, and by extension, of the organisations. The overall result is that these communities do not usually assimilate the narratives, and some communities became actively critical of them, preferring instead to formulate their own narratives.

The following table outlines the range of communities that emerged during the online analysis, an explanation of their *raison d’être* and a link to a specific example of a particular group. It is worth noting at this point that the methodological process for determining the composition of the online communities is located in Chapter Three.

Table Six: Online Communities Discussing the 11 March 2004 Attacks

|  |  |  |
| --- | --- | --- |
| **Community** | **Description** | **Example Source** |
| **11-M** | * Community discussing and posting content directly related to the Madrid Attacks | * [www.3diasdemarzo.blogspot.com](http://www.3diasdemarzo.blogspot.com) * 3 Días de Marzo is a blog that publishes news articles and other user-generated content from around the Web related to the terrorist attacks in Madrid in 2004. * Although the identity of the owner of the site is unknown, they have revealed that the person is 23 years old. The site attracts extensive commentary on the postings from its wide readership |
| **Activist** | * Focus on anti-Government content and discussion | * [www.rebelion.org](http://www.rebelion.org) * Rebelion is a website that syndicates essays and other writings from political activists from across the world * The identity of the owner of the site is unknown, however, the site attracts extensive commentary on the articles from readers. |
| **Architecture** | * Group focused on discussing the latest developments in architecture | * [www.erlik.blogspot.com](http://www.erlik.blogspot.com) * Arquitecturas Imaginarias is a blog which ceased in July 2010. Its owner, who is not identified, posted content related to his interest in architecture, particular Spanish architecture. |
| **Ethnic** | * Focus on ethnic and cultural discussion | * [www.forum.stirpes.net](http://www.forum.stirpes.net) * Stirpes was a popular discussion forum whose members discussed issues relating to Spanish culture and identity. It is unclear when the forum ceased to exist but had a active and engaged user-base from 2004 to 2007 |
| **General Public** | * Group that has no particular focus and comments sparingly on 11-M | * [www.auxarmescitoyen.livejournal.com](http://www.auxarmescitoyen.livejournal.com) * Auxarmes Citoyen is a blog that ceased to exist in 2005. The author (who is not identified) posted content related to personal issues and current affairs. |
| **Government** | * Sources that are Government sponsored or originate from Government staff members | * [www.radiomundial.com](http://www.radiomundial.com) * Radio Mundial is an international radio station that reports news articles in a range of languages across its numerous country-specific. The ownership of the site is unclear however, it features a wide range of articles and commentary directly from government sources. |
| **Journalism** | * Sources that focus on journalism | * [www.periodistas21.blogspot.com](http://www.periodistas21.blogspot.com) * Periodistas21 is a blog that was created by Juan Varela, a journalist and consultant based in Madrid and Coruña. While the blog focuses on produces content relevant to the issue of journalism, it posts articles occassionaly on terrorism |
| **Mainstream Media** | * Content and discussions contained on mainstream media sources | * [www.elmundo.es](http://www.elmundo.es) * El Mundo is an influential and popular newspaper. It has an international audience and a large team of journalists who post articles daily on current affairs issues, especially terrorism. El Mundo also attracts widespread commentary on its articles from its large readership. |
| **Military** | * Sources focused on military issues | * [www.militar.org.ua](http://www.militar.org.ua) * Foro Militar General is a discussion forum dedicated to the discussion of issues related to the world’s armed forces, security studies, military service, security services, military police, war, arms etc. * It is unclear as to who owns this site however, it attracts a considerable membership of Spanish-speaking military-focused users |
| **NGO** | * Portals dedicated to issues affecting non-governmental organisations | * [www.aissma.org](http://www.aissma.org) * The Asociación de Inspección de Servicios Sanitarios de Madrid is a blog which represents doctors, inspectors, pharmacists and nurses. * The owner of the site is not revealed but they post content primarily concerning public health |
| **Political** | * Portals dedicated to discussing political issues | * [www.kickjor.blogspot.com](http://www.kickjor.blogspot.com) * Kick Jor is a blog which ceased to exist in August 2008 and focused on publishing opinon dedicated to a wide range of political issues and current affairs * The identity of the owner is not revealed, however, the site attracted considerable commentary from the once-active readership |
| **Religious** | * Religious-focused online portals | * [www.labranzadedios.com](http://www.labranzadedios.com) * La Branza de Dios is a website that focuses on posting multimedia content related to the major world’s religions. * The identity of the owner is not revealed however, it is clear that some of the site’s content occasionally focuses on the political impact of religion |
| **Terrorism** | * Sites that focus exclusively on the issue of terrorism | * [www.terrorismosigloxx.wordpress.com](http://www.terrorismosigloxx.wordpress.com) * Terrorismo Siglo XX is a site that focuses exclusively on the issue of global terrorism and its impact * The site is run by Alexis Urrutia, an architecture student from the Universidad de la República en Montivideo, Uruguay and David Vasquez, a medical student at the Universidad de Valparaiso, Chile. |
| **Youth** | * Online portals focused on youth issues | * [www.forojovenes.com](http://www.forojovenes.com) * Foro Jovenes is a community that is dedicated to the discussion of youth issues by young people. * It is unclear who manages the forum, however, it has attracted many people who occasionally discuss terrorism in Spain |

Source: Lawrence Ampofo

### Monitoring and Analysis of the Behaviour of Online Communities Over Time (2004-2010)

#### a. Results from 11 March 2004 to 11 August 2004

The analysis of online commentary highlighted that the composition of online communities consisted of a small number of groups, namely the Mainstream Media, General Public and Political communities. Figure Twenty-Two below shows the top seven communities in 2004 by sentiment.[[88]](#footnote-88)

Figure Twenty-Two: Bar Chart of Online Communities by Sentiment in 2004

Source: Lawrence Ampofo n=146

The most active community to generate content in 2004 referencing the Madrid attacks was the Mainstream Media community, which sought to update its readership on the main occurrences surrounding the event. Content emanating from the Mainstream Media community was replete with core Government narratives such as ‘ETA is responsible for the attacks’ and ‘Unity is the most important narrative to get over the terrorist attacks’.

The Mainstream Media community was numerically predominant in the early discussions surrounding the event in 2004 generating 48 per cent of the content (or 70 posts). The high level of activity within this community can be explained by its ability to attract a high number of people who desired to discuss the issues raised in the publications and be informed of the passage of events of that day. In addition, the trajectory of commentary from the Mainstream Media community correlates strongly with high levels of slightly and strongly negative commentary. One such example is seen in an article by the prominent publication *el Périodico* with the story that the Partido Popular claimed that Zapatero and the PSOE had won the General Election because of the 11 March 2004 attacks.[[89]](#footnote-89) The content of user commentary on the article was indicative of the majority of content from this community in which commentators were principally concerned with expressing anger and frustration in their discussions.

Online behaviour in 2004 was also characterised by a high volume of commentary from the General Public community. This community featured discussion from a wide range of general online users in tandem with a predominance of negative sentiment, which underscored the indignation and outrage felt by the general Spanish public and their readiness to engage in detailed discussion about it online.

An example of this is seen in a post to the *Aika* web log in which the user, who recently returned to Madrid following the attacks, expressed surprise and dismay at the destruction caused by the bombs;

‘Yesterday was 11 M. I have just arrived from Madrid. I think that we were more than one million people, I have not seen the news yet. Right now, I have no words to express how I feel’.[[90]](#footnote-90)

It would be erroneous to conceptualise the existence of negative sentiment one dimensionally based on this type of description. The corpus of data encompassing negative sentiment (strongly negative and slightly negative) contains a range of information that requires a more granular analysis to gain a deeper level of insight into the nature of the behaviour and understandings of online communities. This analysis will be presented subsequently in this chapter.

#### b. Results from 11 March 2005 to 11 August 2005

Mainstream Media and Political communities ranked highest in 2005, collectively generating 75 per cent of the content in 2005 (or 133 and 95 posts respectively), as these groups held more nuanced discussions about the wider impact of the attacks on Spain. Figure Twenty-Three below shows the communities that posted most frequently in 2005 by sentiment.

Figure Twenty-Three: Bar Chart of Online Communities by Sentiment in 2005

Source: Lawrence Ampofo n=305

The highest volume of content in 2005 was generated by the Mainstream Media community as in 2004. Although the Mainstream Media community was the most active in terms of the number of comments from its user base, other communities similarly assumed importance in the online debate on the Madrid attacks. The Political community was one such group that became significantly more active in 2005 than 2004. This community’s members debated vociferously the issue that the Aznar administration had misinformed the general public by suggesting that ETA was responsible for the attacks and not al-Qaeda. Members of the community were outraged that attempts had been made by the State to divert attention from the real perpetrators of the attack and towards an explanation, which to them was made more for political gain than any other reason. An example of this is seen in a lengthy discussion on the portal *Escolar,* which examined the impact of the bombings in Madrid. Although the users of this service were united in their condemnation of the attacks, online users from all communities condemned the Government’s refusal to deliver accurate information to the general public:

‘In the sadness of 11M, the only thing the people complained about were the lies from the government, claiming that everything had been caused by ETA. Here, it is possible to see the conflation of imprudence to give information too quickly with the presumed interest of those who thought that it was not Islamic terrorism. This is my opinion’.[[91]](#footnote-91)

Interestingly, the 11-M community also increased its activity significantly during 2005, concerned as it was with the question of whether Spain would again become the focus of another international terrorist attack. The rise in activity from communities such as the Political, General Public and 11-M communities is illustrative of the shock and disbelief that the attacks had been carried out and that the attacks influenced voter decision (Moreno, 2004, Ginesta & Sopena, 2009).

#### c. Results from 11 March 2006 to 11 August 2007

2006 saw a notable decrease in the volume of content as virtually all communities commented less on the bombings than they had in the two years previously, generating 154 data points.

Figure Twenty-Four: Bar Chart of Online Communities by Sentiment in 2006 and 2007

Source: Lawrence Ampofo N=154

Only the Activist community recorded an increase in the volume of content generated (57 posts or 33 per cent) as shown in Figure Twenty-Four. This community came to the fore in the absence of a strong presence from the previously dominant Mainstream Media (36 posts or 23 per cent) and Political communities (14 posts or nine per cent). The Political community members often expressed more polarised views on the potential ramifications of the Madrid bombings. For example, an online user on the *BBC Mundo* Have Your Say forum claimed that Jihadist-inspired Moroccan immigrants were responsible for the attack, meaning that Spain’s current immigration regulations were too relaxed, encouraging those with questionable motives to reside in Spain to carry out more attacks (*BBC News*, 2004). Other members of the Activist community claimed that Spain’s involvement in the Coalition invasion of Afghanistan and Iraq was the motivation for the attack. One user in a lengthy discussion thread on the *Noticias de Eurabia* blog claimed that the attacks in Madrid were tantamount to a *coup d’état*. ‘[t]he other thing is that Aznar lied to the Spanish nation with the weapons of mass destruction in Iraq and has not yet paid with justice.’[[92]](#footnote-92)

Discussion from the Activist and Political communities questioned whether al-Qaeda might not be responsible for the attack and whether ETA had more involvement in the attacks. Discussion of this kind indicates that two years after the 11-M Commission announced the findings of its investigation into the attacks, a significant number of online users still mistrusted the official version of events.

In addition, activist groups also expressed a significant degree of trepidation that the threat of international terrorism to Spain had increased following the attacks. This sentiment was utilised by critics of the Government who believed that the response to terrorism both before and after the event was inadequate. This is demonstrated by a contributor to a discussion thread on the *Libertad Digital* blog who claimed that the misinformation provided to the media by the Aznar Government and the subsequent counter-terrorism strategy implemented by the Zapatero Government had increased the resolve of terrorist organisations to perpetrate more attacks in Spain (*Libertad Digital*, 2009).

It is possible that the intense media scrutiny on these counter-terrorism operations compelled other online commentators to focus their attention on other aspects of the Government’s counter-terrorism programmes and away from the Madrid bombings. The Government had launched a range of counter-terrorism programmes and operations that were perhaps responsible for deflecting attention away from discussion on the Madrid bombings. The mainstream media provided in-depth coverage of the Government’s range of counter-terrorism operations such as *Operación Sello* I & II and *Operación Nova* I & II[[93]](#footnote-93).

#### d. Results from 11 March 2008 to 11 August 2009

2008 saw an increase in the volume of content, as the General Public, Mainstream Media and Terrorism communities became the most active in this period. The reason for this increase in coverage is, however, unclear.

Figure Twenty-Five: Bar Chart of Online Communities by Sentiment in 2008 and 2009

Source: Lawrence Ampofo N=171

In 2008 and 2009 online users generated an increase in strongly positive commentary than that produced in previous years (37 posts or 22 per cent). This is explained by the proclivity of online users to provide emotional support for their respective communities as they sought to pay homage to the victims of the attack in the years following the bombings, and not to solely castigate other organisations. This behaviour is illustrative of a softening of the sentiments of online users over time.

One of the most active communities was the General Public group (43 per cent of coverage in 2008 and 2009 or 73 posts), which was more active than the Mainstream Media community (19 per cent of coverage in 2008 and 2009 or 32 posts). The two main reasons for its increased activity are seen in its discussion of the misinformation supplied by the Aznar administration to the people in the aftermath of the bombings. In addition, however, members of the General Public community in 2008 and 2009 were apt to remember the victims of the attack in their discussions, providing support and a platform for catharsis for its members. An example of this behaviour is seen in a post to the blog *Martha Colemenares* in which a participant to a discussion thread following a post on the legacy of the 11 March victims claimed that ‘[f]ive years afterwards, many of us still want to know the truth about 11-M. Others prefer to bury what happened and not talk about what happened that day and in the days afterwards. In the end, we have Zapatero in the Government because of the attacks.’[[94]](#footnote-94) It is interesting to note that the participants in this discussion thread were quick to link their comments about the victims to their condemnation of the Government’s progress in releasing more information about the attacks. This emphasises that five years after the attacks, the Government had failed to convince the general populous that it had managed the response to the attacks effectively.

2008 and 2009 also saw a slight increase in the volume of content from the Terrorism Community after a comparatively low level of activity in 2006 and 2007 (154 posts in 2006 and 2007 and 171 in 2008 and 2009). It appears that the five-year anniversary of the attacks inspired terrorism-focused commentators to reflect on the political, social and security consequences for the country. The *Islamización de Europa* blog was an example of this, posting that five years after the attacks in Madrid, al-Qaeda cells remained prominent in the country and could potentially launch another attack without warning. In particular, the terrorism community focused on the presence of radicalised members of the general public and the potential danger posed by people such as Raquel Burgos, a Spanish citizen who married Amer el Azizi, a self-professed member of al-Qaeda in Europe.[[95]](#footnote-95)

#### e. Results from 11 March 2010 to 11 August 2010

The Mainstream Media community produced a greater volume of content in 2010 than during the 2007 to 2009 period with 31 posts or 30 per cent of coverage. There was also a notable increase in the volume of content emanating from the Activist community that focused on the Government’s inadequate response to the terrorist attacks. It was clear that the community still exhibited a great deal of frustration at the Government’s reaction to the 11-M attacks and to the terrorist threat in general, and did not feel as though its questions had been adequately responded to.

Figure Twenty-Six: Bar Chart of Online Communities by Sentiment in 2010

Source: Lawrence Ampofo N=103

‘Remembrance for the victims’ was a concurrent theme amongst the Political community, which posted an increased volume of content on the topic. It was clear that the six-year anniversary of the attacks was the main pretext for discussion of this kind, as the community appeared to focus less on apportioning blame for the attacks, and more on remembering the victims and how the attacks affected the population at large. This sentiment was exhibited most prominently by the General Public community who, as mentioned previously, attempted to provide support and catharsis for other members of the community. One of the best examples of this phenomenon is seen in a discussion thread on the *Juventud Naranjas* blog, which focused on the potential feelings of those affected by the attacks six years after the event. One participant of this thread commented:

‘My heart truly clenched when I read the names of the victims or see the images of the attack on Atocha or hear the families. We cannot even imagine what they are going through. Jose María Naranjo has implemented a very good initiative by making a monument to the victims here in Torrejón and the gesture of flowers yesterday. It seems to me very emotive and, at a personal level, I am going to follow you.’[[96]](#footnote-96)

#### f. Analysis of Negative Sentiment Over Time (2004-2010)

While the predominance of compassion, catharsis and anger was exhibited in 2010, it is important to consider, as mentioned previously, the composition of the negative sentiment category from 2004 to 2010. Due to the fact that it is the most frequent sentiment category in the dataset, it was felt that a more detailed analysis would yield further insight on the behaviour of online communities.

As described previously, 738 data points, or 84 per cent of the total volume of data analysed, were negative. Of these 738 data points, 194 were slightly negative and 544 were strongly negative. Figure Twenty-Seven below shows the total volume of negative sentiment within the dataset, year-by-year in relation to the different key narratives.

Figure Twenty-Seven: Line Chart Presenting the Negative Sentiment by Key Narrative Over Time

Source: Lawrence Ampofo N=738

The stacked bar chart above demonstrates that the ‘Government lies about 11-M’ was the most frequently delivered narrative with 279 posts or 38 per cent of the total volume. While this particular narrative was the most frequently delivered, it is also clear that there is a ‘long tail’ of other narratives that was commented upon negatively by online communities such as the ‘Spain is still an object of terrorism’ and ‘Remembrance for the victims’ narratives. Negative commentary within the ‘11-M encourages xenophobia’narrative focused on the notion that the attacks had generated a heightened sense of apprehension of entering into discussion about the immigrant Muslim community for fear that they might be perceived as racist. Such commentary was witnessed in a post to the discussion forum *Militar.org* in which a participant to the lengthy discussion thread claimed the following:

‘What I don’t understand or believe, however much I try, is how when we talk of two people, almost everyone agrees that there is danger with Muslims. But when we are three or more we close our mouths so that we are not accused of racism.’[[97]](#footnote-97)

In addition to this quotation underscoring the participant’s heightened sense of trepidation of xenophobia in Spain, it is also revealing of the proclivity to commensurate religion and immigration with terrorism and counter-terrorism. In addition, it is significant that the message ‘Government lies over 11-M’ was the most frequently discussed narrative. In order to understand the various ways in which online users discussed this narrative negatively over time, the data has been presented in the subsequent chart:

Figure Twenty-Eight: Line Chart Showing the Principal Negative Commentary Associated with the ‘Government Lies About 11-M’ Narrative Over Time

Source: Lawrence Ampofo N=279

The presence of such a high volume of negative commentary for this particular narrative (30 per cent of the total volume of negative coverage, or 279 posts) is significant. It is indicative of the model outlined previously in this chapter by Lance Bennett that online users are able, in this instance, to converge and form a bespoke community based on their frustration of their perception that the Government did not provide the general public with the correct information of the culpability of the Madrid attacks in the immediate aftermath. This community, therefore, manifested itself as a result of the feelings exhibited by online users of the ‘emotional attachments to issues based on their meaningful associations with social identity claims’ (Bennett, 2002: 4).

The commentary associated with this narrative is closely linked with the media contest model, as enunciated previously in Chapter Five, by Simon Cottle (2006). The negative commentary produced is manifested through direct opposition with the policies and narratives released by the Government. However, it is clear that the emergence of large volumes of negative social media content focusing on government counter-terrorism policy contradicts the Manufacturing Consent model outlined by Herman and Chomsky (1988). This is due to the fact that online communities are demonstrably not consenting to the narrative offered by the Government. Rather, it seems as though the Government actively manufactured dissent from online communities by blaming ETA for the attacks.

It is clear that a range of online communities has engaged with this narrative over an extended period of time for a range of reasons. From 2004 to 2005, the principal reason for online user engagement in discussion on this topic was the expression of frustration and catharsis amongst like-minded people, as outlined previously. The motivation for negative engagement in this narrative changed between 2006, 2007 and 2008, however, as the initial high volume of content subsided (Figure Twenty-Seven), and the nature of the negative sentiment changed from general expressions of anger to that of responsibility for putting pressure on the Government to publicise the true account of events of the day of the attacks. An example of this is seen in a post to a lengthy discussion thread from the *Desiertos Lejanos* blog, in which a participant claimed that after three years, the public is no further aware of who detonated the bombs. ‘I do not agree with many things that are going on, Spanish people of today are not the same as in ‘36…we need clarity and this government isn’t giving it to us and this just increases our ignorance.’[[98]](#footnote-98) This demonstration of frustration, coupled with participants’ desire to take responsibility for lobbying the Government for more information on the issue, emerged particularly after online users became aware that a significant time period has elapsed and they still had not received the information they demanded.

Finally, 2010 generated negative discussions of the ‘Government lies about 11-M’ narrative, principally bounded within sentiments of sympathy and support for other online users and members of the Spanish public affected by the attacks. This is demonstrated in a post to the *La Nueva España* website in which an article focused on the sixth anniversary of the terrorist attacks in Madrid. One participant to the ensuing discussion argued that ‘[t]he best homage that could be given to the victims of the attacks would be the deliverance of the truth and to punish those responsible…In the Zapatero Government, there is a shadow of doubt which needs clarifying.’ [[99]](#footnote-99)

This quotation again demonstrates the pervasive undercurrent of frustration exhibited over six years by online users in relation to discussion of the Madrid terrorist attacks. However, it is also noteworthy that the composition of negative commentary concerning this issue was changeable. As in 2010, online communities appeared to focus most prominently on providing support for one another while simultaneously campaigning for more accountability from the Government.

## Conclusion

The terrorist attacks on 11 March 2004 drastically altered Spain’s national security focus, and led to a shift in its strategic focus and resources from the long-standing conflict with ETA to the threat posed by international terrorism. The realisation that more emphasis needed to be placed, not only on combatting al-Qaeda-inspired terrorism, but also better engagement with immigrant communities became a priority for the Zapatero Government.

Zapatero’s Government placed enormous emphasis on implementing programmes that focused on inter-cultural and inter-religious dialogue with Muslim communities. In addition, the Government bolstered its bilateral relationships with other countries and strengthened the capacities of the security services as a means of countering Spain’s newfound dual security threat (Celso, 2006).

While progress may have been made in engaging with Spanish immigrant Muslim communities, the findings of the internet research above and in Chapter Four, have shown that communities of people coalesce online around the issue of immigration and terrorism and actively express and share their grievances. It emerged that there was a considerable amount of angst and discontent online in which users continued to link the immigrant Muslim community with acts of terrorism.

The analysis also indicates the importance of changing the narrative linking Islam with terrorism and creating an effective online and offline public diplomacy strategy with the objective of building long-term relationships with the immigrant Muslim communities, empowering them to overcome the terrorist threats they face. Professor Fernando Reinares of the Real Instituto Elcano supported this assertion, claiming that a public diplomacy strategy employed as part of a counter-terrorism policy should be ‘focused, interministerial in dimension and [include] the relevant players from civilian society. This public diplomacy must be part of a national strategy on international terrorism and be complementary to other collective programmes to which the Spanish government must either contribute or promote’ (Reinares, 2006: 8).

Attaining influence online should become a priority of the Government and other organisations if they are to effectively counter contemporary terrorist organisations. This argument is particularly salient with respect to the continued development of the Web, which is now witnessing the introduction of new technologies collectively described as Web 3.0 such as cloud computing, 4g mobile telecommunications and the Semantic Web. As the introduction of these technologies becomes widespread, the distinction between the online and offline worlds will blur so as to become indivisible. In the future, in order to understand and influence the behaviour of offline communities, it will be essential to understand and influence online behaviour. Therefore, as terrorist organisations continue to make use of the Web as a means of influencing new groups of people, and an increasing number of people become connected to the internet, the ability to influence behaviour and build relationships online will become increasingly valuable for the Government and other organisations.

In addition, cultivating an ability to influence people and develop strong relationships online using Web 3.0 could lead to the uncovering and creation of engagement strategies with hitherto unknown communities that hold extreme views before they become dangerous to society. In this way, an enhanced ability to influence online behaviour, both now and in the age of Web 3.0, might well have the effect of making the clandestine more visible. Similarly, understanding the behaviour of online communities and attaining influence within them, can yield opportunities for the Spanish Government to identify and engage communities in online dialogue to find solutions to address grievances as they arise.

Finally, Web 3.0 may have the effect of changing the nature of terrorism in the 21st century. Although it may well continue to be defined by the violent attacks perpetrated by terrorist organisations, they might also be more defined by their ability to craft and propagate narratives to their target audiences. The following chapter will strive to establish why, in the age of Web 3.0, governments should adapt similar counter-terrorism strategies that not only mobilise online communities from helping potential terrorists, but also work to counteract narratives in public spaces, including online portals.

# **Chapter Eight: Online Life Online Death: Terrorism 3.0, Recommendations and the Death of Osama Bin Laden**

## The Concept of Terrorism 3.0

Gaining insight into the nature of online behaviour in relation to terrorism, counter-terrorism and technology in Spain, coupled with the introduction of new communications technologies, will result from a new collaborative, ubiquitous and more populated engagement with terrorism online and offline, Terrorism 3.0.

During the course of this thesis, conclusions emerged which both supported and enhanced analysis of the central hypothesis. The concepts of online engagement and influence were two such conclusions that came forth from the empirical analyses. It was apparent from the semi-structured interviews, internet research and literature review that some online communities and users engaged with the issues of technology, terrorism and counter-terrorism to influence others of their specific viewpoints, as well as engage with others of like-mind.

The internet research of discussion related to the 11 March 2004 terrorist attacks in Madrid showed that online users and communities initially demonstrated a strong propensity towards the expression of anger and frustration in 2004 and 2005, that the Spanish Government had not, in their opinion, divulged accurate information pertaining to the culpability of the attacks. However, the composition of these emotions changed markedly during 2006, 2007 and 2008 as online users and communities articulated concerns that immigrant populations in the country were a potential cause of terrorism and emphasised that measures should be taken to monitor and stem the flow of immigrants, particularly illegal immigrants, into Spain. In 2009 and 2010, the overriding emotions expressed were compassion and empathy for the victims of the attacks five and six years on from 11-M.

The range of emotions expressed by online users and communities over time (including the various narratives used to deliver these emotions) is indicative of the nature of interaction and engagement between them in relation to terrorism and counter-terrorism. The formation of online communities that engage in terrorism and counter-terrorism was enabled by the use of Web 2.0 technologies to facilitate discussion amongst disparate communities and users. In addition, the complexity of the range of occurrences of engagement and interactions amongst online users in relation to terrorism and counter-terrorism will increase significantly, especially with the onset of Web 3.0 technologies.

Web 3.0, as outlined previously, is an umbrella term used to describe a range of technologies that will be employed to upgrade the current functionality of the Web and its services such as the Semantic Web, the real-time Web and the internet of things[[100]](#footnote-100). The continued development and subsequent introduction and diffusion of these technologies will lower the barrier to entry for millions more people to connect to the internet and the Web. In addition, such technologies, mediated by other communications technology infrastructure such as 4g cellular networks, IPv6 and motion sensors, will make online experiences more ambient and tightly interwoven with real-world experiences. This will give rise, as a result, to an even greater amount of social interactions taking place online, ensuing in a significant increase in the volume of social interactions.

The rising complexity and volume of social interactions raises the question: based on the conclusions derived from the empirical research, is it analytically useful to introduce the concept of Terrorism 3.0? Based on the research conducted in this thesis, the author suggests that Terrorism 3.0 is a concept that defines the distinct nature of discussion and engagement with the issue of terrorism online that both utilises and reflects the new online experiences and interactions of communities and users facilitated by Web 3.0.

Terrorism 3.0 is a multi-layered, emergent concept, which mandates that engagement with the issue of terrorism be mediated by Web 3.0 technologies. The use of the word emergent is intentional as it accurately explains the nature of the phenomenon of Terrorism 3.0 as ‘one that is described by atomic concepts available in the macrolanguage, but cannot be so described in the microlanguage…[emergence is] the concept of some new phenomenon arising in a system that wasn’t in the system’s specification to start with’ (Standish, 2008: 3). Standish’s definition can be attributed to the concept of Terrorism 3.0 as online community and user engagement and interaction within the issue of terrorism with the collective presence of Web 3.0 technologies. However, this phenomenon is more difficult to describe when analysing online behaviour independent of Web 3.0 technologies.

Emergence in the context of Terrorism 3.0 refers to the evolution of the issue of terrorism in socio-technical systems, such as the Web. Use of the term “emergence” is taken from the conceptualisation of Terrorism 3.0 as a specific issue, or structure, which exists within a self-organising socio-technical system that embraces particular actors and specific structures.

The term “emergence” in this way is taken from evolutionary systems theory, coined by Ervin Laszlow, Vilmos Csanyi and Susantha Goonatilake, referring to the merger of systems theory and evolutionary theory. It is defined as the reference to ‘evolving systems and as a theory that is the result of the merger of systems theory and evolutionary theory which nowadays not only applies to biotic and human or social systems but also to physical systems, that is, to the cosmos itself’ (Hofkirchner, 2005: 4). Evolutionary Systems Theory becomes relevant to this thesis in consideration of ‘a leap in quality [that] exists between the state of the system at one point of time and the following state…in the case of level shifts’ (Hofkirchner, 2005: 5). To conceptualise this point more clearly, the nature of emergence in the area of Terrorism 3.0 is characterised by the self-organising, socio-technical interactions between Web 3.0, online user and community engagement and the various terrorism narratives emerged and vanished from the public consciousness online. It stems from the idea that ‘the Web is a social [and technical] system…[u]sing networked computer networks as means, humans interact in these three social forms by using and producing information. In consequence they collectively generate an emergent informational structure on a system’s scale. In a top down process this structure in turn enables and constrains their actions regarding information use and production’ (Raffl et al., 2011: 3). This perspective of the emergent nature of Web 3.0 is particularly relevant when considering Web 3.0 as a ‘community of action…Usually such communities consist of actors who do not only share a common interest or passion, but also develop associative social relationships and common goals for starting collective activities, thus achieving the possibility of bringing about a real change of given structures’ (Raffl et al. 2011: 5).

In this way, Terrorism 3.0 could be said to be conceptually different from Terrorism 1.0, which would entail an online user’s one-way interaction with the issue of terrorism online. This kind of phenomenon is seen in the production of online content that does not encourage the information consumer to contribute to the content, and is evinced in press releases from counter-terrorism organisations, or content from news agencies such as Reuters and *Agence France-Presse* (AFP). Scholars such as Brian Jenkins allude to the presence of Terrorism 1.0 in his description of terrorist acts being created especially for traditional media channels such as radio and television, or terrorism as theatre where the audience is required to watch and not participate. Similarly, Terrorism 2.0 could denote online users who engage with the issue in a more collaborative and two-way manner, facilitated by Web 2.0 technologies such as discussion forums, social networks and blogs. Examples of Terrorism 2.0 could be seen in the influential blog *3 Días de Marzo*, which posts mainstream media content pertaining to the Madrid bombings and facilitates discussion on the topic. Similarly, Terrorism 2.0 has been outlined indirectly by scholars of terrorism and the internet in this thesis. Conway & McInerney (2008), in their analysis of the prevalence of auto-radicalisation of people on social networking sites, indicated that terrorism online was a participatory process that encouraged contributions from target audiences.

Terrorism 3.0 is different to the aforementioned descriptions as it is a phenomenon that is mediated by Web 3.0 technologies, which promote pervasive, mobile and cloud-based computing, and connect online users to the internet and the Web constantly. Online user and community experiences of engagement on this issue will be instantaneous, global in reach and all around them, facilitated by devices such as tablet computers, mobile phones and web-enabled objects such as Quick Response (QR) codes.

Figure Twenty-Nine: Emergent Model of Terrorism 3.0

Source: Lawrence Ampofo

Figure Twenty-Nine above depicts Terrorism 3.0 as the result of a collection of concentric circles where the inner circle, or the nucleus, is comprised of Web 3.0 technologies within which all social and cultural interactions take place and through which Terrorism 3.0 is facilitated.

The second circle denotes the phenomenon of online community and user engagement, which is placed at the centre of the chart to highlight the pervasiveness of such behaviour. In addition, the centrality of community and user interaction underscores the importance of the concept of a socio-technical explanation for Terrorism 3.0.

The outer circle is depicted as the issue of terrorism online, which emerges from the interactions and engagement of online communities and Web 3.0 technologies. This engagement is significant by the fact that it is as pervasive, mobile and decentralised as the Web 3.0 technologies, facilitating the focus of engagement on enhancing one’s ability to influence the attitudes and behaviours of other users.

This conception of Terrorism 3.0 has been formulated through a detailed examination of the understandings that exist of the relationships between technology, terrorism and counter-terrorism in Spain. Terrorism 3.0 resonates strongly with the theoretical frameworks for contemporary terrorism set out by the scholars Thomas P.M. Barnett (2005) and Philip Bobbitt (2008), the relevance of which is discussed in detail in Chapter Two.

