LEABHARLANN CHOLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH | TRINITY COLLEGE LIBRARY DUBLIN
Ollscoil Átha Cliath | The University of Dublin

Terms and Conditions of Use of Digitised Theses from Trinity College Library Dublin

Copyright statement

All material supplied by Trinity College Library is protected by copyright (under the Copyright and Related Rights Act, 2000 as amended) and other relevant Intellectual Property Rights. By accessing and using a Digitised Thesis from Trinity College Library you acknowledge that all Intellectual Property Rights in any Works supplied are the sole and exclusive property of the copyright and/or other IPR holder. Specific copyright holders may not be explicitly identified. Use of materials from other sources within a thesis should not be construed as a claim over them.

A non-exclusive, non-transferable licence is hereby granted to those using or reproducing, in whole or in part, the material for valid purposes, providing the copyright owners are acknowledged using the normal conventions. Where specific permission to use material is required, this is identified and such permission must be sought from the copyright holder or agency cited.

Liability statement

By using a Digitised Thesis, I accept that Trinity College Dublin bears no legal responsibility for the accuracy, legality or comprehensiveness of materials contained within the thesis, and that Trinity College Dublin accepts no liability for indirect, consequential, or incidental, damages or losses arising from use of the thesis for whatever reason. Information located in a thesis may be subject to specific use constraints, details of which may not be explicitly described. It is the responsibility of potential and actual users to be aware of such constraints and to abide by them. By making use of material from a digitised thesis, you accept these copyright and disclaimer provisions. Where it is brought to the attention of Trinity College Library that there may be a breach of copyright or other restraint, it is the policy to withdraw or take down access to a thesis while the issue is being resolved.

Access Agreement

By using a Digitised Thesis from Trinity College Library you are bound by the following Terms & Conditions. Please read them carefully.

I have read and I understand the following statement: All material supplied via a Digitised Thesis from Trinity College Library is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of a thesis is not permitted, except that material may be duplicated by you for your research use or for educational purposes in electronic or print form providing the copyright owners are acknowledged using the normal conventions. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone. This copy has been supplied on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

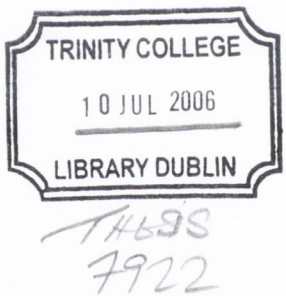
Reality Bytes: Cyberterrorism and Terrorist Use of the Internet

Maura Conway

Thesis submitted to University of Dublin, Trinity College for the degree of PhD in Political Science

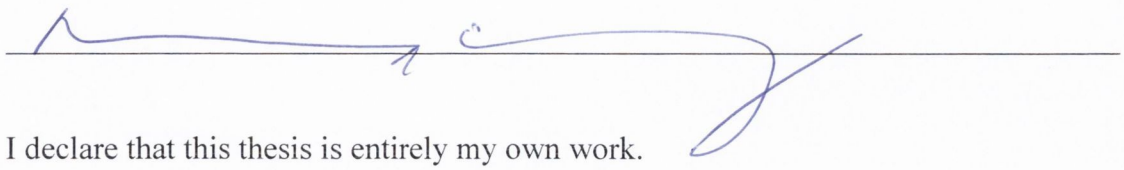
2006

FOR
My Mom & Dad, Kak, Hube, Ger & D. And Mike.
With Love. And Thanks. Always.

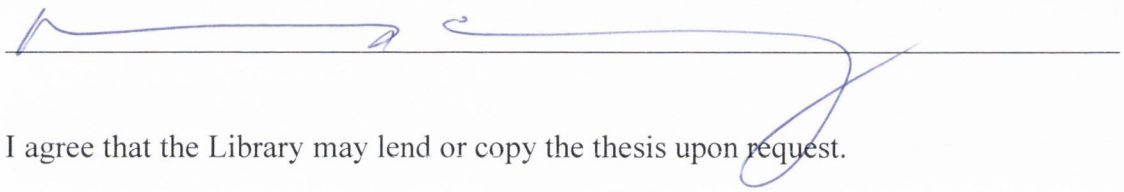

TRINITY COLLEGE
10 JUL 2006
LIBRARY DUBLIN
THESIS
7922

DECLARATIONS

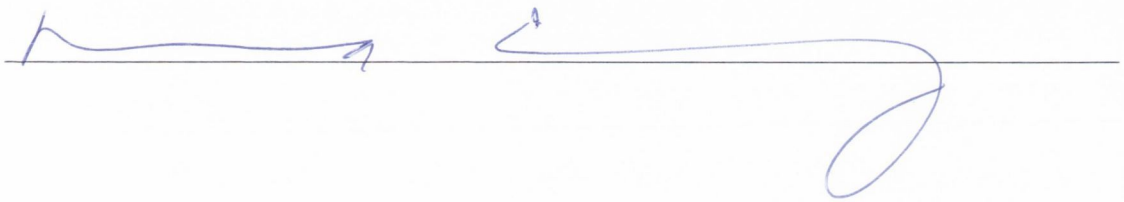
I declare that thesis has not been submitted for a degree at this or any other university.



I declare that this thesis is entirely my own work.



I agree that the Library may lend or copy the thesis upon request.



SUMMARY

The analysis contained herein treats the relationship between terrorism and the Internet. Instead of treating cyberterrorism as the most important conjunction of terrorism and the Internet (as has been the tendency to date--even amongst those who doubt the efficacy of the cyberterrorist threat), this study illustrates how terrorist use of the Net is an everyday 'reality' and one that ought to attract far more attention than it has yet received. The study places a particular emphasis on terrorist Web sites as the vehicles for terrorist publicity and propaganda, one of the most prominent contemporary terrorist uses of the Net, but also seeks to balance claims about the power of 'small media,' such as the Internet, against the continued dominance of the traditional mass media (i.e. 'big media').

Given the paucity of previous research addressing these issues, this study cannot be anything other than preliminary. Nevertheless, the aim in this text is to clarify what is meant by cyberterrorism by investigating both academic and media portrayals of the term in conjunction with an in-depth treatment of the problem of definition. This is followed by a description and analysis of the mass-media's role in the origins of the current cyber-angst. The spotlight is then shifted from the much-hyped cyberterrorism to an analysis of the Internet as a soft power tool employed by terrorists with increasing success.

The latter is achieved by the provision of a description and analysis of the five major terrorist uses of the Net (information provision, fundraising, networking, recruitment, and information gathering), with the alleged terrorist use of steganography for secure communication purposes receiving in-depth treatment. As it is asserted herein that information provision via terrorist Web sites is the most important aspect of contemporary terrorist Net use, a substantial portion of the text is concerned with exploring the latter. The English-language Web sites of ten terrorist groups are the object of both a content analysis and close reading in order to determine these sites' functioning and effectiveness, and to draw out their discursive structuring and framing mechanisms respectively. A determination of audience impact is also attempted here. Finally, the Lebanese Shi'a group Hizbollah has instituted a particularly effective cyber-strategy and so this group's Web sites are the subject of a detailed case study.

In terms of conclusions: on the micro level, this text shows that the cyberterrorist threat has been over hyped and that we ought to be more concerned instead with the way in which terrorists are currently using the Internet, particularly for the purposes of information dissemination. On the macro level, the text illustrates the way in which the Internet is contributing to the reshaping of international relations, particularly in terms of the way in which power is conceived therein, while at the same time advocating for the retention of a balanced view of the relationship between 'big' and 'small' media. Summing up, if the Internet is a sling and content the stone with which terrorists in the guise of David are seeking to overcome the Goliath that remains traditional mass media, then David's opening shot is on target, but there's still a way to go before he overpowers the giant.

TABLE OF CONTENTS

ACKNOWLEDGMENTS x

LIST OF TABLES xi

LIST OF FIGURES xii

INTRODUCTION 1

Introduction
Background
Relevance
Theoretical Underpinnings
Instrumental Power
Soft Power
Terrorism and (Mass) Communication(s)
Structure of Study
Scope of Study
Case Selection
Limitations
Design of Study
Data
Methods

PART I: ON CYBERTERRORISM

1. **Cyberterrorism: Academic Perspectives** 33

Introduction
The Birth of a Concept
From 'Real World' Terrorism to Cyberterrorism
Virtual Violence?
Hacking Versus Cyberterrorism
Hackers as Terrorists
Hacktivism versus Cyberterrorism
Cybercrime versus Cyberterrorism
Computer as Target Versus Computer as Tool
Conclusion

2. **Media and Cyberterrorism: A Study in the Construction of 'Reality'** 62

Introduction
Theoretical Underpinnings: Threat Politics
Threat Framing
Agenda Setting
Methodology
Fear of Technology, Fear of Terrorism
Shut-Down-the-Power-Grid Scenarios
Reasoning by Analogy
Electronic Pearl Harbour

Weapons of Mass Disruption
Identifying Antagonistic Actors
Terrorist Hackers
Hacker Terrorists
Emergency Measures
The Pre-9/11 Environment
The Post-9/11 Environment
Conclusion

PART II: ON TERRORIST 'USE' OF THE NET

3. Terrorist 'Use' of the Internet and Fighting Back.....103
Introduction
Conceptualising Terrorist Activity on the Net
The 'Use' Approach
What Makes the Internet Different?
Why Terrorists are Launching Into Cyberspace
Five Terrorist Uses of the Net
Information Provision
Financing
Networking
Recruitment
Information Gathering
Other Types of Use
Misuse
...and Offensive Use
Fighting Back
The Role of Law Enforcement and Intelligence Agencies
Other Agencies: Sanitising Government Sites
Hackers and Hacktivists
Conclusion

4. Terrorist Use of Digital Steganography: Real or Imagined?..... 161
Introduction
A Brief History of Steganography
Digital Steganography
Steganography Hits the Headlines
Against Terrorist Use of Digital Steg
Jack Kelley as Issue Entrepreneur
Steganalysis
Alternative Secure Communication Methods
Low-Tech Steg
E-Mail & E-Groups
Contrary Views
Conclusion

PART III: ON TERRORIST WEB SITES

5. **Terrorist Web Sites: Their Contents, Functioning, and Effectiveness... 193**
   Introduction
   Comparing Terrorist Web Sites: Methodology
      Functionality
      Delivery
   Analysis of Content
      Downward Information Flows
      Upward Information Flows
      Hyperlink Analysis: Lateral/Horizontal Information Flows
      Interactive Information Flows
      Terrorist Web Site Delivery
   Conclusion

6. **The Discursive Structuring of Terrorist Web Sites: Narratives of Religion, Revolution, and Rights..... 224**
   Introduction
   Increasing the Scope of Conflict
      Domestic vs. International Mobilization
   Terrorist Web Sites' Audiences
      The Internet and Domestic Mobilization
      International Audiences and Their Role(s)
   The Discursive Structuring of Terrorist Sites
      Religious Narratives
      Revolutionary Narratives
      Rights-Based Narratives
   Responses to US Terrorism Designation
   The Impact of Photographs and Other Visuals
      Recruitment Images
   Audience Responses to Terrorist Sites
      States as Audiences
      International Society as Audience
   Conclusion

7. **Cybercortical Warfare: Hizbollah's Internet Strategy..... 271**
   Introduction
   Szafranski's Neo-Cortical Warfare
      The New Public Diplomacy
      The Increasing Importance of Soft Power
      Cybercortical Warfare
   Background Information on Hizbollah
      The US Position
      Hizbollah's Cyber Capabilities
   Hizbollah's Internet Strategy
      The Major Web Sites
      Discursive Structuring of Sites
   An Integrated Media Strategy
      Al-Manar Television
      'Special Force'

Electronic Interfada
Cybercortical Warfare: The Effects
Conclusion

CONCLUSION..... 305
Introduction
Desecuritizing the Cyberterrorist Threat
Focusing on Terrorist 'Use' of the Net
Future Research

APPENDICES..... 315
Appendix A. What is the Internet and How Does it Differ From the Web?
Appendix B. Definitions of Cyberterrorism, 1997-2003
Appendix C. Five Major Categories of Terrorist Internet Use

BIBLIOGRAPHY..... 321

Web sites are notoriously ephemeral. All links and URLs contained herein were operational on October 31, 2005. However, it is more than likely that many will have changed location or simply disappeared since.