In particular, Bobbitt contended that contemporary terrorist organisations would become more cellular, networked and diffuse in structure and, by implication, more difficult to counter as they emerge in response to the modern market state. Bobbitt used the discourse of technology to describe contemporary terrorist organisations as: ‘global, networked, decentralised, and devolved’ (Bobbitt, 2008: 44).

In addition, other theories were pivotal in providing explanatory frameworks to the formulation of Terrorism 3.0. An example of this is Bruno Latour’s conceptualisation of technological development as a socio-technical mess in which a variety of actors and contexts affect the nature of its development (1988). Latour’s theoretical framework is in contrast to the notion of technological determinism propounded by experts such as Isaac Asmiov who argued that ‘[t]he whole trend in technology has been to devise machines that are less and less under direct control and more and more seem to have the beginning of a will of their own. A chipped pebble is almost part of the hand it never leaves. A thrown spear declares a sort of independence the moment it is released. The clear progression away from direct and immediate control made it possible for human beings, even in primitive times, to slide forward into extrapolation, and to picture devices still less controllable, still more independent than anything of which they had direct experience’ (Asimov, 1980: 130).

Asimov’s description of the theory of technological determinism was also used to evaluate the utility of the notion that technological development and human agency are intrinsically linked. In addition to the socio-technical theory of technological development and technological determinism, Simon Cottle’s (2006) media contest theory was used to explain the nature of online communication that emerged in the internet research conducted for this thesis. Cottle claimed that media content is created as a result of the content creator’s contestation with the official position or policies of government actors. Examples of media contest theory were witnessed most explicitly in the findings from the internet research in which it was determined that the most frequently delivered narrative amongst the range of online communities over time was the ‘Government lies about 11-M’, or that which directly contested the narratives offered by the Spanish Government.

It was in this context that the hypothesis was constructed and tested, namely that the availability of new technologies increases the capacities of terrorist and counter-terrorist agencies to achieve their communication objectives. The hypothesis was tested by conducting semi-structured interviews, literature reviews and internet research investigating reaction from online users and communities to the 11 March 2004 terrorist attacks in Madrid. From the analyses conducted, it emerged that discussion on the topic focused on four central topics; immigration, narratives, cybercrime and communities. Whilst the core findings from the research are outlined below in greater detail, it should be noted that the hypothesis was eventually validated, and that access to new technologies increased the capacities of terrorist organisations to communicate. In spite of this however, it also emerged that the creation and effective use of compelling narratives was of consummate importance when investigating the extent to which new technologies were useful in increasing the capacities of terrorist and counter-terrorist organisations to reach their communications objectives. Indeed, it emerged that in addition to having access to new technology, the creation and maintenance of myths, narratives or memes is vitally important to achieving the objectives of terrorist and counter-terrorist organisations. It is therefore the position of the thesis that in addition to the hypothesis being validated, the findings from the research processes have brought forth new insight that has aroused inspiration for further research avenues.

The research methodologies and processes conducted for this thesis were outlined in detail in Chapter Three. The internet research process complemented the other research methods, in particular, by analysing, in an unobtrusive way, the responses of online communities and individual users to discussion of the 11 March 2004 terrorist attacks in Madrid. The internet research also encompassed an analysis of the ways in which online users interpreted core narratives related to the 11 March attacks, and how this interpretation evolved over time.

The final result of these analyses made the conceptualisation of the central hypothesis more profound and nuanced. It appeared in Spain that understandings of technology, terrorism and counter-terrorism were predicated on the maintenance of influential narratives in order to affect the behaviour of other online and real-world communities. It is, therefore, the author’s contention that the central hypothesis be changed to the following: the creation and maintenance of influential narratives is central to forging understandings of technology, terrorism and counter-terrorism in Spain.

A final empirical analysis of the immediate reaction of online communities to the death of Osama bin Laden with reference to the 11 March 2004 terrorist attacks in Madrid was conducted in real-time from 01 May 2011 to 05 May 2011. This internet research sought to analyse the extent to which the death of Osama bin Laden re-awoke understandings of technology, terrorism and counter-terrorism in Spain among online users and communities. In addition, the analysis investigated the further validation of the main conclusions elucidated within this chapter.

## Main Conclusions from the Thesis

The Internet and the Web are Socio-Technical in Nature

The exercise of political, economic and technological control over the development of the internet and the Web results in enhanced communication capabilities, or the propensity to wield influence, for certain actors. This argument was elucidated within the framework of the theory from the field of science and technology studies of technological determinism, by the French sociologist and anthropologist Bruno Latour (Latour, 1988). Latour, amongst others, argued in support of the notion that technology in itself is not simply a physical object. Agency and power with high technology reside within human actors. Other theorists argued in support of Latour’s socio-technical explanation of the development of the internet and the Web such as Wanda Orlikowski (Orlikowski, 2006) who claimed that technology developers and end users influence the final development of the objects.

As humans have agency over the development of these technologies, therefore, scholars of terrorism and the internet such as Gabriel Wiemann (Wiemann, 2006) have postulated that the internet can be used as a force multiplier ‘to launch psychological campaigns, recruit and direct volunteers, raise funds, incite violence and provide training…plan, network, and coordinate attacks’, (Wiemann, 2006: 2). As a result, it was the initial position of this thesis that such technologies be considered as social and cultural spaces that reflect the interactions of numerous daily human activities (Markham, 2008: 9).

As the internet and the Web are socio-technical in nature, the thesis suggested the importance of advancing and utilising the notion that these technologies constitute an entirely new “battleground” for 21st century states of terror (Bobbitt, 2008).

However, it is noteworthy that the findings generated by the research processes have demonstrated that technology has not simply empowered terrorism and counter-terrorism organisations. Over the course of the chapters, it has become apparent that when considering immigration, narratives, cybercrime, communities and public diplomacy in Spain, the results of empowerment due to access to new technology have not been linear, rather they have been uneven. The reason for this can be attributed to Latour’s (1998) assertion, outlined in Chapter One, that technological development is a “socio-technical mess” and that linear development from new technology to clear political communication is not likely to occur.

Engagement with Narratives by Online Communities is not Linear but Complex

As has been presented in earlier chapters, the nature of communication amongst online communities is not a linear process. Narratives are not presented to target audiences on pre-defined media channels and subsequently assimilated. Rather, online communities are exposed to a range of narratives and viewpoints simultaneously and, as a result, engagement with the issues of technology, terrorism and counter-terrorism is not a top-down process but rather a complex, multi-directional process.

This complexity, therefore, makes it difficult to create and disseminate effective narratives for counter-terrorism strategies. This is due to the lack of clarity as to whether target audiences will assimilate such content and meet the strategic communication objectives of the organisation that produced the content when the narrative has been created.

In addition, the issue of complexity raises questions about the trust, credibility and authority of the Spanish Government and other organisations trying to project particular narratives and understandings. The fact that online users widely perceived that the Government had lied about the true course of events relating to 11-M shows the the creator(s) of narratives can become tainted so in the end, narratives from particular sources become unreliable to their intended target audiences.

Online Communities are the “New Intellectuals”, Shaping Discussion and Opinions of Others

An improved understanding of the dynamics of general online behaviour could be incorporated into counter-terrorism programmes in Spain. This understanding could enhance the principles of Spain’s long-running public diplomacy programmes, contributing to shaping attitudes and behaviours with foreign and domestic publics online. Although the Spanish Government is not able to control the interpretations of its key narratives online, by gaining greater influence online and harnessing the propensity of its citizens to participate in a collaborative counter-terrorism programme, it stands a greater chance of lowering instances of general sympathy for terrorist ideologies. The propensity for Spanish citizens to participate in counter-terrorism programmes has been witnessed repeatedly during this thesis, from the mass public demonstrations in the days following the Madrid bombings, to the public displays of empathy and support to other victims of the attacks in the form of online homages.

It is important to analyse and monitor the role played by online communities in the sphere of terrorism in Spain and how they influence the perceptions of those users with a lesser interest in terrorism both online and in the wider world. As indicated in the internet research, such communities are composed of large numbers of people with disparate interests and professional specialties. The internet research suggested that communities may be able to influence terrorism-focused discussions in other communities to such an extent that this may conflate the problems for counter-terrorism agencies in engaging specific individuals and communities online. This was evinced in the way that certain narratives, such as ‘Al-Qaeda will launch repeat attacks if necessary’, permeated the discussions of online communities, instilling a sense of trepidation in online users that Spain might be subject to future attacks.

It appears that online communities are, in many ways, the “new intellectuals” in which online users and communities are ‘testament to the ideological diversity currently available causing many to point to cyberspace as the new market place for ideas…those responsible for the content of websites can be considered the “transmitter of ideas within civil society” and, therefore, fulfil the role of the intellectual’ (Fisher, 2003: 2). Fisher, and the findings of the internet research, support the notion that some online communities actively shape and influence the opinions of key people and organisations involved in counter-terrorism and opinion formers involved in the public discourse on terrorism.

The Creation and Maintenance of Effective Narratives or Myths is Critical in Influencing Online Communities and Terrorism

The notion that terrorist organisations would attempt to assert influence online by shaping the attitudes and behaviours of the wider online population in the hope of gaining sympathy and understanding for their *raison d’être*, was elucidated in early chapters, as a result of the utility of the initial hypothesis, that access to high technology results in increased capabilities for certain actors. However, the premise of the secondary, more nuanced hypothesis, has been argued, which maintains that the maintenance of myths or memes (Blackmore, 1998) that reinforce predefined strategic objectives is the most important element in shaping understandings of the relationships between terrorism, technology and counter-terrorism in Spain (Reinares, 2006).

The reasons for the presence of a secondary, more effective hypothesis can be explained in a number of ways; the first being that in order to attain online influence, it is important to be as visible as possible, something that is not conducive to achieving the strategic operational goals of market state terrorists such as al-Qaeda. Terrorism, as has been written previously, relies on stealth, covertness and surprise, which is not conducive to the general influence of attitudes and behaviours online. Certainly, this viewpoint was elucidated in an interview with the think tank analyst Jamie Bartlett who claimed that “if you’re willing to blow yourself up or other people up, I think it takes more than spending time online, looking at images and talking to people online. You need the face-to-face interaction and more importantly you need the training which you can’t get from the internet.”[[101]](#footnote-101)

In place of the apparent absence of terrorist organisations in the “Visible Web”, however, is the assertion that said organisations have restricted their activities to designated forums and websites where they are free, in relative isolation, to air their views and to convince other members of the merits of their endeavours, to potential members who are already on their way to becoming radicalised (Bobbitt, 2008).

It was also apparent that a number of online users expressed sympathy and understanding with the ideals and objectives of terrorist organisations and thus played an instrumental role in perpetuating the key narratives of such organisations to new networks and communities. It is, therefore, posited that the narratives espoused by terrorist organisations are intrinsically more pervasive, and by implication dangerous insofar as creating fear, than the overt presence of a terrorist organisation online could have been. This phenomenon underscores the importance of curtailing the influence of such narratives by a thorough understanding of online behaviour, in addition to the implementation of adequate tools and methodological processes needed to analyse the social and cultural content emanating from these sites.

The pre-eminence of myths as the preponderant factor in achieving online communication strategies also alludes to the fact that the thesis has moved beyond governmentality as a theoretical framework for explaining the diffusion of power online. Although government actors may exert power over the nature of the development of internet and Web technologies as outlined in Chapter One, the findings from the empirical research have shown that, in reference to the nature of online behaviour related to 11-M, government actors are not influential.

Evidence of the Commensuration of Terrorism with other Issues to make One Dependent Variable is Widespread

There are many examples of commensuration as a social process where online users and communities use the issue of terrorism as a platform to attain influence in their own issue areas. For example, commensuration was prevalent in discussions on immigration in Chapter Four and on issues discussed around the topic of cybercrime in Chapter Six, as online users expressed the sentiment that these issues were the root cause of the terrorism threat in Spain.

The use of commensuration to analyse independent variables, such as immigration and terrorism, and conflate them to form one issue (Espeland & Stevens, 1998) led to the securitisation of immigration, evinced in the implementation of more stringent border controls and securitisation of the discourse of immigration in Spain (Colás, 2010, Sánchez, 2011).

Web 3.0 Could Present an Opportunity for the Formulation of More Effective Counter-terrorism Strategies

With the number of people and devices connected to the internet and the Web set to increase and, *ergo*, the number of social and cultural interactions, it follows that the Spanish Government could revise its online public diplomacy effort, and adopt a strategy that focuses on engagement and interaction with online communities and users to assert a greater degree of influence in the ways their narratives are interpreted.

The findings derived from the internet research process, in particular, highlighted the complex behaviour of certain communities of users that sought to influence the general discussion of terrorism online to benefit their own interests, such as the strongly positive sentiments generated by the General Public community, shown in Chapter Seven, in which users displayed calls to action for members of other communities to unite in support for the victims of 11-M and stand against terrorism. The fact that the online space is composed of various groups seeking to assert their influence on discussions of terrorism and counter-terrorism underscored the ample opportunity that exists for the Spanish Government to create and assert its own influence over discussions about terrorism online by seeking to attain the same level of influence as the most influential users online.

As the internet and the Web are socio-technical in nature, it follows that the same social and cultural space is dominated by collections of narratives that jockey for the attention of online users. This is not to discount the range of long-term beliefs and narratives that already exist in the minds of users that new narratives must compete with. It is, therefore, incumbent upon counter-terrorist organisations to develop compelling narratives and, more importantly attain online influence, if they are to decrease the level of negative commentary and behaviour that is sympathetic to the aims of terrorist organisations. In addition, it follows that a more nuanced and profound understanding of user behaviour on the contemporary Web is imperative if influence is to be attained and the online agency of terrorist organisations is to be diminished.

To achieve this, the Government and other Spanish counter-terrorism agencies could take stock of the examples set by the UK and the US Governments in which their digital public diplomacy efforts have become an intrinsic part of their counter-terrorism strategies. It follows that the internet should not only be used as yet another tool to project a positive image of Spain but as a platform for negotiation, engagement and understanding that will forge long-term relationships with target populations.

Some Official Narratives do not Reach Target Audiences

The revised hypothesis, which was formulated as a result of the analyses of the empirical research, highlighted the importance of developing a comprehensive understanding of the behaviour of users online, before constructing and disseminating influential narratives amongst online users and communities.

The behaviour of online users became the focus of the internet research, particularly the ways in which online communities act and react to each other and the interpretation of core narratives by online users. It was concluded that the Spanish Government and its counter-terrorism organisations at times failed to generate positive sentiment of their key narratives by citizens and diaspora communities. This occurrence was witnessed most prominently in the internet research and the preponderance of the ‘Government lies about 11-M’narrative during the entire date range. In addition, the interviews conducted yielded similar conclusions, particularly the following comment from the former Head of Communications and Institutional Relations for the Congreso de los Diputatados, Maria Llorach, that the core narratives created and delivered by the Spanish Government are not reaching target audiences:

“[The Government] doesn’t know how to communicate correctly. They are utilising strategies from the 20th century when we are now in the 21st century and everything is different. Apart from this, there are very few people who are really prepared to design these strategies because they all have the mentality of someone in the 20th century…when the Web arrived many people within the Government said, what do we do with the Web? Because we don’t know how to do it. They know how to engage with the press, but they don’t consider [digital communications] because it has been perceived it as if it was an alien monster, they do not know how to use it.”[[102]](#footnote-102)

In the internet research, widespread misinterpretation of Government narratives occurred in spite of the proclivity of some online users and communities to strive to assist counter-terrorism organisations in preventing more attacks. The responses from the participants in the interviews conducted, and from the internet research indicate, therefore, that the official narratives from the Government and other counter-terrorism agencies are not being interpreted positively by online users.

Maria Llorach’s previous comments also highlighted the Government’s lack of involvement with internet and Web technologies as part of their counter-terrorism strategies. The Government’s apparent inability or unwillingness to engage with internet and Web technologies to influence understandings on technology, terrorism and counter-terrorism could be a contributing factor to the high volume of negative commentary directed at it. If we are to accept this conclusion, however, the corollary is that the volume of negative sentiment will increase significantly with the introduction of Web 3.0 technologies. The author contends that the presence of Web 3.0 technologies and the increase in social interactions will lead to the development of Terrorism 3.0 which, as outlined previously, will render online engagement with terrorism and counter-terrorism in Spain more mobile, pervasive and participatory as the barriers to entry for engagement in these issues lowers considerably. As such, the practice of influencing online conversation according to the strategic objectives of organisations will be more difficult. The Government could leverage this increasingly prescient issue to its advantage by continuing to monitor and analyse closely online behaviour, and using the conclusions to implement well-targeted public diplomacy campaigns both online and in the real-world.

## Internet Research on the 11-M Attacks: Spanish Reaction to the Death of Osama Bin Laden

This empirical research analysed the nature of online Spanish-language discussion about the death of the leader of al-Qaeda, Osama bin Laden on 02 May 2011, while making reference to the Madrid bombings of 11 March 2004. The analysis enhances the internet research conducted in the previous chapters which interrogated the ways in which online users discussed terrorism and counter-terrorism in relation to the 11-M bombings.

The date range of the analysis was established over five days from 01 May to 05 May 2011 and the research was conducted in real-time. The number of relevant online items of content over the five-day period was 137. Data was aggregated from a range of social media sources including weblogs, micromedia[[103]](#footnote-103), forums, websites and social networking sites using the methodology described in detail in Chapter Three. Content was accumulated manually in the public domain during the date range to support the content aggregated by the proprietary software. Search engines were employed by the author including Google Blog Search and Group Search, Board Reader, IceRocket, Big Boards and Blogdigger.

Online content was aggregated using a range of keywords associated with the death of Osama bin Laden and making reference to the 11 March 2004 terrorist attacks. The subsequent content analysis allowed the data to be segmented into the following categories:

**Table Seven: Description of Segmentations Used for Empirical Analysis**

|  |  |
| --- | --- |
| **Segmentation** | **Description** |
| * Community | * Online content was categorised by community group based on the principal issue focus of the online portal from which the content was sourced. |
| * Most Frequent Narrative | * The most frequent narrative category refers to the principal narrative contained within a specific post. It was critical to include this category to understand how the principal motivations of online communities and users evolved over time. |
| * Narrative Source | * The narrative source refers to the community that originated the most frequent message in question |
| * Sentiment | * A five-point sentiment measurement scale was created that reflected the polarity of feelings online. The scale was comprised of strongly negative, slightly negative, neutral, slightly positive and strongly positive measures. In order to limit the propensity for bias, each post was analysed in individual context units. The totality of the sentiment ratings for a particular post was then tallied to yield a final sentiment score. |
| * Media Type | * Each online portal was assigned a specific media type. The media types were categorised as forums, blogs or websites. |
| * Issue | * The issue category refers to the principal focus of a particular post or discussion thread. |

Source: Lawrence Ampofo

### Volume of Content

The internet research process revealed that the main volume of content relating to discussion of the death of Osama bin Laden with reference to the 11 March 2004 terrorist attacks occurred on the 02 May 2011, the day that news of his death was announced by mainstream media organisations. Figure Thirty demonstrates that the volume of discussion declined steadily after 02 May 2011 until 04 May 2011, by which time levels of content had fallen to 20 relevant posts.

Figure Thirty: Volume of Online Content Over Time

Source: Lawrence Ampofo N=137

### Key Narrative Analysis

As this research process was conducted in real-time, the range of key narratives was analysed as they emerged. As outlined in Chapter Three, the process of analysing core narratives as they emerge is a different process to the internet research process used in the previous chapters, in which the key narratives were defined before the research process was undertaken. Conducting a research process in real-time thus required the author to aggregate, categorise and analyse the most salient content immediately. The internet research that was the focus of chapters Four, Five, Six and Seven was conducted retrospectively and, therefore, mandated that the author spend more time identifying which narratives should be analysed.

It is significant that online reaction linking the death of Osama bin Laden to the 11 March 2004 attacks was not greater in terms of volume of content. This indicates that Spanish language online users, in general, did not commensurate the two issues in spite of the fact that the issue of the death of Osama bin Laden is so strongly connected with international terrorism. However, the reason for this is unclear. A table of the key narratives is presented below:

**Table Eight: Key Emergent Narratives on the Death of Osama Bin Laden with Reference to 11-M**

|  |
| --- |
| **Key Emergent Narratives** |
| * Government lies about 11-M |
| * No proof of al-Qaeda involvement in 11-M |
| * Assassination of Bin Laden and GAL are similar |
| * Al-Qaeda was responsible for 11-M attacks not ETA |
| * Retaliation |
| * Justice for 11-M victims |
| * Death is justice to the 11-M victims |
| * Bin Laden death is not applauded |

Source: Lawrence Ampofo

### Narrative Source

In spite of the low volume of online discussion relating to the independent variables, Figure Thirty-One demonstrates that the general volume of key narratives emanated from the General Public. Once again, narratives stemming from the Spanish Government ranked considerably lower than those of the General Public, demonstrating that the Spanish Government had still not established a method for attaining prominence amongst online communities for its core narratives. This is noteworthy, as core narratives from other online communities can influence the attitudes and behaviours of many thousands of users online. This phenomenon was supported in the research findings presented in chapters Four, Five, Six and Seven, in which online Government narratives appeared not to resonate with other online communities.

Figure Thirty-One: Total Volume of Content by Narrative Source

Source: Lawrence Ampofo N=137

The main element responsible for the highest instances of discussion related to the death of Osama bin Laden with reference to the 2004 Madrid bombings, came in the form of numerous responses to comments from the President of the Community of Madrid, Esperanza Aguirre, a member of the Partido Popular, who claimed that Osama bin Laden was yet to admit responsibility for the Madrid bombings. She claimed that Bin Laden:

‘Never admitted responsibility for Madrid. He admitted responsibility for Indonesia, London, the attack on Casablanca and, of course, the Twin Towers. However, he has never admitted responsibility for Madrid’ (*El Plural*, 2011: 1)[[104]](#footnote-104)

The response to Aguirre’s comments are discussed in the following section.

### Sentiment Analysis

The interactions following Aguirre’s comments, as will be outlined below, were decidedly passionate as online users and communities responded to her comments within their networks. Figure Thirty-Two below details the overall volume of content in relation to the sentiment of discussion amongst online users and communities.

Figure Thirty-Two: Sentiment Over Time

Source: Lawrence Ampofo N=137

Figure Thirty-Three illustrates that strongly negative coverage was the dominant sentiment amongst online users when discussing the death of Osama Bin Laden with reference to the 2004 Madrid attacks. It is interesting to note at this point that some online users commensurated the two topics, as they believed that Bin Laden’s death was a demonstration of retribution for the Madrid bombings. However, there were other users and online communities who used the topic as an excuse to engage with other terrorism-focused commentators about the Madrid bombings. This will be discussed in greater detail below.

As outlined previously, comments from Esperanza Aguirre generated widespread commentary, the majority of which was strongly negative in nature. Some users claimed that Aguirre’s comments were incorrect and insensitive to the memories of the 11 March 2004 victims such as this user on the *Ventanas del Falcón* blog who stated:

‘It is necessary to state clearly that the attack on 11-M was claimed by Al-Qaeda and was *even reported by El Mundo*. Here is an article showing that Bin Laden *implicitly claimed responsibility for the 11-M attacks in Madrid* in a personal interview’[[105]](#footnote-105) (*Ventanas del Falcón*, 2011: 1 emphasis in original).

Other sources, such as the influential mainstream news source *El País* also disagreed with Aguirre’s comments but simultaneously emphasised other elements of Aguirre’s speech, such as her claim that Bin Laden’s death was a positive step in global counter-terrorism:

‘In [contrast] to Aguirre’s opinion, Al Qaeda has claimed responsibility for the attacks on various occasions, which ended the lives of 192 people in 2004…Aguirre, who has referred to Bin Laden as the “assassin of more than 2,300 innocent people”, commented…“this event reflects a step forward in the fight against terrorism”’[[106]](#footnote-106) (*El País*, 2011: 1).

Positive commentary was of a comparatively low level in relation to the dominant levels of negative commentary. However, a selection of commentators expressed happiness that Osama bin Laden had been killed as it meant, in their opinion, that the world was more secure and that justice had been meted out to the victims of the 11 March attacks. One such commentator, the personal blogger David Gerbolés, claimed ‘[t]his Monday, we awoke to the news of the death of Osama Bin Laden, and the [person] most responsible for the terrorist attacks of 11-S and 11-M…I am profoundly happy that this event has occurred’[[107]](#footnote-107) (*Mi Punto de Vista*, 2011).

### Key Narrative Analysis by Sentiment

In spite of the fact that discussion on the topics was polarised in terms of sentiment, the internet research also revealed a wide range of narratives that formed the focus of discussion online. The chart below demonstrates the most prominent narratives to emerge from analysis of online discussion by sentiment.

Figure Thirty-Three: Most Frequent Narratives by Sentiment

Source: Lawrence Ampofo N=137

Figure Thirty-Three emphasises the prominence of the narrative ‘Government lies about 11m’. The prominence of this narrative is similar to that evinced in the retrospective internet research findings in chapters Four, Five, Six and Seven. It can be inferred that the death of Osama Bin Laden provoked or renewed negative sentiments within a large proportion of users that the Spanish Government had still not revealed the truth about the 11 March attacks, which they believe they had a right to know. Such statements included conspiracy theories. One such example of this came from the activist blog *Escolar* which claimed that the death of bin Laden had ‘opened up the debate over…the conspiracy of 11M’. According to one commentator:

‘Did Aznar organise [11-M] to attribute it to ETA in order to win, by absolute majority, the General Election that he was going to lose?’[[108]](#footnote-108) (*Escolar*, 2011)

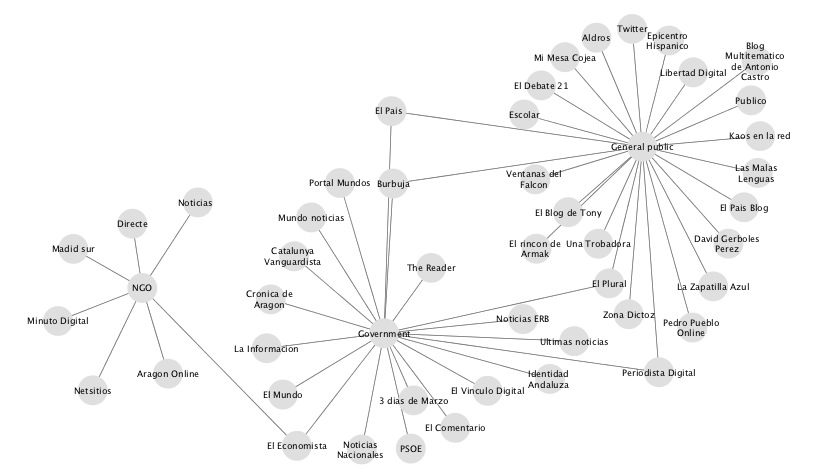
In addition to the previous quotation, the content of Figure Thirty-Three underscores the sentiment of some users regarding the Government’s perceived continued inability to influence the nature of discussion concerning the 11 March attacks and the subsequent public investigation. Such analysis of online behaviour may have offered the Spanish Government at least some opportunity to exert greater influence over the ways in which core narratives are perceived by the general public. That said, it had a credibility problem given the widespread understanding that it failed to offer an adequate explanation of the events surrounding 11-M. This is indicative of the ways in which narratives can become entrenched and hard to shift.

Furthermore, there was a strong undercurrent of fear in discussions amongst online users that the death of Osama bin Laden would provoke other terrorist organisations, or those inspired by al-Qaeda, to perpetrate more attacks against the Spanish populace. An example of such commentary appeared on the blog *La Crónica* *de Aragón* in which it was reported that the Government had raised the national alert level to Two as a result of the fear of reprisals following the death of Osama bin Laden.[[109]](#footnote-109) Another example of the expression of fear amongst online users and communities is demonstrated in a post to the *Una Trobadora del Segle XXI* blog in which the commentator argued that other al-Qaeda members were capable of continuing operations and fulfilling the strategic objectives of the organisation without Osama bin Laden. It is for this reason, they argued, that the death of Bin Laden should not be celebrated but, rather, should be greeted with trepidation lest his followers in retaliation perpetrate subsequent attacks.[[110]](#footnote-110) Such a statement indicates an understanding that al-Qaeda continues to be capable of attacks in Spain.

### Network Analysis

Figure Thirty-Four shows the extant relationships inherent within discussions of the death of Osama bin Laden with reference to the Madrid terrorist attacks of 11 March 2004. A detailed description of the methodology for network analysis can be found in Chapter Three.

Figure Thirty-Four: Network Analysis of Communities Involved in Discussion of the Death of Osama Bin Laden with Reference to 11-M



Source: Lawrence Ampofo N=137

The network analysis from 02 May 2011 to 05 May 2011 demonstrates that online communities had fractured into eminently discernible clusters that were indelibly linked to one another. The NGO cluster of sources is positioned on the fringes of online discussion, and was tenuously linked to government sources of information. This indicates the lack of activity by NGOs during the period of analysis, with only six sources cited as part of the analysis, but also the link between NGOs and Government sources of information for engagement within this issue. The reason for NGOs’ tendency to link to government sources related to a series of articles from *El Economista* in which comments from the Asociación de las Victimas de Terrorismo supporting the government’s position on the death of Osama bin Laden were recorded (*El Economista*, 2011: 1).

The cluster of Government narratives was strongly linked to those of the General Public, in contrast to that of the Government to the NGO cluster, via mainstream media publications which published narratives in articles from both communities. However, it is noticeable that the General Public community did not link at this time with the NGO community in discussions on this topic. While the reason for this is unclear, it suggests that the General Public may not be picking up narratives from NGOs.

It is also noticeable that Government narratives are central to all discourse online concerning the death of Osama bin Laden with reference to the terrorist attacks of 11 March 2004. However, when interpreted in tandem with a sentiment analysis of the narratives, both statistically and over time, it is clear that these narratives were not interpreted positively. This crucial finding underscores the importance of attaining influence online in order to manage the perception of narratives in a way that supports strategic objectives. It also underscores that online communication, in particular the delivery of key narratives, is not a top-down phenomenon. Rather, it is a multi-directional phenomenon in which online users are exposed to a variety of viewpoints at any one time, as the public connected to Government narratives but did not accept them.

## Final Analysis

The empirical research conducted has provided valuable information that helped to shape the findings contained within this thesis and provide a more nuanced hypothesis that would justify additional study. This was illustrated in the above analysis examining the understandings that exist concerning the relationships between technology, terrorism and counter-terrorism within discussions of the death of Osama bin Laden.

The high volume of content from general online users and the broad collection of narratives generated emphasise that a large base of online users exists who are extremely active and can be engaged by a comprehensive online communications strategy that develops positive, long-term relationships with them. This is important because as digital diplomacy programmes in other countries such as the UK and the US have shown, if strong relationships can be cultivated amongst online users by governments, then they are more likely to be perceived as credible counter-terrorism communication strategies. In addition, such communications strategies would ensure that in an age of many-to-many communication, counter-terrorism organisations would deliver core narratives to a more targeted group of “new intellectuals” who could ensure that the content of the narratives was delivered to members of their networks.

Not possessing a clear understanding of the identity of important audiences (journalists, activists and other potential conduits or “influencers”, as well as publics) when conducting important online communication strategies, and a clear strategy on how best to engage them, potentially presents opportunities for other actors to co-opt online discussions and influence the opinions of others.

Different types of emotion were exhibited by online communities, which at times were comprised of comfort, catharsis and support from wider online group members as well as feelings of reproach and frustration. This is significant because an opportunity was presented to the Spanish Government to positively engage with citizens who, for over six years, have called for the presence of a representative to engage with them online. It is clear that an influential representative from the Government could have actively engaged with people to show the Government’s support to the public in a time of national crisis.

The internet research of the death of Osama bin Laden has shown that it is imperative, at a time when the internet and the Web are undergoing significant changes to their technological architecture which will in turn lead to new and innovative ways of using them, that a more complete understanding of online behaviour is obtained in this new context of Terrorism 3.0. As an increasing amount of people become connected to the Web with access to a host of new services, it is imperative that measures are taken to understand how people behave and the optimal ways of engaging with them.

As seen, it is critical that any attempt to engage with online users and communities implements an engagement strategy supported with a comprehensive influence attainment strategy. The purpose of this strategy would not be to simply engage with every online user or community that comments on this particular issue. Rather, it is important that counter-terrorist practitioners factor into their strategies an overarching plan of the most optimal ways of attaining and monitoring online influence.