ACKNOWLEDGMENTS

I have benefited from the assistance of several institutions and many individuals while undertaking this research. Firstly, thank you to the staff of the Department of Political Science at Trinity College Dublin, particularly my Supervisor, Nalini Persram, and Eddie Hyland, who read and commented upon the completed text.

This text has also benefited from the comments and inputs of Fiona Adamson, Lee Armistead, Dorothy Denning, Myriam Dunn, James Der Derian, Sarah Oates, Magnus Ranstorp, Philip Seib, and Gabriel Weimann. Any errors are solely mine.

Thanks are also due to the staff of the School of International Relations at the University of St. Andrews for their support. I am particularly grateful to John Anderson and William Walker for giving me the opportunity to teach at St. Andrews. Special mentions also for Sally Cummings, Mark Imber, and Fiona Oviatt.

I'm also grateful to Robert Elgie and all those in the School of Law & Government at Dublin City University for giving me the opportunity to return home and making settling in at DCU a breeze. Particular thanks with regard to the latter to the remainder of the 'Trinity Three': Eoin and Francesco.

An extra special thank you to all the 'girls' at TCD, especially Shiera, Nic, Karen, and Gemma for their unwavering support.

Finally, this text would never have come to fruition without the love and support of my Mom and Dad, Anne and Hubert Conway, my sister, Kathryn, my brother, Hubie, and my brother Gerard and his wife, Deirdre. Thanks guys!

LIST OF TABLES

I.1 Characteristics of 'Old' vs. 'New' Terrorism.....28
1.1 Articles on Cyberterrorism Appearing in Journal Special Issues..... 35
1.2 Articles on Terrorism and the Internet Appearing in Major Terrorism Studies Journals, 1997-2003..... 37
2.1 Cyberterrorism in US Newspapers Before and After September 11, 2001..... 92
2.2 Cyberterrorism in UK Newspapers Before and After September 11, 2001.....92
2.3 US Government Documents: Cyberterrorism and Critical Infrastructure Protection, 1998-2004..... 96
3.1 Typology of Cyber Activism and Cyber Attacks..... 108
3.2 Terrorist Uses of the Net..... 112
3.3 Increasing Use of Government-Related Web Sites Post 9/11..... 154
5.1 Terrorist Group Web Sites.....195
5.2 Information & Communication Flows on Ten Terrorist Web Sites..... 196
5.3 Site Delivery Indicators for Ten Terrorist Web Sites..... 198
5.4 Results of Google Search for Terrorist Group Information (10 April 2005)..... 214
7.1 Numbers of Internet Users in the Middle East, 2001..... 299

LIST OF FIGURES

1.1 Google Screenshot: Results from Search for 'Cyberterrorism'..... 38
2.1 Graphic Accompanying 'The Great Cyberwar of 2002'..... 75
3.1 Screenshot: Ulster Loyalist Information Service Web Site (March 2003)..... 116
3.2 Evolution of MI5 Web Site, December 1998 to December 2004..... 153
4.1 Overview of Generic Steganographic Scheme..... 168
4.2 Screenshot: Abualbukhary.net (July 2004)..... 190
5.1 Screenshot: Top Page of Hamas Children's Site..... 207
5.2 Screenshot: Page from ETA's Online Art Gallery..... 216
6.1 Screenshot: Top Page of 'Readers Letters' Section of Hizbollah's Moqawama Web Site..... 263
7.1 Screenshot: Image from Top Page of Hizbollah.org..... 285

INTRODUCTION

"Power itself is being so endlessly redistributed and redefined that it's changing nature is one of the principle destabilizing forces in the world today, and a source of strength for those who can adapt to it most quickly...The realpolitik *of the new era is* cyberpolitik, *in which actors are no longer just states, and raw power can be countered or fortified by information power"*

- David J. Rothkopf (1998)

INTRODUCTION

This thesis is--to the best of my knowledge--the first extended academic study to treat the relationship between terrorism and the Internet[1] in an integrated manner. There are a fairly large number of studies that address the issue of cyberterrorism, but only a tiny number of political scientists, international relations scholars, or even those whose exclusive focus is the study of terrorism, have engaged in research in other areas of terrorism and the Internet. No attempt has yet been made to uncouple cyberterrorism and terrorist 'use' of the Net, as the present work attempts to do.

At its core this study seeks to address two basic questions:

- Is cyberterrorism the most important aspect of the terrorism-Internet relationship?
- If it is not, what other aspects of this relationship are more important and why?

Over the course of the research, however, these questions came to be supplemented by others, chief amongst which were the following:

- What is 'cyberterrorism'?
- Is it purely a media construct?

[1] The terms 'Internet' and 'Web' are capitalised throughout this project. For a discussion of case-sensitivity in relation to the term Internet, see Schwartz 2002, 3.

- Is there a difference between 'cyberterrorism' and terrorist 'use' of the Net?
- What are the most important contemporary terrorist uses of the Internet?
- Why has just one of these uses, steganography, received such an inordinate amount of attention?
- Are allegations of habitual terrorist use of digital steganography plausible?
- Is it possible to show that terrorist Web sites are vehicles for more routine and yet potentially more powerful uses than the latter?
- What are some of the alternative functions of such Web sites and how effective are they?
- What type of information is provided and what type of rhetoric employed on such sites?
- Who are the target audiences for terrorist Web sites?
- Taking all of the above into account, is it accurate to contend that the Internet is an increasingly effective soft power tool for terrorist organisations worldwide?

The title of this study, *Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Net*, hints at its core thesis. Instead of treating cyberterrorism as the most important conjunction of terrorism and the Internet (as has been the tendency to date--even amongst those who doubt the efficacy of the cyberterrorist threat), this study illustrates how terrorist use of the Net is an everyday 'reality' and one that ought to attract far more attention than it has yet received. Here, a particular emphasis is placed on terrorist Web sites as the vehicles for terrorist publicity and propaganda, one of the most prominent contemporary terrorist uses of the Net. Given the paucity of previous research addressing these issues, this study cannot be anything other than preliminary. Nevertheless, the aim has been to clarify what is meant by cyberterrorism, explain the origins of the current cyber-angst and, having accomplished these, shift the spotlight from the much-hyped cyberterrorism to an analysis of the Internet as a soft power tool employed by terrorists with increasing success.

BACKGROUND

The Internet is the instrument of a significant political power shift. In the space of thirty years, it has metamorphosed from a US Department of Defence command-and-control network consisting of less than one hundred computers to a network that criss-crosses the globe: today, the Internet is made up of tens of thousands of nodes (i.e. linkage points) with over 105 million hosts spanning more than 200 countries. With a current estimated population of regular users of over 600 million people, the Internet has become a near-ubiquitous presence in many world regions. That ubiquity is due in large part to the release in 1991 of the World Wide Web (see Norris 2001, 27-28).[2] In 1993 the Web consisted of a mere 130 sites, by century's end it boasted more than one billion pages. Such high levels of interconnectivity produce both positive and negative externalities, however. Perhaps the single greatest drawback is the Western world's ever-increasing information network dependency. More and more, the effective functioning of the developed world is reliant on the sustained and effective functioning of our information infrastructure(s).

While natural disasters (e.g. earthquakes, hurricanes, tornadoes, etc.), accidents, operator error, hardware and software failure, can result in the disruption or destruction of critical infrastructure, deliberate attacks upon that infrastructure, particularly when employed in conjunction with physical threats, could potentially cause even greater harm. The threat of attack is two-fold: physical attacks against those facilities that house components of the information infrastructure and cyber attacks against the computer networks that facilitate control of that infrastructure. In the wake of the events of 9/11, there is widespread concern that cyber attack is imminent.

The Internet presents more than one avenue for terrorist activity, however. There is the potential for cyberterrorist attack, but the Internet is also a useful vehicle for communication, command, and control by terrorists. Media have for decades been attributed with considerable significance in processes of cultural and political transformation. The Internet is daily heralded as a new media technology of enormous

---

[2] Essentially, the Web is a component of the Net. However, see Appendix A for a more detailed description of the relationship between the Internet and the WWW.

and increasing significance; it is the first many-to-many communication system and the instrument of a political power shift. The ability to communicate words, images, and sounds, which underlies the power to persuade, inform, witness, debate, and discuss (not to mention the power to slander, propagandize, disseminate bad or misleading information, engage in misinformation and/or disinformation, etc.) is no longer the sole province of those who own or control printing presses, radio stations, or television networks. Every machine connected to the Internet, from expensive laptop computers to lowly mobile phones, is potentially a printing press, a broadcasting station, a place of assembly (Rheingold 1998). And in the twenty first century, terrorists are availing of the opportunity to connect.

In 1998, it was reported that approximately half of the (then) thirty terrorist groups designated as 'Foreign Terrorist Organisations' under the US Antiterrorism and Effective Death Penalty Act of 1996 operated Web sites. Today, virtually every active terrorist group--there are approximately seventy operating worldwide--has an online presence, and many groups are the subjects of more than one site. Nationalist-separatist groups that maintain Web sites include the Irish Republican Army (IRA), *Armata Corsa* (the Corsican Army), the Moro Islamic Liberation Front (MILF) in the Philippines, and various Chechen organisations. Islamist groups also maintain a prominent online presence with sites representing al-Qaeda, Palestinian Islamic Jihad, *Ansar al Islam* (Supporters of Islam), the Kashmiri *Hizb-ul Mujehideen*, the Islamic Movement of Uzbekistan (IMU), the Pakistan-based *Lashkar-e-Taiba*, and others. Both traditionally conceived right-wing and left-wing terrorist organisations are also present on the Web. Left-wing terror group sites include those maintained by the Popular Front for the Liberation of Palestine (PFLP), the Turkish-based Popular Democratic Liberation Front (DHKP/C), Peru's *Tupac Amaru*, and the Japanese Red Army (JRA). Right-wing terrorist groups who maintain an online presence--though much less numerous than their leftist counterparts--include the Colombian National Liberation Army (ELN) and the United Self-Defence Forces of Colombia (AUC), amongst others.[3]

[3] There is a tendency to equate far-right or 'hate' groups with terrorist groups, especially amongst Internet researchers and proponents of the 'new' terrorism. Such an equation does not hold up under scrutiny; Web sites maintained by terrorist and hate groups differ markedly in terms of appearance, content, functioning, and effectiveness. Analyses that uncritically lump terrorists and hate groups--and

A majority of the thirty-six groups that appear on the US State Department's current list of Designated Foreign Terrorist Organizations have an established online presence. A number of these groups have already shown a clear understanding of the power of the global information network to publicise their position. The Lebanese Hizbollah have clearly demonstrated this ability, as have the Tamil Tigers, Al-Qaeda, and numerous other terrorist organisations that maintain a Web presence.[4]

RELEVANCE

The majority of the literature dealing with terrorism and the Internet focuses on cyberterrorism. In particular, it focuses on the vulnerability of critical information infrastructure(s) to cyber attack. This literature has a number of difficulties, however. Chief among these is the absence of definitional clarity arising out of the tendency to conflate 'cyberterrorism,' hacktivism (i.e. politically motivated hacking), and terrorist 'use' (and 'misuse') of the Net. Second, a large part of the discussion surrounding cyberterrorism has taken place not within the confines of academe, but in the mass media. In other words, a vast amount of the 'literature' is not literature at all, but journalism. Nonetheless, both types of account have been consistently alarmist in nature, focusing on the potentially disastrous consequences of a successful future cyberterrorist attack, while skipping blithely over the proven role played by the Internet in a vast amount of current terrorist activity. This study differs from previous studies not just in its central thesis, but also in its sustained analysis of both academic and media portrayals of cyberterrorism, its in-depth treatment of the problem of definition, and its integration of the cyberterrorism issue with the other major issues surrounding terrorism and the Internet.

---

their Web sites--together include Chalk 1999, Crilley 2001, Damphousse & Smith 1998, Levin 2002, Nacos 2002, Whine 1999.

[4] A relatively comprehensive list of all such sites, both official and unofficial, is maintained by an individual in the United States and is available online at http://www.cromwell-intl.com/security/netusers.html.