In addition, over the course of this thesis, the author has developed a set of recommendations for further research into terrorism and counter-terrorism that build upon the conclusions that emerged and highlight the following opportunities:

Further Multilingual Internet Research

An increased level of insight would be revealed if cross-cultural or cross-lingual research into understandings of technology, terrorism and counter-terrorism could be conducted. This would help interpret the ways different cultures perceive the dependent variables and could help counter-terrorism practitioners formulate more effective strategies. Such internet research needs to be robust to provide accurate conclusions, and could dovetail well with traditional research methods (focus groups, surveys, interviews) to become part of other research programmes.

Internet Research into the Spanish Diaspora

It could also prove useful to conduct research into the opinions of Spanish diaspora communities on their understandings of the research question. This is particularly relevant as very few online users revealed their true identities. However, if research were to be conducted on the opinions of Spanish diaspora communities, it could provide the Government with a more holistic picture on the sentiments of its citizens and other Spanish nationals residing abroad, while informing efforts to refine engagement strategies.

An Increased Number of Online Data Points, as Web 3.0 Technologies become More Widely Available

Finally, it would be useful to conduct the internet research with an increased number of data points in order to gain a further level of insight into the findings. For example, it would prove useful to include additional data on gender, geographic location, and other social media forms such as images, video and audio. The opportunity to aggregate and analyse a wide variety of information will be increasingly available with the introduction of Web 3.0 technologies and services such as Big Data and the Semantic Web. It is also likely to be more cost-effective to gather this insight but, as mentioned earlier, the introduction of Web 3.0 poses considerable opportunities or considerable problems for counter-terrorism practitioners if the nature of the behaviour of its users is not understood.

If such research were conducted then it would provide a great deal of insight into terrorism, counter-terrorism and the behaviour of online and real-world communities. Indeed, the emergence of Terrorism 3.0 mandates that attainment of this insight is of critical importance in countering terrorism in Spain and understanding the optimal methods of engaging with citizens in the event of terrorist attacks. The benefits to be gained from a detailed understanding of Terrorism 3.0 could be considerable for counter-terrorism practitioners. It suggests a new way of conducting counter-terrorism by placing influence and socio-technical strategies at its core and as complementary tools to the existing technological and database-driven solutions in Spain’s security strategy.

# **Appendix One: List of Interviewees**

**Felix Arteaga** – Head Researcher in Security and Defence, Real Instituto Elcano. Telephone interview, 04 August 2010

**Jamie Barlett** – Head of Violence and Extremism, DEMOS. London, 28 April 2011.

**Stewart Bertram** – Cyber Intelligence Analyst, VeriSign. London, 09 September 2010

**Ali Fisher** – Chief Executive Officer, Mappa Mundi Consulting, Telephone Interview, 05 July 2010.

**Carlos Fragoso** – Board of Directors, Centre de Seguretat de la Informació de Catalunya (CESICAT). Email interview 8 August 2010.

**Robert Imre** – Deputy Head of Politics and International Relations. Newcastle Business School. Telephone Interview, 21 July 2010.

**Javier Jordán** – Professor of the Department of Political Science and Administration, University of Granada. Telephone Interview, 24 November 2010

**Maria Llorach** – Former Head of Communications and Institutional Relations, Congreso de los Diputados. Barcelona, 20 January 2011

**Jonathan Githens-Mazer** – Co-Director, European Muslim Research Centre (EMRC), Co-Director, Exeter Centre for Ethno-Political Studies (EXCEPS), Senior Lecturer, Institute of Arab and Islamic Studies (IAIS). Telephone Interview, 12 November 2010.

**José María López-Navarro** – Information Officer, Public Diplomacy Unit, North Atlantic Treaty Organization. Wilton Park, 08 June 2010.

**Nicolas de Pedro** – Researcher, CIDOB. Barcelona, 09 November 2010.

**Manuel Pérez** – Deputy Head Religious Diversity Department, UNESCO Centre of Catalonia, Barcelona, 05 July 2010, Barcelona, Spain.

**John Postill** – Senior Lecturer, Sheffield Hallam University. Barcelona, 02 August 2010.

Head of Research – United Kingdom Security Services, Telephone Interview, 15 September 2010

**Alfred Rolington** – Chief Executive Officer, Oxford Analytica. Telephone Interview, 10 June 2011

**Elena Sánchez** – Researcher, CIDOB. Barcelona, 09 December 2010.

**Manuel Torres Soriano** – Professor of Political Science and Administration, Universidad Pablo de Olavide de Sevilla. Telephone Interview, 24 November 2010

**Giles Tremlett** – Spain Correspondent, *The Guardian*. Telephone Interview, 12 November 2010.

**Justin Webster** – Television Producer. Telephone Interview, 29 November 2010

# **Appendix Two: Detailed Methodology for Semi-Structured Interviews**

It was decided that semi-structured interviews would be conducted to gather data from academic and industry experts in the fields of technology, terrorism and counter-terrorism.[[111]](#footnote-111) These interviews were elected over structured interviews because they provided greater opportunity for the interviewees to speak more freely about the topic in question in relation to their areas of expertise.

In addition, the use of semi-structured interviews was chosen as the author is able to conduct such interviews in the Spanish language as well as English. It was decided that the purpose of the semi-structured interviews would be to compliment the findings from the internet research and provide greater qualitative richness.[[112]](#footnote-112)

The interview questions were all open-ended questions, designed to elicit as much information as possible from the interviewee and were translated into Spanish from English. As such, the questions were segmented into three categories: academia, business/commercial and government and are listed below in English:

## Questionnaires Used

### Government

1: To what extent does government action influence terrorist activity?

2: Has the introduction of technology influenced the activity of terrorists? If so, how?

3: What methods do governments use to monitor the activities of terrorists or would be terrorists?

4: Is the government happy to work with ISPs? Or is it developing its own technologies in line with the policies it is planning to enact?

5: What influences the development of technology and counter-terrorism policies?

6: Do governments have a sense of the sentiment of public discourse towards technology and terrorism?

7: Does the government see the development of technology and the propagation of terrorism as mutually exclusive?

8: If the government does see technology playing a role in the propagation of terrorism, how does it see the role of Web 3.0 playing its part specifically?

### Academia

1: Are there influences of terrorism in Spain other than the impact felt by the internet?

2: Has the government commissioned any research into terrorism and the Web?

3: What are organisations such as technology companies and Governments afraid of?

4: What counts as terrorism in Spain in the digital age?

5: Do you have a position on the methodologies used to analyse terrorism? E.g. data mining, qualitative methodologies, etc.?

### Business

1: Are the problems faced by Spain uniquely Spanish? Or do you think they are a global phenomenon?

2: Are ISPs happy to work with government?

3: What technologies are you using to track the activities of terrorists?

* + What technologies are being used in different countries?
  + Is foreign language content analysed? Or do you only analyse content in Spanish?

4:Do you perceive any noticeable differences in nefarious behaviour on the Web following the introduction of Web 3.0 technologies?

5: Do you think that technology is the mobilising element in contemporary terrorist activity?

6: In your opinion, how can the development of technology be directed towards mitigating terrorist acts?

## Challenges to the Conduct of the Semi-structured Interviews

A range of obstacles was encountered during the fieldwork, which made the effective conduct of the semi-structured interviews more challenging. The most prominent obstacle manifested itself in the proclivity of people to decline the invitation for an interview. This occurred in the case of many eminent academics and high-ranking journalists, Government officials and media technology experts who felt that the topic of the thesis was outside their areas of expertise. This phenomenon was confirmed by one of the interviewees who claimed that very few people in Spain are qualified to comment with authority about the topic in question outside the security services.[[113]](#footnote-113)

In addition, it was discovered, in an interview with John Postill of Sheffield Hallam University, that the issue of terrorism is seldom openly discussed in Spain. The author, therefore, resolved to overcome this problem by re-phrasing the introductory email sent to the interviewees to reflect an emphasis on *security* in Spain and not terrorism and counter-terrorism. This change in tactic was more successful and resulted in more interviews with Spanish experts.

The questions were translated into Spanish for Spanish nationals and kept in English for English speakers. They were conducted via a variety of means. Some interviews were conducted by email, some by telephone and some in person at a neutral location.

The interviews were recorded on a digital voice recorder and transcribed manually using a word processing software program. At the request of one interviewee, his name has been anonymised due to his senior position in the UK security services. In addition, due to his role as the Spain Correspondent for *The Guardian*, Giles Tremlett requested that he approve the inclusion of his comments within the thesis.

# **Appendix Three: Glossary of Terms**

**Actor Network Theory:** In his 2004 chapter for Hepp, A. et al (2004), Nick Couldry defines Actor Network Theory as a ‘highly influential account within the sociology of science that seeks to explain social order not through an essentialised notion of “the social” but through the networks of connections between human agents, technologies and objects. Entities (whether human or non-human) within those networks acquire power through the number, extensiveness and stability of the connections routed through them, and through nothing else.’ It is Couldry’s definition that will be used as the basis of this thesis.

**Blogs**: Weblogs or blogs are websites that allow its users to create and publish a variety of computer content such as video, audio, text and images (Kolari et al. 2006).

**Bulletin Boards**: Bulletin boards are an older form of social media in which users submit posts or bulletins to topics of interest (Rafaeli, 1986). Bulletin boards have all but been superseded by discussion forums.

**Cloud Computing**: This thesis will take as its definition of cloud computing that offered by the US National Institute of Standards and Technology (NIST) ‘Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction’ (NIST, 2011: 6).

**Crisis Mapping**: Crisis mapping is a form of collaborative computing where individual users upload information to a central site in the case of an emergency. Such information can include images of the ground situation or GPS locations of survivors. The most prominent crisis mapping site is the Africa-based Ushahidi (Meier, 2008).

**Distributed Computing**: Distributed computing is a form of computing where many computers in various locations can be accessed by users to perform tasks (Cummings & Huskamp, 2005).

**Functioning Core / Non-Integrating Gap**: The term Functioning Core, which was developed by Thomas P.M. Barnett, is outlined in his thesis *The Pentagon’s New Map* and is defined thusly: ‘[t]hose parts of the world that are actively integrating their national economies into a global economy and that adhere to globalization’s emerging security rule set. The Functioning Core at present consists of North America, Europe both “old” and “new,” Russia, Japan and South Korea, China (although the interior far less so), India (in a pockmarked sense), Australia and New Zealand, South Africa, and the ABCs of South America (Argentina, Brazil, and Chile). That is roughly 4 billion out of a global population of more than 6 billion’ (Barnett, 2011: 1). In addition, he added a definition for those countries which lie outside the Functioning Core which he termed the non-Integrating Gap. Barnett defined these countries thusly, ‘Regions of the world that are largely disconnected from the global economy and the rule sets that define its stability. Today, the Non-Integrated Gap is made up of the Caribbean Rim, Andean South America, virtually all of Africa, the Caucasus, Central Asia, the Middle East, and most of the South-East Asian littoral. These regions constitute globalization’s “ozone hole,” where connectivity remains thin or absent in far too many cases. Of course, each region contains some countries that are very Core-like in their attributes (just as there are Gap-like pockets throughout the Core defined primarily by poverty), but these are like mansions in an otherwise seedy neighborhood, and as such are trapped by these larger Gap-defining circumstances’ (Barnett, 2011: 1).

**Identity Theft**: Identity theft is the term given to the unsanctioned use of one person’s personal details by another person for their own purposes, according to the Identity Theft in the UK Blog. (2010). Identity Theft is on the Rise in the UK [online]. Available at <<http://id-theft-uk.blogspot.com/2010/02/identity-theft-is-on-rise-in-uk.html>> [Accessed 01 August 2011].

**Information Terrorism**: Information terrorism is a concept developed by the scholars Post, Ruby and Shaw (2000) to describe acts of terrorism which use information technology to ensure the successful completion of their strategic objectives.

**Instant Messaging**: Instant messaging is a form of computer mediated communication in which a software program uses internet relay chat to perform real-time communication with users. Early proponents of this include Microsoft Messenger and ICQ.

**Internet of Things**: This thesis takes as its definition of the Internet of Things the International Telecommunications Union’s definition as the connection of devices and objects to the internet and the Web in which ‘[c]onnections will multiply and create an entirely new dynamic network of networks – an internet of things’ (ITU, 2005: 8).

**Internet Penetration**: The term internet penetrationrefers to the definition offered by the Organisation for Economic Development (OECD) for both fixed line and wireless penetration. The number of Digital Subscriber Lines (DSL) offering internet connectivity at speeds of at least 256 kilobytes are counted for fixed line DSL lines while wireless penetration is measured by the number of subscriptions to services of at least 256 kilobytes. Organisation for Economic Development, (2011). Broadband and Telecom. *Organisation for Economic Development Directorate for Science, Technology and Industry*. [online] Available from <<http://www.oecd.org/document/46/0,3746,en_2649_34225_39575598_1_1_1_1,00.html>> [Accessed 13 June 2011].

**Market State Terror**: Market State Terror is a term defined by the scholar Philip Bobbitt (2008). He contends that market state terror is a direct reaction to the market state which he claimed ‘does not see the State as more than a minimal provider or redistributor. Whereas the nation state justified itself as an instrument to serve the welfare of the people (the nation), the market state exists to maximize the opportunities [of its citizens]. Such a state depends on the international capital markets and, to a lesser degree, on the modern multinational business network [including the news media and NGOs]…in preference to management by national or transnational political bodies.’ Market state terror by extension is ‘just as global, networked, decentralised, and devolved and relies just as much on outsourcing and incentivizing as the market state. It does not depend upon state sponsorship; indeed, in some cases it would appear that al-Qaeda had more influence over the government in whose jurisdiction it worked than did that government over it’ (Bobbitt, 2008: 42).

**Micromedia / Microblog**: Micromedia is the name given to social media content that is pithy and condensed. Examples of this include the status updates on the social networking site Facebook and LinkedIn. Another prominent example of micromedia is Twitter. Users of this service post updates to their individual profile of no more than 140 characters (Owyang, 2007).

**Moore’s Law**: Moore’s Law refers to a prediction made by the co-founder of the semiconductor company Intel that ‘transistor density on integrated circuits doubles about every two years’ enabling the increasing computational power of microprocessors used in personal computers. Intel, (2005). Moore’s Law: Raising the Bar. Intel Corporation. [online] Available at <<http://download.intel.com/museum/Moores_Law/Printed_Materials/Moores_Law_Backgrounder.pdf>> [Accessed 19 June 2011].

**Natural Language Processing**: NLP is the term given to software programs that attempt to comprehend items of text in natural language and not as structured forms. This type of software seeks to understand the complexities of language such as slang and sarcasm for example.

**Net Neutrality**: Internet neutrality refers to the notion that online users are free to use any internet application without interference from internet service providers (Save the Internet Coalition, 2011).

**Open Source Software**: Open source software is the definition given to software whose source code is available for developers to work with. According to the Open Source Initiative, the term can be defined as any software that adheres to the following code: free redistribution, access to the source code, permission to allow modifications and alterations, if patches are required then only the redistribution of the modified source code is permitted, the software cannot discriminate against any person or group of persons, no discrimination against the industry of use is permitted, the software must not restrict other software, and the software must be technology neutral. (Open Source Initiative, 2011).

**Phishing**: Phishing is the name given to a criminal practice that involves criminals posing as a trustworthy source with the intent of defrauding people of either money or information. (2011). The Phishing Guide. Technical Info [online]. Available at <<http://www.technicalinfo.net/papers/Phishing.html>> [Accessed 01 August 2011].

**Semantic Web**: The Semantic Web is a different version of the World Wide Web in which software protocols are developed in order to make content on the Web more accessible by other services such as search engines and social networks. This thesis will take as its overarching definition of the Web the following from the WC3 Consortium ‘[t]he Semantic Web is the extension of the World Wide Web that enables people to share content beyond the boundaries of applications and websites. It has been described in rather different ways: as a utopic vision, as a web of data, or merely as a natural paradigm shift in our daily use of the Web. Most of all, the Semantic Web has inspired and engaged many people to create innovative semantic technologies and applications’ (WC3.org, 2011: 1).

**Source Code**: the thesis will take as its explanation of source code the definition offered by the Linux Information Project as ‘the version of [software](http://www.linfo.org/software.html) as it is originally written (i.e., typed into a computer) by a human in [plain text](http://www.linfo.org/plain_text.html) (i.e., human readable [alpha](http://www.linfo.org/alphabet.html)numeric [characters](http://www.linfo.org/character.html))’ (Linux Information Project, 2011: 1).

**Tethered Appliances**: Zittrain (2007) uses the term *tethered appliances* in which he claims that devices such as iPods, iPhones and PlayStations, can only be modified by the makers of the appliance. This is in contrast to the scope of creativity possible on the internet and the Web. Zittrain claims that the ‘shift to tethered appliances and locked-down PCs will have a ripple effect on long-standing cyberlaw problems, many of which are tugs-of-war between individuals with a real or perceived injury from online activity and those who wish to operate as freely as possible in cyberspace…A shift to tethered appliances also entails a sea change in the regulability of the Internet. With tethered appliances, the dangers of excess come not from rogue third- party code, but from the much more predictable interventions by regulators into the devices themselves, and in turn into the ways that people can use the appliances… It invites regulatory intervention that disrupts a wise equilibrium that depends upon regulators acting with a light touch, as they traditionally have done within liberal societies.’ (Zittrain, 2007: 102).

**Transit Country**: A Transit Country is the name given to a country that is perceived to act as transit points into Europe for illegal immigrants from other countries. Morocco, for example, is seen as just such a transit country for illegal immigration into Spain (Düvell, 2007).

**Top Level Domains**: Top level domains are the country domains denoted by the Internet Corporation for Assigned Names and Numbers such as .com, .co.uk, .fr.

**User Generated Content**: User generated content (UGC) is used to denote computer users who create computer-readable content (Hetcher, 2007).

**Visible Web**: The Visible Web is the name given to the pages of the Web that have been indexed by commercial search engines and are therefore searchable. The converse of the Visible Web is the Invisible Web or Deep Web which contains a vast amount of web pages that have not yet been indexed by commercial search engines (Sherman & Price, 2002).

# **Bibliography**

(1999). Code of Ethics and Policies and Procedures of the ASA Committee on Professional Ethics. *American Sociological Association*.

(2001). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. *Senate and House of Representatives of the United States of America*.

(2002). ETA Según el Nacionalismo Catalán. *Bye Bye Spain* [online]. Available at <[http://nacionalismo.blogs.com/byebyespain/2007/06/eta\_segn\_el\_nac.html>](http://nacionalismo.blogs.com/byebyespain/2007/06/eta_segn_el_nac.html%20) [Accessed 24 March 2011].

(2004). Con las Victimas para Derrotar el Terrorismo. *Aika*. [online]. Available at <<http://puchuaika.blogspot.com/2004/03/con-las-victimas-para-derrotar-el.html>> [Accessed 01 February 2011].

(2004). Masacre en Madrid. *El Mundo* [online]. Available at <<http://www.elmundo.es/elmundo/2004/03/11/espana/1078988734.html>> [Accessed 19 July 2011).

(2004). Integrismo Islámico en España. *Militar* [online]. Available at < <http://www.militar.org.ua/foro/integrismo-islamico-en-espana-t6386.html>> [Accessed 01 February 2011].

(2005). Assembly of Western European Union. *The Interparliamentary European Security and Defence Assembly*, June 2005.

(2005). ¿Cómo es España después del 11-M? *BBC Mundo* [online]. Available at <http://news.bbc.co.uk/hi/spanish/forums/newsid_4336000/4336173.stm>> [Accessed 01 February 2011].

(2005). El Espejo de Madrid. *Es.charla.actualidad* [online]. Available at <http://groups.google.com/group/es.charla.actualidad/browse_thread/thread/fa085e57851a3e8b/962995989791975a?q=11-m+OR+11m+colaboracion+internacional&lnk=ol&>> [Accessed 01 February 2011].

(2005). España envía a expertos en terrorismo islámico a Londres *20 Minutos*. [online]. Available at <<http://www.20minutos.es/noticia/37428/0/LONDRES/ESPANA/EXPERTOS/>> [Accessed 01 February 2011].

(2005). Evaluation of the Public Diplomacy Program of Foreign Affairs Canada. *Foreign Affairs and International Trade Canada* [online]. Available at <<http://www.international.gc.ca/about-a_propos/oig-big/2005/evaluation/diplomacy_program-programme_diplomatie.aspx?lang=eng>> [Accessed 21 January 2011].

(2005). False Freedom: Online Censorship in the Middle East, *Human Rights Watch*, Vol. 17, No. 10 [online], Available at: <<http://www.hrw.org/reports/2005/mena1105/>> [Accessed 13 November 2008].

(2005). International Intellectual Property Alliance. Spain. *Special Mention*, 301.

(2005). Los Autores del 11-M Amenazaban en el Vídeo al Nuevo Gobierno por Seguir la lucha contra el Islam. *El Mundo* [online]. Available at <<http://www.elmundo.es/elmundo/2004/04/13/enespecial/1081852985.html>> [Accessed 24 March 2011].

(2005). Un Testimonio desde Londres *Escolar.net.* [online] Available at <<http://www.escolar.net/MT/archives/2005/07/un_testimonio_d.html> > [Accessed on 01 February 2011]

(2006). Open Source Intelligence. *Headquarters, Department of the Army.*

(2007). El CNI Advierte del Nuevo Grupo para la Liberación de Al Andalus. *Stirpes Forum* [online]. Available at <<http://forum.stirpes.net/ibero-romance-ibero-aquitanian/11031-cni-advierte-nuevo-grupo-para-liberacion-al-andalus.html>> [Accessed 01 February 2011].

(2008). 11 de Marzo. *El Blog que nos Acerca* [online]. Available at <<http://elblogquenosacerca.wordpress.com/2008/03/11/11-de-marzo/>> [Accessed 01 February 2011].

(2008). *Cisco Annual Security Report*. Cisco Systems Inc.

(2008). La Oreja de Van Gogh. 11 de Marzo. *Palabras Retorcidas* [online]. Available at [<http://palabrasretorcidas.wordpress.com/2008/07/20/11-de-marzo-presentcion-en-vivo-y-letra/](http://palabrasretorcidas.wordpress.com/2008/07/20/11-de-marzo-presentcion-en-vivo-y-letra/)> [Accessed 01 February 2011].

(2008). Software, Portal Target, Predict Terrorist Behavior, *Network World*, [online]. <<http://www.networkworld.com/community/node/25390>> [Accessed July 2008].

(2008). *The French White Paper on Defence and National Security*. Présidence de la République.

(2008). *The National Security Strategy of the United Kingdom: Security in an Interdependent World*. Cabinet Office. March 2008.

(2009). *Code of Ethics of the American Anthropological Association*. American Anthropological Association.

(2009). *El Ciberdelito: Guía Para Los Países En Desarollo*. Unión Internacional de Telecomunicaciones. División de Aplicaciones TIC y Ciberseguridad (CYB).

(2009). Ley Orgánica 2/2009 de 11 de diciembre, de reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social. [online] < <http://www.tt.mtin.es/periodico/LEY_EXTRANJERiA%28BOE12-12-2009%29.pdf>> [Accessed 21 June 2011].

(2010). Ataque Islámico del 11 M ¿Para qué? *Labranza de Dios* [online]. Available at <<http://www.labranzadedios.com/2010/03/el-11-de-marzo-sera-recordado-en-la.html>> [Accessed 01 February 2011].

(2010). Call to South East Communities to Help Beat Terrorism. *BBC News* [online] Available at <<http://www.bbc.co.uk/news/uk-england-11257942>> [Accessed 17 November 2010].

(2010). *Electronic Media Engagement Evaluation Design and Methodology*. United States Department of State Third Annual Conference on Program Evaluation: New Paradigms for Evaluating Diplomacy in the 21st Century.

(2010). El PP de Rajoy Dispuesto a Echarse en Brazos del Nacionalismo Vasco. *Minuto Digital* [online] Available at <<http://www.minutodigital.com/noticias/2010/07/07/el-pp-de-rajoy-dispuesto-a-echarse-en-brazos-del-nacionalismo-vasco/>> [Accessed 02 February 2011].

(2010). *Engaging Foreign Audiences. Assessment of Public Diplomacy Platforms Could Help Improve State Department Plans to Extend Engagement*. United States Government Accountability Office.

(2010). España pierde interés para el trabajador inmigrante. *RRHH Digital* [online]. Available at <<http://www.rrhhdigital.com/ampliada.php?sec=45&id=69039>> [Accessed on March 2010].

(2010). GLITC Conmemora el Sexto Aniversario del 11-M. *Juventudes Naranjas* [online]. Available at <<http://juventudesnaranjas.blogspot.com/2010/03/glitc-conmemora-el-sexto-aniversario.html>> [Accessed on 01 February 2011].

(2010). Social Networks/Blogs Now Account for One in Every Four and a Half Minutes Online. *NielsenWire* [online]. Available at <<http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/>> [Accessed 19 July 2011].

(2010). The Well.com [online]. Available at <<http://www.well.com/aboutwell.html>> [Accessed 10 December 2010].

(2010). Ushahidi.com [online]. Available at <<http://ushahidi.com/>> [Accessed 19 December 2010].

(2011). Asociación 11M Afectados Terrorismo [online]. Available at <<http://www.asociacion11m.org/index.php>> [Accessed March 2011].

(2011). Bin Laden i els “Bons Demòcrates” Americans, *Una Trobadora* [online]. Available at <<http://unatrobadora.wordpress.com/2011/05/02/bin-laden-i-els-bons-democrates-americans/>> [Accessed 03 May 2011].

(2011). Bin Laden.-La presidenta de la AVT, madre de una víctima del 11-M, se alegra pero pide a los gobiernos que estén atentos [online]. *El Economista*. Available at <<http://ecodiario.eleconomista.es/politica/noticias/3031892/05/11/Bin-LadenLa-presidenta-de-la-AVT-madre-de-una-victima-del-11M-se-alegra-pero-pide-a-los-gobiernos-que-esten-atentos.html>> [Accessed 06 May 2011].

(2011). Bin Laden - Gómez dice a Aguirre que "hasta el Gobierno de EEUU atribuye los atentados del 11-M a Bin Laden". [online] *El Economista.* Available at [<http://ecodiario.eleconomista.es/politica/noticias/3032746/05/11/Bin-Laden-Gomez-dice-a-Aguirre-que-hasta-el-Gobierno-de-EEUU-atribuye-los-atentados-del-11M-a-Bin-Laden.html](http://ecodiario.eleconomista.es/politica/noticias/3032746/05/11/Bin-Laden-Gomez-dice-a-Aguirre-que-hasta-el-Gobierno-de-EEUU-atribuye-los-atentados-del-11M-a-Bin-Laden.html)> [Accessed 06 May 2011].

(2011). ETA Website: [online]. Available at: <<http://osis.ucsd.edu/~ehj/html/eta.html>> [Accessed May 2009].

(2011). Esperanza Aguirre exculpa a Bin Laden de la autoría del 11-M (con argumentos falsos). *Ventanas del Falcón* [online]. Available at < <http://ventanasdelfalcon.blogspot.com/2011/05/esperanza-aguirre-exculpa-bin-laden-de.html>> [Accessed 03 May 2011].

(2011). Facts about the Schengen Information System (SIS): What is Schengen Information System? *Information Commissioner Republic Of Slovenia* [online]. Available at <<http://www.ip-rs.si/index.php?id=345>> [Accessed 21 June 2011].

(2011). Gómez Critica las Declaraciones de Aguirre sobre la Autoría del 11-M, *El Plural* [online]. Available at < <http://www.elplural.com/politica/gomez-critica-las-declaraciones-de-aguirre-sobre-la-autoria-del-11-m/>> [Accessed 02 May 2011].

(2011). La Ley de Economía Sostenible. *La Moncloa*. [online]. Available at <<http://www.economiasostenible.gob.es/>> [Accessed from 14 June 2011].

(2011). *Multilevel Governance in a Changing World. Bringing the Regions of the Mediterranean Closer to the Citizens*. MedGovernance Project. Final Policy Paper.

(2011). The Phishing Guide. *Technical Info* [online]. Available at <<http://www.technicalinfo.net/papers/Phishing.html>> [Accessed 01 August 2011].

Abbasi, A., & Chen, H., (2005). Applying Authorship Analysis to Extremist – Group Web Forum Messages. *IEEE Computer Security*, September/October 2005.

Aguillo, I.F. Cybermetric Indicators. A Methodological Approach 2009. 2nd International Workshop on University Web Rankings CCHS – CSIC, Madrid (Spain). April 21st 2009.

Akindele, S.T., & Adebo, A. (2005). A Revistational Assessment of the Rise of Behavioural Approach in Political Science. *Journal of Social Science*, 10(1): 61-64, (2005).

Ali, R., (2009). Technological Neutrality. *Lex Electronica*, vol. 14 No. 2 (Automne / Fall 2009).

Allison, (2010). Ushahidi Enables Real-Time Crisis Mapping in Haiti Mobile Behavior [online]. Available at <http://www.mobilebehavior.com/2010/01/26/ushahidi-enables-real-time-crisis-mapping-in-haiti/> [Accessed 12 July 2010].

Almind, T.C., & Ingwersen, P. (1997). Informertric Analyses on the World Wide Web: Methodological Approaches to ‘Webometrics’. *Journal of Documentation*, 53(4), pp.404-426.

Alonso, R., (2007). Information or Propaganda? The Hunger Strike of ETA Terrorist Ignacio de Juana Chaos and its Coverage in the Times. *Real Instituto Elcano*, ARI 28/2007.

Alvarez Amaro, J. (2004). Los Populares Extremeños Reprochan a Zapatero que Haya Ganado por el 11-M. El Periódico. [online] Available at <<http://www.elperiodicoextremadura.com/noticias/noticia.asp?pkid=101412>> [Accessed 29, March, 2011].

Amado, I., (Date Unknown). Ciberterrorismo. Una Apriximación a su Tipificación como Conducta Delictiva. *Derecho Penal*.

Amnesty International, (2009). *Spain: Out of the Shadows – Time to End Incommunicado Detention*. Amnesty International Publications 2009.

Amoore, L., (2007). Vigilant Visualities: The Watchful Politics of the War on Terror. *Security Dialogue* 2007, 38; 215.

Amoore, L. & Goede, M. (2004). Transactions after 9/11: the Banal Face of the Preemptive Strike. *Transactions of the British Institute of British Geographers*. Volume 33, Issue 2, pages 173-185, April 2008.

Ampofo. L., (2010). Public Diplomacy, From Policy to Practice. *Wilton Park*, United Kingdom 7-9 June 2010.

Angus Reid, (2004). Zapatero Enters Make or Break Year. [online] Available at < <<http://www.angus-reid.com/analysis/39866/zapatero_enters_make_or_break_year_in_spain/>> [Accessed 01 February 2011].

Anstead, N., & Chadwick, A. (2008). Parties, Election Campaigning, and the Internet: Toward A Comparative Institutional Approach in Chadwick, A., & Howard, P.N. (eds.) *The Routledge Handbook of Internet Politics*. Routledge, 2008.

Antoniades, A., O’Loughlin, B., & Miskimmon, A., (2010). Great Power and Strategic Narratives. *Working Paper No. 7, The Centre for Global Political Economy*, University of Sussex.

Antonio Remiro Brotóns and Carlos Espósito, (2002). “Spain,” in *Combating Terrorism*, ed. Jonah Alexander (Ann Arbor: University of Michigan Press, 2002), 163 – 83.

Armstrong, M. (2010). GAO and US Advisory Commission on Public Diplomacy Discuss Evaluation Tools. Mountain Runner. [online] Available at <<http://mountainrunner.us/2010/07/gao.html>> [Accessed 21 January 2010].

Arrington, M, 2010. State of the Blogosphere 2009, Technorati Inc. [online] <http://technorati.com/blogging/feature/state-of-the-blogosphere-2009/> [Accessed 20 August 2010].

Arquilla, J., & Ronfeldt, D., (1997). *In Athena’s Camp: Preparing for Conflict in the Information Age*. RAND.

Arquilla, J., & Ronfeldt, D., (2000). *Swarming and the Future of Conflict*. RAND.

Arquilla, J., & Ronfeldt, D., (2001). *Networks and Netwars: The Future of Terror, Crime and Militancy.* California: RAND.

Ars Technica. (2008). Big Sister is Watching, *Ars Technica* [Online]. Available at: <<http://arstechnica.com/news.ars/post/20080909-big-sister-is-watching-edvige-and-the-angry-french.html>> [Accessed 10 September 2008].

Atran, S. (2006). The Moral Logic and Growth of Suicide Terrorism. *The Washington Quarterly*, 29:2 pp.127-147.