The fact remains that despite the presence of many terrorist organisations online, worldwide no act of cyberterrorism has ever yet occurred. The point is not that cyberterrorism cannot happen or will not happen, but that it has not happened yet. Why persist then in addressing the cyberterrorism issue? Because, to reiterate, it is important to be clear as regards what types of acts might constitute cyberterrorism and to distinguish these from contemporary terrorist 'use' of the Net, which does not. On a more personal note, but relatedly, it has been the author's experience--at conferences, in lectures, etc.--that a failure to address the cyberterrorism issue causes considerable confusion for audiences who are then under the misapprehension that when one is speaking about contemporary terrorist Net use, one is actually referring to 'cyberterrorism,' but have some unspecified difficulty with employing the term. It is absolutely crucial in a project of this sort, therefore, to devote some considerable space to a description and analysis of the cyberterrorist threat in which there is considerable public interest, but about which there is also considerable public fear and confusion.

Given the complete absence of cyberterrorism to date, the state of research into terrorist group's very real online presence is curious on two counts. As a cursory glance in any bookstore or library reveals, the majority of what passes for knowledge about the intersection of terrorism and the Internet is based on opinion and impression, not on social science theory or empirical investigation. Further, most of the research that is available is small scale, focused on specific groups, and dispersed across space and time such that meaningful synthesis is next to impossible. The present research, on the other hand, provides an integrated and up-to-date analysis of various terrorist uses of the Net including, data mining, fundraising, recruitment and mobilisation, covert communication, networking, sharing information, planning and coordination, etc. The assertion that terrorists routinely employ digital steganography for secure communication purposes is also interrogated here. The latter has come to be accepted as an article of faith amongst terrorism scholars on the sole basis, it appears, of newspaper reports of dubious provenance. In addition to further illuminating an important aspect of the terrorism-Internet nexus, exploration of the steganography issue serves as an additional example of the enduring power of 'old' media.

Finally, this research also explores the primary materials provided by modern terrorists, in the form of their Web sites, to say something about the efficacy of the Internet as a political tool, particularly the increasing role of soft power in our information society and the way in which Internet-savvy terrorist groups have wielded this. These Web sites have not yet been the subject of any sustained academic investigation (Donohue 2003, 232; Tsfati & Weimann 2002, 319; Weimann 2004b, 7). A majority of the research and analysis pertaining to the Internet and Web sites as political tools has focused on the power of transnational advocacy groups, such as Green Peace, Amnesty International and other civil society actors, and their ability to harness the power of international communications technologies to forward their goals. Much less attention has been paid to those groups that compose 'uncivil society,' with research on terrorist groups' online presence, in particular, still in its embryonic stages (Arquilla & Ronfeldt 2001, 20).[5] This may be due to a number of factors, including the difficulty associated with fitting groups that employ violence into the various frameworks devised to categorize social movements, and a certain 'feel good factor' that imbues the work of scholars concerned with issues of transnationalism and international advocacy.

An alternative reason why the academic community has essentially ignored Web sites maintained by terrorist organizations may be that scholars doubt the efficacy of the Internet as a political tool. Walter Laqueur, a respected figure in terrorism studies, made the following observation in 1999:

> No amount of e-mail sent from the Baka Valley to Tel Aviv, from Kurdistan to Turkey, from the Jaffna peninsula to Colombo, or from India to Pakistan will have the slightest political effect. Nor can one envisage how in these conditions virtual power will translate into real power (p.262).

This statement is doubly startling when one considers that a few lines previously Laqueur admits that audiocassettes smuggled into Iran played a key role in the

[5] It's worth mentioning that Arquilla, Ronfeldt, and their Rand colleagues were some of the first researchers to draw attention to the potential of the Internet as a terrorist tool, but without building empirically on their assertion to any significant extent (Lesser et al 1999).

Khomeini revolution.[6] In more recent times, numerous (coalitions of) civil society actors have conducted successful campaigns via the Internet that have had significant political effects. For example, e-mail was credited with halting a US banking plan aimed at combating money laundering; the Nobel Prize-winning International Campaign to Ban Landmines, which successfully lobbied for a treaty stopping the use, production, stockpiling, and transfer of antipersonnel mines, coordinated it's activities via the Net (see Rutherford 2002); the Web site MoveOn.org, best known today for its efforts to mobilize opponents of both George W. Bush and the Iraq war, has attracted over two million subscribers to join its e-mail list and was responsible for instituting a US-wide TV advertising campaign paid for by online donations (see Gallo 2003; Hara & Estrada 2003; Jacobs 2005; Williams 2003). In each case 'virtual' or 'soft' power was translated into 'real' power, whether financial, legal, or otherwise. These and similar successes[7] have not gone unnoticed by terrorist groups and their supporters who realize that establishing a meaningful virtual power-base is reliant on a well-designed Web site that performs effectively.

THEORETICAL UNDERPINNINGS

The forms of politics enabled by the current climate of rapid global change are incapable of being accounted for by the dominant strains of international relations (IR) theory, and neo-realism in particular. This understanding of the political as something which only legitimately emanates from the state means that conventional IR theory reproduces notions of political power unsuited to an era in which political identities and processes are configured both within and without bounded forms of political community. The upshot of this is that IR, as a discipline, is effectively blind to many of the important new forms of 'international' politics taking place in the world today.

---

[6] For an account of the use of small media (e.g. audio and video cassettes) in the Iranian revolution, see Sreberny-Mohammadi & Mohammadi 1994. Fandy (1999) discusses the use of both small media and the Internet by opposition groups in Saudi Arabia.

[7] Although not 'successful' in the accepted sense of emerging from a contest the winner, Howard Dean's innovative use of the Internet in his bid for the Democratic party's nomination for the 2004 US presidential race received extensive coverage stateside (see Cornfield 2005, 1-3; Jacobs 2005; Rainie *et al* 2005, 1-2)

Certainly, the IR community has neglected the study of both terrorism and the Internet, though both are undoubtedly 'international' in their scope and each 'powerful' in their own right.

Power is one of those ubiquitous terms that everyone seems to understand but few can actually define. It is a foundational concept of political science and a central pillar of International Relations, but one that has been subject to vast change in the last decade. Many IR scholars have contributed texts that have addressed the nature of power and its effects on the global system (Morgenthau 1967; Keohane & Nye 1989; Waltz 1979). Hans Morganthau, in his book *Politics Among Nations: The Struggle for Power and Peace* (1967), defined the elements of national power as geography, natural resources, industrial capacity, military preparedness, population, national character, national morale, and the quality of diplomacy and government (p.xviii). These are the traditional power resources focused upon by IR scholars. Information-based power was not totally neglected, however. Writing in 1939, the great British realist E.H. Carr identified three categories of international power: military, economic, and power over opinion (1964, 108). It wasn't until the 1990s, however, that Joseph Nye and other IR scholars began to theorize about information-based power as a distinct type of power, distinguishable from hard power.[8] Nye first argued for the concept of 'soft power' in his book *Bound to Lead*. The journal *Foreign Affairs* followed up with a number of articles speaking to the issue of information as power (Cohen 1996; Keohane & Nye 1998; Nye & Owens 1996; Wriston 1997; see also Rothkopf 1998 & Berkowitz 1996). These ideas were mirrored in books such as Rosencrance's *The Rise of the Virtual State* (1999) and a number of collaborative works produced by John Arquilla and David Ronfeldt, which discuss the role of information and how it influences international affairs (1996a, 1997, 1999, 2001).[9]

---

[8] Of course, the idea of power having an agenda-setting dimension in the shaping of consciousness was addressed by political theorists long before such approaches came to prominence in IR; such a position was famously summarized and expanded upon by Steven Lukes in his three-dimensional conception of power as laid out in *Power: A Radical View* (1974).

[9] In the realm of practice, as opposed to theory, it should be noted that US military strategists were particularly quick to grasp the potential force-multiplier effects of new information technologies. Analyses of the so-called Revolution in Military Affairs (RMA) are included in the collection entitled *In Athena's Camp* (1997), edited by Arquilla and Ronfeldt and referred to above, while other worthwhile contributions on this subject and related issues include Goldman 2004, Hammes 2004, Khalilzad & White 1999, Lonsdale 2004, and Schwartzstein 1996.

Arquilla and Ronfeldt's contention that information is the most important element of power is not yet widely accepted. Traditional Realists and Neo-Realists still promote ideas of classical power politics, while Neo-Liberals focus on globalization and economic power. Both have something to contribute to debates, but neither camp has been able to adequately explain the changes in world events, especially in the last decade. Other theorists accept the power of information, but do not believe that it will change the fundamentals of world politics. Traditional measures of military force, gross national product, population, energy, land, and minerals have therefore continued to dominate discussions of the balance of power. These power resources still matter. Today, however, information is also an important element of power. Critics of the new view of power have argued that because only sixteen percent of the world has access to the Internet,[10] information cannot truly change global politics. Everyday however more people are going online. The Internet has the fastest rate of penetration of any communication technology in history. In the United States, the radio took thirty years to reach sixty million people; television reached this level of diffusion in fifteen years; the Internet did it in three years (after the development of the WWW) (Castells 2000, 382). Information is a central element of power because of its fungibility. The ability to transfer the power of information is what makes it so useful politically (Baldwin 1979, 166). The huge explosion in technology, particularly the rise of the Internet, has transformed the power paradigm. Groups, organizations, nation-states, and even individuals can now influence policy at the systemic level by employing information power. The ability to manipulate information will be a primary capability in future conflicts and is already making an impact in the present, as will be demonstrated.

This project explores the relationship between terrorism and the Internet through the lens of information power. Two 'types' or 'categories' of information-based power are deemed key to this relationship; these are instrumental power and soft power, both of which are described below. Updating the arguments set forth by Robert Keohane and Joseph Nye in their seminal book, *Power and Interdependence* (1989), the argument here is that the use of information is changing the idea of what we look

[10] According to ClickZ Stats, there were 945 million Internet users worldwide in 2004. The US Census Bureau reported that the world's population stood at just over six billion in August 2004.

for in terms of power capabilities within the realm of international politics. It is important to state here, however, that to the extent that this text is 'about' power, it is in the manner of a "contextual power analysis" (Baldwin 1979, 167) as advocated by Laswell and Kaplan: "What is common to all power and influence relations is only effect on policy. What is affected and on what basis are variables whose specific content in a given situation can be determined only by inquiry into the actual practices of the actors in that situation" (1950, 92). And again: "Political analysis must be contextual and take account of the power practices actually manifested in the concrete political situation" (1950, 94). This project is, therefore, centrally concerned with the range of tools provided by the Internet and through which terrorist actors can exert influence; it reaches far beyond traditional accounts of power and argues, in effect, that the rise of the Net rather than being regarded as an interesting side-show must increasingly be regarded as one of the key mechanisms of agency in international politics.

Instrumental Power

"Instrumental power focuses on the capacity or capability of power holders to effect particular outcomes" (Singh 2002, 7). IT, or any technology for that matter, is a force that enhances these capabilities. From an instrumental perspective, new technologies can empower political actors--in this case, violent sub-state groups. Modern terrorists consider the Internet an invaluable tool for achieving their goals. Indeed most theories of 'armed propaganda' are partly technologically driven. In his *Mini-Manual of the Urban Guerrilla* (1971), Carlos Marighella wrote:

> The urban guerrilla must never fail to install a clandestine press and must be able to...produce clandestine newspapers, pamphlets, flyers, and stamps for propaganda and agitation against the dictatorship....The urban guerrilla engaged in clandestine printing facilitates enormously the incorporation of large numbers of people into the revolutionary struggle....Tape recordings, the

> occupation of radio stations, and the use of loudspeakers, drawings on the walls...are other forms of propaganda (p.104).

On a more fundamental, though perhaps less visible level, information technologies (IT) can also influence the very nature of power itself. This aspect of the Internet will be returned to below, but for now the focus is on the Internet as a source of instrumental power.

One of the first ways in which political scientists and policy makers examined the relationship between information technologies and power was to focus on IT as a source of instrumental power. J.P. Singh describes how the instrumentality of the telecommunication infrastructure was apparent historically in the US Department of Justice's concerns about AT&T's use of monopoly power in the early 1940s. In the 1960s, he says, security concerns began to spill over into the economic realm when enhancing national wealth through information infrastructures became linked to concerns about national power, while in the 1980s instrumental power concerns were most obvious in national debates about economic competitiveness. During the course of the 1990s, traditional concerns like security and political change were joined to those about economic power and technologies (Wriston 1988). At around this time, conceptions of security changed in two major ways. First, information technologies were deployed to enhance capabilities in tasks ranging from the manufacture of 'smart weapons' to organizational ones like defense preparedness (Arquilla & Ronfeldt 1997; Deibert 1997; Nye & Owens 1996). Second, and one of the issues with which this project is concerned, protecting critical information infrastructures against varied threats became a core concern of many states, particularly the United States (Singh 2002, 7-9). The precise nature of these threats and responses to them are described and analyzed in Chapters One and Two.