Atkinson, S.E., Sandler, T. & Tschirhart, J. (1987). Terrorism in a Bargaining Framework. *Journal of Law and Economics*, Vol. 30, No. 1, (Apr., 1987), pp.1-21.

Author Unknown, (2010). International Intellectual Property Alliance (IIPA) 2010 Special 301 Report on Copyright Protection and Enforcement. International Intellectual Property Alliance. 18 February 2010.

Avilés, J., (2003). Balance del terrorismo en España en el año 2003 *Grupo de Estudios Estratégicos*, [Online] Análisís No. 64. Available at: <<http://www.gees.org/articulo/571/>> [Accessed 28 July 2005].

Ba, S, Whinston, A.B., Zhang, H, (2003). Building Trust in Online Markets Through an Economic Incentive Mechanism, *Design Support Systems*, No. 35, pp. 273-286.

Bains, P., O’Shaughnessy, N.J., Moloney, K., Richards, B., Butler, S. & Gill, M., (2006). *Muslim Voices: The British Muslim Response to Islamic Video Polemic – An Exploratory Study*. Research Paper Series. Cranfield University School of Management.

Baldwin, M., (2009). How to Measure Online Influence. Mashable [online]. Available at <<http://mashable.com/2009/03/02/measuring-online-influence/>> [Accessed on 10 December 2010].

Ballesteros, M.Á, (2005). El papel de la OTAN en la lucha contra el terrorismo internacional Real Instituto Elcano de *Estudios Internaciónales y Estrategicas*. No. 138 [online]. Available at: <<http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/Elcano_es/Zonas_es/Terrorismo+Internacional/ARI+138-2005>> [Accessed 28 July 2008].

Baquero, A., (2004). La Cantera de Al-Qaeda. *Diario Córdoba*. [online] Available at <<http://www.diariocordoba.com/noticias/noticia.asp?pkid=114378>> [Accessed 01 February 2011].

Barak, S., (2004). Between Violence and E-Jihad: Middle Eastern Terror Organizations in the Information Age. In L Nicander & M. Ranstorp (Eds.). *Terrorism in the Information Age-New Frontiers?* (pp. 83-96).

Barber, S. (1992). Jihad Vs McWorld, *The Atlantic*. [Online]. Available at: <[http://www.theatlantic.com/doc/199203/barber> [Accessed August 2006](http://www.theatlantic.com/doc/199203/barber%3e%20%5bAccessed%20August%202006)]

Barkus, L, Dey, A, (2003). Location-Based Services for Mobile Telephony: A Study of Users Privacy Concerns, Proceedings of the INTERACT 2003 9TH IFIP TC13 *International Conference on Human-Computer Interaction*, Intel Berkeley Research.

Barnett, T.P.M. & Gaffney, Jr., H.H., (Date Unknown). The Global Transaction Strategy. *Transformation Trends* – 16 December Issue.

Barnett, T., (2005). *The Pentagon’s New Map: War and Peace in the Twenty-First Century*. Reprint Edition. Berkeley Publishing Group.

Bassett, E.H., O’ Riordan, K, (2002). Ethics of Internet Research: Contesting the Human Subjects Research Model, Internet Research Ethics, New York University. <http://www.nyu.edu/projects/nissenbaum/ethics\_bas\_full.html> [Accessed 12 July 2010].

Baudrillard, J., (2003). *The Spirit of Terrorism and Other Essays*. London and New York, Verso.

Baudrillard, J., (1983). *Simulations*, Semiotext.

Baudrillard, J., (1995). *The Gulf War did not Take Place*. Bloomington: Indiana University Press.

Baudrillard, J, Maclean, M, (1985). The Masses: The Implosion of the Social in the Media. *New Literary History*, Vol. 16, No. 3, pp. 577-589.

BBC Mundo, (2005). ¿Cómo es España después del 11-M? [online] Available at <<http://news.bbc.co.uk/hi/spanish/forums/newsid_4336000/4336173.stm>> [Accessed 01 February 2011].

BBC News. (1986). 1986: French Car Chief Shot Dead, *BBC News* [online] [<http://news.bbc.co.uk/onthisday/hi/dates/stories/november/17/newsid\_2540000/2540123.stm](http://news.bbc.co.uk/onthisday/hi/dates/stories/november/17/newsid_2540000/2540123.stm) > [Accessed October 2008].

BBC News. (2003), Europe-Africa Rail Tunnel Agreed, *BBC News* [Online]. Available at: <<http://news.bbc.co.uk/1/hi/world/africa/3317149.stm>> [Accessed July 2005].

BBC News, (2004). Madrid Attacks Timeline. [online] Available at <<http://news.bbc.co.uk/1/hi/world/europe/3504912.stm>> [Accessed on 22 July 2011].

BBC News, (2010). Saudi Arabia begins Blackberry Ban, Users Say. [online] Available at <<http://www.bbc.co.uk/news/world-middle-east-10888954>> [Accessed 13 July 2011].

Beck, L., (2008), The Mezquita-Garaje, Mezquita-Sótano, and Islam in Spain Since 11-M, *HAOL*, No. 17, 147-158

Beck, U., (1999). *World Risk Society*. Blackwell Publishers Ltd.

Beckmann, S, Langer, R, (2005). Netnography: Rich Insights from Online Research. *Insights*, No. 14.

Bell, G., & Dourish, P. (2006). *Yesterday’s Tomorrows: Notes on Ubiquitous Computing’s Dominant Vision*. Springer-Verlag London Limited.

Bell, D., & Kennedy, B. (eds.) (2000). *The Cybercultures Reader*. London and New York, Routledge.

Beck, L., (2008). The Mezquita-Garaje, Mezquita-Sótano, and Islam in Spain Since 11-M. *HAOL*, Núm. 17, (Otoño, 2008), 147-158.

Bendrath, Ralf. (2001). The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection. *Information and Security. Volume 7, 2001 (80-103).*

Bennett, L.W., in de Donk, W., Loader, B.D., Nixon, P.G. & Rucht (eds) (2002). Communicating Global Activism: Some Strengths and Vulnerabilities of Networked Politics in *Cyberprotest: New Media, Citizens and Social Media*. London: Routledge.

Bennett, L., (2003). Communicating Global Activism. Information, Communication & Society [online] Available at <<http://depts.washington.edu/ccce/assets/documents/pdf/communicatingglobalactivism.pdf>> [Accessed October 2008].

Berenskoetter, F. Williams, M.J. (eds), (2007). *Power in World Politics*, Routeledge

Berkowitz, B., (2002). The New Protracted Conflict: Intelligence and the War on Terrorism. Foreign Policy Research Institute, Elsevier Science Limited, Spring 2002, 289-303

Bermingham, A., Conway, M., McInerney, L., O’Hare, N. & Smeaton, A.F. (Date Unknown). Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation. CLARITY Centre for Sensor Web Technologies.

Bernard Lewis, (1990). ‘The Roots of Muslim Rage,’ *The Atlantic Monthly*, vol. 266, September 1990, p. 60; June 15,1992, pp. 24-28.

Berelson, B., (1952). *Content Analysis in Communication Research*. Free Press.

Bermudez, G., (2010). La Ley Cerca al Yihadismo. *La Razon* [online]. Available at <<http://www.larazon.es/noticia/8747-al-juez-javier-gomes-bermudez-gana-el-premo-de-hoy>> [Accessed on 01 March 2010].

Berners-Lee, T., (1999). *Weaving the Web: The Original Design and Ultimate Destiny by its Inventor*, Harper Collins.

Berners-Lee, T. Hendler, J. Lassila, O., (2001). The Semantic Web, *Scientific American*, [online]. Available at <<http://www.sciam.com/article.cfm?articleID=00048144-10D2-1C70-84A9809EC588EF21>> [Accessed October 2008).

Berners-Lee, T, (2010). Long Live the Web: A Call for Continuing Open Standards and Neutrality. Scientific American. [online] <http://www.scientificamerican.com/article.cfm?id=long-live-the-Web&page=2> [Accessed 22 November 2010].

Bertola, V., (2010). Power and the Internet. *Journal of Information, Communication and Ethics in Society*, Vol. 8, Iss: 4, pp.323-327.

Best, S.J., & Krueger, B.S., (2008). Political Conflict and Public Perceptions of Government Surveillance on the Internet: An Experiment of Online Search Terms. *Journal of Information Technology and Politics*, Vol, 5(2), 2008

Betz, D.J., (2006). The More You Know, the Less You Understand: The Problem with Information Warfare. *Journal of Strategic Studies*, 29:3, 505-533.

Betz, D., (2011). Communication Breakdown: Strategic Communications and Defeat in Afghanistan. *Foreign Policy Research Institute*, Fall 2011.

Beutel, A.J., (2007). Radicalization and Homegrown Terrorism in Western Muslim Countries: Lessons Learned for America. *Minaret of Freedom Institute*, pp. 1-16

Bezunartea, P., Lopéz, J.M., & Tedesco, L., (2009). Muslims in Spain and Islamic Religious Radicalism. *MICROCON Policy Working Paper 8,* Brighton: MICROCON.

Bimber, B., (1990). Karl Marx and the Three Faces of Technological Determinism. Working Paper No. 11 Program in Science, Technology and Society Massachusetts Institute of Technology.

Birnbaum, M.H., (2004). Human Research and Data Collection via the Internet. *Annual Review of Psychology*. 2004, 55: 803-32

Bishop, J., (2006). Increasing Participation in Online Communities: A Framework for Human-Computer Interaction. *Computers in Human Behaviour*, 23 (2007) 1881-1893.

Bishop, J., (2003). *Building Social and Economic Relationships through Avatars and Characters*. Increasing Capital Revenue in Social Networking Communities. IGI Global

Blackmore, S. (1998). Imitation and the Definition of a Meme. Journal of Memetics – Evolutionary Models of Information Transmission [online]. Available at <<http://jom-emit.cfpm.org/1998/vol2/balckmore_s.html>> [Accessed 29 July 2011].

Bobbitt, P., (2008). *Terror and Consent, Wars for the 21st Century*, Allen Lane

Bobbitt, P. (Date Unknown). Terrorism and the Market State. *Macalester International*, Vol. 14.

Bolt, N., Betz, D. & Azari, J., (2008). Propaganda of the Deed: Understanding the Phenomenon. *Whitehall Report* 3-08, The Royal United Services Institute.

Booth, K., (1991), Security and Emancipation. *Review of International Studies* (1991), 17, 313-326.

Borland, J. (2007). A Smarter Web: New Technologies Will Make Online Search More Intelligent – and May Even Lead to a “Web 3.0.” [online]. <<http://www.technologyreview.com/magazine/toc/>> [Accessed 23 January 2008]

Borgatti, S. (Date Unknown). Flow Processes and the Structural Importance of Nodes. *Presentation to Harvard University, Boston College*.

Bowles, S., Gintis, H. & Osborne, M., (2001). The Determinants of Earnings: A Behavioural Approach. *Journal of Economic Literature*, Vol. 39, No. 4, (Dec., 2001), pp. 1137-1176.

Boyd, D, Ellison, N, 2007. ‘Social Network Sites: Definition, History and Scholarship’, *Journal of Computer-Mediated Communication*, Vol. 13 No. 1.

Boyle, J., (1997). Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors. *Duke University* [online]. Available at <<http://www.law.duke.edu/boylesite/foucault.htm>> [Accessed May 2008].

Brachman, J.M., (2006). High-Tech Terror: Al-Qaeda’s Use of New Technology. *The Fletcher Forum of World Affairs*, Vol. 30:2 Summer 2006.

Brandt, P.T., & Freeman, J.R. (2005). Advances in Bayesian Time Series Modeling and the Study of Politics: Theory Testing, Forecasting, and Policy Analysis. *Political Analysis*, pp.1-36.

Briscoe, I., (2004), Dreaming of Spain: Migration and Morocco. *Open Democracy*, [online]. Available at <<http://www.opendemocracy.net/conflict-africa_democracy/article>> [Accessed 02 August 2010].

British Council, 2005. Lord Carter of Coles Public Diplomacy Review. [online] Available at <http://www.britishcouncil.org/home-carter-report> [Accessed 03 January 2011].

Brin, S., & Page, L., (1998). The Anatomy of a Large Scale Hypertextual Web Search Engine. *Computer Networks and ISDN Systems* 30(1-7), pp. 107-117.

Bromley, M., (2001). *No News is Bad News: Radio, Television and the Public*. Pearson Education Limited.

Brotóns, A., (Date Unknown). *Terrorismo, Mantenimiento de la Paz y Nuevo Orden. Catedrático de Derecho Internaciónal Público y Relaciones Internacionales*, Universidad Autónoma de Madrid.

Brown, R., (2002). The Contagiousness of Conflict. E.E. Schattschneider as a Theorist of the Information Society. *Information, Communication and Society*. 5:2 2002 258-275.

Browne, A., (2005). Threat of Islamic Extremism that Stretches Across Europe. *The Times of London.* [online]. Available on <<http://www.timesonline.co.uk/tol/news/uk/article548063.ece>> [Accessed on 17 November 2010].

Bruckman, A, (2002). ‘Ethical Guidelines for Research Online’ *Georgia Institute of Technology College of Computing*.

Burke, J., (2004). *Al-Qaeda: The True Story of Radical Islam*. Penguin Books.

Burke, C., (2007). *Freeing Knowledge, Telling Secrets: Open Source Intelligence and Development*. Bond University.

Burstein, P., (2003). The Impact of Public Opinion on Public Policy: A Review and an Agenda. *Political Research Quarterly*. March 2003, vol. 53, no. 1 29-40.

Burton, F., (2006). The Web of Jihad: Strategic Utility and Tactical Weakness. [online] Available at <http://www.stratfor.com

/Web\_jihad\_strategic\_utility\_and\_tactical\_weakness?fn=8415164985> [Accessed 16 September 2010].

Buscaglia, E., Ruiz, S., Fumarulo, S., Palma, C. (2002). *Delincuencia Organizada y Terrorismo. Su Combate a Través de la Convención de Palermo*.

Buzan, B., Wœver, O, de Wilde, J., (1998). *Security: A New Framework for Analysis*. Lynne Reinner Publishers, Inc.

(2011). Cytoscape Wiki. Basic Network Navigation. [online] Available at <<http://cytoscape.wodaklab.org/wiki/Cytoscape_User_Manual/Navigation_Layout>> [Accessed 19 July 2011].

Calás, M. B. & Smircich, L., (1999), Past Postmodernism? Reflections and Tentative Directions, *The Academy of Management Review*, Vol 24, No. 4 (Oct., 1999)

Calavita, K., (2006). Notas de población, Volume 33, *Issues* 82-85, United Nations publications, 2007.

Calishain, T., & Dornfest, R., (2003). *Google Hacks. Industrial-Strength Tips & Tools*. O’Reilly Associates Inc.

Callon, M., (1991). *Techno-Economic Networks and Irreversibility* in Law, J. (ed.), *A Sociology of Monsters: Essays on Power Technology, and Domination*. Routledge.

Campbell, D., (1992), *Writing Security*. Manchester University Press.

Capurro, R., (Unknown). Angeletics – A Message Theory. *Steinbeis-Transfer-Institute Information Ethics* (STI-IE), Karlsruhe, Germania

Carley, K., McCulloch, I., Webb. M., (2002). Social Network Monitoring of Al Qaeda.

Carley, K.M., Reminga, J., Kamneva, N., (2003). Destabilizing Terrorist Networks. Dynamic Networks Project Paper, *Carnegie Mellon University*, pp. 1-6.

Castells, M., (2000), *The Power of Identity* WileyBlackwell 2nd Edition.

Castells, M., (2000) *The Rise of the Network Society*, WileyBlackwell 2nd Edition.

Castells, M., (2000). Toward a Sociology of the Network Society. *Contemporary Sociology*, Vol. 29, No. 5 (Sep., 2000), pp.693-699.

Castells, M., Fernandez-Ardevol, M., Qiu, J. & Sey, A. (2004). The Mobile Communication Society. A Cross-Cultural Analysis of Available Evidence on the Social Uses of Wireless Communications Technology. A research report prepared for the International Workshop on Wireless Communication Policies and Prospects: A Global Perspective, held at the Annenberg School for Communication, University of Southern California, Los Angeles, October 8th and 9th 2004.

Castells, M. & Cardoso, G., (2005). *The Network Society: From Knowledge to Policy*. Johns Hopkins Center for Transatlantic Relations, 2005.

Castells, M., (2007). Communication, Power and Counter-Power in the Network Society. International Journal of Communication 1 (2007), 238-266.

Cavelty, M.D., (2007). Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics*. Vol. 4(1) 2007.

Cavicchioli, M.I., (Date Unknown). A Period of Turbulent Change: Spanish – US Relations Since 2002. The Whitehead Journal of Diplomacy and International Relations. Pp.113-131.

Cebrowski, A.K. & Barnett, T.P.M., (Date Unknown). The American Way of War. *Transformation Trends* – 13 January Issue.

Celaya, F. (2009), The Terrorist Threat is being Materially and Normatively Shaped by National and Global Institutions of Law and Order: Spain and Beyond. *Athena Intelligence Journal* Vol. 4, No.1 January – March 2009

Cellan-Jones, R., (2009). Mapping the Afghan Elections. *BBC News* [online]. Available at <<http://www.bbc.co.uk/blogs/technology/2009/08/mapping_the_afghan_elections.html>> [Accessed 18 July 2010].

Celso, A.N., (2005). The Tragedy of Al-Andalus: The Madrid Terror Attacks and the Islamization of Spanish Politics. *Mediterranean Quarterly*, Volume 16, Number 3, Summer 2005, pp.86-101.

Celso, A. N., (2006). Spain’s Dual Security Dilemma: Strategic Challenges of Basque and Islamic Terror during the Aznar and Zapatero Eras. *Mediterranean Quarterly*, Volume 17, Number 4, Fall 2006, pp.121-141.

Celso, A.N., (2008). Al Qaeda in the Maghreb: The “Newest” Front in the War on Terror. *Mediterranean Quarterly* 19:1

Celso, A.N., (2009). Spanish post-3/11 Antiterror Policy: Zapatero’s Tyranny of Circumstance and the Dashing of Good Intentions. *Mediterranean Quarterly*. 20(2): 11-25.

Celso, A.N., (2010). ‘Phase IV’ Operations in the War on Terror: Comparing Iraq and Afghanistan. *Foreign Policy Institute*, Spring 2010, 184-199.

Centre UNESCO de Catalunya, (2008). *Security, Living Together and Cultural Diversity*. *Generaliat de Catalunya*. Departament d’Interior, Relacions Institucionals I Participació.

Cesari, J., (2009). *The Securitisation of Islam in Europe. Challenge Liberty and Security*. CEPS Challenge Programme.

Chakrabarti, P.D., (1976). Behaviouralism: A Challenge to Marxism? *Social Scientist*, Vol. 4, No. 9 (Apr., 1976), pp.55-59.

Cha, V.D., (2000). Globalization and the Study of International Security. *Journal of Peace Research*, Vol. 37, No. 3, (May 2000), pp. 391-403.

Chadwick, A. (2006). *Internet Politics: States, Citizens, and New Communication Technologies*. Oxford University Press.

Chaintreau, A., Fraignaud, P. & Lebhar, E. (2008). Opportunistic Spatial Gossip over Mobile Social Networks. *WOSN’08,* August 18, 2008, Seattle, Washington, USA.

Chamorro, E.F. & Villalba, Á.F.S. (2010). Cyber Security in Spain:  A Proposal for its Management (ARI). *Real Instituto Elcano*. ARI 102/2010.

Chandler, D. (1995). Technological or Media Determinism [online]. Available at <<http://www.aber.ac.uk/media/Documents/tecdet/tecdet.html>> [Accessed 13 June 2011].

Charrett, C., (2009). A Critical Application of Securitization Theory: Overcoming the Normative Dilemma of Writing Security. *Institut Català Internacional per la Pau*.

Chau, D., (2008). U.S. Counter-terrorism in Sub-Saharan Africa: Understanding Costs, *Cultures, and Conflicts* [Online]. September 2008. Available at <<http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB821.pdf>> [Accessed 01 October 2008]

Chen, H., Thoms, S. & Fu, T.J., (2008). Cyber Extremism in Web 2.0: An Exploratory Study of International Jihadist Group. Forthcoming, IEEE International Conference on Intelligence and Security Informatics, 2008.

Chepsiuk, R., (2001). Get Ready for Cyberwars. [online]. Available at <<http://www.afcea.org.ar/publicaciones/chepsiuk.htm>> [Accessed 28 March 2009].

Chen, Y, Liu, C, Wong, R, (2007). The Adoption of Synchronous and Asynchronous Media in the Teaching of a Second Language. *Issues in Information Systems*, Volume III, No. 1.

Chen, H., Thoms, S. & Fu, T.J., (2008). Cyber Extremism in Web 2.0: An Exploratory Study of International Jihadist Groups. *IEEE International Conference on Intelligence and Security Informatics*, 2008.

Chernaik, W., Deegan, M. & Gibson, A. (1996). Beyond the Book: Theory, Culture and the Politics of Cyberspace. Office for Humanities Communication Publications, No. 7, The Centre for English Studies, University of London.

Chesters, G., (2003). Shape Shifting: Civil Society, Complexity and Social Movements, *Anarchist Studies*, 11, 1:42-65

Civis, L., (2009). *La Lucha Contra el Terrorismo en el Marco de la Seguridad y Defensa en España*. Real Instituto Elcano. ARI No. 45/2009.

Clark, R., (1998). Information, Technology and Dataveillance. *Communications of the ACM.* May 1998, Volume 13, Number 5.

Clifton, B., (2010). *Advanced Web Metrics with Google Analytics*. Wiley Publishing Inc. Indianapolis, Indiana.

Club de Madrid., (2005). International Summit on Democracy, Terrorism and Security, Madrid: *Club de Madrid*

Colás, A., (2010). An Exceptional Response? Security, Development and Civil Society in Spanish Policy after 11-M. *Development and Change*. Volume 41, Issue 2, pages 313-333, March 2010.

Colin, B.C., (Date Unknown). The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. *11th Annual International Symposium On Criminal Justice Issues*.

Colmenares, M., (2009). Quinto Aniversario del Ataque Terrorista del 11M. Martha Colmenares.” [online] <<http://www.marthacolmenares.com/2009/03/11/quinto-aniversario-del-ataque-terrorista-del-11m/>> [Accessed 01 February 2011].

Colomer, J., (2005). The General Election in Spain, March 2004 *Electoral Studies*, 24, (1), p. 123-160

Comscore, (2009). Fast Growing U.K. Online Newspaper Market Attracting Even Larger Audiences from Beyond the Pond. [online] Available at <<http://www.comscore.com/Press_Events/Press_Releases/2009/5/U.K._Newspaper_Sites_Aattract_Visitors_from_Around_the_World>> [Accessed on 23 July 2011].

Conway, M., (2002) *Cyberterrorism: The Story so Far* in Hutchinson, B., (2002). *Proceedings of the European Conference on Information Warfare and Security*. Brunel University Uxbridge, United Kingdom 8-9 July 2002.

Conway, M., (2002). Reality Bytes: Cyberterrorism and Terrorist ‘Use’ of the Internet. First Monday, 7. [online] Available at <<http://www.firstmonday.org/issues/issue7_11/conway>> [Accessed 01 June 2007].

Conway, M., (2003). Hackers as Terrorists? Why it Doesn’t Compute. *Computer Fraud and Security,* 2003, (12) (December): 10:13.

Conway, M., (2003). Code Wars: Steganography, Signals Intelligence, and Terrorism. *Knowledge, Technology and Policy* (Special issue entitled ‘Technology and Terrorism’) Vol. 16, No. 2 (Summer 2003): 45-62 and reprinted in David Clarke (Ed.), *Technology and* Terrorism. New Jersey: Transaction Publishers (2004): 171-191.

Conway, M., (2005). Terrorist ‘Use’ of the Internet and Fighting Back. Paper prepared for presentation at the conference *Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities,* Oxford Internet Institute (OII), Oxford University, UK, 8-10 September, 2005

Conway, M., (2006). Terrorism and the Internet: New Media – New Threat? Parliamentary Affairs, 2006.

Conway, M., (2007). Terrorism and Internet Governance: Core Issues. *Disarmament Forum*, 2007 (3) pp.23-34 ISSN 1020-7827.

Conway, M., & McInerney, L. (2008). *Jihad Video & Auto-Radicalisation: Evidence from an Exploratory YouTube Study*. School of Law & Government, Dublin City University, Glasnevin, Dublin, 9, Ireland.

Cornish, P., (2009). Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. *European Parliament*, 2 February 2009.

Corning, P.A. (2002). The Re-Emergence of “Emergence”: A Venerable Concept in Search of a Theory. *Complexity* (2002) 7(6): 18-30.

Cosidó, I., 2002 Spanish Policy Against Terrorism: The Guardia Civil and ETA, *Grupo de Estudios Estratégicos*, [Online]. Available at: <<http://gees.org/articulo/299/>> Accessed 29 July 2008

Cottle, S., (1998). Ulrich Beck, ‘Risk Society’ and the Media. A Catastrophic View? *European Journal of Communication*. Vol. 13, (1): 5-32.

Couldry, N., (2004). *Actor Network Theory and the Media: Do They Connect And On What Terms?* London School of Economics And Political Science [Online]. Available at: <<http://www.lse.ac.uk/collections/media@lse/pdf/Couldry_ActorNetworkTheoryMedia.pdf>> [Accessed 01 November 2008].

Couper, M., (2010). ‘Visual Design in Online Surveys: Lessons for the Mobile World’ *Mobile Research Conference Paper* 8-9 March 2010.

Coyle, D., & Meier, P., (2009). *The Role of Information and Social Networks*. UN Foundation and Vodafone Foundation Partnership.

Crain, M., (1999). New North African Immigration to Spain, *Middle East Report*, No. 211 (Summer 1999), pp.23-25.

Crenshaw, M., (1981). The Causes of Terrorism. *Comparative Politics*, Vol. 13, No.4. (Jul., 1981), pp.379-399.

Crisis Mappers Net, (Date Unknown). The Crisis Mappers Network [online]. Available at <<http://www.crisismappers.net/>> [Accessed 15 November 2010].

Crenshaw, M., (1981). The Causes of Terrorism. *Comparative Politics*, Vol. 13, No. 4, (Jul 1981), pp. 379-399.

Cronauer, K., (2001). Activism and the Internet. Uses of Electronic Mailing Lists by Social Activists. A Review of Crucial Issues, Research Findings, and Open Questions. University of British Columbia.

Cronin, A.K. (2003). Behind The Curve. Globalization and International Terrorism. *International Security*, Vol. 27, No. 3 (Winter 2002/03), pp.30-58.

Cronin, A.K., (Date Unknown). Submission and Consent: Law, War, and the Search for New Strategic Paradigms. Syracuse Journal of International Language and Communication. Vol. 37:23.

Crossley N., Prell, C. & Scott, J., (2009). Social Network Analysis: Introduction to Special Edition. *Methodological Innovations Online* 4 (2009) 1-7.

Croushore, D., (2008). *Working Paper No. 08-4 Frontiers of Real-Time Data Analysis*, Research Department, Federal Reserve Bank of Philadelphia.

Crossley, N., Prell, C., & Scott, J. (2009). Social Network Analysis: Introduction to the Special Edition. *Methodological Innovations Online*, 4, 1-7.

Csányi, V., (1998). *Evolutionary Systems and Society. A General Theory*. Duke University Press.

Cummings, M.P., & Huskamp, J.C., (2005). New Horizons. Grid Computing. *Educause Review*. November / December 2005.

Curto, G. et al. (2007). Informe Sobre La Situacion De Telemadrid Tratamiento Informativo Y Contenidos En Telemadrid. *Fundación Sindical de Estudios*

Dahl, R.A., (1961). The Behavioural Approach in Political Science: Epitaph for a Monument to a Successful Protest. *The American Political Science Review*, Vol. 55, No. 4, (Dec., 1961), pp.763-772.

Dahlgren, P., (2005). The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation. *Political Communication*, 22:147-162.

Davis, R., (1999). *The Web of Politics*. Oxford University Press.

Davis, B., (2006). *Ending The Cyber Jihad: Combating Terrorist Exploitation Of The Internet With The Rule Of Law And Improved Tools For Cyber Governance*. The Catholic University of America, Columbus School of Law.

Davis, Paul, et al. (2009). *‘Representing Social-Science Knowledge Analytically’*, in *‘Social Science for Counterterrorism: Putting the Pieces Together.’* RAND Monograph.

De Kerckhove, D. (1997). *Connected Intelligence: The Arrival of the Web Society*. Kogan Page.

De la Fuente, J.V. (2003). Terrorismo de E.T.A. The Matrix 666. [online] Available at <<http://www.matrix666.net/?page_id=14>> [Accessed 24 March 2011].

De Laat, M., (2000). Network and Content Analysis in an Online Community Discourse, *University of Nijmegen, Department of Education*, pp. 1-8.

De La Corte Ibáñez, L., (2007). Algunas Claves psicosociales Para el Análisis y la Explicación de los Fenómenos Terroristas. *Athena Paper*, Vol. 2, No. 3, Artículo 3/4.

De La Corte, L., (2007). Explaining Terrorism: A Psychosocial Approach. Perspectives on Terrorism [online]. Available at <<http://www.terrorismanalysts.com/pt/index.php/pot/article/view/8/html>> [Accessed 25 January 2012].

De La Corte, L., Kruglanski, A., De Miguel, J., Sabucedo, J. & Díaz, D. (2008). Seven Psychosocial Principles for Explaining Terrorism. *Psychology in Spain*, 2008, Vol. 12, No. 1, 70-80.

Dean, M.M., (1999). *Governmentality: Power and Rule in Modern Society*, Sage Publications Ltd

Dearlove, R., & Quiggin, T. (2006). Contemporary Terrorism and Intelligence. IDSS Commentaries (78/2006).

Del Pino, E., Colino, C., (2010), *National and Subnational Democracy in Spain: History, Models and Challenges*. Instituto de Politícas Y Bienes Públicos, CCHS – CSIC

Denning., D. & Baugh, W.E. (2000) in Thomas, D. and Loader, B. (eds). *Cybercrime: Law Enforcement and Surveillance in the Information Age*. Routledge.

Denning, D., (2001). Is Cyberterrorism Next? *Wired.com* [online]. Available at <<http://www.ssrc.org/sep11/essays/denning/html>> [Accessed on 01 November 2007].

Denning, D., (2000). Cyberterroism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives.

Denning, D. (2002). A*ctivism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Nautilus.

Denning, D. (2001). *Activism, Hacktivism, And Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy* in *Networks and Netwars: The Future of Terror, Crime, and Militancy*. RAND.

Dery, M., (1993). *Flame Wars: The Discourse of Cyberculture*. Duke University Press.

Desiertos Lejanos (2007). Las Tramas Superpuestas de 11-M. *Desiertos Lejanos* [online]. Available at <<http://www.desiertoslejanos.com/blog/?p=34>> [Accessed 01 February 2011].

Devost, M., Houghton, B.K., & Pollard, N.A. (1997). Information Terrorism: Political Violence in the Information Age. *Terrorism and Political Violence*, 9, 72-83.

Diaz, A., (2008). La adaptación de los servicios de inteligencia al terrorismo internacional, *Real Instituto Elcano de Estudios Internaciónales y Estrategicas* [Online]. Available at <<http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/Elcano_es/Zonas_es/Terrorismo+Internacional/ARI+52-2006>> [Accessed 30 July 2008]

DiGiacomo, S.M., (2004). Terrorism and Spanish Democracy. Anthropology News. Fundació Sant Joan de Déu, Barcelona. University of Massachusetts at Amherst.

Directives for Human Experimentation, (1949). The Nuremburg Code, Office of Human Subjects Research [online]. Available at <http://ohsr.od.nih.gov/guidelines/nuremberg.html> [Accessed 13 August 2010].

Domínguez, F., (2008). Operación Nova. El 11-M fue la Bofetada que nos Enseñó la Realidad del Terrorismo Internacional. La Vanguardia. [online] Available at <<http://www.lavanduardia.es/premium/publica/publica?COMPID=533556257524&ID_pagina=22088&ID_FORMATO=9&turboul=false>> [Accessed 08 October 2008].

Douglass, W.A., & Zulaika, J. (1990). On the Interpretation of Terrorist Violence: ETA and the Basque Political Process. *Comparative Studies in Society and History*, Vol. 32, No. 2 (Apr., 1990), pp. 238-257

Drake, D. (2010). 3 Blogging Principles: Simple Yet Important. *ComMetrics* [online]. Available at <<http://commetrics.com/articles/blogging-best-practices-content-consistency-and-congruency/>> [Accessed 19 July 2011].