Of course, the instrumental features of IT extend beyond state concerns. Information is the new lifeblood of the international system. World politics today transcends simple international relations, and much of the change has taken place as a result of the spread of information infrastructures (Luke 2001, 113). The information revolution is driving dramatic changes in political, diplomatic, military, economic,

social, and cultural affairs. In the second half of the twentieth century, economically advanced countries made the shift into what has been termed the 'information society' or the 'information age.' The futurist Alvin Toffler (1980) has labelled this transition the 'Third Wave,' suggesting that it will ultimately be as consequential as the two previous waves in human history: from hunter gatherer to agricultural societies, and from agricultural to industrial ones. The rapid expansion and diffusion of new International Communications Technologies (ICTs), particularly evident in the growth of the Internet, contribute to the set of phenomena collectively labelled globalisation and cut across traditional temporal and spatial boundaries.

The way that these technologies empower less privileged groups is particularly important in recognizing the promise of technology in instrumental contexts. In terms of IR scholarship, James Rosenau's *Turbulence in World Politics* (1990), which claims that the diffusion of IT has enhanced the competence of citizens and undercut the authority of states, is perhaps the most articulate example of this argument. That instrumental power can have negative as well as positive consequences unhinges this purely positive conception of instrumental power, however. It is imperative that analyses of instrumental power continue beyond not just those of states and firms, but also civil society actors, to examine how IT, and the Internet in particular, empowers those groups composing uncivil society. Chapter Three seeks to do this by describing and analyzing how terrorists use the Internet and how this use has enhanced their capability to effect particular outcomes. But because communications technologies cannot be separated from the conditions in which they operate, the present analysis does not stop at use, instead it is particularly concerned with content.

Soft Power

"Modern communication is indeed about technology, but is also about human creativity. Because *something* is communicated to *someone*, an *impact* or an *influence* is likely to be the result, which often depends on how *creatively* the *content* of communications is *deployed*" [italics in original] (Taylor 1997, 5). In the field of IR, this type of argument is most commonly grafted onto the argument for instrumental

power described above. This is because soft power may be conceived of as a type of instrumental power, both of which differ from hard power in the way they achieve their effects. For example, in *Parchment, Printing, and Hypermedia* (1997) Ronald Deibert argues that the diffusion of new digital communications technologies fosters a social epistemology favouring non-territorial institutions and fragmented identities over that of the nation-state. A similar argument is put forward here, namely that the diffusion of the Internet empowers sub-state actors, in this case terrorist groups, in numerous ways, the most important of which is an increased ability to effect their goals through the judicious use of information-based power via their Web sites.

The analytical framework adopted here is based largely upon Joseph Nye's theorisation of soft power. However, other frameworks have been suggested:

- *Cyberpolitik*: In 'Cyberpolitik: The Changing Nature of Power in the Information Age,' David Rothkopf argued that "the *realpolitik* of the new era is *cyberpolitik*, in which actors are no longer just states, and raw power can be countered or fortified by information power" [italics in original] (1998, 326).
- *Noopolitik*: In 1999, John Arquilla and David Ronfeldt produced *The Emergence of Noopolitik* for RAND. The term originates with Pierre Teilhard de Chardin's concept of the 'noosphere' denoting the realm or sphere of ideas. "Noopolitik is an approach to statecraft, to be undertaken as much by non-state as by state actors, that emphasises the role of soft power in expressing ideas, values, norms and ethics through all manner of media" (p.29).
- *Netpolitik*: According to the Aspen Institute, "Netpolitik is a new style of diplomacy that seeks to exploit the powerful capabilities of the Internet to shape politics, culture, values, and personal identity. But unlike *Realpolitik*--which seeks to advance a nation's political interests through amoral coercion--Netpolitik traffics in 'softer' issues such as moral legitimacy, cultural identity, societal values, and public perception" (Bollier 2003, 2).[11]

Within the discipline of IR, the idea of soft power is probably most closely associated with the work of Joseph Nye, which nonetheless shares significant overlaps with the various 'politiks' described above.

---

[11] For a rundown of other relevant power analyses, see Dunn 2002, 33-36.

Nye first put forward his thesis in *Bound to Lead* (1990), but has returned to the idea on several occasions since. In 1996, in an article with William Owens, Nye defined soft power as "the ability to achieve desired outcomes in international affairs through attraction rather than coercion" (Nye and Owens 1996, 21 fn.1). Nye returned to the subject in 1998, in an article jointly authored with Robert Keohane. In that paper Keohane and Nye draw a distinction between free information (such as scientific information, advertising, political propaganda), commercial information (that is information that is sold), and strategic information (information that is useful because it is possessed by one actor, but not others). They argue that the most important political shift has been produced by the dissemination of free information due to the way in which it increases the potential for persuasion internationally. Thus states and NGOs can today much more readily influence the beliefs of foreign publics than in the past. Keohane and Nye argue further that free information, if sufficiently convincing, can alter perceptions of interest and thus change how hard power and strategic information are deployed (Keohane & Nye 1998, 89-92).

In 2002, Nye contributed *The Paradox of American Power* in which he defined soft power as "getting others to want what you want" (p.9). He also reiterated that soft power was concerned with cooption rather than coercion. According to Nye,

> Soft power rests on the ability to set the political agenda in a way that shapes the preferences of others...[P]olitical leaders and thinkers such as Antonio Gramsci have long understood the power that comes from setting the agenda and determining the framework of a debate. The ability to establish preferences tends to be associated with intangible power resources such as an attractive culture, ideology, and institutions. If I can get you to *want* to do what I want, then I do not have to force you to do what you do *not* want to do...Soft power is not merely the same as influence. After all, I can also influence you by threats and rewards. Soft power is also more than persuasion or the ability to move people by argument. It is the ability to entice and attract. And attraction often leads to acquiescence or imitation [italics in original] (Nye 2002, 9; see also Nye 2004, 6).

The Internet is integral to the spread of soft power because the Internet creates a system where power over information is much more widely distributed. Compared with the control exercised over radio, television, and newspapers by broadcasters and editors (see Jacobs 2005, 70), the Internet creates unlimited communication one-to-one, one-to-many, many-to-one, and many-to-many (Nye 2002, 52).

Credibility is an important aspect of soft power. "Communities tend to cluster around credible cue givers, and, in turn, perceived credibility tends to reinforce communities" (Nye 2002, 67). In particular, Internet users tend to frequent Web sites that provide information that they find both interesting and credible. The upshot of this is that politics is transformed into "a contest of competitive credibility" (Nye 2002, 68; see also Bollier 2003, 10 & 29). Governments are forced to compete with each other and with other organisations to increase their own credibility and decrease that of their opponents. Reputation has always been an important consideration in international politics, but the flood of free information and the resultant 'paradox of plenty' obtaining in our 'information society,' has meant that the possession of high levels of credibility is an increasingly important power resource (Nye 2002, 68). Whether those employing an Internet information strategy establish the credibility to get and hold anyone's attention is thus a key political question (2002, 89).

> Plenty of information leads to scarcity--of attention. When people are overwhelmed with the volume of information confronting them, they have difficulty discerning what to focus on. Attention rather than information becomes the scarce resource, and those who can distinguish valuable information from background clutter gain power. Editors and cue givers become more in demand, and this is a source of power for those who can tell us where to focus our attention (Nye 2004, 106).

Clearly established media outlets have an edge here.

Another issue concerns the actual movement of ideas and information, which is virtually instantaneous, but their comprehension and acceptance depend on political and cultural differences (Nye 2002, 90; Bollier 2003, 20-21 & 32-33).

> Global effects are powerful, but they do not enter societies in an unmediated way. On the contrary, they are filtered through domestic political alignments. How global information is downloaded in different countries is a function of domestic politics. In that sense, even in an age of globalisation, all politics remains local (Nye 2002, 100).

Context is a related factor, and also plays a crucial role.

> All power depends on context--who relates to whom under what circumstances--but soft power depends more than hard power upon the existence of willing interpreters and receivers. Moreover, attraction often has a diffuse effect, creating general influence rather than producing an easily observable specific action (Nye 2004, 16).

In other words, soft power resources sometimes take years to produce desired outcomes and are often heavily reliant on external events--which can open windows of opportunity--although a detectable causal link may not, even then, be immediately identifiable.

Terrorism and (Mass) Communication(s)

The traditional focus of mainstream IR theories on states as the most important actors in international relations has tended to alienate terrorism researchers[12]--for whom the actions of sub-state actors are paramount--and obliged them to seek theoretical sustenance elsewhere. This tendency is exacerbated by the disinterest in media and communications evidenced by most IR scholars. Terrorism and communication(s) are inherently linked and there is a large body of work devoted to analysing the

[12] The number of texts explicitly addressing the nexus of terrorism and IR are few. Adrian Guelke's *The Age of Terrorism and the International Political System* (1998) fails to live up to its title; it is a straightforward description of the course of international terrorism, which pays no particular attention to the role of the international political system in structuring same. The only text with which I am familiar that employs IR theory to say something new about terrorism is Ihekwoaba Onwudiwe's *The Globalization of Terrorism* (2001), which uses World Systems Theory to seek to explain the causes of terrorism.

relationship(s) between these two (see Alali & Byrd 1994). Since the advent of the printing press using industrial age technologies in the 19th century, terrorists and extremist movements have employed every available mass communications technology: from Marighela's advice to his comrades to use photocopying machines to produce large numbers of pamphlets and manifestos to Hizbollah's establishment of its Al Manar television station in the early 1990s. For their part, scholars interested in the relationship between terrorism and the media have tended to focus on the role of the news media, particularly newspapers and television and, in fact, terrorism is often portrayed as a strategy characterized by the intentional manipulation of the news media.

Nineteen sixty eight, the year that witnessed the birth of modern international terrorism, was the same year in which the United States launched the first television satellite, heralding the second great revolution in mass communications that directly impacted terrorism (Hoffman 1998 136-137; see also Carruthers 2000, 168; Chaliand 1985, 13-14; Schmid & De Graaf 1982, 16). Much of the explanation of the power of terrorism is said to hinge on how the news media operate: "Journalists are attracted to drama and few political spectacles offer greater dramatic appeal than violence" (Livingston 1994, 2). Terrorists are cognisant of this and use it to their advantage. In his seminal 1975 paper, Brian Michael Jenkins argued "terrorist attacks are often carefully choreographed to attract the attention of the electronic media and the international press" (p.16). The news media have proved unable to ignore events "fashioned specifically for their needs" (Bowyer Bell 1978, 50).[13]

This explains Cherif Bassiouni's contention that

> The correlation between the escalation of global terror-violence in the past twenty years and the innovations in media technology that facilitate rapid dissemination of information is more than mere coincidence. In essence, this correlation illustrates the symbiotic relationship between 'terrorism' and the media: the *terrorists rely on the media to further their terror-inspiring goals,*

[13] In the wake of 9/11, Suman Gupta was moved to question: "What is 'international terrorism' apart from being a media event?" (2002, 15).

> *the media utilises the terrorists' acts as necessary or rewarding news items* [italics in original] (1983, 200).

This alleged symbiosis has been reiterated many times since. In his text *The Anatomy of Terrorism*, David Long had this to say: "The Media's mission to cover the news and the terrorist's ability to 'create' news have led to a symbiotic relationship between the two, one in which the media not only convey the news but help the terrorists create it (1990, 119; see also Carruthers 2000, 168; Hoffman 1998, 142; Szumski 1986, 70; Wardlaw 1982, 76).

Long goes on to employ the metaphor of theatre to explain terrorism; Brian Jenkins has also repeatedly used this metaphor, as has Gabriel Weimann (see Jenkins 1978, 1980, 1981; Weimann 1983; Weimann & Winn 1993). Mark Juergensmeyer drawing on the same metaphor suggests that we view terrorism not as a tactic but as what he calls "performance violence," which has two major components. First, such acts are dramas designed to have an effect on their audiences. In the case of terrorist violence, those who witness it via the news media are part of what occurs. Second, according to Juergensmeyer, the term 'performance' also implies the notion of 'performative,' which refers to certain kinds of speech that are able to perform social functions (i.e. their utterance has a performative impact).

> Like vows recited during marriage rites, certain words not only represent reality but also shape it: they contain a certain power of their own. The same is true of some nonverbal symbolic actions, such as the gunshot that begins a race, the raising of a white flag to show defeat, or acts of terrorism (2000, 124).

The performative and propagandistic nature of terrorist acts is central to many of the available definitions of terrorism. According to Schmid and De Graaf: "Terrorism cannot be understood only in terms of violence. It has to be understood primarily in terms of propaganda. Violence and propaganda have much in common. Violence aims at behaviour modification by coercion. Propaganda aims at the same through persuasion. Terrorism is a combination of the two" (1982, 14).

If the intention of terrorism is to induce terror then it follows, according to numerous analysts, that the ultimate targets are those watching, not those who directly suffer violent attack (Carruthers 2000, 167; Guelke 1998, 191; Hoffman 1998, 131; Nacos 1994, 8; Nacos 2002, 66; Schmid & De Graaf 1982, 15). Terrorism is therefore often viewed as a strategy of 'armed propaganda' calculated to generate maximum response amongst target audiences who will then pressurise states to accede to the terrorists' demands (Stohl 1990, 93). Terrorist violence is thus attributed an agenda-setting function in and of itself. This publicity-seeking soft power component of terrorist violence is probably what Nye was referring to when he wrote "Terrorism depends crucially on soft power for its ultimate victory. It depends on its ability to attract support from the crowd at least as much as its ability to destroy the enemy's will to fight" (Nye 2004, 22). The advent of the Internet has added a significant new tool to the terrorists' soft power arsenal.

Terrorist 'spectaculars' can, there is no doubt, hijack media attention: witness the attack on the Israeli athletes at the Munich Olympics, the hijacking of TWA flight 847, the events of 9/11 and their aftermath. This is not to suggest, however, that the terrorists themselves actually control the news agenda, or can determine the ways in which their behaviour is framed. Even where terrorists gain 'disruptive access' to the media, in their repackaging of events the media still largely rely on official sources and dominant understandings of where legitimacy lies (Dobkin 1992; Paletz & Schmid 1992, 19). In the British case, for example, the tabloid press often exceeded the language of the state in stigmatising the IRA as 'scum,' 'cowardly murderers,' and 'bastards' (Carruthers 2000, 191).

In the past, those characterised as 'terrorists' were rarely accepted by the mass media as legitimate or authoritative sources of news in their own right. Neither were they accepted as reliable commentators upon the political situation that had given rise to the violence: "Certainly, on the few occasions when the BBC or ITV interviewed Republican para-militaries in the 1970s and 1980s, they were emphatically not, as a matter of policy, treated as individuals whose opinions could be accorded the same respect and due consideration as others" (Carruthers 2000, 191). By concentrating almost exclusively on the violent dimension of terrorism, making no attempt to

contextualise its causes, media reports often leave readers, viewers, or listeners mystified as to the motivation of violent acts (Martin 2003, 280). The upshot of this is that many in the media audience take these acts to be simply the senseless, inexplicable behaviour of psychotic fundamentalists or extremist lunatics (Gerbner 1992, 96).

Nobel's invention of dynamite in 1867 was the technological breakthrough that ushered in the era of modern terrorism. The economy of means afforded by the use of dynamite ensured that terrorist bombings proliferated. High levels of illiteracy in nineteenth century Europe imposed serious limitations on conventional text-based propaganda. Conversely, 'propaganda by deed' could show, as the French anarchist Paul Brousse explained lucidly at the time, "the weary and inert masses...that which they were unable to read, teach them socialism in practice, make it visible, tangible, concrete" (Townshend 2002, 55). When the anarchist Albert Parsons was arraigned for his alleged involvement in the Haymarket bombing in Chicago in 1886, he insisted in court that dynamite "made all men equal and therefore free" (Townshend 2002, 25). However, while modern terrorists may still seek to convey a message through their performance violence, they must also employ written and spoken language in an effort to legitimise, rationalise and, ultimately, advertise their actions. With the advent of the Internet, however, they are no longer reliant on intermediaries to interpret their deeds.

Terrorists generally accompany their violent acts with a flurry of threats, communiqués, and manifestos, leading one commentator to assert "the violence of terrorism is positively verbose" (Segaller 1987, 62). Previous to the widespread use of the Internet, the mainstream media were held by many to be complicit in the attainment of the terrorists' objectives. This was because media attention to terrorist violence was held to be considerably more significant than the terrorists' own propaganda: "[the terrorists'] own self-generated posters, manifestos, leaflets, and broadcasts are unlikely, after all, to reach a wide audience and even less likely to convince any other than the already converted" (Carruthers 2000, 170). This may have been true when cultures and politics could be contained within national borders. Historically, leaders and elites were generally the only ones who knew the world first hand. Thus they were relied upon to interpret the motives and behaviours of other leaders and elites, and to formulate responses. Today, that reliance has all but vanished. The Internet presents those with

access and the requisite interest with the opportunity to know and interpret the world for themselves, and therefore decreases the historical control by the media and political elites over individual worldviews (Appadurai 1996).

"In the modern era, the truism that 'information is power' is very clearly understood by the media and governments; it is also understood by terrorists, their audiences, and their adversaries" (Martin 2003, 279). Terrorists now have the ability to tell their own stories via their Web sites. The success, or otherwise, of these Web-based information strategies is explored at length throughout this text. Before proceeding, however, it is important to state that while terrorists may be challenging the power of the news media, the information power wielded by the latter over national and global publics is still very much pre-eminent. Mass-mediated political communication is integral to politics and public life in contemporary society. In fact, "many polities have reached a point where governance, along with a host of related processes such as opinion formation, could not occur in their present forms without various uses of media" (Bennett & Entman 2001, 1).

The idea that "Power is the ability to define and limit the questions to be asked, not just the ability to influence decisions" (Livingston 1994, 7), is touched upon by Nye on a number of occasions (Keohane & Nye 1998, 91), but is never fully worked out. It is nonetheless a key soft-power resource and is illustrated here with a description and analysis of the cyberterrorist threat discourse and its effects as produced by the US media, which is the subject of Chapter Two and also informs the analysis of terrorist's alleged use of steganography contained in Chapter Four. Using Olé Wæver's securitization thesis, which is a well-developed approach designed specifically to analyse security issues, the soft power of the established news media organisations is evidenced. If one facet of soft political power is, therefore, the ability to define the content of the issue agenda in the first place, this is an ability of which established news media are certainly possessed, but one which terrorist groups will find it much more difficult to attain.

However, it is also true that small players now have the opportunity to outsmart huge opponents by using asymmetrical, information-based strategies. And many of these small players have taken up this opportunity with alacrity. On the other hand, and

as already pointed out, acts of violence, especially 'spectacular' acts of political violence, can be utilised to command the media agenda and influence public opinion, thus it is important to underline here the function of political violence as an already existing coercive power resource at the disposal of terrorist groups (as opposed to those 'small players' that are non-violent), which is leveraged by these groups in furtherance of their cyber-strategies. There is certainly no requirement that soft power be employed only by the 'good guys,' however. Further, Nye (2006) has observed more recently that "it is a mistake to rely on hard or soft power alone." The ability to combine them effectively he now terms 'smart power,' the employment of which by terrorist groups is detailed at length in Part III of this text.

Such detailing is absolutely crucial as our understanding of such conflicts and their multifaceted dynamics remain limited at best. If victory, in the information age, is ultimately about "whose story wins" (Arquilla & Ronfeldt 1999, 53; see also Bollier 2003, 32-36), the crucial questions become what messages are sent and received by whom under which circumstances, and how that affects the ability of actors to obtain the outcomes they want (Nye 2004, 44). This project analyses the information power at the disposal of the big and small players, the news media and terrorist groups respectively, in order to illustrate that although the news media remain the big hitters in terms of information power, the Internet as a soft power tool has revolutionized the relationship between terrorism and communication(s).

SCOPE OF STUDY

Case Selection

There is no single universally accepted definition of what constitutes 'terrorism'; it remains an "essentially contested concept" (Gallie 1962). This stumbling block may be overstated, however. Although a widely accepted and usable definition of terrorism remains elusive, there are a number of prominent definitions that share some acceptance. In academic circles the most widely known (accepted?) definition of

terrorism is that put forward by Schmid and Jongman in their *Political Terrorism* (1988). This is certainly the most rigorous definition available, based as it is on the compilation and analysis of 109 separate definitions. Schmid was searching for an objective and, as he saw it, 'scientific' definition of terrorism, which prompted him to come up with the following:

> Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-)clandestine individual, group, or state actors, for idiosyncratic, criminal, or political reasons, whereby--in contrast to assassination--the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organisation), (imperilled) victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought (as quoted in Guelke 1998, 18).

In policy circles, one of the most widely known definitions is that devised by the US State Department and contained in Title 22 of the United States Code, Section 2656f(d) according to which "the term 'terrorism' means premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience."

These definitions are both interesting and relevant on a number of counts, though my comments here will be restricted to their significance for the present project.[14] It is worth noting, for example, that both definitions share a recognition of political violence as having an essentially communicative element. More important, however, is the explicit recognition by Schmid that terrorist attacks may be carried out by or on the part of state actors. The State Department definition is not quite as clear on

[14] For good general analyses of the difficulties associated with defining terrorism, most of which make some reference to the definitions laid out above, see Badey 1998; Bhattia 2005; Dedeoglu 2003; Schmid 2004; Weinberg, Pedahzur, & Hirsch-Hoefler 2004.

this issue: it is debatable to whom the term 'clandestine agents' might apply. Within mainstream terrorism studies adherence to Max Weber's dictum that states have a monopoly of legitimate violence means that many believe that terrorism can by definition only be carried out by non-state groups. Certainly, in practice the US and other governments have, for the most part, restricted themselves to identifying as terrorist only non-state actors.

Others point to the iniquity of such an approach, however, underlining the origins of the term 'terrorism' in the actions of the French state during the Revolution and focusing on the massive numbers of casualties arising out of terroristic violence instituted by states and/or their representatives and targeting domestic and/or foreign populations (Stohl & Lopez 1986a & 1986b). Prominent examples include the so-called 'terror bombing' of German civilians during World War II, Stalin's reign of terror, and Pol Pot's 'killing fields.' For some, of course, the 'real' terrorists are the agencies and satellites of the United States (Chomsky 1991; George 1991; Herman 1982; Herman & Chomsky 1988); a position which, interestingly, is also espoused on the Web sites of many of the terrorist groups explored here. Although such assertions will be returned to later in the text, it was decided that for practical purposes the US State Department definition of terrorism would be employed here with the result that the 'type' of terrorism focused on in this study is exclusively of the sub-national variety.

The bulk of the analysis contained herein is focused on those groups appearing on the US State Department's list of Designated Foreign Terrorist Organisations (FTOs), which is drawn up in accordance with the Title 22 definition laid out above. This concentration on the State Department list grew out of the realisation that, having no desire to start from scratch and draw up a master list of terrorist organisations for use in this project, only to be subjected to endless questions and criticisms regarding the criteria for inclusion on such a list, some reasonably authoritative existing source would have to be employed instead. The US State Department list was chosen because it is well known in the field and has the requisite authority. While there are many people who would contest the labelling of this or that listed group as 'terrorist,' this would almost certainly be true of any such list. And there is reason to believe that, for

many people--and perhaps Westerners in particular--if the United State's government labels an organisation 'terrorist' that this is sufficient evidence of same.

The US government has maintained a list of Foreign Terrorist Organizations since October 1997 when former US Secretary of State Madeline Albright approved the designation of the first thirty groups under the Immigration and Nationality Act (as amended by the Antiterrorism and Effective Death Penalty Act 1996).[15] Of the thirty-six groups that appeared on the list which was current when this research was initiated (see Department of State 2004), fifteen maintained official Web sites. Ten of these sites were available in English and these ten cases--Aleph, Basque Homeland and Liberty (ETA), the New People's Army (NPA), Hamas, Hizbollah, Kahane Chai (Kach), the Kurdish Workers Party (PKK), the Liberation Tigers of Tamil Eelam (LTTE), the Revolutionary Armed Forces of Colombia (FARC), and Sendero Luminoso--were subjected to close scrutiny. The sampling procedure was clearly non-random; it is probably best described as a convenience sample. This is not a drawback, however, as the aim was not to develop a comprehensive map of all terrorists online worldwide, but rather a more limited attempt to isolate and compare some of the key components of terrorist Web sites. Finally, a number of these groups responded on their Web sites to their inclusion on the US list; these responses are described and analysed in Chapter Six.