Duffy, M.E., (2002). Methodological Issues in Web Based Research. *Journal of Nursing Scholarship*, 2002; 34, 1, 83-88.

Dumitriu, E., (2004). The E.U.’s Definition of Terrorism: The Council Framework Decision on Combatting Terrorism. *German Law Journal*. Vol. 05, No. 5.

Durbin, P., (2006). Philosophy of Technology: In Search of Discourse Synthesis. *Techné: Research in Philosophy and Technology.* Volume 10, Number 2, Winter 2006.

Duvenage, M.A., (2010). Intelligence Analysis in the Knowledge Age. An Analysis of the Challenges Facing the Practice of Intelligence Analysis. Thesis Presented in Fulfilment of the Requirements for the Degree of Master of Philosophy.

(2010). EE.UU. Considera que Espana Siguió Siendo Base para Organizaciones Terroristas en 2009. La Vanguardia, [online]. Available at <<http://www.lavanguardia.es/internacional/noticias/20100805/53977366737/ee.uu.-considera-que-espana-siguio-siendo-base-para-organizaciones-terroristas-en-2009-estado-eta-al.html>> [Accessed 02 august 2010].

EFE, (2010). *EE.UU Considera Que España Siguió Siendo Base Para Organizaciones Terroristas en 2009*. La Vanguardia.

El País, (1989). Madrid, Capital Cultural 1992, Carece de Dirección y Proyectos 16 Meses Después de la Designación. [online] Available at: <<http://www.elpais.com/articulo/madrid/Madrid/Capital/Cultural/1992/carece/direccion/proyectos/meses/despues/designacion/elpepiautmad/19890912elpmad_2/Tes>> [Accessed 19 April 2011].

El Mundo, (2004). 11-M Masacre en Madrid. El Mayor Atentado en la Historia de España. [online] Available at < <http://www.elmundo.es/documentos/2004/03/espana/atentados11m/hechos.html>> [Accessed on 22 July 2011].

El Mundo, (2004). Al Qaeda Reinvidica los Atentados en un Vídeo Hallado en Madrid. [online] Available at < <http://www.elmundo.es/elmundo/2004/03/13/espana/1079203531.html>> [Accessed on 22 July 2011].

Electronic Privacy Information Center (2011). *USA Patriot Act*. [online] <<http://epic.org/privacy/terrorism/usapatriot/>> [Accessed 09 July 2011].

Elliot, E., Ho, K., & Holmes, J.S., (2009). Political Science Computing: A Review of Trends in Computer Evolution and Political Science Research. *Journal of Information Technology and Politics*. 6:166-175, 2009.

Elorza, A. (2005). Alianza de Civilizaciones. El País. 20 de septiembre de 2005.

Escher, T., Margetts, H. & Petricek, V. (2006). Governing from the Centre? Comparing the Nodality of Digital Governments. *American Political Science Association*. Prepared for delivery at the 2006 Annual Meeting of the American Political Science Association, August 31 - September 4, 2006

Escolar.net (2005). Un Testimonio Desde Londres. [online] Available at <<http://www.escolar.net/MT/archives/2005/07/un_testimonio_d.html>> [Accessed 01 February 2011].

Espeland, W.N., Stevens, M.L. (1998) Commensuration as a Social Process. *Annual Review of Sociology*. Vol. 24, pp. 313-343

Esposito, J.L. & Mogahed, D., (2007). *Battle for Muslims’ Hearts and Minds: The Road Not (Yet) Taken*. Middle East Policy Council.

Ess, C, Association of Internet Researchers, (2002). Ethical Decision-making and Internet Research. Recommendations from the AOIR Ethics Working Committee, *AOIR Ethics Document* – Final Version, 1.

Estrella, R., (2006). Diplomacia pública de España: un caso práctico. [online] Available at <<http://www.estrella.lamatriz.org/diplomacia-publica-de-espana-un-caso-practico>> [Accessed 01 April 2011]

Etling, B., Kelly, J., Faris, R., & Palfrey, J. (2009). Mapping the Arabic Blogosphere: Politics, Culture, and Dissent. Internet and Democracy Project. *Berkman Center Research Publication No. 2009-06*. The Berkman Centre for Internet and Society at Harvard University.

Eurabian News, (2007). 3 Anos de Golpe de Estado del 11-M. [online] <<http://noticiasdeeurabia.wordpress.com/2007/03/11/3-anos-del-golpe-de-estado-del-11-m/>> [Accessed 01 February 2011].

Eysenbach, G, Till, J.E., (2001). Ethical Issues in Qualitative Research on Internet Communities, *British Medical Journal*; 323: 1103-1105.

Facebook, (2010). Statement of Rights and Responsibilities. [online] Available at <http://www.facebook.com/terms.php> [Accessed 13 August 2010]

Facebook.com (2011). Ahmadinejad is NOT my president! [online] Available at <<http://www.facebook.com/pages/Ahmadinejad-is-NOT-my-president/86964552573>> [Accessed 28 March 2011].

Falk, R., (1995). *On Human Governance: Towards A New Global Politics*. Polity Press.

Fafinski, S., & Minassian, N., (2008). *UK Cybercrime Report 2008*. Garlik, September 2008.

Fauser, M., (2006). Transnational Migration – A National Security Risk? Secutitization of Migration Policies in Germany, Spain and the United Kingdom. Center for International Relations.

Ferligoj, A., & Hlebec, V. (1999). Evaluation of Social Network Measurement Instruments. *Social Networks* 21 (1999) 111-130.

Freelon, D., (2010). Analyzing Online Political Discussion Using Three Models of Democratic Communication. *New Media & Society*, pp. 1-19.

Freedman, L., (1998). A Western Way of War? The Revolution in Strategic Affairs. *Adelphi Papers*, 38:318, 11-17.

Fisher, A. (2003). Gramsci and the New Intellectuals. Mappa Mundi Consulting. *49th Parallel*, no. 12, 2003.

Fisher, A., (2008). Music for the Jilted Generation: Open-Source Public Diplomacy. *The Hague Journal of Diplomacy* 3 (2008), 1-24.

Fisher, A., (forthcoming). Frail and Bedazzeled; Identifying Coordination Points, Structures and Structural Holes in Digital Networks. *Terrorism and New Media Conference*, Dublin, 1-18.

Floyd, R. (2007). Human Security and the Copenhagen School’s Securitization Approach: Conceptualizing Human Security as a Securitizing Move. *Human Security Journal*. Volume 5, Winter 2007.

Franks, J., (Date Unknown). *Rethinking the Roots of Terrorism: Beyond Orthodoxy Terrorism Theory – A New Research Agenda*. University of St. Andrews.

Franz, B., (2007). Europe’s Muslim Youth: An Inquiry into the Politics of discrimination, Relative Deprivation, and Identity Formation. *Mediterranean Quarterly*, Volume 18, Number 1, Winter 2007.

Freelon, D.G., (2010). Analyzing Online Political Discussion Using Three Models of Democratic Communication. *New Media Society*. XX(X), 1-19, Sage Publications.

Friedman. B., Kahn, P.H., & Howe, D., (2000). Trust Online. *Communications of the ACM*. December 2000/Vol. 43, no. 12.

Friedman, T., (2000). *Lexus and the Olive Tree*, Harper Collins Publishers

Fossi, M., et al, (November 2008) Symantec Report on the Underground Economy July 2007 – June 2008, Symantec Corporation. [online]. Available at <<http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf>> [Accessed 02 October 2010].

Foucault, M., (1979). *Discipline and Punish*. Prentice Hall.

Foucault, M. (1980). *Power/Knowledge*. Harvester and Wheatheaf.

Franda, M., (2002). *Internet Development and Politics in Five World Regions*. Lynne Reinner.

Franz, B., (2007). Europe’s Muslim Youth: An Inquiry into the Politics of Discrimination, Relative Deprivation, and Identity Formation. *Mediterranean Quarterly*, Volume 18, Number 1, Winter 2007.

Garcia, R., Rueda Laffond, J., Ruiz, C. (2009). La Historia Inmediata En La Television Espanola: La Representación Del Terrorismo. *The Hebrew University of Jerusalem*. Vol. 2 No. 1.

García R., (2011). Alex de la Iglesia deja la Academia de Cine por su desacuerdo con la 'ley Sinde'. El País. [online] Available at < <http://www.elpais.com/articulo/cultura/Alex/Iglesia/deja/Academia/Cine/desacuerdo/ley/Sinde/elpepucul/20110125elpepucul_8/Tes>> [Acessed 30 January 2011].

Garapon, A., (2005). Tiene Francia una ventaja en la lucha antiterrorista? *Real Instituto Elcano de Estudios Internaciónales y Estrategicas* [Online]. Available at: <<http://www.realinstitutoelcano.org/wps/portal/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLN4w3dgHJmMWbxDv56UciixjEO8IFgvS99X098nNT9QP0C3JDI8odHRUBfjhEiQ!!/delta/base64xml/L3dJdyEvd0ZNQUFzQUMvNElVRS82XzRfQk4!?WCM_GLOBAL_CONTEXT=/wps/wcm/connect/Elcano_es/Zonas_es/ARI%20110-2005>> [Accessed 30 July 2008].

Gerboles, D. (2011). Obama Venga el 11-M, El Terror Continua. *Mi Punto de Vista* [online]. Available at <<http://davidgerbolesperez.blogspot.com/2011/05/compasion-con-bin-laden.html>> [Accessed 03 May 2011].

Gerstenfeld, P.B., Grant, D.R. & Chiang, C.P., (2003). Hate Online: A Content Analysis of Extremist Internet Sites. *Analyses of Social Issues and Public Policy*, Vol. 3, No. 1, 2003, pp. 29-44.

Gibson, S., (2004). Open Source Intelligence. An Intelligence Lifeline. *RUSI Journal* February 2004.

Giddens, A., (1984). *The Constitution of Society: Outline of the Theory of Structuration*. University of California Press.

Gilboa, E., (2005). The CNN Effect: The Search for a Communication Theory of International Relations. *Political Communication,* 22:27-44.

Gilpin, R., (2005). War Is Too Important to Be Left to Ideological Amateurs. *International Relations*, 2005; 19; 5.

Gíminez C.M., (2010). En Recuerdo a las Víctimas del Atentado del 11 de Marzo. [online] Available at <<http://www.masciudadania.es/cmonton/2010/03/11/en-recuerdo-a-las-victimas-del-atentado-del-11-de-marzo/>> [Accessed 01 February 2011].

Ginesta, X., & Sopena, J. (2009). Spanish Social Movements in the Digital Age: The Demonstration Against the Popular Party and the Call for the “Botellón”. *American Communication Journal*. Vol. 11, No. 2, Summer 2009.

Global Network Initiative. (2008). Internet Rights Protection Initiative Launches. Global Network Initiative. [online]. Available at <<http://www.globalnetworkinitiative.org/>> [Accessed 01 November 2008].

Goldschmidt, E., (2005), Storming the Fences: Morocco and Europe’s Anti-Migration Policy, *Middle East Report*. [online]. Available at <<http://www.merip.org/mer/mer239/goldschmidt.html>> [Accessed 03 August 2010].

Goodman, A., (2008). Extremists Plotted Attacks Across Europe, Spanish Paper Says. [online] Available at <<http://edition.cnn.com/2008/WORLD/europe/01/27/spain.europe.terror.plot/index.html>> [Accessed on 18 June 2011].

Goonatilake, S., (1998). *Toward a Global Science: Mining Civilizational Knowledge*. Indiana University Press.

Gordon S., Ford, R., (2003). Cyberterrorism? Symantec Security Response White Paper. Symantec Corporation.

Gottfredson, M., Hirschi, T., (1990). *A General Theory of Crime*. Stanford University Press.

Graffy, C., (2009). The Rise of Public Diplomacy 2.0. *The Journal of International Security Affairs*. Fall 2009, No. 17.

Granovetter, M., (1973). The Strength of Weak Ties. *The American Journal of Sociology*, Vol. 78, No. 6, (May 1973), pp.1360-1380

Grusin, R., (2004). Premediation. *Criticism*, Winter 2004, Vol. 46, No. 1, pp.17-39.

Gonzales, A.R., (2006). *Remarks by Attorney General Alberto R. Gonzales at the International Institute for Strategic Studies*. London England.

The Guardian (2007). The Madrid Bombings. [online] Available at <<http://www.guardian.co.uk/world/2007/oct/31/spain.menezes>> [Accessed on 22 July 2011].

Guertner, G., (2007). European Views of Preemption in US National Security Strategy, *Parameters*, [Online]. Available at: <<http://www.carlisle.army.mil/USAWC/parameters/07summer/guertner.pdf>> [Accessed 14 August 2008]

Guha, S., Tang, K. & Francis, P. (2008). NOYB: Privacy in Online Social Networks. *WOSN ’08*, August 18, Seattle, Washington, USA.

Gurutz Jaruegi., (2006). National Identity and Political Violence in the Basque Country, *European Journal of Political Research*, [Online] Available at: <[http://www3.interscience.wiley.com/journal/119497883/abstract> [Accessed 27 November 2008](http://www3.interscience.wiley.com/journal/119497883/abstract%3e%20%5bAccessed%2027%20November%202008)]

Halverson, J.R., (2011). *The Tariq ibn Master Narrative*. Consortium for Strategic Communication. Report #1101.

Ham, S., Atkinson, R.D., (2002), *Using Technology to Detect and Prevent Terrorism*. Progressive Policy Initive, January 2002.

Hansen, L., (2007). The Clash of Cartoons? The Clash of Civilisations? Visual Securitization and the Danish 2006 Cartoon Crisis. 48th Annual ISA Conference Paper, Chicago, Illinois.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security and the Copenhagen School. *International Studies Quarterly (forthcoming).*

Harris, J., (2005). The Ordering of Things: Organization in Bruno Latour. *The Sociological Review*, Volume 53, Issue Supplement s1, pages 163-177, October 2005.

Haythornwaite, C. (1996). Social Network Analysis: An Approach and Technique for the Study of Information Exchange. *LISR* 18, 323-342.

Helibroner, R., (1994) *Technological Determinism Revisited* in Roe Smith, M., (1994), *Does Technology Drive History?* MIT Press.

Hetcher, S., (2007). User-Generated Content and the Future of Copyright: Part One – Investiture of Ownership. *Vanderbilt Journal. of Entertainment and Technology. Law* Vol. 10:4:863.

Herman, E.S., & Chomsky, N. (1988). *Manufacturing Consent, A Propaganda Model*. Pantheon Books.

Hernández, L., (2007). *Crímines,y Delincuencia en Internet*. Laboratorio de Seguridad Informática. Centro Tecnológico Aragón.

Hirsch, M., (2004). *Bernard Lewis Revisited. What if Islam Isn’t an Obstacle to Democracy in the Middle East, but the Secret to Achieving It*? The Washington Monthly.

Hoffman, B., (1993). *“Holy Terror”: The Implications of Terrorism Motivated by a Religious Imperative*. Rand, 1993.

Hoffman, B., (2002). Rethinking Terrorism and Counterterrorism Since 9/11. *Studies in Conflict and Terrorism*, 25: 303-316, 2002.

Hoffman, B. (2006). *Inside Terrorism*. Columbia University Press.

Hofkirchner, W., (2005). *Ludwig von Bertalanffy Forerunner of Evolutionary Systems Theory.* ICT&S Center for Advanced Studies and Research in Information and Communication Technologies & Society, University of Salzberg, Austria, 1-6.

Hooper, J., (1986). *The New Spaniards*. Penguin Books.

Hope, S. (2009). Public Diplomacy and Local Staff: The Cornerstone of Long-Term Relationship Building. *Public Diplomacy Magazine*. Winter, 2009.

Horgan, J., (2008). Deradicalization or Disengagement? A Process in Need of Clarity and a Counterterrorism Initiative in Need of Evaluation. Perspectives on Terrorism [online]. Available at <<http://terrorismanalysts.com/pt/index.php/pot/article/view/32/html>> [Accessed 17 January 2012].

Horgan, J., (2009). *Walking Away from Terrorism: Accounts of Disengagement from Radical and Extremist Movements*. Routeledge.

Hoskins, A., & O’Loughlin, B. (2010). Remediating *jihad* for Western news audiences: the renewal of gatekeeping? Tuning In: Diasporic Contact Zones at the BBC World Service. *Working Paper Series*. Working Paper No. 21

House of Lords, (2005). *After Madrid: the EU’s Response to Terrorism*. UK Government.

Hu, Y., Wang, Y. & Di, Z. (2009). The Scaling Laws of Spatial Structure in Social Networks. Department of Systems Science, School of Management and Center for Complexity Research, Beijing Normal University, Beijing 100875, China

Huberman, B.A., Romero, D.M., & Wu, F., (2009). Social Networks that Matter: Twitter Under the Microscope. *First Monday*, Volume 14, Number 1-5 January 2009

Hudson, R.A., Majeska, M., Saveda, A.M. & Metz, H.C. (1999). The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why? A Report Prepared Under an Interagency Agreement by the Federal Research Division, Library of Congress.

Human Rights Watch, (2005). False Freedom: Online Censorship in the Middle East, Human Rights Watch, Vol. 17, No. 10 [online]. Available at: <<http://www.hrw.org/reports/2005/mena1105/>> [Accessed on 01 May 2008].

Human Rights Watch, (2005). Setting an Example? Counter-terrorism Measures in Spain. *Human Rights Watch*. [Online]. Available at <<http://www.hrw.org/en/node/11860/section/1> > [Accessed 07 July 2008]

Human Rights Watch, (2008). Pre-empting Justice, *Human Rights Watch* [Online]. Available at <<http://www.hrw.org/en/reports/2008/07/01/preempting-justice>>. [Accessed 06 September 2008].

Hunter, M.L., & Wassenhove, L.N. (2010). Disruptive News Technologies: Stakeholder Media and the Future of Watchdog Journalism Business Models. *INSEAD The Business School*. Working Paper.

Huntington, S.P., (1993). The Clash of Civilisations. *Foreign Affairs*; Summer 1993; 72, 3.

Huntington, S. (2002). *Clash of Civilisations: And the Remaking of World Order*, Free Press

Ikenberry, J., (1999). Why Export Democracy? The Hidden Agenda of American Foreign Policy. *The Wilson Quarterly*. 23, (2).

Identity Theft in the UK Blog. (2010). Identity Theft is on the Rise in the UK [online]. Available at <<http://id-theft-uk.blogspot.com/2010/02/identity-theft-is-on-rise-in-uk.html>> [Accessed 01 August 2011].

(2010). Index of/pub/academic/communications logs/Gulf-war, *iBiblio*. [online] <<http://www.ibiblio.org/pub/academic/communications/logs/Gulf-War/>> [Accessed] 12 August 2010

Intel, (2005). Moore’s Law: Raising the Bar. Intel Corporation. [online] <<http://download.intel.com/museum/Moores_Law/Printed_Materials/Moores_Law_Backgrounder.pdf>> [Accessed 19 June 2011].

International Center for Religion & Diplomacy, 2011. Faith-based Diplomacy Yields Results. [online] Available at <<http://www.icrd.org/index.php?option=com_content&task=view&id=297&Itemid=297>> [Accessed 06 April 2011].

International Institute of Strategic Studies, (2000). Basque Separatist Terrorism. A Bloody Resurgence. *IISS Strategic Comments*. Volume 6, Issue, 8, October 2000, Basque Separatism.

Internet World Stats., (2008) Internet Usage Statistics: The Internet Big Picture. [Online] Available at <<http://www.internetworldstats.com/stats.htm>> [Accessed 27 October 2008].

Internet World Stats. (2011). World Internet Usage Statistics News and World Population Stats. [online] Available at <<http://www.internetworldstats.com/stats.htm>> [Accessed on 13 June 2011].

Irrepressible.info, *Amnesty International*, [online]. Available at <<http://irrepressible.info/>> [Accessed 23 May 2008].

Isaacs, R.J., (2009). The North African Franchise: AQIM’s Threat to U.S. Security. *Strategic Insights*, Volume III, Issue 5 (December 2009).

Izquierdo, J.M., (2011). Hay GAL y GALES. El Ojo Izquierdo, *El País* [online]. Available at < <http://blogs.elpais.com/ojo-izquierdo/2011/05/hay-gal-y-gales.html>> [Accessed 03 May 2011].

Jackson, R., (2005). Security, Democracy, and the Rhetoric of Counter-Terrorism. *Democracy and Security*, 1:147-171, 2005.

Jackson, R., (2006). Religion, Politics and Terrorism: A Critical Analysis of Narratives of “Islamic Terrorism”. *Centre for International Politics Working Paper Series*, No. 21, October 2006.

Jackson, R., (2007). *Terrorism Studies and the Politics of State Power*. Paper Prepared for International Studies Association (ISA) 47th Annual Convention, 28 Feb. – 3 March, 2007, Chicago, United States.

Jackson, R., Gunning, J. & Smyth, M.B., (2007). The Case for a Critical Terrorism Studies. Prepared for Delivery at the 2007 Annual Meeting of the American Political Science Association, August 30 – September 2, 2007.

Jackson, R., (2007). The Core Commitments of Critical Terrorism Studies. European Political Science. (1-8), 2007, European Consortium for Political Research, 1680 – 4333/07 530.

Jackson, R., (2008). *The Ghosts of State Terror: Knowledge, Politics and Terrorism Studie*s. Paper Prepared for the International Studies Association (ISA) Annual Conference 26-29 March, 2008, San Francisco, USA.

The Japan Exchange and Teaching Programme. 2011. *Welcome to the JET Programme*. [online] Available at <http://www.jetprogramme.org/e/introduction/index.html> [Accessed 06 April 2011].

Jenkins, B., (1974). *International Terrorism: A New Kind of Warfare*. RAND.

Jenkins, B.M., (2006). *Unconquerable Nation. Knowing Our Enemy Strengthening Ourselves*. RAND.

Jentleson, B.W., (2002). The Need for Praxis: Bringing Policy Relevance Back In. *International Security,* Vol. 26, No. 4 (Spring 2002), pp. 169–183

Jesús, C., (2008). La Radicalización Islamista en España Hoy. *Grupo de Estudios Estratégicos*, Análisis No. 273 10 de Abril 2008.

Johns, M, Chen, S, Hall, G., (2004). *Online Social Research. Methods, Issues & Ethics*. Peter Lang Publishing.

Johnson, J., (1988). Mixing Humans and Nonhumans Together: The Sociology of a Door-Closer. *Social Problems*, Vol. 35, No. 3, June 1988.

Jones, C, & Munro, R., (2005). *Contemporary Organization Theory*. The Editorial Board of the Sociological Review.

Jordan, K, Hauser, J, Foster, S., (2003). The Augmented Social Network: Building Trust into the Next-generation Internet. *First Monday*, Vol. 8, No. 4.

Jordán, J. (2003). Islamist Terrorist Rings in Spain. Current Situation and Future Outlook. *Real Instituto Elcano de Estudios Internacionales y Estrátegicos*. ARI No 119/2003.

Jordán, J., (2005). El Terrorismo Yihadista en España: Evolución después del 11-M. *Real Instituto Elcano de Estudios Internacionales y Estratégicos*, Documento de Trabajo, No 7/2009.

Jordán, J. (2005). *El Terrorismo Yihadista En España*. Jihad Monitor.

Jordán, J., 2005. El yihadismo en España: situación actual, *Real Instituto Elcano de Estudios Internacionales y Estratégicas*, [Online]. Available at: <<http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/Elcano_es/Zonas_es/Defensa+y+Seguridad/ARI+93-2005>> [Accessed 15 July 2008].

Jordán J., Torres, M., (2007). Internet y actividades terroristas: el caso del 11-M. *El profesional de la información*, 2007, marzo-abril, v. 16, n. 2, pp. 123-130

Jordán, J., Torres, M., (2007). *Nueva Amenaza Indirecta Contra Espana*. Jihad Monitor Special Report.

Jordán, J., (2008). Las Nuevas Insurgencias. Análisis de un Fenómeno Estratégico Emergente. *Anuario de Derecho Internacional*, Vol. XXIV.

Jordán, J., (2009). Procesos de Radicalización Yihadista en España. Análisis Sociopolítico en Tres Niveles. *Revista de Psicología Social*, 2009, 24 (2), 197-216

Jordán, J., (2009). Politicas De Prevencion De La Radicalizacion Violenta En Europa: Elementos De Interes Para Espana. *Revista Electrónica de Ciencia Penal y Criminología*

Jutlia, M. (2009). *Critical Approaches to Security: Securitization*. University of Helsinki.

Jones, S., (1999). *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. Routledge.

Kaldor, M., (2006). *New & Old Wars*. Cambridge, Polity.

Kanayama, H., Nasukawa, T., and Watanabe, H. (2004). Deeper Sentiment Analysis Using Machine Translation. Tokyo Research Laboratory, IBM Japan.

Kaplan, A.M. & Haenlein, M., (2010). Users of the World, Unite! The Challenges and Opportunities of Social Media. *Business Horizons* (2010), 53, 59-68.

Karatzogianni, A., (2008). *Cyber-Conflict and Global Politics*. Routledge.

Katona, Z., Zubcseck, P.P., & Sarvary, M. (2010). Network Effects and Personal Influences: The Diffusion of an Online Social Network. *Haas School of Business*.

Kearns, I., & Gude, K. (2008). The New Front Line: Security in a Changing World. IPPR Commission on National Security, Baseline Paper.

Keen, P., (2010). ‘Increasing Importance of Real-Time Search’, Keenpath. [online] <<http://keenpath.com/blog/increasing-importance-of-real-time-search>> [Accessed 13 July 2010].

Kellogg, D., (2010). ‘iPhone Vs Android.’ Nielsenwire. [online] <<http://blog.nielsen.com/nielsenwire/online_mobile/iphone-vs-android/>> [Accessed 13 August 2010].

King, G., (2009). The Changing Evidence Base of Social Science Research in Chapter 38, Pp. 91–93, Gary King, Kay Scholzman, and Norman Nie eds., *The Future of Political* Science: 100 Perspectives. New York: Routledge Press, 2009.

Kim, D.Y. & Chen, Z. (2010). Effects of Narrative vs. Non-Narrative Message on Attitudes and Memory: Comparison of Implicit and Explicit Attitude Measures. International CHRIE Conference-Refereed Track. Paper 9.

Kephart, J., (2006). Immigration and Terrorism: Moving Beyond the 9/11 Staff Report on Terrorist Travel. *The Quarterly Journal*, Fall 2006.

King, G., Lehman Schlozman, K., & Nie, N.H., (2009). *The Future of Political Science: 100 Perspectives*. Routeledge, 2009.

Kirkpatrick, M., (2010). Explaining the Real-Time Web in 100 Words or Less, Read Write Web. [online] <http://www.readwriteWeb.com/archives/explaining\_the\_real-time\_Web\_in\_100\_words\_or\_less.php> [Accessed 13 August 2010].

Kjeldskov, J, Graham, C., (2003). ‘A Review of Mobile HCI Research Methods’, *Mobile HCI 2003 Conference Paper.*

Knight, Alan and Kasun Ubayasiri (2003), *eTerror : Journalism, Terrorism and the Internet* [online]. Available at <http://www.ejournalism.au.com/ejournalist/alkas.pdf> [Accessed 12 May 2008].

Knight, C. & Murphy, M. & Mousseau, M., (2003). Correspondence: The Sources of Terrorism, *International Security*, Vol. 28, No. 2

Kranzberg, M. (1959) *Technology and History: “Kranzberg’s Laws”*, John Hopkins University Press

Krazit, T., (2010). ‘Making the Real-Time Web Relevant’, CNET. [online] <<http://news.cnet.com/8301-30684_3-20001715-265.html>> [Accessed 13 August 2010].

Krebs, V.E., (2002). Mapping Networks of Terrorist Cells. *Connections*. 24 (3): 43-52.

Krishnamurthy, B., Gill, P., & Arlitt, M. (2008). A Few Chirps about Twitter. *WOSN’08,* August 18, 2008, Seattle, Washington, USA.

Kolari, P., Finin, T., & Joshi, A. (2006). *SVMs for the Blogosphere: Blog Identification and Splog Detection*. American Association for Artificial Intelligence.

Kozinets, R.V., (2002). The Field Behind the Screen: Using Netnography for Marketing Research in Online Communities. *Journal of Marketing Research*, Vol. 39, No.1, (Feb., 2002), pp.61-72.

Kozinets, R.V., (2010). *Netnography: Doing Ethnographic Research Online*. SAGE Publications Ltd.

Kozinets, R.V., (2010). *Netnography: The Marketer’s Secret Weapon. How Social Media Understanding Drives Innovation*. Netbase Solutions, Inc.

Kranzberg, M. (1986). Technology and History: “Kranzberg’s Laws”. *Technology and Culture*, Vol. 27, No.3 (Jul., 1986), pp.544-560.

Kratochwil, F., & Ruggie, J.G., (1986). International Organization: A State of the Art on an Art of the State. *International Organization.* 40, 4, Autumn 1986.

Krebs, V.E., (2002). Mapping Networks of Terrorist Cells. *Connections*, 25(3): 43-52.

Kurzweil, R., (2006). The Third Generation Web Is Coming, Kurzweil AI Net [Online], Available at: <<http://www.kurzweilai.net/meme/frame.html?main=/articles/art0689.html>> [Accessed 28 March 2009].

de Laat, M., (2002). Network and Content Analysis in an Online Community Discourse. In: G. Stahl (Ed.), Proceedings of Computer Support for Collaborative Learning (CSCL) 2002 Conference, Jan. 7-11, Boulder, CO. Mahwah, NJ: Lawrence Erlbaum, 625-626, <<http://newmedia.colorado.edu/cscl/62.pdf>> [Accessed November 2007].

La Porte, T. (2011). The Power of the European Union in Global Governance: A Proposal for a New Public Diplomacy. *CPD Perspectives on Public Diplomacy*. Paper 1, 2011.

La Rue, F. (2011). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. United Nations General Assembly, Human Rights Council. A/HRC/17/27

Laciner, S., 2006. The West and Terrorism: PKK as a Priveliged Terrorist Organisation, *The Journal of Turkish Weekly*, [Online] Available at: <<http://www.turkishweekly.net/editorial.php?id=29>> [Accessed November 2008].

Lacquer, W., *The Terrorism to Come,* Policy Review, 126.

Latour, B. (1988). *The Prince for Machines* in Elliot, ed. *Technology and Social Process*, Edinburgh University Press.

Law, J. (1992). Notes on the Theory of the Actor Network: Ordering, Strategy and Heterogeneity. [online] < <http://comp.lancs.ac.uk/sociology/soc054jl.html>> [Accessed 09 July 2011].

Law, J., & Callon, M., (1988). Engineering and Sociology in a Military Aircraft Project: A Network Analysis of Technological Change. *Social Problems*, Vol. 35, No. 3, June 1988.

Law, J., (1992). *Notes on the Theory of the Actor Network: Ordering, Strategy and Heterogenity*. Centre for Science Studies Lancaster University.

Law, J., & Hassard, J. (1999). *Actor Network Theory and After*. Blackwell Publishing.

Leiner, B.M. et al., (2003). A Brief History of the Internet, Internet Society, [Online]. Available at: <<http://www.isoc.org/Internet/history/brief.shtml#Future>> [Accessed 10 December 2008].

Leonard, M. (2002). Diplomacy by Other Means. *Foreign Policy*, No. 132 (Sep – Oct 2002), pp.48-56

Lesser, I., Hoffman, B., Arquilla, J., Ronfeldt, D., & Zanini, M., (1999). *Countering the New Terrorism*. Rand Corporation.

Lessig, L., (2006). *Code 2.0,* Basic Books

Lessig, L., (2003), *The Future of Ideas: The Fate of the Commons in a Connected World*, Random House USA Inc.

Lev-On, A., & Hardin, R., (2007). Internet-based Collaborations and their Political Significance. *Journal of Information Technology and Politics*, Vol. 4(2), 2007.

Levi, M., Wall, D.S., (2004), Technologies, Security, and Privacy, in the Post-9/11, European Information Society. *Journal of Law and Society*, Vol. 31, Number 2, June 2004.

Los GRAPO, (2005) Terroristas Germinados en los Anos 60. El Mundo, [online]. Available at <http//www.elmundo.es/elmundo/200505/31/espana/1117527674.html> [Accessed on 08 August 2010].

Lewis, J.A., (2002). Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies.

Lia, B., & Heggenhammer, T. (2004). *Study Preceding the Madrid Bombings. Studies in Conflict and Terrorism*. Taylor & Francis Inc.

LNE.es, (2010). Víctimas y Políticos Recuerden por Separado el 11-M. [online] Available at <<http://www.lne.es/espana/2010/03/11/silencio-reina-homenaje-victimas/884914.html?pCom=2#EnlaceComentarios>> [Accessed 01 February 2011].