Limitations

The almost exclusive focus on English-language sites is to be regretted, but cannot be changed. Being familiar with none of the groups' native languages (e.g. Arabic, Japanese, Spanish, Tamil, etc.), and with only limited resources, it was not possible to have the Web sites produced in the groups' native languages translated on a scale large

[15] Groups designated as Foreign Terrorist Organizations by the US Secretary of State, in consultation with the Attorney General and the Secretary of the Treasury, are subject to a number of legal restrictions. It is unlawful, for example, for a person in the United States or subject to the jurisdiction of the United States to provide any kind of financial or material support to such organizations. Both representatives and members of these groups may be denied visas or excluded from the United States, and US financial institutions must block the funds of these groups and their agents and report the blockage to the Office of Foreign Assets Control of the US Department of the Treasury.

enough to provide some balance. Unfortunately, this narrowing of focus results in a major drawback: many of the Web sites maintained by Islamic fundamentalist groups, such as al-Qaeda, Ansar al-Islam, Al-Gama'a al-Islamiyya, Egyptian Islamic Jihad, Lashkar-e-Tayyiba, and others (all of which appear on the US terrorism list), are available only in Arabic. So, although some of these groups are mentioned in this study, it was not possible to subject their Web sites to either a content analysis or close reading.

What are the implications for this study of the omission of these Web sites from the empirical analysis? Firstly, it means that the Web sites of many of the groups that are currently in the public eye were unable to be observed in any great depth and thus all treatment of them within this study is based on the observations and translations of others. More importantly, however, it means that the sites closely analysed herein are those maintained by 'old' as opposed to 'new' terrorist groups.

Terrorism scholars increasingly distinguish between 'old' and 'new' terrorism. The 'new' terrorism is said to have at least seven identifiable characteristics:

1. Religiously inspired terrorism predominates (e.g. Islam, cults, anti-abortion).
2. The 'new' terrorism tends to adopt more networked and less hierarchical organisational structures.
3. This networked form is assisted by the growing use of information and communication technologies (esp. satellite phones, mobile phones, and the Internet).
4. The 'new' terrorists frequently do not claim responsibility for their attacks.
5. Many of these terrorists are amateurs or operate on a part-time basis.
6. The 'new' terrorists operate at all four levels of the international system: domestically, internationally, transnationally, and globally.
7. The 'new' terrorism is more lethal than the 'old' (because its goals are more amorphous) (Chalk 1999; Laqueur 1999; Lesser *et al* 1999; Nacos 2002, 13-14 & 21-24).[16]

[16] For critiques of the concept of 'new' terrorism see Burnett & Whyte 2005, Duyvesteyn 2004, Spencer 2006, Tucker 2001, Zimmermann 2003.

Obviously all of the groups referred to herein, because they are Internet users, fulfil the third requirement above. However, the ten groups that receive the most in-depth analysis in this study do not fulfil many of the other criteria: few of the groups are religiously inspired; many of them retain hierarchical organisational structures; almost all claim responsibility for their attacks; most of these groups' operatives are full-time, professionals; none of these groups could be said to act globally; and although they have been responsible for very large numbers of casualties, this is because they have been engaged in terrorism for long periods--most for decades--and their attacks, although generally small scale, are committed often (see Table I.1).

Table I.1 Characteristics of 'Old' vs. 'New' Terrorism

Characteristic	**'Old' Terrorism**	**'New' Terrorism**
Ideology	Leftist &/or Ethno-Nationalist	Religious (e.g. Islam, cults, anti-abortion)
Organizational Structure	Hierarchical	Networked
Role of Media & Technology	Reliance on 'old' (i.e. mass) media (e.g. Newspapers, radio, terrestrial television)	'New' Media & ICTs (e.g. Internet, satellite television, Mobile and satellite phones)
Claims of Responsibility	Yes	No
Status of Individual Operatives	Professional	Amateur
System Level at Which Operate	National & International	National, International, Transnational, & Global (i.e. all levels)
Threat Level	Relatively Low ('want a lot of people watching, not a lot of people dead')	High ('want a lot of people watching and a lot of people dead')

Web sites maintained by Hamas and Hizbollah are included in the empirical section of the study, and these groups are considered by some to embody the 'new' terrorist mindset (Zanini 1999). Others contest this assertion however and the structure and content of their Web sites appears to place them squarely in the 'old' terrorism category. The upshot of this is that the findings reported here are not generalizable to all terrorist Web sites. In particular--and this issue will be addressed further in the text--Web sites maintained by groups such as al-Qaeda appear to differ dramatically in their

contents and discursive structures to those maintained by 'older' groups, including Hamas and Hizbollah. Nevertheless, I have aimed at generalizations where these could be responsibly undertaken.

DESIGN OF STUDY

Data

Three different kinds of data have been employed in this study. On the one hand, I have collected a large number of texts dealing with terrorism and, to a lesser extent, the Internet. I have also collected and evaluated those few works dealing with both areas. The bibliography reflects this database. The second database--which also finds reflection in the bibliography--consists of media reports, mainly drawn from newspapers and newsmagazines. The third database consists of the terrorist Web sites, particularly direct observation of the ten sites mentioned previously. These were downloaded in their entirety a number of times between January and May 2004.

The analysis provided herein draws upon primary data, but also relies heavily on information drawn from secondary materials. The latter include previously published academic analyses, along with government documents and research institutes' reports. This is accepted practice within the social sciences. However, it will be noticed that media reports, particularly newspaper and newsmagazine articles, are relied upon here to a much greater extent than would 'normally' be the case. There are a number of reasons for this. Firstly, much information about terrorism is classified or very difficult to obtain. However, journalists often elicit useful scraps of information, which then appear in the press. Secondly, this topic is a current one and, as with many similar hot button issues, there are an enormous number of press people working on it. Media reports are oftentimes dismissed as low quality sources because of the time pressures under which journalists work, their limited knowledge of the subjects they cover, their uncritical reliance on poor sources, and the media's commercial nature and political biases. While it is true that journalism is by nature immediate, and lacks the

hindsight incorporated into historical analyses, when studying contemporary phenomena such as terrorism and the Internet, it is suggested that the media and especially the genre of investigative journalism is one of the best sources of knowledge. Journalists all over the globe have managed, through contacts with terrorists and their supporters, to ferret out new information about the intersection of terrorism and the Net. Reports appearing in quality newspapers and newsmagazines are therefore invaluable sources of information, and it is for this reason that scholarly information on terrorism generally flows from external sources toward academic research (Nesser 2004, 16-17; see also Gordon 2001).

Methods

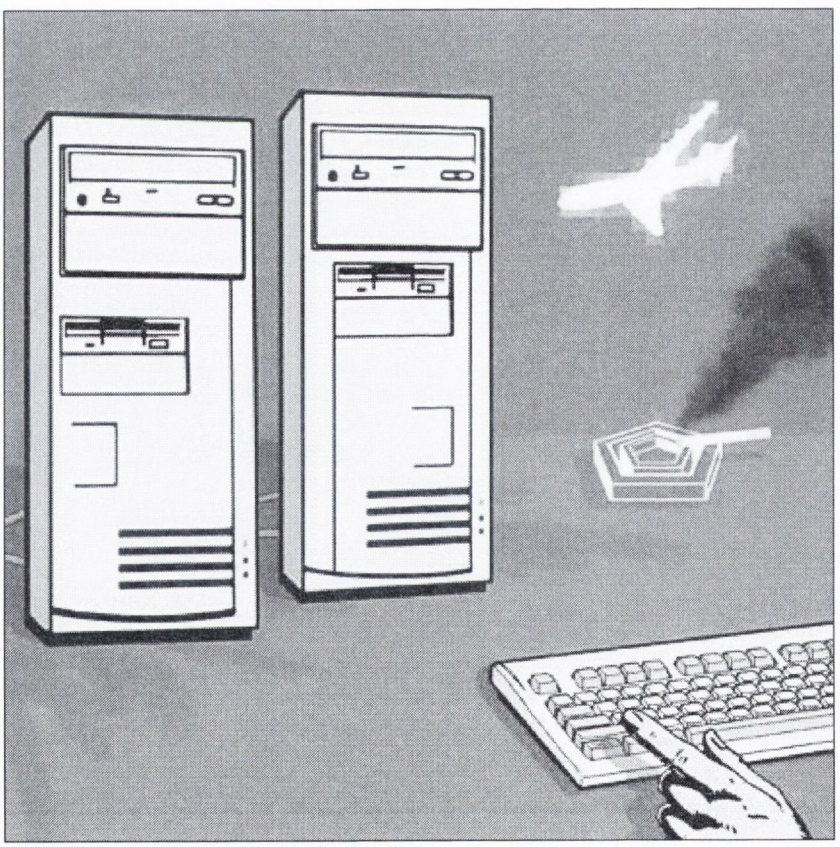
Clearly, no single methodology can claim to capture all of the rich complexity of life on the Internet; an integrated research approach is therefore employed here. The idea behind so-called 'integrated research' is to employ a combination of methods typically used to analyse empirical results or interpretations. The rationale is that the weakness of any single method--quantitative or qualitative--is balanced by the strengths of other methods. In reality, however, the qualitative and quantitative analyses are usually distinct, mutually exclusive components of the research, as is the case here. Parts I and II of the study are composed of a loosely structured description and comparison of texts, and a small amount of material arising out of direct observation. Part III, on the other hand, is more tightly structured and largely composed of observations made directly by the author. Chapter Five draws upon numerical and other data arising out of a content analysis of the ten terrorist Web sites chosen for comparative analysis. A detailed description of this process is contained in the same chapter. Chapter Six relies upon unstructured textual data drawn from the same Web sites and analysed with an interpretative method. Finally, Chapter Seven is a case study of Hizbollah's Internet strategy. The result is an integrated view that is focused on a particular political phenomenon: the intersection of terrorism and the Internet.

STRUCTURE OF STUDY

One can study terrorism and the Internet for three main reasons: to get to know more about terrorism, to get to know more about the Internet, or to get to know more about their relationship. This study is firmly focused on the latter and, to that end, is divided into three major sections. Part I is concerned with cyberterrorism. Chapter One examines existing definitions of cyberterrorism and identifies the problems inherent in many of them, particularly the conflation of hacking and cyberterrorism. Chapter Two is concerned with the media portrayal of the cyberterrorist threat; through an analysis of newspaper and newsmagazine articles, along with a couple of relevant television documentaries and films, it examines the securitization of cyberterrorism. Part II addresses terrorist 'use' of the Net. Chapter Three defines three levels of use, which guide a more detailed analysis of how terrorists are currently employing the Internet to aid in their activities. Shortly after 9/11, various media outlets claimed that the hijackers had hidden their plans for the attacks on pornographic Internet sites using a process called steganography. Chapter Four examines the validity of such claims. Part III explores terrorist Web sites. Chapter Five is composed of a content analysis of ten sites. The aim of the chapter is to determine the functions and effectiveness of terrorist Web sites. In Chapter Six, the same ten sites are the subject of an interpretative analysis in order to draw out their discursive structures and framing mechanisms. The audiences for terrorist sites are also discussed in this chapter. The Web sites maintained by the Lebanese Shi'a group Hizbollah are particularly high profile and effective. Hizbollah's Internet strategy is explored in Chapter Seven. The final chapter presents conclusions and recommendations for future research.

PART I

ON CYBERTERRORISM



1

CYBERTERRORISM: ACADEMIC PERSPECTIVES

Short of electrocuting one's self with the power supply or being so unfortunate as to walk under a falling machine, we cannot, directly, be killed or injured by a computer.

- Mark M. Pollitt (1998)

INTRODUCTION

This chapter seeks to elucidate the origins and development of the concept of cyberterrorism within academe through a description and analysis of the academic literature on the subject with a view to showing how the inconsistencies evidenced within this literature have a.) fuelled the contemporary cyber-angst to be discussed in Chapter Two, and b.) exacerbated the confusion over what precisely constitutes cyberterrorism and what terrorist 'use' of the Net, and how these differ (an issue that will be reprised in Chapter Three). Through surveying the bulk of the literature dealing with terrorism and the Internet, the chapter also serves to illustrate how the idea of cyberterrorism has taken on such mythic proportions that it has (until very recently) usurped literally all other issues that might otherwise have fallen into the terrorism-Internet research nexus.

The academic literature devoted to cyberterrorism is not vast, the term only having been invented in the mid-1980s and sustained academic interest in the concept only having developed since the mid- to late-1990s. In 1998 the Global Organized Crime Project of the Center for Strategic and International Studies in Washington DC published a report entitled *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo*. This was the first major contribution to the field. Just one book-

length academic manuscript dealing with cyberterrorism has yet been published. Prepared for the Defense Intelligence Agency's Office for Counterterrorism Analysis by officers attached to the US Naval Postgraduate School in Monterey, California, *Cyberterror: Prospects and Implications* appeared as a white paper in 1999. There is almost a complete absence of edited volumes dealing specifically with the cyberterrorism issue.[17]

American Behavioral Scientist is the only academic journal to have devoted an entire issue to research on 'cyberterrorism' very broadly defined. The Australia-based *Journal of Information Warfare* included five articles on cyberterrorism in its February 2003 edition (see Table 1.1).[18] Neither of the two major journals in the field of terrorism studies, *Studies in Conflict and Terrorism* and *Terrorism and Political Violence*, have paid particular attention to the issue of cyberterrorism. *Terrorism and Political Violence* has included just four articles dealing with terrorism and the Internet since it published 'Information Terrorism: The Debate'--which included the seminal article 'Information Terrorism: Political Violence in the Information Age'-- back in 1997. *Studies in Conflict and Terrorism* has been the venue for publication of just three articles devoted to analyses of terrorism and the Internet, none of which focused exclusively on the issue of cyberterrorism (see Table 1.2).

Perhaps the greatest single contribution in this field to date has been made by Professor Dorothy Denning, formerly of Georgetown University and currently at the US Naval Postgraduate School. Denning's testimony before the United States Congress's House Armed Services Committee Special Oversight Panel on Terrorism in May 2000 is consistently the top returned item on searching for 'cyberterrorism' in the Google online database, which contains approximately 319,000 items that include

---

[17] *Cyberterrorism and Information Warfare: Threats and Responses* is a volume edited by Yonah Alexander and Michael S. Swetnam, which appeared in 2001. It is a collection of short essays (averaging 4-5 pages) by prominent figures in government, industry, academia and the legal profession, along with a selection of documents treating the issue of cyberterrorism that have emanated from the White House, the US Congress, the FBI, and the US General Accounting Office between 1997 and 2001. Despite its title, however, this collection deals not just with cyberterrorism and information warfare, but also with infrastructure protection, the controversy surrounding encryption technologies, and "bio-cyberterrorism." Given that it is quite a slim volume and that many of the contributions are not original to this publication, it would be misleading to identify this collection as a major contribution to the field.

[18] While including just one article that addresses cyberterrorism *per se*, in 2003 the US journal *Knowledge, Technology, Policy* produced two special issues dealing with the links between technology and terrorism more generally: Tech Terrorism I 16(1) and Tech Terrorism II 16(2).

Table 1.1
Articles on Cyberterrorism Appearing in Journal Special Issues

Title of Article	Author(s)
American Behavioral Scientist *Cyberterrorism in the 21st Century* Vol. 45, No. 6, February 2002	
Persuasive Storytelling by Hate Groups Online	Elissa Lee & Laura Leets
Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America	Brian Levin
Technological Facilitation of Terrorism: Definitional, Legal and Policy Issues	James D. Ballard, Joseph G. Hornik & Douglas McKenzie
Terror in Cyberspace: Terrorists Will Exploit and Widen the Gap Between Governing Structures and the Public	John J. Stanton
Cyberterrorism: Are We Under Siege?	Ayn Embar-Seddon
Journal of Information Warfare **Special Section on Cyberterrorism** Vol. 2, No. 2, February 2003	
Cyberterrorism: An Examination of the Critical Issues	Mark Henych, Stephen J. Homes & Charles Mesloh
Combating Cyberterrorism: Improving Analysis and Accountability	Michael W. David & Kouichi Sakurai
The Law and Cyberterrorism	Matthew Warren & William Hutchinson
Cyberterrorism: The Story So Far	Maura Conway
Is Task Force Smith Rushing to an Electronic Pearl Harbour?	Curtis M. Hellenbrand, Jr.

this term.[19] Her 1999 paper, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,' sponsored by the Nautilus Institute, is the third returned item in the Google line-up (see Figure 1). Denning has also published on the cyberterrorist threat in *Global Dialogue* (2000b), the *Harvard International Review* (2001b), the edited volume *Understanding September 11*, and elsewhere. Her book

[19] Google is the world's leading Internet search engine. It ranks Web pages using software called PageRank. PageRank relies on the uniquely democratic nature of the Web by using its vast link structure as an indicator of an individual page's value. In essence, Google interprets a link from page A to page B as a vote, by page A, for page B. But, Google looks at more than the sheer volume of votes, or links a page receives; it also analyses the page that casts the vote. Votes cast by pages that are themselves "important" weigh more heavily and help to make other pages "important." For more, see http://www.google.com/technology/index.html. Interestingly, the number of hits for 'cyberterrorism' has increased considerably since this research was first begun in 2001 when just 28,100 hits were returned.

Information Warfare and Security (1999) also contains treatment of cyberterrorism. In addition to Denning, others who have contributed seminal papers in this field include Mark Pollitt and Barry Collin. Pollitt's 'Cyberterrorism: Fact or Fancy?' (1998) is second on the Google list, while Collin's paper, 'The Future of Cyberterrorism' (1996) is seventh overall (See Figure 1.1).[20]

The academic literature on cyberterrorism is overwhelmingly the product of US academics and institutions, and is fairly evenly split between those researching in the areas of information technology, computer security, and related subjects and those engaged in the study of terrorism, politics, international relations, and associated disciplines. What many of these authors have in common, whether computer scientists or social scientists, is the tendency to fall into a number of related traps: they construct or employ overly broad and/or inaccurate definitions of cyberterrorism, which results in them confusing hacking and/or hacktivism with cyberterrorism, conflating cyber crime and cyberterrorism, etc. This chapter seeks to untangle these inconsistencies. It begins with an explanation of how and why the concept of cyberterrorism was generated. The remainder of the chapter is concerned with the description and analysis of those articles and papers dealing with the definition of cyberterrorism. These are interrogated with the following questions in mind: What is cyberterrorism? Is it any use of computers or new information technologies by terrorist groups? Is it just the use of those technologies by traditional terrorist groups or those we think of as terrorists? Is there a broader set of persons who might use cyber tools that we would think of as cyberterrorists? Does the definition of terrorism change in the cyber world or can we use the definitions currently employed in the 'real' world?

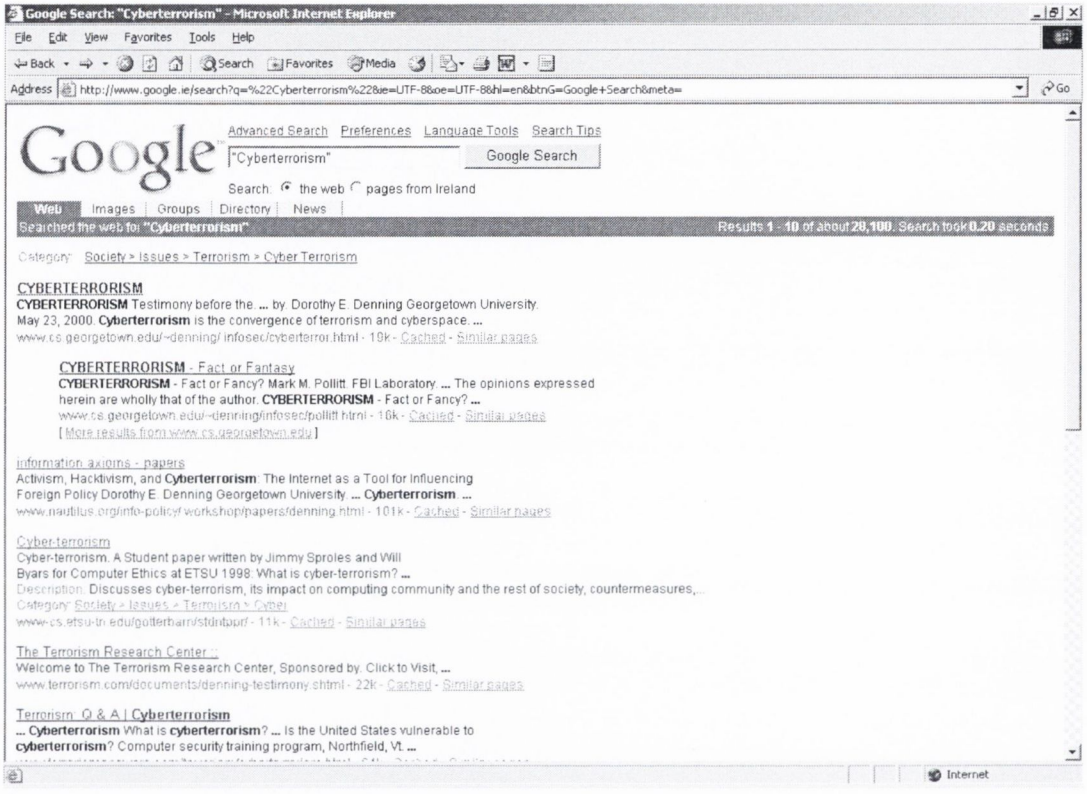
[20] Ashgate publishers have recently produced a volume entitled *Cyberterrorism* (O'Day 2004), which contains twenty-two previously published articles, many of which are referred to herein. Somewhat surprisingly, neither Pollitt's nor Collin's articles are contained in this volume.

Table 1.2
Articles on Terrorism and the Internet Appearing in Major Terrorism Studies Journals, 1997-2003

Title of Article	Volume & Year of Publication	Author(s)
Studies in Conflict and Terrorism		
www.terrorism.com: Terrorism on the Internet	Vol. 25, No. 5 September – October 2002	Yariv Tsfati & Gabriel Weimann
Cyberspace-A New Medium for Communication, Command, and Control by Extremists [Special Issue on Netwar]	Vol. 22, No. 3 July – September 1999	Michael Whine
Middle Eastern Terrorism and Netwar [Special Issue on Netwar]	Vol. 22, No. 3 July – September 1999	Michele Zanini
Terrorism and Political Violence		
From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism	Vol. 12, No. 2 2000	Jerrold M Post, Kevin G Ruby & Eric D Shaw
Affecting Trust: Terrorism, Internet and Offensive Information Warfare	Vol. 12, No. 1 2000	Lorenzo Valeri & Michael Knights
Islamist Organizations on the Internet	Vol. 11, No. 1 1999	Michael Whine
Terrorism on the Internet: Discovering the Unsought [Research Note]	Vol. 9, No. 4 1997	Avishag Gordon
Information Terrorism: Political Violence in the Information Age	Vol. 9, No. 1 1997	Matt G Devost, Brian K Houghton & Neal Allen Pollard
Information Warfare and Strategic Terrorism	Vol. 9, No. 1 1997	Frank J Cilluffo & Curt H Gergely
Response to Cilluffo and Gergely	Vol. 9, No. 1 1997	Matt G Devost, Brian K Houghton & Neal Allen Pollard

Related Articles: *Studies in Conflict and Terrorism*, Rathmell, Andrew. 2003. 'Controlling Computer Network Operations.' 26(3): 215-232; Valeri, Lorenzo. 2000. 'Securing Internet Society: Toward an International Regime for Information Assurance.' 23(2): 129-146; Ronfeldt, David. 1999. 'Netwar Across the Spectrum of Conflict: An Introductory Comment.' 22(3): 189-192; Arquilla, John & David Ronfeldt. 1999. 'The Advent of Netwar: Analytic Background.' 22(3): 193-206; Danitz, Tiffany & Warren P. Strobel. 1999. 'The Internet's Impact on Activism: The Case of Burma.' 22(3): 257-270. *Terrorism and Political Violence*, Bunker, Robert J. 2000. 'Weapons of Mass Disruption and Terrorism.' 12(1); Dartnell, Michael. 1999. 'A Legal Inter-Network for Terrorism: Issues of Globalization, Fragmentation and Legitimacy.' 11(4).