Loayza, J. (2008). How to Quiet Twitter Noise. Mashable. [online] <<http://mashable.com/2008/12/08/how-to-quiet-the-twitter-noise/>> [Accessed 19 July 2011].

Loscertales, V.G. (2010). Advancing Public Diplomacy Through World Expos. Public Diplomacy Magazine. Winter 2010. [online] Available at <<http://publicdiplomacymagazine.com/advancing-public-diplomacy-through-world-expos/>> [Accessed 20 Apr 2011].

Ludes, J.M., (2004). *Attacking Terrorism: Elements of a Grand Strategy*. Georgetown University Press.

Lynn, P, Kaminska, O., (2010). ‘The Impact of Mobile Phones on Survey Measurement Error’ *Institute for Social and Economic Research Paper*.

Luengo O.G., (2001). Los Medios de Comunicación y las Nuevas Tendencias del Terrorismo Internacional. *Conferencia Internacional “La Seguridad Europea en el Siglo XX1”* Universidad de Granada, 5-9 de Noviembre de 2001.

Lynch, M., (2004). Shattering the “Politics of Silence:” Satellite Television Talk Shows and the Transformation of Arab Political Culture. *Arab Reform Bulletin*, December 2004, Volume 2, Issue 11.

Mackey, R. (2009). Landslide or Fraud? The Debate Online Over Iran’s Election Results. *The New York Times*. [online] Available at <<http://thelede.blogs.nytimes.com/2009/06/13/landslide-or-fraud-the-debate-online-over-irans-election-results/>> [Accessed 14 January 2011].

Mackensie, D. & Wajcman, J., (1999). *The Social Shaping of Technology*, Open University Press

MacKinnon, A.D., (2007). Counterterrrosim and Checks and Balances: The Spanish and American Examples. *New York University Law Review.*

Madey, G., Freeh, V., Tynan, R., 2002, The Open Source Development Phenomenon: An Analysis Based on Social Network Theory, Eighth Americas Conference on Information Systems [Online], Available at: <<http://www.nd.edu/~oss/Papers/amcis_oss.pdf>> [Accessed 28 May 2009].

Makarenko, T., (2004). The Crime-Terror Continuum: Tracing The Interplay Between Transnational Organised Crime And Terrorism. *Global Crime*, Vol. 6, No. 1, February 2004, pp. 129-145.

Manheim, J.B. and Albritton, R.B., (1984). Changing National Images: International Public Relations and Media Agenda Setting. *American Political Science Review. American Political Science Association*. Vol. 78, No. 3, Sep. 1984

Mann, M., (2002). Globalisation As Violence, *University of California*, [Online]. Available at <<http://www.sscnet.ucla.edu/soc/faculty/mann/globasviol%5B1%5D.pdf>>, [Accessed 27 July 2006]

Markham, A.N. (2005). Disciplining the Future: A Critical Organizational Analysis of Internet Studies. *The Information Society*, 21: 1-11, 2005.

Markham, A.N. (2005). The Methods, Politics, and Ethics of Representation in Online Ethnography. *Handbook of Qualitative Research*. Routledge.

Markham, A. N. (2011). *Internet Research*. In Silverman, D. (Ed.). *Qualitative Research: Theory, Method, and Practices*, *3rd Edition*. London: Sage.

Markoff, J., 2006. Entrepreneurs See a Web Guided by Common Sense New York Times [Online], Available at: <[http://www.nytimes.com/2006/11/12/business/12Web.html?ex=1320987600&en=a54d6971614edc62&ei=5090&partner=rssuserland&emc=rss](http://www.nytimes.com/2006/11/12/business/12web.html?ex=1320987600&en=a54d6971614edc62&ei=5090&partner=rssuserland&emc=rss)> [Accessed 11 December 2006].

Marsaud, O., (2006). Le juge Bruguière démenti par Ruzibiza, l’un de ses témoins-clés, *Rwanda Development Gateway*, [Online]. Available at: <<http://www.rwandagateway.org/article.php3?id_article=3795>> [Accessed November 2008].

Martín, J.L., Labari, N., Figueras, A., & Martín, N., (2004). Explosiones en Atocha, Santa Eugenia y El Pozo. [online] Available at < <http://www.elmundo.es/elmundo/2004/03/11/espana/1078988734.html>> [Accessed on 22 July 2011].

Marx, K. & Engels, F. (ed.) (2007). *Capital: A Critique of Political Economy Vol. I – Part I, The Process of Capitalist Production*. Cosimo, Inc.

Mateo, L. (2003). Recomendado. Asociación Víctimas del Terrorismo. [online] Available at < <http://www.lolamateo.es/recomendado-asociacion-victimas-del-terrorismo/>> [Accessed 23 July 2011].

Mayer, J.M., (2011). Attentats en Norvège: idéologie et motivations du terroriste. Terrorisme.net. [online] Available at <<http://www.terrorisme.net/p/article_245.shtml>> [Accessed 25 July 2011].

Mayo, M.G. & Page, D., (2010). España cierra la puerta a la inmigración: sólo 18.000 nuevos permisos de trabajo. El País. [online] Available at <<http://www.expansion.com/2010/05/24/economia-politica/1274703180.html>> [Accessed on 25 May 2010].

McColgan, M. & Attanasio, A., (1999). France: La porte ouverte á l’arbitraire”, *Féderation Internationale des Ligues des Droits de l’Homme*, 1-35.

McConnell, M., (Date unknown). Overhauling Intelligence. *Foreign Affairs* 86 No.4.

McCulloh, I., Carley, K., & Webb, M. (Date Unknown). Social Network Monitoring of Al-Qaeda.

McInerney, L., (2007). *Virtual* Theatre of Terror: Spotlight on the Audience. Working paper prepared for presentation at the PSAI Postgraduate Conference The University of Dublin, Trinity College, May 2007.

McLaughlin, A. (2006). Google in China, Google Blog, [Online] Available at: <<http://googleblog.blogspot.com/2006/01/google-in-china.html>> [Accessed 01 February 2008].

Meier, P.P., (2009). A Brief History of Crisis Mapping (Updated). iRevolution. [online] Available at <<http://irevolution.wordpress.com/2009/03/12/a-brief-history-of-crisis-mapping/>> [Accessed 20 July 2010].

Meier, P., & Leaning, J., (2009). *Applying Technology to Crisis Mapping and Early Warning in Humanitarian Settings.* Crisis Mapping Working Paper I of III. Harvard Humanitarian Initiative.

Mejova, Y., (2009). Sentiment Analysis: An Overview. Comprehensive Exam Paper. *Computer Science Department*, University of Iowa.

Melissen, J., (2005). Wielding Soft Power: The New Public Diplomacy. Netherlands Institute of International Relations Clingendael.

Mell, P., & Grance, T., (2011). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology*. Special publication 800-145 (Draft).

Mercer, J., (1996). *Reputation and International Politics*. Cornell University Press.

Metz, S., & Kievit, J., (1995). Strategy and the Revolution in Military Affairs: From Theory to Policy. U.S. Army.

Michavila, N., (2005). Guerra, terrorismo y elecciones: incidencia electoral de los atentados islamistas en Madrid, [Working Paper] *Real Instituto Elcano de Estudios Internaciónales y Estrategicas*, 1-35.

Mika, P., (2005). Flink: Semantic Web Technology for the Extraction and Analysis of Social Networks. *Web Semantics: Science, Services and Agents on the World Wide Web 3* (2005) 211-223.

Millet, E., (2008). Arrests Worry Barcelona’s Pakistanis. *BBC News* [online]. Available at <<http://news.bbc.co.uk/2/hi/south_asia/7202393.stm>> [Accessed on 17 November 2010].

Milner, H., (1992). International Theories of Cooperation Among Nations. Strengths and Weakneses. *World Politics*, 44(April 1992), 466-96.

Minchoa, S. (2009). A Study on the Effective Use of Social Software by Further and Higher Education in the UK to Support Student Learning and Engagement. The Open University.

Ministerio de la Defensa,. (2003). *Revisión Estratégica de la Defensa*, [Online]. Available at: <http://www.mde.es/descarga/red.pdf> [Accessed 20 August 2008].

Ministerio del Interior (2006). Interior Destina 1,000 Policías a la Lucha Contra el Terrorismo Islamista. Gobierno de España. [online] Available at < <http://www.mir.es/DGRIS/notas_prensa/ministerio_interior/2006/np021703.htm>> [Accessed 01 February 2009].

Mislove, A., Druschel, P., Marcon, M., Bhattachargee, B., & Gummadi, K.P. (2007). Measurement and Analysis of Online Social Networks. *IMC ’07,* October 24-26, 2007.

Mitra, S. (2007). Web 3.0 & the Semantic Web. [online]. <<http://www.sramanamitra.com/200706/28/web-30-the-semantic-web/>> [Accessed 08 February 2008].

Mislove, A., Gummadi, K.P. & Druschel, P. (2006). Exploiting Social Networks for Internet Search. *In Proceedings of the 5th Workshop on Hot Topics in Networks* (HotNets-V), Irvine, CA, Nov 2006.

Moffitt, S., & Dover, M., (2011). *Wikibrands. Reinventing your Company in a Customer-Driven Marketplace*. McGraw Hill Books.

Moghaddam, F.M., (2005). The Staircase to Terrorism: A Psychological Exploration. *American Psychologist*, February – March 2005, Vol. 60, No. 2, 161-169.

Monmar, (2010). Islamización de Europa “Eurabia”. Más pruebas de la presencia de Al Qaeda en España. [online] Available at <[http://alianzacivilizaciones.blogspot.com/2009/11/mas-pruebas-de-la-presencia-de-al-qaeda.html>](http://alianzacivilizaciones.blogspot.com/2009/11/mas-pruebas-de-la-presencia-de-al-qaeda.html%20) [Accessed on 01 March 2011].

Moore, M., (2005). End of Terrorism? ETA and the Efforts for Peace. *Harvard International Review* [online]. 27 (2), 2005. Available at <<http://www.harvardir.org/articles/1354/> >[Accessed 01 July 2005].

Moreno, L. (2004). The Madrid Bombings in the Domestic and Regional Politics of Spain, *Spanish National Research Council*, (2004), Working Paper.

Mueller, J. (2004). Why Isn’t There More Violence? *Security Studies* 13, No. 3 (Spring 2004): 191-203

Munro, R., (2009) *Actor-Network Theory* in Clegg, S. & Haugaard, M. (eds.), *The SAGE Handbook of Power*. SAGE Publications Inc.

Muñiz A.M., & Schau, H.J., (2007). Vigilante Marketing and Consumer-Created Communications. *Journal of Marketing*, vol. 36, No. 3 (Fall 2007).

Murphy, M., (2010). War in the Fifth Domain. Are the Mouse and Keyboard the New Weapons of Conflict? The Economist, 1st July 2010. [online]. Available at <<http://www.economist.com/node/16478792>> [Accessed 08 July 2010].

Nacos, B., (2003). Terrorism as Breaking News: Attack on America. *Political Science Quarterly*, Vol. 118, No.1 (Spring, 2003), pp.25-32.

Naím, M., (2005). Post Terror Surprises, *Foreign Policy*, [online]. Available at: <<http://www.foreignpolicy.com/users/register.php?story_id=2460&registered_only=1&URL=http://www.foreignpolicy.com/story/cms.php?story_id=2460>> [Accessed June 2006].

Napolenoi, L, (2004). Money and Terrorism. *Strategic Insights*, Volume III, Issue 4 (April 2004).

Napoleoni, L., (2005). *The New Economy of Terror*. Open Democracy.

Nash, E., (1997). Spain Gripped by Mass Protest Against the ETA Gunmen. The Independent.

National Cybersecurity Alliance, 2010. *Stay Safe Online Homepage*. [online] <<http://www.staysafeonline.org/>> [Accessed 20 August 2010].

Network World, (2008). Software, Portal Target, Predict Terrorist Behavior, Network World, Feb. 2008, [Online] Available at: <<http://www.networkworld.com/community/node/25390>> [Accessed 28 May 2009].

Neuendorf, K.A., (2002). *The Content Analysis Guidebook*. SAGE Publications Inc.

Neumann, P.R., (2007). Negotiating with Terrorists. *Foreign Affairs*, Vol. 86, No. 1 (Jan. – Feb., 2007), pp. 128-138.

Neumann, P.R., (2008). *Terrorism in the 21st Century. The Rule of law as a Guideline for German Policy*. Friedrich Ebert Stiftung.

Nisbet, D., (2004). Measuring the Quantity and Quality of Online Discussion Group Interaction. *Journal of eLiteracy*, Vol. 1 (2004) 122-139.

Noya, J., (2006). Una diplomacia pública para España. *Real Instituto Elcano de Estudios Internacionales y Estrategia*. Documento de trabajo 11/2006. Julio de 2006.

Noya, J., (2006). Inmigración y diplomacia pública. *Real Instituto Elcano de Estudios Internacionales y Estrategia*. ARI No 108/2006. 23 octubre 2006.

Noya, J., (2009). La imagen exterior de España: nuevos escenarios y viejos problemas. *Real Instituto Elcano de Estudios Internacionales y Estrategia*. Documento de trabajo 60/2009.

Nuñez, M.M., & Sierra, A.M., (Date Unknown). La Manipulación en los Medios de Comunicación. Tratamiento Informativo del 11M. *Jornades de Foment de la Investigació*.

Nunes, M., (1995). Baudrillard in Cyberspace: Internet, Virality and Postmodernity. *Style*, 29: 314-327.

Nye, J. (1990). Soft Power. *Foreign Policy*, No. 80, Twentieth Anniversary (Autumn 1990), pp.152-171.

O’Connor, B., Balasubramanyan, R., Routledge, B., & Smith, N. (2010). From Tweets to Polls: Linking Text Sentiment to Public Opinion Time Series. Proceedings of the Fourth International Association for the Advancement of Artificial Intelligence Conference on Weblogs and Social Media. 2010.

OECD, (2007). Participative web and user-created content: Web 2.0, wikis, and social networking. Paris: Organisation for Economic Co-operation and Development.

Oikarinen, J. (Date Unknown). ‘IRC History by Jarkko Oikarinen,IRCNet.’ [online] <http://www.ircnet.org/History/jarkko.html> [Accessed 12 August 2010].

Olmeda, J., (2005). Fear or Falsehood? Framing the 3/11 Terrorist Attacks in Madrid and Electoral Accountability [Working Paper] *Real Instituto Elcano de Estudios Internaciónales y Estrategicas*.

Olmeda, J., (2005). Miedo o engaño? El encuadramiento de los atentados terroristas del 11-M en Madrid y la redición de cuentas electoral”, *Real Instituto Elcano de Estudios Internaciónales y Estrategicas*, 2005, No. 24.

O’Loughlin, B., (2007). Transnational Media, Public Diplomacy, and the Potential Impact of Networked Power: The Case of CENTCOM. Paper Presented to the International Broadcasting, Public Diplomacy and Cultural Exchange Conference, *SOAS*, London, 18-19 December 2007.

O’Reilly, T., 2007. Today’s Web 3.0 Nonsense Blogstorm Radar O’Reilly [Online] Available at: <[http://radar.oreilly.com/archives/2007/10/todays-Web-30-nonsense-blogsto.html](http://radar.oreilly.com/archives/2007/10/todays-web-30-nonsense-blogsto.html)> [Accessed October 2007].

Organisation for Economic Development, (2011). Broadband and Telecom. Organisation for Economic Development Directorate for Science, Technology and Industry. [online] Available from <<http://www.oecd.org/document/46/0,3746,en_2649_34225_39575598_1_1_1_1,00.html>> [Accessed 13 June 2011].

Orlikowski, W.J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. Organization Science, Vol. 3, No. 3, Focused Issue: *Management of Technology* (Aug., 1992), pp.398-427.

Orlikowski, W.J. Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations, *Organization Science*, 11, 4, 2000: 404-428.

Orlikowski, W.J. & Iacono, C.S. in King, J.L. & Lyytinen (eds) (2006). *Information Systems: The State of the Field*. John Wiley & Sons Ltd.

Organisation for Economic Development, (2011). Broadband and Telecom. *Organisation for Economic Development Directorate for Science, Technology and Industry*. [online] Available from <<http://www.oecd.org/document/46/0,3746,en_2649_34225_39575598_1_1_1_1,00.html>> [Accessed 13 June 2011].

Page, D., (2010). Efectos de la crisis: en 2014 no llegarán inmigrantes a España. El País [online]. Available at <<http://www.expansion.com/2010/03/03/economia-politica/1267620653.html>> [Accessed on 04 March 2010].

Page, D., & Mayo, M.G., (2010). Con crisis o sin ella, harán falta más inmigrantes. El País [online]. Available on <<http://www.expansion.com/2010/02/19/economia-politica/1266583356.html>> [Accessed on February 2010].

Palicio, I., (2010). El Intercambio de Información Financiera y la Lucha Contra la Financiación del Terrorismo: El Acuerdo UE-EEUU sobre SWIFT. *Real Instituto Elcano*, ARI 49/2010. 16 March 2010.

Pandora, 2008. Pandora.com, [online] Available at: <<http://www.pandora.com/restricted>> [Accessed 01 October 2008].

Pang, B., & Lee, L., (2008). Opinion Mining and Sentiment Analysis. *Foundations and Trends in Information Retrieval*. Vol. 2, No. 1-2 (2008) 1-135.

Papastamou. S., Iatridis. T., & Prodromitis, G., (2008). The Question of Content in the Study of Terrorism and the Timely Link to Social Influence. *Psicología Política*, No. 36, 2008, 51-76.

Park, H. W., (2003). Hyperlink Network Analysis: A New Method for the Study of Social Structure on the Web. *Connections*, 25(1), pp, 49-61.

Pascual, L.B. (2005). Modernisme and the 1888 Universal Exposition of Barcelona. Historical Lab 1 Bruxelles, 22 October 2005.

Paz, R. (2004). A Message to the Spanish People: The Neglected Threat by Qa`idat al-Jihad. Global Research in International Affairs (GLORIA) Center *The Project For The Research Of Islamist Movements (PRISM)*. Volume 2, Number 2.

Pearson, R., (2009). The London Summit 2009: Evaluation of Key Performance Indicators. Foreign and Commonwealth Office, July 2009. <<http://www.londonsummit.gov.uk/en/about1/evaluation-kpi/>> [Accessed January 2011].

Perez, C., (Date Unknown). Structural Change and Assimilation of New Technologies in the Economic and Social Systems, Carlota Perez, [Online] Available at <<http://www.carlotaperez.org/papers/scass%20v04.pdf>> [Accessed February 2010].

Pernick, R., Figallo, C., Williams, G.A., (1995). A Timeline of the First Ten Years of the WELL. WELL.com. [online]. Available at <<http://www.well.com/conf/welltales/timeline.html>> [Accessed 09 December 2010].

Del Pino, E., & Colino, C., (2010). National and Subnational Democracy in Spain: History, Models and Challenges. Working Paper. *Instituto de Políticas y bienes Públicos*. [IPP].

Pollitt, M.M., (1998). Cyberterrorism – Fact or Fancy? *Computer Fraud & Security*, February 1998.

Portero, F. Alianza de Civilizaciones: la democracia como amenaza. *Cuadernos de Pensamiento Político*, No. 8 (Oct. – Dec., 2005), pp. 113-128.

Portugués, J., (2009). Nuevos Avances y Retos en la Lucha Contra el Terrorismo. *Revista Electrónica de Estudios Internacionales*.

Portugués, J., (2010). Terrorism, Drug-Trafficking, Money Laundering, Human Trafficking, Smuggling of Migrants, Arms Trafficking: Global Fight Against Transnational Organised Crime. *Reflexión Politica*. Ano 12, No. 23, Junio de 2010.

Post, J.M., Ruby, K.G. & Shaw, E.D., (2000). From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. *Terrorism and Political Violence*, Vol.12, No.2, (Summer 2000), pp.97-122.

Prabowo, R., Thelwall, M., (2008). Sentiment Analysis: A combined approach. Journal of Informetrics 3 (2009) 143-157.

Prahl, L. (2007), More than a Political Shift: 11-M and its Impact on the Spanish Democracy. Honors Thesis, Political Science.

Prentice, S., Hoskins, A., O’Loughlin, B., Rayson, P., (2009). *Analysing the Semantic Content and Persuasive Composition of Extremist Media: A Case Study of Texts Produced During the Gaza Conflict*. Royal Holloway, University of London.

Présidence de le République., (2008). *The French White Paper on Defence and National Security*, [Online]. Available at: <<http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf> > [Accessed 30 June 2008].

Présidence de la République, (2008). *Discours de M. le Président de la République*, [Online]. Available at: <<http://www.elysee.fr/documents/index.php?cat_id=7>> [Accessed 30 June 2008].

Provoost, L., & Bornier, E. (Date Unknown). Service-Oriented Architecture and the Semantic Web: A killer combination? Department of Information and Computing Sciences University of Utrecht

Pang, B, & Lee, L. (2008). Opinion Mining and Sentiment Analysis. *Foundations and Trends in Information Retrieval*. Vol. 2, No. 1-2 (2008) 1-135.

Qin, J., Zhou, Y., Reid, E., Lai, G. & Chen, H., (2007). *Analyzing Terror Campaigns on the Internet: Technical Sophistication, Content Richness and Web Interactivity*. International Journal of Human-Computer Studies 65 (2007) 71-84.

Que.es (2009). 11M !Lo Conseguiremos, Saldrá la Verdad Algún Día! [online] <<http://blogs.que.es/yentel/2009/3/12/11m-conseguiremos-saldra-verdad-algun-dia->> [Accessed 01 February 2011].

Rafaeli, S., (1986). The Electronic Bulletin Board: A Computer-Driven Mass Medium. *Computers and the Social Sciences 2*. Paradigm Press.

Raffl, C., Hofkirchner, W., Fuchs, C. & Schafranek, M., (2011). *The Web as Techno-Social System: The Emergence of Web 3.0*. ICT&S Center, University of Salzberg, Austria, 1-6.

Rapoport, D., (2001). The Fourth Wave: September 11 in the History of Terrorism. *Current History*, Dec. 2001, v100 i650 p.419(6).

Rapoport, D., (2001). *Inside Terrorist Organisations.* Frank Cass Publishers.

Raufer, X., (2002). Organized Crime 1995 - 2002: Mafias, Cartels and "Gangsterrorists". Xavier Raufer.com. [online]. Available at <<http://www.xavier-raufer.com/english_6.php>> [Accessed 31 October 2010].

Raynes-Goldie, K., (2010). ‘Aliases, Creeping and Wall Cleaning: Understanding Privacy in the Age of Facebook’, *First Monday*, Vol. 15 No.1-4.

Read, J., Hope, D., and Carroll, J. (2007). Annotating Expressions of Appraisal in English. *In Linguistic Annotation Workshop*. Pages 93-100, Prague, June 2007.

Reid, E.F., & Chen, H., (2006). Mapping the Contemporary Terrorism Research Domain. *International Journal of Human-Computer Studies* 65 (2007) 42-56.

Reid, E. & Chen, H., (2007). Internet-Savvy U.S. and Middle Eastern Extremist Groups. *Mobilization: An International Quarterly Review*. 12(2): 177-192.

Reid, E. et al., (2007). Terrorism Knowledge Discovery Project: A Knowledge Discovery Approach to Addressing the Threats of Terrorism. *Department of Management Information Systems, The University of Arizona*, pp. 1-21

Reinares, F., (2005). The Mediterranean Region and International Terrorism: A New Framework for Cooperation? *Real Instituto Elcano de Estudios Internaciónales y Estrategicas*, [Online]. Available at: <<http://www.realinstitutoelcano.org/wps/portal/rielcano_eng/Content?WCM_GLOBAL_CONTEXT=/Elcano_in/Zonas_in/International+Terrorism/ARI+149-2005>> [Accessed 01 July 2008].

Reinares, F., (2006). Do Governments and Citizens Agree on How to Combat International Terrorism?, *Real Instituto Elcano de Estudios Internaciónales y Estrategicas*, [Online]. Available at <<http://www.realinstitutoelcano.org/wps/portal/rielcano_eng/Content?WCM_GLOBAL_CONTEXT=/Elcano_in/Zonas_in/Latin+America/ARI+78-2006>> [Accessed 02 July 2008].

Reinares, F., (2006). Hacia una caracterización social del terrorismo yihadista en España: implicaciones en seguridad interior y acción exterior”, *Real Instituto Elcano de Estudios Internacionales y Estratégicas* [Online]. Available at: <<http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/Elcano_es/Zonas_es/Terrorismo+Internacional/ARI+34-2006>> [Accessed 02 July 2008].

Reinares, F., (2006). ¿Coinciden el gobierno y los ciudadanos en que medidas adoptar contra el terrorismo internacional?” *Real Instituto Elcano de Estudios Internacionales y Estratégicas*, No. 78.

Reinares, F., (2006). Towards a Social Characterisation of Jihadist Terrorism in Spain: Implications for Domestic Security and Action Abroad. *Real Instituto Elcano de Estudios Internacionales y Estrátegicas*. ARI No 34/2006.

Reinares, F., (2008). Estamos más seguros frente a al-Qaeda? Reformas en la seguridad interior española y prevención del terrorismo global, 2004-2008, *Real Instituto Elcano de Estudios Internaciónales y Estrategicas*, Working Paper.

(2000). Regulation of Investigatory Powers Act 2000 (c. 23), London: Ministry of Justice.

Ressler, S. (2006). Social Network Analysis as an Approach to Combat Terrorism: Past Present and Future Research. *Homeland Security Affairs*, Volume 2, No. 2, (July 2006).

Rheingold, H., (1991) *Virtual Reality*. Secker and Warburg.

Rheingold, H., (1994). *The Virtual Community: Surfing the Internet*. Minerva.

Rheingold, H., (2003), *Smart Mobs: The Next Social Revolution*, Perseus Books.

Rice, Xan, (2008). Last Piece of Fibre-optic Jigsaw Falls Into Place as Cable Links East Africa to Grid. The Guardian Online. [Online]. Available at: <<http://www.guardian.co.uk/technology/2008/aug/18/east.africa.internet>> [Accessed 20 August 2008].

Richards, B., (2004). Terrorism and Public Relations. *Public Relations Review*, 30 (2004) 169-176.

Richardson, L., (2007). *What Terrorists Want: Understanding the Enemy, Containing the Threat*. Random House Publishing Group.

Rieselbach, L.N., (1969). The Behaviouralism Approach to the Study of Politics: An Overview. *Occasional Paper No. 3*. Office of Education (DHEW), Washington D.C. Bureau of Research.

Riffe, D., Lacy, S., & Fico, F., (1998). *Analysing Media Messages: Using Quantitative Content Analysis in Research*. Lawrence Earlbaum Associates.

Robb, J., (2007). The Coming Urban Terror: Systems Disruption, Networked Gangs and Bioweapons. *City Journal*, Summer 2007.

Roberts, G., 2007. Global Justice and the Future: Web 3.0 Is the Mesh, World, [Online] Available at: <<http://my-world.typepad.com/rworld/2007/09/global-justice-.html>> [Accessed November 2007].

Rodríguez, I.P. & Piella, G.C. (2008). El Enfoque Integral (Comprehensive *Approach)* a la gestión de crisis internacionales. *Real Instituto Elcano*. ARI No 115/2008.

Rodriguez, D., (2009). España Defenderá un Plan de Ciberseguridad a lo Obama en Europa. Soitu, Vida Digital. [online]. Available at <<http://www.soitu.es/soitu/2009/06/10/vidadigital/1244643739>> [Accessed 27 October 2010].

Rodrik. D., (2007). *One Economics. Many Recipes*. Princeton University Press.

Rogan, H., (2006). Jihadism Online - A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes. *FORSVARETS FORSKNINGSINSTITUTT Norwegian Defence Research Establishment*.

Rogers, R., (2008). *The Politics of Web Space*. Govcom.org.

Rogers, R. (2009). The End of the Virtual – Digital Methods. *Text prepared for the Inaugural Speech, Chair, New Media & Digital Culture, University of Amsterdam* 8 May 2009.

Rollins J., Wilson, C. (2007). *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*. Congressional Research Service Report for Congress. The Library of Congress.

Rosand, E., (2010). La Lucha contra el Terrorismo y el Fomento de la Cooperación en el Norte de África: La Trascendencia Potencial de la Estrategia de la ONU contra el Terrorismo Global. *Real Instituto Elcano*. ARI 162/2009.

Rosendorf, N.M. (2006). Be El Caudillo’s Guest: The Franco Regime’s Quest for Rehabilitation and Dollars after World War II via the Promotion of U.S. Tourism to Spain. *Diplomatic History*, Vol. 30, No. 3, (June 2006).

Ross, J.C., (2004), Securitizing Migration after 11 March, Real Instituto Elcano de Estudios Internacionales y Estratégicos, Demography & Population, 2004.

Rotman, D., & Preece, J., (2010). The ‘WeTube’ in YouTube – Creating an Online Community Through Video Sharing. *International Journal of Web Based Communities*, Vol. 6, No. 3, 2010.

(2004). Statement of Ethical Practice for the British Sociological Association. British Sociological Association. March 2002 (Updated May 2004).

(2010). Statistical Bulletin. Internet Access 2010. Households and Individuals. Office for National Statistics. 27 August 2010.

Sageman, M., (2004). *Understanding Terror Networks*. University of Pennsylvania Press.

Sageman, M. (2008). The Next Generation of Terror. *Foreign Policy*, March/April 2008.

Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press, 2008.

Saulatino, (2008). La Oreja de Van Gogh – 11 de Marzo. *Palabras Retorcidas*. [online] Available at <<http://palabrasretorcidas.wordpress.com/2008/07/20/11-de-marzo-presentcion-en-vivo-y-letra/>> [Accessed 01 February 2011].

Salellas, L., (2005). Delitos Informaticos, Ciberterrorismo. *Hadden Security Consulting*.

Salem, A., Reid, E. & Chen, H., (2006). Content Analysis of Jihadi Extremist Groups’ Videos. S. Mehrotra et al. (Eds.): ISI 2006, LNCS 3975, pp. 615 – 620, 2006.

Sanchez-Cuenca, L., (2004). La Selección de Víctimas en ETA. *Revista Española de Ciencia Política*. Núm. 10, Abril 2004, pp.53-79.

Sánchez, G., (2007). Periodistas en la diana. *Treinta años de amenaza terrorista a los* medios de comunicación españoles. Madrid, Asociación de la Prensa de Madrid, 236 págs.

Santana, J., (2009). España Lidera el Plan Europeo de CiberSeguridad en la Red. Panda Security. [online] Available to <<http://www.pandainsight.com/es/espana-lidera-el-plan-europeo-de-ciberseguridad>> [ Accessed 27 October 2010].

Schau, H.J., & Gilly, M.C., (2003). We Are What we Post? Self-Presentation in Personal Web Space. *Journal of Consumer Research*. Vol. 30, December 2003.

Schlosberg, D., Zavestoski, S. & Shulman, S., (2007). Democracy and E-Rulemaking: Web-Based Technologies, Participation, and the Potential for Deliberation. *Journal of Information Technology and Politics*. Vol. 4 (1) 2007.

Schneider, M., (2007). You Have to Accept that Spain isn’t an Islamic Country. Café Babel. [online] Available at <<http://www.cafebabel.co.uk/article/21206/you-have-to-accept-that-spain-isnt-an-islamic-country>> [Accessed 17 November 2010].

Schneider, F., Bruck, T., Meierrieks, D. (2010). The Economics of Terrorism and Counter-Terrorism: A Survey (Part II). CESifo Working Paper No. 3012. April 2010.

Symantec Corporation, (Date Unknown). What is Cybercrime? [online] Available at <<http://us.norton.com/cybercrime/definition.jsp>> [Accessed 01 October 2010].

Schrum, L., (1997). Ethical Research in the Information Age: Beginning the Dialog, *Computers in Human Behavior*, Vol. 13, No. 2, pp. 117-125.

Schwartz, M. (2004). Acebes Afirma que el 11 de Marzo fue peor que el Golpe de Tejero. *La Voz de Asturias*. [online] Available at <<http://archivo.lavozdeasturias.es/html/130714.html>> [Retrieved 24 March 2011].

Scollon, R., & Scollon, S.W. (2004). Nexus Analysis: Discourse and the Emerging Internet. London and New York: Routledge, 2004, pp.xvi-198.

Selway, L., (2006). *Spanish Foreign Policy from (A)znar to (Z)apatero*, Independent Study, [Online]. Available at [<http://66.102.9.132/search?q=cache:DqBkg4DFP5IJ:dspace.nitle.org/bitstream/10090/4267/3/Selway.pdf+Spanish+Foreign+Policy+from+(A)znar+to+(Z)apatero&hl=en&ct=clnk&cd=2&gl=uk&client=firefox-a](http://66.102.9.132/search?q=cache:DqBkg4DFP5IJ:dspace.nitle.org/bitstream/10090/4267/3/Selway.pdf+Spanish+Foreign+Policy+from+(A)znar+to+(Z)apatero&hl=en&ct=clnk&cd=2&gl=uk&client=firefox-a)> [Accessed 03 July 2008].

Seroo, O., (2010). Dia Internacional de les Nacions Unides: del soroll pels Objectius de Desenvolupament del Mil·lenni (ODM) als reptes per a la governança global. El Garbell. [online] Accessed at <<http://garbell.unescocat.org/2010/10/22/24-d%E2%80%99octubre-dia-internacional-de-les-nacions-unides-del-soroll-pels-objectius-de-desenvolupament-del-mil%C2%B7lenni-odm-als-reptes-per-a-la-governanca-global/>> [Accessed on 24 October 2010].

Shapiro, J. & Suzan, B., (2003). The French Experience of Counter-terrorism *Survival*, Vol. 45 No. 1

Shaw, W.H., (1979). “The Handmill Gives you the Feudal Lord”: Marx’s Technological Determinism. *History and Theory*, Vol. 18, No. 2 (May, 1979), pp.155-176

Shelly, L.I., (2003). Organized Crime, Terrorism and Cyberterrorism. Security Sector Reform: Institutions, Society and Good Governance, pp. 303-312.

Sherman, C., & Price, G., (2002). *The Invisible Web. Uncovering Information Sources Search Engines Can’t See*. Cyber Age Books.

Shirky, C., (2011). The Political Power of Social Media: Technology, The Public Sphere and Political Change. *Foreign Affairs*, January/February 2011.

Shubik, M., (2001). Terrorism, Technoloy and the Sociology of Death. *Comparative Strategy*, 16, 399-414.

Shultz R., Beitler, R. (2004). Tactical Deception And Strategic Surprise In Al-Qaida’s Operations. *Middle East Review of International Affairs*, Volume 8, No. 2, June 2004.

Silke, Andrew. (2004). *Research on Terrorism: Trends, Achievements, and Failures*. Cass Series on Political Violence. Routeledge.

Silverman, J. & Thomas, L. (2011). *‘I Feel Your Pain’: Terrorism, the Media & the Politics of Response.* The 61st Political Studies Association Conference, Transforming politics: New Synergies (19-21 April 2011).

Simon, S. & Benjamin, D., (2000). America and the New Terrorism. *Survival*, vol. 42, no.1, Spring 2000, pp.59-75.

Simons, J. (1995). *Foucault and the Political*. Routledge.

Skala, K., (2009). Does Influence Matter? *Social Media Today*. [online] Available at <<http://socialmediatoday.com/kmskala/248679/does-online-influence-matter>> [Accessed 10 December 2010].

Slaughter, A.M. (2004). *A New World Order*. Princeton University Press.

Slaughter, A.M., (2004). Disaggregated Sovereignty: Towards the Public Accountability of Global Government Networks. *Government and Opposition*. Pp.159-191

Slevin, J., (2000). *The Internet and Society*. Polity Press.

Soriano, M., (2007) El Nuevo Contexto de la Amanaza de Zawahiri contra Espana. *Athena Assessment*. No. 4/07.

Soriano, M., (2008) Las Menciones a España en la Propaganda Yihadista. *Athena Assessment*. Assessment 10/08.

Soriano, M., (2010) La nueva estrategia propagandística de al-Qaeda en el Magreb Islámico. *Real Instituto Elcano* ARI 87/2010.

Spivack, N., (2006). *Minding the Planet. The Meaning and Future of the Semantic Web*. Radar Networks.

Spivack, N. (2007). How To Define Web 3.0. [Online] Available at <[http://howtosplitanatom.com/news/how-to-define-Web-30-2/](http://howtosplitanatom.com/news/how-to-define-web-30-2/)> [Accessed 12 December 2007].

Spivack, N., (2007). Web 3.0 – The Best Definition Imaginable Minding the Planet [Online] Available at: <[http://novaspivack.typepad.com/nova\_spivacks\_Weblog/2007/10/Web-30----the-a.html](http://novaspivack.typepad.com/nova_spivacks_weblog/2007/10/web-30----the-a.html)> [Accessed October 2007].

Sramana M., (2007). Web 3.0 & the Semantic Web. Sramanamitra.com [online]. Available at<<http://sramanamitra.com/2007/06/28/web-30-the-semantic-web>> [Accessed 01 July 2008].

Stampnitzky, L., (2010). Disciplining an Unruly Field: Terrorism Experts and Theories of Scientific/Intellectual Production. *Qualitative Sociology*. Volume 34, Number 1, 1-19.

Standish, R.K. (2008). On Complexity and Emergence. *High Performance Computing Support Unit. University of New South Wales*. February 3, 2008.

Stepen, L, Schensul, J.J., Schensul, M., (1999). *Essential Ethnographic Methods: Observations, Interviews and Questionnaires*. Altamira Press.

Stevens, T. & Neumann, P.R. (2009). *Countering Online Radicalisation: A Strategy for Action*. International Centre for the Study of Radicalisation and Political Science.

Strathern, M., (1996). Cutting the Network. *The Journal of the Royal Anthropological Institute,* Vol. 2, No. 3, (Sep., 1996), pp.517-535.

Sullivan, J.P., (2006). Terrorism Early Warning and Co-Production of Counterterrorism Intelligence. Panel 5: In Pursuit of the Analytical Holy Grail: Part 1 Innovation in Analysis, Warning and Prediction 21 October 2005.

Sullivan, J., (2006). *Jeans: A Cultural History of an American Icon*. Gotham Books.

Sveningsson, Malin., (2003). *Ethics in Internet Ethnography*. In Elizabeth A. Buchanan (Red.): *Virtual Research Ethics: Issues and Controversies*. Hershey: Idea Group Publishing.

Szondi, G., (2008). Public Diplomacy and Nation Branding: Conceptual Similarities and Differences. *Discussion Papers in Public Diplomacy*. Netherlands Institute of International Relations ‘Clingendael’.

Tansey, C., (2009), Anti-Radicalization Efforts within the European Union: Spain and Denmark, Naval Postgraduate School, Monterey California.

Tapscott, D., & Williams, A.D., (2010). *Macrowikinomics. Rebooting Business and the World*. Atlantic Books Limited.

Taureck, R., (2006). Securitization Theory and Securitization Studies. *Journal of International Relations and Development,* (9) pp.53-61.

Taylor, M., & Horgan, J., (2001). The Psychological and Behavioural Bases of Islamic Fundamentalism. *Terrorism and Political Violence*, Vol. 13, No.4 (Winter 2001), pp.37-71.

Teslik, L., (2009). New Media Tools and Public Diplomacy. Council on Foreign Relations. [online] Available at <<http://www.cfr.org/public-diplomacy/new-media-tools-public-diplomacy>> [Accessed 01 April 2011].

The Register, (2006), Web Browsing Behind Closed Doors. [Online]. Available at: <<http://www.theregister.co.uk/2006/11/28/psiphon_bypass_censors/>> [Accessed November 2007].

Thelwall, M. (2002). An Initial Exploration of the Link Relationship between UK University Web Sites. *ASLIB Proceedings*, 54(2), pp. 118-126.

Thelwall, M. (2004). Interpreting Social Science Link Analysis Research: A Theoretical Framework. *Journal of Information Science and Technology*. Volume 57 Issue 1.

Thelwall, M. (2009). *Introduction to Webometrics: Quantitative Web Research for the Social Sciences*. Morgan & Claypool Publishers.

Thomas T.L. (2003). Al-Qaeda and the Internet: The Danger of “Cyberplanning”. *Parameters*, Spring 2003, pp.112-124.

Tetu., (2008), L'Intérieur reconnaît qu'«Edvige» sera utilisé pour ficher les militant, Tetu. [Online]. Available at: <<http://www.tetu.com/rubrique/infos/infos_detail.php?id_news=13236>> [Accessed 24 July 2008].

Thomas, T., (2003). Al Qaeda and the Internet: The Danger of “Cyberplanning”. *Parameters*, Spring 2003, pp. 112-123.

Torres, M., (2008). Al Qaeda Utiliza Imágenes de los Atentados del 11-M en su Ultimo Video Propagandistico. *Athena Assessment*. No. 8/08.

Touboul, D., (2005). Francophone Internet Forums Shed Light On Concerns And Issues Of Islamists In Europe. *Global Research in International Affairs (GLORIA) Center.*

Tremlett, G. (2007). *Ghosts of Spain. Travels Through a Country’s Hidden Past*. Faber & Faber.

Troitiño, J.M.R., (1992). Desinformación y Terrorismo: Analisis de las Conversaciones entre el Gobierno y ETA en Argel (Enero-Abril 1989) en Tres Diarios de Madrid. Universidad Complutense de Madrid. Facultad de Ciencias de la Información Departamento de Periodismo.

Tucker, D., (2001). What’s New About Terrorism and How Dangerous Is It? *Terrorism and Political Violence*. 13 (Autumn, 2001) pp. 1-14.

Twitter Inc, (2010). Twitter Developers Page. [online] <http://dev.twitter.com/> [Accessed 20 August 2010].

U.K. Government, (2011). *PREVENT Strategy*. Crown Copyright 2011.

Ulph, S., (2009). A Guide to Jihad on the Web. *Terrorism Focus*. Volume 2, Issue 7.

Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (2005). Cooperación Internacional En La Lucha Contra El Terrorismo Y Las Vinculaciones Entre El Terrorismo Y Otras Actividades Delictivas. Naciones Unidas Oficina Contra la Droga y el Delito.

United Nations Alliance of Civilizations, 2011. Mission Statement. [online] Available at <http://www.unaoc.org/content/view/39/187/lang,english/> [Accessed 06 April 2011].

UNWTO, (2010). UNWTO World Tourism Barometer. [online] Available at <<http://www.unwto.org/facts/eng/pdf/barometer/UNWTO_Barom10_update_april_en_excerpt.pdf>> [Accessed 19 April 2011].

United Nations (Date Unknown). El papel que desempeñan el Comité contra el Terrorismo y su Dirección Ejecutiva en las Actividades Internacionales de Lucha Contra el Terrorismo.

Vaas, L., (2005). ‘Database Legend: How Real-Time Data Analysis Will Transform Society’ *eWeek*. [online] Available at <<http://www.eweek.com/index2.php?option=content&task=view&id=312>> [Accessed 01 July 2010].

Valdeón, R.A., (2009). Discursive Constructions of Terrorism in Spain: Anglophone and Spanish Media Representations of ETA. *International Journal of Applied Linguistics*. Vol. 19, No. 1, 2009.

Van Couvering, E. (2005). *The Power of Search: Strategies for Gatekeeping the Internet*. Department of Media & Communications, London School of Economics and Political Science.

Varela, J. (2004). El Dia que los SMS Cambiaron la Politica. *Periodistas 21* [online]. Available at <<http://periodistas21.blogspot.com/2004/03/el-da-que-los-sms-cambiaron-la-poltica.html>> [Accessed 01 February 2011].

Vicente, P., Reis, E., & Santos, M., (2009). Using Mobile Phones for Survey Research. A Comparative Analysis Between Data Collected via Mobile Phones and Fixed Phones. *International Journal of Market Research*. Vol. 51, Issue 5.

Vilar, P., & Mendoza L.E., (2004). El Triangulo Ampliación-Inmigración-Terrorismo. Los Grandes Retos Actuales de Europa. *Working Paper from the Jean Monnet Cathedral of Economic Intregration. European Commission & Universidad Complutense de Madrid*.

Vinter, L. & Knox, D., (2008). *Measuring the Impact of Public Diplomacy: Can it be Done? In Engagement, Public Diplomacy in a Globalised World*. Foreign and Commonwealth Office.

Virino Cascajosa C (2003), En Días Como Hoy No Aptece Reírse: Actos Terroristas Y La Necesidad De Evasión En La Programación Televisiva. *Department of Audiovisual Comunication, Advertising and Literature, University of Seville.*

Waldmann, P., (2006). El impacto del terrorismo sobre la opinion pública y política, *Real Instituto Elcano de Estudios Internaciónales y Estrategicas*, [Online]. Available at: <<http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/Elcano_es/Zonas_es/Terrorismo+Internacional/ARI+76-2006>> [Accessed 15 August 2008].

Walther, J.B., DeAndrea, D., Kim, J. & Anthony, J.C. (2010). The Influence of Online Comments on Perceptions of Antimarijuana Public Service Announcements on YouTube. *Human Communication Research* **36** (2010) 469-492.

Wang, J., (2005). Managing National Reputation and International Relations in the Global Era: Public Diplomacy Revisited. *Public Relations Review*, 32 (2006) 91-96.

Watkins, M. Edwards, M. and Thakrar, U. (2001). *Winning the Influence Game. What Every Business Leader Should Know about Government*. John Wiley & Sons Inc.

Wang, J.H., Fu, T., Lin, H.M. & Chen, H. (2006). A Framework for Exploring Gray Web Forums: Analysis of Forum-Based Communities in Taiwan. S. Mehrotra et al. (Eds.): ISI 2006, *LNCS* 3975, pp. 498 – 503, 2006.

Watson, R., (2008). *The One True God, Allah*. Granta, 103. Granta Publications.

Warah, R., (2009). Mobile Telephony: Kenya’s Not-So-Silent Revolution. Daily Nation. [online] <<http://www.nation.co.ke/oped/Opinion/-/440808/683686/-/4plo8t/-/index.html>> [Accessed 19 July 2010].

Warren, D., & Rainey, D., (1980). *Terrorism as Communication*. The Speech Communication Association National Convention.

Watkins, M. Edwards, M. and Thakrar, U. 2001. Winning the Influence Game. What Every Business Leader Should Know about Government. John Wiley & Sons Inc.

Webb, A., (2008). *Public Diplomacy: Meeting New Challenges*. Report on Wilton Park Conference 902.

Wei, C., (2007). ‘*Capturing Mobile Phone Usage: Research Methods for Mobile Phones*’, Professional Communications Conference.

Weimann, G. (2004). *www.terror.net: How Modern Terrorism Uses the Internet*.

Washington DC: United States Institute of Peace.

Weimann, G. (2005). How Modern Terrorism Uses the Internet, *Journal of International Security Affairs*, Spring 2005, No. 8

Weimann, G. (2006). *Terror on the Internet: The New Arena, the New Challenges*. Haifa University.

Wells, T., (2006). The Read-Write Executable Web Search Engine News, [Online] Available at: <<http://www.seochat.com/c/a/Search-Engine-News/Web-30-and-SEO/3/>> [Accessed May 2010].

Wendt, A. (1992) Anarchy is What States Make of It: The Social Construction of Power Politics. *International Organization,* Vol. 46, No.2 (Spring, 1992), pp. 391-425.

Wenger, E. (1998) *Communities of Practice – Learning, Meaning and Identity*, Cambridge University Press, Cambridge, MA.

Western, B., & Jackman, S. (1994). Bayesian Inference for Comparative Research. *The American Political Science Review*, Vol. 88, No. 2, (Jun 1994), pp.412-433.

Whitefield, S., (2006). *Behavioural and Institutional Approaches to Political Science.* Department of Politics and International Relations, University of Oxford.

Whitworth, D., (2008). ‘Facebook Users Hit by Virus’, BBC News. [online] <<http://news.bbc.co.uk/newsbeat/hi/technology/newsid_7773000>> [Accessed 20 July 2010].

Widgren, J., Jandl, M., Hofmann, M. (2005), Migration and Security in Europe after the Madrid Bombings. *Migraciones*, No. 17, June 2005.

Wilson, T., Wiebe, J., & Hoffmann, P., (2005). Recognizing Contextual Polarity in Phase-Level Sentiment Analysis. *Proceedings of Human Language Technology Conference and Conference on Empirical Methods in Natural Language Processing* (HLT/EMNLP), pages 347-354. Vancouver, October 2005.

Williams, C., (2008). BT and Phorm Secretly Tracked 18,000 Customers in 2006. The Register, [online] Available at: <<http://www.theregister.co.uk/2008/04/01/bt_phorm_2006_trial/>> [Accessed April 2008].

Williams, M., (2003). Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly* (2003) **47,** 511-531.

Wilkinson, P., (1997). The Media and Terrorism: A Reassessment. *Terrorism and Political Violence*, Vol. 9, No. 2, (Summer 1997) pp.51-64.

Wilton Park, (2011). *Tackling Online Jihad: Understanding the Issues and how to Respond?* United Kingdom 31 January to 2 February 2011.

Winer, D., (2002). ‘What is the Real-Time Web?’ Scripting. [online] Available at <<http://www.scripting.com/stories/2009/09/22/whatIsTheRealtimeWeb.html>> [Accessed 11 August 2010].

Winner, L. (1993). Upon Opening the Black Box and Finding it Empty: Social Constructivism and the Philosophy of Technology. *Science, Technology and Human Values*, Vol. 18, No. 3, (Summer 1993), pp. 362-378.

Witt, A. (2005), Challenges in the Area of Immigration, Integration and Security, Center for International Relations, May 2005.

Wiseman, G. (2004). “Polylateralism” and New Modes of Global Dialogue. Discussion papers No. 59 (Leicester: Leicester Diplomatic Studies Programme, 1999).

Witker, J. (Date Unknown). *Globalización y Delitos Económicos*. Instituto de Investigaciónes Jurídicas

Wood, D., (2007). Spain Struggles for New ETA Plan. *BBC News* [Online). Available at <http://news.bbc.co.uk/1/hi/world/europe/6228201.stm> [Accessed 28 December 2008]

Woodward, J.D., (2005), Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism. Rand Corporation, National Security Research Division, October 2005

World Paddle Sport Foundation, (2011). Diplomacy & Leadership Through Paddle Sports. [online] Available at <<http://www.worldpaddle.com/>> [Accessed 06 April 2011].

Wu, J, Wang, S., (2004). ‘What Drives Mobile Commerce? An Empirical Evaluation of the Revised Technology Acceptance Model’, *Information and Management* 42, pp. 719-729.

Xenitidou, M., & Gilbert, N., (2009). Innovations in Social Science Research Methods. ESRC National Centre for Research Methods. University of Surrey.

Xu, J., Chen, H., Zhou, Y., & Qin, J. (2006). On the Topology of Dark Web Terrorist Groups*. ISI 2006, LNCS*, pp. 367-376.

Yang, C.C., & Ng, T.D. (2007). Terrorism and Crime Related Weblog Social Network: Link, Content Analysis and Information Visualisation. *Department of Systems Engineering and Engineering Management* at the Chinese University of Hong Kong.

Zhou, Y., Qin, J., Lai, G., Reid, E. & Chen, H. (2005). Building Knowledge Management System for Researching Terrorist Groups on the Web. Proceedings of the Eleventh Americas Conference on Information Systems, Omaha, NE, USA August 11th-14th 2005.

Zhou, Y., Reid, E., Qin, J., Chen, H., & Lai, G. (Date unknown). U.S. Domestic Extremist Groups on the Web: Link and Content Analysis. The University of Tuscon, Arizona.

Zittrain, J., (2007), The Future of the Internet and How to Stop It, Yale University Press.

Zunzunegui, S., (2008). El Ciberterrorismo: Una Perspectiva Legal y Judicial. Eguzkilore, Numero 22, San Sebastían, Diciembre 2008, 169-187.

1. “Internet” is often spelled with a capital “I.” In keeping with other works in contemporary internet studies and for the purpose of this thesis, the author will spell with the lower case “i.” Capitalising suggests that the “internet” is a proper noun and implying that either it is a being, or a place. Both metaphors suggest that the internet has agency and power that are better granted to its users and developers. [↑](#footnote-ref-1)
2. See Glossary of Terms. [↑](#footnote-ref-2)
3. ‘Terrorismo exterior es el terrorismo que actúa fuera de las fronteras de los Estados de origen o bien dentro de ellas pero contra intereses de otros países, entendiendo por “actuación” la realización de acciones armadas (atentados, sabotajes, asesinatos, secuestros). Existen otros aspectos ligados al terrorismo internacional que deben ser tenidos en cuenta. La existencia de mercenarios y de material bélico muy sofisticado, procedente del periodo de la Guerra Fría, así como las posibilidades que ofrecen las nuevas tecnologías para obtener información sobre material susceptible de ser empleado en actos terroristas, añaden un factor de inestabilidad al fenómeno terrorista. Terrorismo interior: Es aquel que nace dentro de un Estado y actúa contra dicho Estado. Este terrorismo puede mantener lazos internacionales para apoyarse entre grupos, emplear campos de adiestramiento o refugiarse en santuarios, pero tiene otra naturaleza distinta. España conoce bien esta lacra, que constituye el principal problema al que se enfrenta nuestra sociedad.’ (2003). Revisión Estratégica de la Defensa, Gobierno Español. [↑](#footnote-ref-3)
4. See Glossary of Terms. [↑](#footnote-ref-4)
5. See Glossary of Terms [↑](#footnote-ref-5)
6. Interview with Giles Tremlett, Spain Correspondent, *The Guardian*. Telephone Interview, 12 November 2010 [↑](#footnote-ref-6)
7. See Glossary of Terms [↑](#footnote-ref-7)
8. See Glossary of Terms. [↑](#footnote-ref-8)
9. See Glossary of Terms [↑](#footnote-ref-9)
10. See Glossary of Terms [↑](#footnote-ref-10)
11. See Glossary of Terms [↑](#footnote-ref-11)
12. See Glossary of Terms [↑](#footnote-ref-12)
13. See Glossary of Terms [↑](#footnote-ref-13)
14. See Glossary of Terms [↑](#footnote-ref-14)
15. Interview with Justin Webster, JWP Productions, Telephone interview, 29 November 2010. [↑](#footnote-ref-15)
16. Interview with Robert Imre, Deputy Head Politics and International Relations. Newcastle Business School. Telephone Interview, 21 July 2010. [↑](#footnote-ref-16)
17. Interview with Jamie Barlett, Head of Violence and Extremism for DEMOS. London, 28 April 2011. [↑](#footnote-ref-17)
18. Interview with Justin Webster, JWP Productions, Telephone interview, 29 November 2010. [↑](#footnote-ref-18)
19. Interview with John Postill, Sheffield Hallam University. Barcelona, Spain, 02 August 2010. [↑](#footnote-ref-19)
20. ‘Sin embargo, en la segunda mitad de la década de los 90 las redes yihadistas comenzaron a dirigir su propaganda y reclutamiento hacia la creciente comunidad islámica inmigrada. Sin caer en la simpleza de criminalizar la inmigración, es indudable que este hecho ha complicado las labores de vigilancia policial y de inteligencia, y ha ampliado la cantera de potenciales candidatos entre los inmigrantes que llegan radicalizados o entre aquellos, que una vez en España, se aproximan a la órbita de captación yihadista.’ Jordán, J., 2005. El yihadismo en España: situación actual, *Real Instituto Elcano de Estudios Internacionales y Estratégicas*, [Online]. Available at: <<http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/Elcano_es/Zonas_es/Defensa+y+Seguridad/ARI+93-2005>> [Accessed 15 July 2008]. [↑](#footnote-ref-20)
21. As of 31 March 2011, a total of 29,093,984 people were connected to the internet in Spain representing 62.2% penetration of the population. (2011). World Internet Usage and Population Statistics. Internet World Stats. [Online] <<http://www.internetworldstats.com/stats.htm>> [Accessed, 16 June 2011]. [↑](#footnote-ref-21)
22. Incorrect data in this case is information which is factually incorrect and could lead to the contamination of the data sample. [↑](#footnote-ref-22)
23. ‘Noise’ refers to the instance of non-relevant content that occurs within a given dataset. [↑](#footnote-ref-23)
24. The definition of semi-structured interviews will be that given by Stephen et al. (1999) in which it is claimed that they ‘consist of predetermined questions related to domains of interest administered to a representative sample of respondents to confirm study domains, and identify factors, variables, and items or attributes of variables for analysis or use in a survey.’ Stepen, L, Schensul, J.J., Schensul, M., (1999). *Essential Ethnographic Methods: Observations, Interviews and Questionnaires*. Altamira Press. [↑](#footnote-ref-24)
25. Interview with Elena Sánchez, Researcher CIDOB. Barcelona, 09 December 2010. [↑](#footnote-ref-25)
26. More detailed definitions of both the Functioning Core and the non-Integrating Gap can be found in Chapter Two in a more detailed discussion of the theories, as well as in the Glossary of Terms. [↑](#footnote-ref-26)
27. A detailed definition of Nation States and Market States as provided by Philip Bobbitt is outlined in Chapter Two, as well as in the Glossary of Terms. [↑](#footnote-ref-27)
28. ‘El primer intento de regular la estancia de los extranjeros en España fue la Ley Orgánica 7/1985 de Extranjería. Ésta consideraba a los inmigrantes como visitantes temporales y no como inmigrantes. Limitaban su tiempo de estancia y las posibilidades de permanencia definitiva en territorio español.’ Calavita, K., (2006). Notas de población, Volume 33, Issues 82-85, United Nations publications, 2007. [↑](#footnote-ref-28)
29. “El ministro portavoz del Gobierno, Eduardo Zaplana, ha atribuido la autoría a ETA aunque el responsable de Batasuna [Arnaldo Otegi](http://www.elmundo.es/elmundo/2004/03/11/espana/1079003714.html) ha atribuido la culpa a la 'resistencia árabe'. Éste sería el ataque más sangriento de la banda terrorista.” *El Mundo*, (2004). Masacre en Madrid. [online] Available at <<http://www.elmundo.es/elmundo/2004/03/11/espana/1078988734.html>> [Accessed 19 July 2011). [↑](#footnote-ref-29)
30. “Las células islámicas por la zona del Raval, yo creo que hay células por aquí…Yo creo que hay un movimiento. Esto es el terrorismo islámico. El terrorismo etarra que ya está acabado. Que todavía hay gente radical que quiere independencia, y aquí están en el País Vasco pero los islámicos nos dan miedo que nos hagan algo en Barcelona.” Interview with Maria Llorach, Former Head of Communications and Institutional Relations, Congreso de los Diputatdos. Barcelona, 20 January 2011 [↑](#footnote-ref-30)
31. See Glossary of Terms. [↑](#footnote-ref-31)
32. A number of countries are involved in the creation of the Schengen Information System: France, Germany, Belgium, the Netherlands, Luxembourg, Italy, Spain, Portugal, Greece, Austria, Denmark, Finland, Iceland, Norway, Sweden, Estonia, the Czech Republic, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia. In addition, the United Kingdom and the Republic of Ireland are able to take part in some or all of the Schengen Agreements. The mandate of the SIS is to collect a range of data including ‘surname and forenames, any aliases, any specific objective and physical characteristics not subject to change, first letter of second forename, date and place of birth, sex, nationality, whether the persons concerned are armed, whether the persons concerned are violent, reason for alert and action to be taken. (2011). Facts about the Schengen Information System (SIS): What is Schengen Information System? Information Commissioner Republic Of Slovenia. [online] <<http://www.ip-rs.si/index.php?id=345>> [Accessed 21 June 2011]. [↑](#footnote-ref-32)
33. Interview with Robert Imre – Deputy Head Politics and International Relations. Newcastle Business School. Australia. Telephone Interview, 21 July 2010 [↑](#footnote-ref-33)
34. “Se ha vinculado más con el terrorismo, la seguridad y la población inmigrante, y no ocurrió éste en España. Ocurrió las primeras semanas después de lo que hizo en Madrid, pero a partir de allí, el vinculo no ha sido muy fuerte. Probablemente porque la población inmigrante es de origen latino americano, o sea, decimos que la comunidad marroquí es la segunda población con más inmigrantes en España…Con lo cual, el problema de inmigración y terrorismo en España, tengo la opinión de que las encuestas que tome la opinión de la población española, sustentan el hecho de que efectivamente, las cosas que asusten los españoles no es la población inmigrante sino la situación de empleo.” Interview with Elena Sánchez, Researcher, CIDOB. Barcelona, 09 December 2010. [↑](#footnote-ref-34)
35. ‘La conexión marroquí de Al Qaeda es cada vez más inquietante. El 11-M ha confirmado la importancia de los terroristas procedentes de Marruecos en la red de Bin Laden. “Los líderes de Al Qaeda siguen siendo saudíes y egipcios, pero en el nivel de ejecución de atentados, los marroquíes tienen un papel fundamental…El uso de marroquíes como mano de obra terrorista obedece al espíritu pragmático de Al Qaeda, que ha encargado a marroquíes y argelinos los ataques en suelo europeo. Para atentar en España no hay mejor que los marroquíes", dice Darif.” En este país y en casi toda Europa Occidental-argumenta-hay comunidades marroquíes muy numerosas, lo que permite a los terroristas instalarse sin levantar sospechas…la organización Al Qaeda "estudia utilizar a la inmigración magrebí para crear una nueva vanguardia terrorista capaz de atacar a Europa desde dentro.’ Baquero, A., (2004). La Cantera de Al-Qaeda. *Diario Córdoba*. [online] Available at <<http://www.diariocordoba.com/noticias/noticia.asp?pkid=114378>> [Accessed 01 February 2011]. [↑](#footnote-ref-35)
36. ‘Pero si no estás a favor de la mezcla de culturas y religiones eres un facha. Yo no soy ni racista ni xenófobo. En todo caso EGOÍSTA porque no quiero compartir mi país con gente tan distinta a mí. Gente que me merece todo mi respeto e incluso mi colaboración para que puedan vivir mejor en sus respectivos países. Pero no en el mío.’ (2007). 3 Anos de Golpe de Estado del 11-M. Eurabian News. [online] <<http://noticiasdeeurabia.wordpress.com/2007/03/11/3-anos-del-golpe-de-estado-del-11-m/>> [Accessed 01 February 2011]. [↑](#footnote-ref-36)
37. ‘El 11 m fue una reacción normal al mísero papel que jugó el ánsar en la guerra de Iraq España estaba en estado de guerra contra un estado extranjero si o no? que nadie mi diga que España no declaro la guerra a Iraq aunque oficialmente no en practica lo había echo una guerra que ha causado miles y miles de muertos la mayoría civiles’ (2007). 3 Anos de Golpe de Estado del 11-M. *Eurabian News*. [online] <<http://noticiasdeeurabia.wordpress.com/2007/03/11/3-anos-del-golpe-de-estado-del-11-m/>> [Accessed 01 February 2011]. [↑](#footnote-ref-37)
38. ‘El 11-m fue el atentado más sangriento de España y de Europa. Pero no el único atentado árabe en suelo español. Desde 1976, al menos una treintena de ataques han sucedido en España, Madrid, Barcelona, Sevilla, Málaga etc. Con muertos civiles (españoles y extranjeros). ¿Tenemos que recordar todas las células de Al Qaeda desmanteladas en España desde 2004? ¿Tenemos que recordar que según un estudio de los cuerpos de seguridad de estado, afirman que desde Cataluña salen islamistas a inmolarse y / o entrenarse en Irak? El 20% de la reclutación yihadista en toda Europa está en Cataluña.’ (2009). 11M ¡Lo Conseguiremos, Saldrá la Verdad Algún Día! *Que.es* [online] < <http://blogs.que.es/yentel/2009/3/12/11m-conseguiremos-saldra-verdad-algun-dia->> [Accessed 01 February 2011]. [↑](#footnote-ref-38)
39. ‘Nadie pensó que podía darse un atentado como el del 11-M en España(pero después del atentado de Casablanca, debiera de haberse considerado claramente, esta posibilidad),pero en los ambientes musulmanes se daban las condiciones para ello y mucho más entre los más excluidos culturales y sociales(más que económicos),pues si bien la xenofobia no es patente, si se da cierto rechazo ambiental. La inmigración musulmana no es de calidad cultural y la no integración, que siempre va ser difícil entre ambos mundos, genera resentimientos que alimentados por ideólogos religiosos de carácter integrista e iluminado, pueda dar lugar y dio, al nacimiento de grupos de este carácter que con la razón que sea(y hay muchas en los sucesos políticos diarios)pueden actuar como ya les es tradicional, es decir con desprecio de su vida y de las de los demás, desde la profunda desesperación emocional. La solución es muy difícil y los españoles esto no lo van a olvidar nunca. Y de hecho, pesé a que no ha habido venganzas notorias, él rechazo es más patente, aunque en parte esté mitigado por el vuelco político, producido más por los despropósitos del Partido Popular, qué por la popularidad o aciertos de Zapatero y mucho menos, del gobierno. Sin embargo el grave problema de polaridad con el mundo musulmán, sigue ahí y no se va a resolver en una sola generación, sino en varias y solamente, si el mundo tiende a una laicidad social y política y si los responsables políticos de los países musulmanes asumen el difícil momento. De no ser así, la evolución será aún más violenta, pero inevitablemente, será pues la globalización podrá modularse, pero es imparable en la humanidad y este mismo foro, es un ejemplo.’ (2005). ¿Cómo es España después del 11-M? *BBC Mundo*. [online] <<http://news.bbc.co.uk/hi/spanish/forums/newsid_4336000/4336173.stm>> [Accessed 01 February 2011]. [↑](#footnote-ref-39)
40. ‘Ya hay en España un partido político musulmán que les acerca al poder, por tanto hemos entrando en un nuevo estadio de máximo peligro para la sociedad española, cada día el enfrentamiento cruento generalizado está más peligrosamente cerca. En Granada, España, ha sido creado el primer partido musulmán, se llama ‘Renacimiento y Unión’, el cual ‘pretende representar a los islamistas residentes en España y a los inmigrantes, sean o no musulmanes según Webislam’. Informes de dominio público nos dicen que de mencionada web de carácter islámico, recibe fondos del gobierno actual ¿Qué piensa de ello?’ (2010). Ataque Islámico del 11 M ¿Para qué? *Labranza de Dios*. [online] <<http://www.labranzadedios.com/2010/03/el-11-de-marzo-sera-recordado-en-la.html>> [Accessed 01 February 2011]. [↑](#footnote-ref-40)
41. Interview with Manuel Torres Soriano, Professor of Political Science and Administration, University Pablo de Olavide de Sevilla. Telephone Interview, 24 November 2010 [↑](#footnote-ref-41)
42. ‘La propaganda es la clave que permitirá a la filial magrebí conseguir más con menos. Aunque en el futuro su capacidad para seguir ejecutando actos de terrorismo pudiese verse gravemente mermada, la percepción de inseguridad por parte de la población (por definición subjetiva), puede multiplicarse como consecuencia de un uso inteligente de la comunicación. Así, por ejemplo, la apuesta en los últimos tiempos por los secuestros de occidentales y la explotación mediática de los mismos supone un buen indicador del nuevo paradigma de operaciones: acciones que exigen pocos recursos humanos y materiales, pero capaces de concitar la atención mundial sobre el grupo y sus objetivos.’ Soriano, M., (2010). La nueva estrategia propagandística de al-Qaeda en el Magreb Islámico. *Real Instituto Elcano* ARI 87/2010. [↑](#footnote-ref-42)
43. Interview with Justin Webster, Television Producer. Telephone Interview, 29 November 2010 [↑](#footnote-ref-43)
44. See Glossary of Terms. [↑](#footnote-ref-44)
45. (2002). ETA Según el Nacionalismo Catalán. *Bye Bye Spain*. [online] Available at <[http://nacionalismo.blogs.com/byebyespain/2007/06/eta\_segn\_el\_nac.html>](http://nacionalismo.blogs.com/byebyespain/2007/06/eta_segn_el_nac.html%20) [Accessed 24 March 2011]. [↑](#footnote-ref-45)
46. De la Fuente, J.V. (2003). Terrorismo de E.T.A. *The Matrix 666*. [online] Available at <<http://www.matrix666.net/?page_id=14>> [Accessed 24 March 2011]. [↑](#footnote-ref-46)
47. See Glossary of Terms. [↑](#footnote-ref-47)
48. Facebook.com (2011). Ahmadinejad is NOT my president! [online] Available at <<http://www.facebook.com/pages/Ahmadinejad-is-NOT-my-president/86964552573>> [Accessed 28 March 2011]. [↑](#footnote-ref-48)
49. ‘TODOS los islamistas fuera de Europa. Problema resuelto. Que es un poco radical, si, pero efectivo. Que ya lo hicieron los Reyes Catolicos y durante 5 siglos no hemos tenido ningun problema. A [sic] sido a partir de la entrada masiva de moros en España cuando estamos teniendo estos problemas. Vale, No todos los arabes son malos, pero ante la duda....mas vale prevenir.’ (2005). España envía a expertos en terrorismo islámico a Londres. *20 Minutos*. Retrieved 01 February 2011 from <http://www.20minutos.es/noticia/37428/0/LONDRES/ESPANA/EXPERTOS/> [↑](#footnote-ref-49)
50. Schwartz, M. (2004). Acebes Afirma que el 11 de Marzo fue peor que el Golpe de Tejero. *La Voz de Asturias*. Retrieved 24 March 2011 from <http://archivo.lavozdeasturias.es/html/130714.html> [↑](#footnote-ref-50)
51. ‘Han pasado 4 años desde ese 11 de marzo. Mi vida ha cambiado, tengo otro trabajo, vivo en otro país, tengo la suerte de hacer lo que me gusta, viajo, conozco aquí y allá a gente admirable, y hoy pienso que, por el contrario, la vida de esas 192 personas se detuvo esa mañana de marzo, marcando para siempre la vida de sus familiares y amigos. Para ellos el recuerdo no es una cuestión de aniversarios o ceremonias anuales. Como me decía Pilar Manjón esta mañana, para ellos, desde entonces, ‘hay días malos, y días peores’. Desde aquí les hago mi particular homenaje.’ (2008). 11 de Marzo. *El Blog que nos Acerca*. [online] Available at <<http://elblogquenosacerca.wordpress.com/2008/03/11/11-de-marzo/>> [Accessed 01 February 2011]. [↑](#footnote-ref-51)
52. ‘Esta es más que una linda canción, no se ve pero precisamente habla de una vida que acaba en el tren que explosionó en el 11 de marzo, refleja los sueños cumplidos justo en el momento de la muerte. Cuando la escuché se me encogió el corazón. Es la que más refleja el apoyo a las víctimas del terrorismo. Por las voces libres, chicos, que no os callen nunca!!!’ Saulatino, (2008). La Oreja de Van Gogh – 11 de Marzo. *Palabras Retorcidas*. [online] Available at <<http://palabrasretorcidas.wordpress.com/2008/07/20/11-de-marzo-presentcion-en-vivo-y-letra/>> [Retrieved 01 Feb 2011]. [↑](#footnote-ref-52)
53. (2011). Asociación 11M Afectados Terrorismo. [online] Available at <<http://www.asociacion11m.org/index.php>> [Accessed March 2011]. [↑](#footnote-ref-53)
54. (2005). Los Autores del 11-M Amenazaban en el Vídeo al Nuevo Gobierno por Seguir la lucha contra el Islam. *El Mundo*. [online] Available at <<http://www.elmundo.es/elmundo/2004/04/13/enespecial/1081852985.html>> [Accessed 24 March 2011]. [↑](#footnote-ref-54)
55. ‘Mintieron muchas políticos el partido popular mintió mucho…y aparte, el gobierno de Aznar lo saben al principio que no era ETA pero políticamente no les convenciera eso… no estábamos preparados para esto y todo el mundo aquí pensó que fuerte…yo creo que la cuidad está viviendo en otra manera y con respeto a Aznar y Acebes, como pueden mentir tanto a nosotros? Pero los mienten porque les sirven y la gente les engañen, y salieron a la calle, ¿qué está pasando? La gente esta revolucionando en la calle, la gente esta insultado por que si sintieron engañada.’ Interview with Maria Llorach, Former Head of Communications and Institutional Relations for the Congreso de los Diputados. Barcelona, 20 January 2011 [↑](#footnote-ref-55)
56. ‘Del PP, de Rajoy y toda su tropa de votantes, no se puede esperar nada bueno ni mejor o peor que del PSOE. Están unidos hasta que la muerte los separe…. y ni eso, ¡¡¡porque con los que han caído de manos de ETA y todavía siguen negociando y buscando “acuerdos” para sacar tajada!!!..’ (2010). El PP de Rajoy Dispuesto a Echarse en Brazos del Nacionalismo Vasco. *Minuto Digital*. [online] Available at <<http://www.minutodigital.com/noticias/2010/07/07/el-pp-de-rajoy-dispuesto-a-echarse-en-brazos-del-nacionalismo-vasco/>> [Accessed 02 February 2011]. [↑](#footnote-ref-56)
57. ‘El «espejo de Madrid» reflejó en los días useriores al 11-M una imagen deformada de la sociedad española con una oposición que azuzaba a la ciudadanía contra el Gobierno por interés electoral, con sus militantes hostigando las sedes del partido gobernante, con algunos medios de comunicación convertidos en agitadores de la confusión y señalando al presidente de la nación como culpable.” “además de provocar un cambio de Gobierno, lograron romper la unidad de los españoles frente al terror. División que luego se ha prolongado ante el terrorismo etarra.” (2005). El Espejo de Madrid. *Es.charla.actualidad*. [online] Available at <<http://groups.google.com/group/es.charla.actualidad/browse_thread/thread/fa085e57851a3e8b/962995989791975a?q=11-m+OR+11m+colaboracion+internacional&lnk=ol&>> [Accessed 01 February 2011]. [↑](#footnote-ref-57)
58. 3 Dias de Marzo is a complete social profile established to provide information and analysis on the 3 March attacks on Madrid. The identity of the author is unknown but in addition to the influential blog maintained at <http://3diasdemarzo.blogspot.com/> the author also maintains a popular YouTube channel where a repository of videos are kept related to the attacks. The 3 Dias de Marzo social profile is so influential because of its high PageRank by Google (4/10 when read on 23 March 2011) and the high number of people who frequent these profiles to consume content. [↑](#footnote-ref-58)
59. Fundación para el Ánalisis y los Estudios Sociales http://www.fundacionfaes.org/en/home [↑](#footnote-ref-59)
60. Entre confidentes, conexiones etarras, servicios secretos, guardia civil asturiana, espías y presos islamistas y vídeos de FAES y Telemadrid nos quieren intoxicar para que olvidemos qué ocurrió aquellos 3 días y la absoluta imprevisión política anterior. Es no es una réplica a la FAES es un bofetón a las tesis del PP y medios de comunicación afines.” (2005). Desmentido al Documental “Tras la Masacre” de la Fundación FAES Presidida por Aznar. *3 Días de Marzo*. [online] Available at <<http://3diasdemarzo.blogspot.com/2005/03/desmentido-al-documental-tras-la.html>> [Accessed 01 February 2011]. [↑](#footnote-ref-60)
61. ‘En recuerdo de las víctimas del 11-m y del resto de los inocentes asesinados por estos terroristas que son usados como herramientas por los politicos incompetentes que dominan este mundo inundado de injusticias.” (2005). ¿Cómo es España después del 11-M? *BBC Mundo*. [online] Available at <<http://news.bbc.co.uk/hi/spanish/forums/newsid_4336000/4336173.stm>> [Accessed 01 February 2011]. [↑](#footnote-ref-61)
62. ‘La inmigración musulmana no es de calidad cultural y la no integración, que siempre va ser difícil entre ambos mundos, genera resentimientos que alimentados por ideólogos religiosos de carácter integrista e iluminado, pueda dar lugar y dio, al nacimiento de grupos de este carácter que con la razón que sea(y hay muchas en los sucesos políticos diarios) pueden actuar como ya les es tradicional, es decir con desprecio de su vida y de las de los demás, desde la profunda desesperación emocional.’ (2005). ¿Cómo es España después del 11-M? *BBC Mundo*. [online] Available at <http://news.bbc.co.uk/hi/spanish/forums/newsid_4336000/4336173.stm>> [Accessed 01 Februaru 2011]. [↑](#footnote-ref-62)
63. ‘No sé, si esto sucederá, pero cuando los musulmanes hagan atentados suicidas para conquistar Ceuta y Melilla y nos rindamos sin pegar un tiro, será el principio del fin.’ (2007). El CNI Advierte del Nuevo Grupo para la Liberación de Al Andalus. Stirpes Forum. [online] Available at <<http://forum.stirpes.net/ibero-romance-ibero-aquitanian/11031-cni-advierte-nuevo-grupo-para-liberacion-al-andalus.html>> [Accessed 01 February 2011]. [↑](#footnote-ref-63)
64. A detailed description of the sentiment analysis used for the analysis of empirical data within this thesis is located in Chapter Three. [↑](#footnote-ref-64)
65. ‘Me ha dejado helada, esta canción. Se me erizan los pelos de sólo imaginar ese fatal 11 de Marzo. Increíble que aún en esta época exista terrorismo como si fueramos bestias sin razón. Besos a España.’ (2008). La Oreja de Van Gogh. 11 de Marzo. *Palabras Retorcidas*. [online] Available at <<http://palabrasretorcidas.wordpress.com/2008/07/20/11-de-marzo-presentcion-en-vivo-y-letra/>> [Accessed 01 February 2011]. [↑](#footnote-ref-65)
66. Sopena, E. (2010). La Actitud de Acebes ante el Proceso de Paz, un Espectáculo Borchornoso. *El Plural*. [online] Available at <http://www.elplural.com/politica/detail.php?id=4527>> [Accessed 03 February 2011]. [↑](#footnote-ref-66)
67. Interview with Jonathan Githens-Mazer, Co-Director, European Muslim Research Centre (EMRC), Co-Director, Exeter Centre for Ethno-Political Studies (EXCEPS), Senior Lecturer, Institute of Arab and Islamic Studies (IAIS). Telephone Interview, 12 November 2010. [↑](#footnote-ref-67)
68. Interview with Felix Arteaga, Investigador Principal de Seguridad y Defensa. Real Instituto Elcano. Telephone interview, 04 August 2010. [↑](#footnote-ref-68)
69. “La tecnología es un medio cada vez más utilizados [sic] por los terroristas para realizar sus actividades. Los puntos positivos de la tecnología en el mundo real también son beneficiosos en el mundo criminal o del ciberterrorismo en aspectos como flexibilidad o ubicuidad. La tecnología permite especialmente un intercambio de información más continuo y la conveniencia del acceso a recursos remotos de manera instantánea.” Interview with Carles Fragoso Board of Directors, Centre de Seguretat de la Informació de Catalunya (CESICAT). Email interview, 8 August 2010. [↑](#footnote-ref-69)
70. ‘Algunas definiciones tratan de integrar los objetivos o intenciones y de definir el término con mayor precisión, por ejemplo, constituye ciberdelito "la actividad realizada mediante un computador que es ilícita o que algunas Partes considera [sic] ilícita y que puede realizarse a través de las redes electrónicas mundiales.’

    (2009). *El Ciberdelito: Guía Para Los Países En Desarollo*. Unión Internacional de Telecomunicaciones. División de Aplicaciones TIC y Ciberseguridad (CYB). [↑](#footnote-ref-70)
71. See Glossary of Terms. [↑](#footnote-ref-71)
72. Interview with Jamie Bartlett, Head of Violence and Extremism for DEMOS. London, 28 April 2011. [↑](#footnote-ref-72)
73. See Glossary of Terms. [↑](#footnote-ref-73)
74. ‘Por otra parte, los nexos entre el Terrorismo y la Delincuencia Organizada son intensos. Tales relaciones delictivo-criminales quedaron manifiestamente claras en el marco del XI Congreso de las Naciones Unidas sobre Prevención del delito y Justicia Penal 5. En la doctrina, hay estudios profundos sobre la transformación de los terroristas en delincuentes, aunque puede operar la transformación en sentido contrario 6. Es por ello que los terroristas y los delincuentes aprenden recíprocamente unos de los otros especialmente a la hora de establecer vías ilícitas para la comisión de sus actividades delictivas.’ Úbeda-Portugués, J., (2009). Nuevos Avances y Retos en la Lucha Contra el Terrorismo. Revista Electrónica de Estudios Internacionales. [↑](#footnote-ref-74)
75. ‘Terrorismo exterior es el terrorismo que actúa fuera de las fronteras de los Estados de origen o bien dentro de ellas pero contra intereses de otros países, entendiendo por “actuación” la realización de acciones armadas (atentados, sabotajes, asesinatos, secuestros). Existen otros aspectos ligados al terrorismo internacional que deben ser tenidos en cuenta. La existencia de mercenarios y de material bélico muy sofisticado, procedente del periodo de la Guerra Fría, así como las posibilidades que ofrecen las nuevas tecnologías para obtener información sobre material susceptible de ser empleado en actos terroristas, añaden un factor de inestabilidad al fenómeno terrorista. Terrorismo interior: Es aquel que nace dentro de un Estado y actúa contra dicho Estado. Este terrorismo puede mantener lazos internacionales para apoyarse entre grupos, emplear campos de adiestramiento o refugiarse en santuarios, pero tiene otra naturaleza distinta. España conoce bien esta lacra, que constituye el principal problema al que se enfrenta nuestra sociedad.’ (2003). Revisión Estratégica de Defensa, Gobierno Español. [↑](#footnote-ref-75)
76. Mochilero is the colloquial name given to people who sell counterfeit goods from backpacks. Manteros is another colloquial name given to people who sell counterfeit goods from blankets in a fixed location (Intellectual Property Alliance, 2005). [↑](#footnote-ref-76)
77. ‘Las instalaciones nucleares y las comunicaciones estratégicas no son accesibles por internet; apenas 1% de los hackers tienen los conocimientos necesarios para generar destrozos a gran escala.’ Salellas, L., (2005). Delitos Informáticos, Cíberterrorismo. Hadden Security Consulting. [↑](#footnote-ref-77)
78. Interview with Justin Webster, Television Producer. Telephone Interview, 29 November 2010 [↑](#footnote-ref-78)
79. Interview with Stewart Bertram, Cyber Intelligence Analyst, VeriSign. London, 09 September 2010 [↑](#footnote-ref-79)
80. Interview with Stewart Bertram, Cyber Intelligence Analyst, VeriSign. London, 09 September 2010 [↑](#footnote-ref-80)
81. Interview with Head of Research, United Kingdom Security Services. Telephone Interview, 15 September 2010. [↑](#footnote-ref-81)
82. ‘Los jóvenes y grupos no organizados han utilizado la tecnología para comunicarse, hacer convocatorias y movilizar a los ciudadanos. Un bucle de SMS´s y mensajes de correo electrónico ha sido el medio y el núcleo de la movilización.’ Varela, J. (2004). El Dia que los SMS Cambiaron la Politica. Periodistas 21 [online]. Available at <<http://periodistas21.blogspot.com/2004/03/el-da-que-los-sms-cambiaron-la-poltica.html>> [Accessed 01 February 2011]. [↑](#footnote-ref-82)
83. ‘Los terroristas de Al-Qaeda no corren nunca riesgos innecesarios que puedan poner en peligro su misión…De la misma manera, los terroristas londinenses fabricaron sus propios explosivos utilizando fórmulas químicas fáciles de encontrar en numerosas webs radicales islámicas y empleando compuestos de fácil adquisición en los comercios, porque es ésta una forma de conseguir explosivos mucho menos arriesgada que tratar de introducirlos en Inglaterra desde el exterior o que adquirirlos a algún delincuente local.’ (2005). El Espejo de Madrid. *Es.charla.actualidad*. [online] Available at <<http://groups.google.com/group/es.charla.actualidad/browse_thread/thread/fa085e57851a3e8b/962995989791975a?q=11-m+OR+11m+colaboracion+internacional&lnk=ol&>> [Accessed 01 February 2011]. [↑](#footnote-ref-83)
84. Interview with Head of Research, United Kingdom Security Services. Telephone interview, 15 September 2010 [↑](#footnote-ref-84)
85. Interview with Elena Sánchez, Researcher CIDOB. Barcelona, 09 December 2010. [↑](#footnote-ref-85)
86. (2010). The Well.com [online] Available at <<http://www.well.com/aboutwell.html>> [Accessed 10 December 2010]. [↑](#footnote-ref-86)
87. (2010). Ushahidi.com. [online] Available at <<http://ushahidi.com/>> [Accessed 19 December 2010]. [↑](#footnote-ref-87)
88. A detailed explanation of the methodology used to measure sentiment is located in Chapter Three. [↑](#footnote-ref-88)
89. Alvarez Amaro, J. (2004). Los Populares Extremeños Reprochan a Zapatero que Haya Ganado por el 11-M. *El Periódico*. [online] Available at <<http://www.elperiodicoextremadura.com/noticias/noticia.asp?pkid=101412>> [Accessed 29 March, 2011]. [↑](#footnote-ref-89)
90. ‘Ayer fue 11 M. Acabo de llegar de Madrid. Creo que allí hemos estado mas [sic] de un millón de personas, todavía no he visto las noticias. Ahora mismo no tengo palabras para expresar lo que siento’ (2004). Con las Victimas para Derrotar el Terrorismo. *Aika*. [online] Available at <<http://puchuaika.blogspot.com/2004/03/con-las-victimas-para-derrotar-el.html>> [Accessed 01 February 2011]. [↑](#footnote-ref-90)
91. ‘En el triste 11M de lo único que se quejó la gente fue de las mentiras que estaba diciendo el gobierno, léase que todo indicaba a que había sido ETA. Aquí se unió la imprudencia de dar información demasiado rápido con un presunto interés de algunos en que se pensara que no había sido terrorismo Islamista. Es mi opinión.’ (2005). Un Testimonio desde Londres. *Escolar.net.* [online] <<http://www.escolar.net/MT/archives/2005/07/un_testimonio_d.html> > [Accessed on 01 February 2011]. [↑](#footnote-ref-91)
92. ‘La otra parte es que Aznar mintió al pueblo español con las armas de destrucción masiva en Irak y no ha pagado todavía con un juicio’ (2007). 3 Anos de Golpe de Estado. *Eurabian News*. [online] Available at <<http://noticiasdeeurabia.wordpress.com/2007/03/11/3-anos-del-golpe-de-estado-del-11-m/>> [Accessed on 01 February 20111]. [↑](#footnote-ref-92)
93. Operación Nova was a police operation launched in September 2004 targeted at arresting people suspected of Jihadist terrorism. In total, 32 people from a terror cell directed by Mohamed Acharaf were arrested after proclaiming themselves as “Martyrs for Morocco” and attempting to bomb the Audiencia Nacional.

    Operación Sello was another police operation launched in 2004 and again in 2007 designed to arrest people directly associated with the Madrid attacks in 2004 and international terrorism more generally in 2007. The operation, which was ordered by Judge Ismael Moreno, involved the arrest of eleven people in Barcelona, Madrid, Cádiz, La Coruña, Girona, Lleida and Tarragona. [↑](#footnote-ref-93)
94. ‘Cinco años después, muchos aún queremos saber toda la verdad sobre el 11-M. Otros prefieren enterrar lo ocurrido y que no se hable de lo que pasó ese día y en los días siguientes. A fin de cuentas, tenemos a Zapatero en el Gobierno por culpa de esos atentados.’ (2009). Quinto Aniversario del Ataque Terrorista del 11M. *Martha Colmenares*.’ [online] <<http://www.marthacolmenares.com/2009/03/11/quinto-aniversario-del-ataque-terrorista-del-11m/>> [Accessed 01 February 2011]. [↑](#footnote-ref-94)
95. Monmar, (2010). Islamización de Europa “Eurabia”. Más pruebas de la presencia de Al Qaeda en España. [online] Available at <[http://alianzacivilizaciones.blogspot.com/2009/11/mas-pruebas-de-la-presencia-de-al-qaeda.html>](http://alianzacivilizaciones.blogspot.com/2009/11/mas-pruebas-de-la-presencia-de-al-qaeda.html%20) [Accessed on 01 March 2011]. [↑](#footnote-ref-95)
96. ‘La verdad es que se te hace el corazón un puño al leer los nombres de las víctimas o al ver las imágenes del atentado de Atocha o al oír a los familiares, no podemos imaginarnos siquiera lo que estarán pasando José María Naranjo tuvo muy buena iniciativa haciendo un Monumento a las Víctimas aquí en Torrejón y el gesto de llevar flores ayer, me ha parecido mu emotivo y, a nivel personal, voy a seguiros.’ *Juventudes Naranjas* (2010). GLITC Conmemora el Sexto Aniversario del 11-M. [online] Available at < <http://juventudesnaranjas.blogspot.com/2010/03/glitc-conmemora-el-sexto-aniversario.html>> [Accessed on 01 February 2011]. [↑](#footnote-ref-96)
97. ‘Lo que no entiendo ni creo que por mucha voluntad que ponga pueda hacerlo, es como cuando hablamos de 2 personas , casi todos estamos de acuerdo en que hay peligro con los musulmanes, pero cuando ya somos 3 o mas, nos callamos no vayan a acusarnos de racismo.’ *Militar*, (2004). Integrismo Islámico en España. [online] Available at < <http://www.militar.org.ua/foro/integrismo-islamico-en-espana-t6386.html>> [Accessed 01 February 2011]. [↑](#footnote-ref-97)
98. ‘Tres años después no sabemos que explotó, pero si quienes se beneficiaron no seáis ciegos lo de zp y eta no es normal, donde esta zp quienes son sus amigos en el mundo?; lo peor es que se han de estar robando todo como siempre soy de ccoo, y no estoy de acuerdo con muchas cosas que están pasando los españoles de hoy no somos los del 36 y queremos claridad y esta gobierno no nos la ha dado y cada vez se sumerge mas en las tinieblas’ Desiertos Lejanos (2007). Las Tramas Superpuestas de 11-M. [online] Available at <<http://www.desiertoslejanos.com/blog/?p=34>> [Accessed 01 February 2011]. [↑](#footnote-ref-98)
99. ‘El mejor homenaje que se puede rendir a las victimas, seria el esclarecimiento de la verdad y pedir cuentas a sus responsables, el ejecutivo actual y la izquierda de Cayo y su camarada Llamazares se deberían aplicar y no poner palos alas ruedas de la justicia. En el ejecutivo de ZP hay una sombra de duda mas que deberá aclarar si quiere ser de verdad lo que tanto dice DEMOCRATA.’ LNE.es (2010). Víctimas y Políticos Recuerden por Separado el 11-M. [online] Available at <<http://www.lne.es/espana/2010/03/11/silencio-reina-homenaje-victimas/884914.html?pCom=2#EnlaceComentarios>> [Accessed 01 February 2011]. [↑](#footnote-ref-99)
100. See the Glossary of Terms. [↑](#footnote-ref-100)
101. Interview with Jamie Barlett, Head of Violence and Extremism for DEMOS. London, 28 April 2011. [↑](#footnote-ref-101)
102. “Exacto, que no sabe como comunicar correctamente. Que están utilizando estrategias del siglo 20 cuando ya estamos en el siglo 21 y las cosas son totalmente diferentes y aparte muy poca gente está realmente preparada para diseñar estrategias, porque todos tienen la mentalidad del siglo 20 y no entienden…Cuando llegó el web mucha gente en el gobierno dijo qué hacemos con el web? Porque no sabemos cómo hacer. Sabemos cómo hacer con la prensa pero no se plantean…pero se ha percibido como si fuera un alíen monstruo, no saben cómo utilizarlo.” Interview with Maria Llorach, Former Head of Communications and Institutional Relations for the Congreso del los Diputados. Barcelona, 20 January 2011. [↑](#footnote-ref-102)
103. See Glossary of Terms. [↑](#footnote-ref-103)
104. *‘*Nunca reconoció el de Madrid; reconoció el de Indonesia, el de Londres, el atentado de Casablanca y por supuesto el de las Torres Gemelas, pero jamás ha reconocido el de Madrid”, ha afirmado la presidenta, en declaraciones en la Real Casa de Correos, tras la celebración de los actos oficiales del Día de la Comunidad.’ (2011). Gómez Critica las Declaraciones de Aguirre sobre la Autoría del 11-M. *El Plural* [online]. Available at <<http://www.elplural.com/politica/gomez-critica-las-declaraciones-de-aguirre-sobre-la-autoria-del-11-m/>> [Accessed 02 May 2011]. [↑](#footnote-ref-104)
105. ‘Esperanza Aguirre, como en múltiples [sic] ocasiones, cree que diciendo las cosas categóricamente puede engañar impunemente. Hay que decir bien claro que lo que dice Aguirre es falso. El atentado del 11-M sí fue reivindicado [sic] por Al Qaeda, [hasta lo recogió El Mundo](http://www.elmundo.es/elmundo/2004/04/15/enespecial/1082009222.html). Os dejo un [artículo que demuestra que Bin Laden reivindicó implícitamente los atentados del 11-M de Madrid](http://www.nortecastilla.es/agencias/20110502/mas-actualidad/espana/qaeda-responsable-11-m-amenazado-multiples_201105021313.html) en una entrevista personal.’ (2011). Esperanza Aguirre exculpa a Bin Laden de la autoría del 11-M (con argumentos falsos). Ventanas del Falcón [online]. Available at <[**http://ventanasdelfalcon.blogspot.com/2011/05/esperanza-aguirre-exculpa-bin-laden-de.html**](http://ventanasdelfalcon.blogspot.com/2011/05/esperanza-aguirre-exculpa-bin-laden-de.html)> [Accessed 03 May 2011]. [↑](#footnote-ref-105)
106. ‘En contra de lo que ha opinado Aguirre, Al Qaeda ha reivindicado en varias ocasiones el golpe de Madrid, que acabó con la vida de 192 personas en 2004… Aguirre, que se ha referido a Bin Laden como el "asesino de más de 2.300 personas inocentes", ha apuntado que el Ejército norteamericano, como ha dicho esta madrugada el propio presidente de EE UU, Barack Obama, ha decidido que esto es un paso adelante en la lucha contra el terrorismo’*.* Izquierdo, J.M., (2011). Hay GAL y GALES. El Ojo Izquierdo, *El País* [online]. Available at <<http://blogs.elpais.com/ojo-izquierdo/2011/05/hay-gal-y-gales.html>> [Accessed 03 May 2011]. [↑](#footnote-ref-106)
107. ‘Este lunes nos despertábamos con la noticia de la muerte de Osama Bin Laden, el líder de Al-Qaeda, y máximo responsable de los atentados terroristas del 11-S y del 11-M entre otros muchos atentados de una menor envergadura…Personalmente me alegra profundamente que Osama Bin Laden se encuentre fuera de circulación, lo que no quiere decir que hayamos superado la amenaza del terrorismo de Al-Qaeda. Estoy de acuerdo con la portada de hoy del EL PERIÓDICO, que decía “Obama venga el 11-S, el terror continua”’*.* Gerboles, D. (2011). Obama Venga el 11-M, El Terror Continua. *Mi Punto de Vista* [online]. Available at <<http://davidgerbolesperez.blogspot.com/2011/05/compasion-con-bin-laden.html>> [Accessed 03 May 2011]. [↑](#footnote-ref-107)
108. ‘Que Al Qaeda no había reivindicado el 11M lo dijo delante de Francino y no la cortó por mentirosa. Algo así ¿pero por qué miente usted con tanto desparpajo si lo reivindicó el tal y tal y tal? Y a renglón seguido la gran pregunta que nunca hacéis y que cerraría el debate del 11M para siempre: ¿lo organizó Aznar para atribuírselo a ETA y ganar por mayoría absoluta unas elecciones que tenía perdidas? (los nacionalistas ya no iban a apoyarle*).*’ (2005). Los GAL, el 11-M y la Doble Moral. *Escolar.net*. [online] <http://www.escolar.net/MT/archives/2011/05/los-gal-el-11-m-y-la-doble-moral.html> [Accessed on 01 February 2011] [↑](#footnote-ref-108)
109. (2011). El Gobierno mantiene un nivel de alerta antiterrorista alto después de que EEUU comunicase la muerte del líder Al Qaeda. [online] Available at <http://www.cronicadearagon.es/wordpress/?p=20576> Accessed on 06 May 2011 [↑](#footnote-ref-109)
110. ‘La que ens pot caure a sobre…**la venjança dels grups d’Al-Qaida** que, sorpresa, poden actuar perfectament sense el seu líder i venjar-se ells al seu torn. Ens avisen els especialistes que Al-Qaida no actua de forma jeràrquica. Ens avisa el president Obama que hem d’estar alerta, que es poden produir atacs…i llavors, això de que a través d’aquest assassinat s’elimina el terror  no és un contrasentit?’ (2011). Bin Laden I els “Bons Demòcrates” Americans. [online] Available at <<http://unatrobadora.wordpress.com/2011/05/02/bin-laden-i-els-bons-democrates-americans/>> [Accessed 03 May 2011]. [↑](#footnote-ref-110)
111. A detailed list of the interviewees for this thesis can be found in Appendix One. [↑](#footnote-ref-111)
112. A detailed explanation of the methodology used for the internet research can be found in Chapter Three. [↑](#footnote-ref-112)
113. Interview with Felix Arteaga – Head Researcher in Security and Defence. Real Instituto Elcano. Telephone interview, 04 August 2010 [↑](#footnote-ref-113)