Figure 1.1 Google Screenshot
Results from Search for 'Cyberterrorism'



THE BIRTH OF A CONCEPT

Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term 'cyberterrorism' in the mid-1980s (Collin 1996). The idea of terrorists utilising communications technologies to target critical infrastructure was first mooted more than two decades ago, however. In 1977, Robert Kupperman, then Chief Scientist of the US Arms Control and Disarmament Agency, stated:

> Commercial aircraft, natural gas pipelines, the electric power grid, offshore oil rigs, and computers storing government and corporate records are examples of

> sabotage-prone targets whose destruction would have derivative effects of far higher intensity than their primary losses would suggest. Thirty years ago terrorists could not have obtained extraordinary leverage. Today, however, the foci of communications, production and distribution are relatively small in number and highly vulnerable (as quoted in Devost, Houghton & Pollard 1997, 76).

Such fears crystallised with the advent of the Internet. The opening chapter of *Computers at Risk* (1991), one of the foundation books in the US computer security field, which was commissioned and published by the US National Academy of Sciences, begins as follows:

> We are at risk. America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable--to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb (National Research Council 1991, 7).

Nevertheless, cyberterrorism only became the object of sustained academic analysis in the mid-1990s.

It was the advent of and then the increasing spread of the World Wide Web (WWW) along with the vocal protestations of John Deutch, then Director of the Central Intelligence Agency (CIA), as to the potentiality of the Web as a terrorist tool and/or target that kick-started research into the phenomenon of cyberterrorism in the United States. In 1996, Deutch testified before the Permanent Subcommittee on Investigations of the United States' Senate Governmental Affairs Committee:

> International terrorist groups clearly have the capability to attack the information infrastructure of the United States, even if they use relatively simple means. Since the possibilities for attacks are not difficult to imagine, I am concerned about the potential for such attacks in the future. The methods used could range from such traditional terrorist methods as a vehicle-delivered bomb--directed in this instance against, say, a telephone switching centre or other communications node--to electronic means of attack. The latter methods could rely on paid hackers. The ability to launch an attack, however, are likely to be within the capabilities of a number of terrorist groups, which themselves have increasingly used the Internet and other modern means for their own communications. The groups concerned include such well-known, long-established organizations as the Lebanese Hizballah, as well as nameless and less well-known cells of international terrorists such as those who attacked the World Trade Center (Deutch 1996).[21]

FROM 'REAL WORLD' TERRORISM TO CYBERTERRORISM

It has been pointed out that if you ask 10 people what 'cyberterrorism' is, you will get at least nine different answers (Gordon & Ford 2002, 636). This discrepancy bears more than a grain of truth, as there are a number of stumbling blocks to constructing a clear and concise definition of cyberterrorism. Chief among these are the following:

(a.) A majority of the discussion of cyberterrorism has been conducted in the popular media, where the focus is on ratings and readership figures rather than establishing good operational definitions of new terms.

(b.) The term is subject to chronic misuse and overuse and since 9/11, in particular, has become a buzzword that can mean radically different things to different people.

[21] Deutch's reference is to the first WTC attack masterminded by Ramzi Yousef that occurred on 26 February 1993 and which claimed the lives of six people.

(c.) It has become common when dealing with computers and the Internet to create new words by placing the handle *cyber*, *computer*, or *information* before another word. This may appear to denote a completely new phenomenon, but often it does not and confusion ensues.

(d.) Finally, a major obstacle to creating a definition of cyberterrorism is the lack of an agreed-upon definition of terrorism more generally (Embar-Seddon 2002, 1034; Weimann 2004c, 4).

This does not mean that no acceptable definitions of cyberterrorism have been put forward. On the contrary, there are a number of well thought out definitions of the term available, and these are discussed below.[22] However, no single definition of cyberterrorism is agreed upon by all, in the same way that no single, globally accepted definition of classical political terrorism exists.

Mark M. Pollitt's article 'Cyberterrorism: Fact or Fancy?,' which was published in *Computer Fraud and Security* in 1998, made a significant contribution with regard to the definition of cyberterrorism. Pollitt points out, as many others fail to do, that the concept of cyberterrorism is composed of two elements: cyberspace and terrorism. Cyberspace may be conceived of as "that place in which computer programs function and data moves" (Collin 1996).[23] Terrorism is a less easily defined term. In fact, most scholarly texts devoted to the study of terrorism contain a section, chapter, or chapters devoted to a discussion of how difficult it is to define the term (see Gearty 1991; Guelke 1998; Hoffman 1998; Holms 1994; Schmid & Jongman 1988; Wardlaw 1982). In his paper Pollitt employs the definition of terrorism contained in Title 22 of the United States Code, Section 2656f(d).[24] That statute contains the following definition:

---

[22] One of the most accessible sound bites on what defines cyberterrorism is that it is 'hacking with a body count' (Collin, quoted in Ballard *et al* 2002, 992).

[23] 'Cyberspace' as a term has its origins in science fiction writing. It first appeared in William Gibson's 1984 novel *Neuromancer*, which featured a world called cyberspace, after cyber, the most powerful computer.

[24] Title 22 of the United States Code, Section 2656f(d) may be viewed online at http://www.lii.warwick.ac.uk/uscode/22/2656f.html. This is the definition employed in the US State Department's annual report *Patterns of Global Terrorism*. These are available online at http://www.state.gov.

> The term 'terrorism' means premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience.

Pollitt combines Collin's definition of cyberspace and the US Department of State's definition of terrorism which results in the construction of a narrowly drawn working definition of cyberterrorism as follows:

> Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents (Pollitt 1998, 9).

A similar definition of cyberterrorism has been put forward by Dorothy Denning in numerous articles and interviews, and in her testimony on the subject before the United States Congress's House Armed Services Committee. According to Denning:

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks 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, 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 2001a, 2000a, 2000b, 1999).

Pollitt and Denning are two of only a very small number of authors to recognise and make explicit the way in which the word 'cyberterrorism' is meaningless in and of

itself and that it is only the relational elements of which the word is composed that imbue it with meaning (Gordon & Ford 2002, 637). A majority of authors appear to overlook this connection (see Appendix B)[25]. Numerous authors of articles dealing explicitly with cyberterrorism provide no definition of their object of study at all (see, amongst others, CSIS 1998; Christen, Denney & Maniscalco 2002; Dunnigan 2003; Henych, Holmes & Mesloh 2003; National Communications System 2000; Rattray 2001). Others fall into the trap of either conflating hacking and cyberterrorism or confusing cyber crime with cyberterrorism, while a number of authors fall into both of these traps. Such missteps are less arbitrary than they may first appear however, as two important contributions in this area explicitly allow for such a broadening of the definition of cyberterrorism.

VIRTUAL VIOLENCE?

Traditional terrorism generally involves violence or threats of violence. Although there have been many studies of political violence--and violence more generally--in the physical world, virtual 'violence' is a relatively new phenomenon and thus under-researched. It is accepted, for example, that the destruction of another's computer with a hammer is a violent act. But should destruction of the data contained in that machine, whether by the introduction of a virus or some other technological means, also be considered 'violence'? (Gordon & Ford 2002, 640). This question goes right to the heart of the definition of cyberterrorism.

In a seminal article, which appeared in the journal *Terrorism and Political Violence* in 1997, Devost, Houghton, and Pollard defined 'information terrorism' as "the intentional abuse of a digital information system, network or component toward an end that supports or facilitates a terrorist campaign or action" (1997, 75). They conceive of information terrorism as "the nexus between criminal information system fraud or abuse, and the physical violence of terrorism" (1996, 10; 1997, 76). This allows for attacks that would not necessarily result in violence against humans--

[25] Appendix B contains a list of twelve definitions of cyberterrorism and their sources.

although it might incite fear--to be characterised as terrorist. This is problematic because, although there is no single accepted definition of terrorism, more than eighty percent of scholars agree that the latter has two integral components: the use of force or violence and a political motivation (Guelke 1998, 19; Mates 2001, 2; Schmid & Jongman 1988, 5). Indeed, most domestic laws define classical or political terrorism as requiring violence or the threat to or the taking of human life for political or ideological ends. Devost, Houghton, and Pollard are aware of this, but wish to allow for the inclusion of pure information system abuse (i.e. that does not employ nor result in physical violence) as a possible new facet of terrorism nonetheless (1996, 10).

Nelson *et al*'s reasoning as to why disruption, as opposed to destruction, of information infrastructures ought to fall into the category of cyberterrorism is altogether different:

> Despite claims to the contrary, cyberterrorism has only a limited ability to produce the violent effects associated with traditional terrorist acts. Therefore, to consider malicious activity in cyberspace 'terrorism,' it is necessary to extend existing definitions of terrorism to include the destruction of digital property. The acceptance of property destruction as terrorism allows this malicious activity, when combined with the necessary motivations, to be defined as Cyberterror (1999, 7; see also Littleton 1995).

As we have seen, Mark Pollitt employs the State Department's definition of terrorism to construct his definition of cyberterrorism. Neither the State Department definition, nor Pollitt's, specifically identifies actions taken against property as terrorism. According to Nelson *et al*, however, in practice the Title 22 definition "clearly includes the destruction of property as terrorism when the other conditions for terrorism are satisfied (premeditated, politically motivated, etc.)" (1999, 8). In addition, the FBI definition of terrorism explicitly includes acts against property (as does Dennings, but with the proviso that such destruction be massive). However, Nelson *et al* point out that both the State Department and FBI definitions are subsumed by the Department of Defense definition contained in regulation O-2000.12-H, which includes "malicious

property destruction" as a type of terrorist attack. This regulation also addresses destruction at the level of binary code, which it specifically refers to under the use of special weapons:

> Use of sophisticated computer viruses introduced into computer-controlled systems for banking, information, communications, life support, and manufacturing could result in massive disruption of highly organised, technological societies. Depending on the scope, magnitude, and intensity of such disruptions, the populations of affected societies could demand governmental concessions to those responsible for unleashing viruses. Such a chain of events would be consistent with contemporary definitions of terrorist acts" (as quoted in Nelson *et al* 1999, 9).

Taking the above into account, Nelson *et al* define cyberterrorism as follows: "Cyberterrorism is the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological" (1999, 9). The problem is that this definition massively extends the terrorist remit by removing the requirement for violence resulting in death and/or serious destruction--the 'break things and kill people' (BTKP) rule (Giacomello 2003, 8)--from the definition of terrorism and lowering the threshold to "disruption of digital property."

A related problem is that although Nelson *et al* are quite precise in their categorisations and repeatedly stress that the other conditions necessary for an act to be identified as terrorist must be satisfied (i.e. premeditation, political motivation, etc.) before disruptive cyber attacks may be classified as cyberterrorism, others are less circumspect. Israel's former science minister, Michael Eitan, has deemed "sabotage over the Internet" as cyberterrorism (Sher 2000). According to the Japanese government 'Cyberterrorism' aims at "seriously affecting information systems of private companies and government ministries and agencies by gaining illegal access to their computer networks and destroying data" (FBIS 2002a). A report by the Moscow-based ITAR-TASS news agency states that, in Russia, cyberterrorism is perceived as

"the use of computer technologies for terrorist purposes" (FBIS 2002c). Yael Shahar, Web master at the International Policy Institute for Counter-Terrorism (IPICT), located in Herzliya, Israel, differentiates between a number of different types of what he prefers to call 'information terrorism': 'electronic warfare' occurs when hardware is the target, 'psychological warfare' is the goal of inflammatory content, and it is only 'hacker warfare', according to the ICT Web master, that degenerates into cyberterrorism (Hershman 2000). And Shahar is not alone in painting hackers as potential terrorists.

HACKING VERSUS CYBERTERRORISM

'Hacking' is the term used to describe unauthorised access to or use of a computer system. The term 'hacktivism' is composed of the words 'hacking' and 'activism' and is the handle used to describe politically motivated hacking. 'Cracking' refers to hacking with a criminal intent; the term is composed of the words 'criminal' and 'hacking.' In a majority of academic analyses of cyberterrorism, one or other of these terms--hacking, hacktivism, cracking--or the activities associated with them are equated with or identified as variants of cyberterrorism.

Hackers have many different motives. Many hackers work on gaining entry to systems for the challenge it poses. Others are seeking to educate themselves about systems. Some state that they search for security holes to notify system administrators while others perform intrusions to gain recognition from their peers (Weimann 2004c, 9; see also Taylor 1999, Ch.3). Hacktivists are politically motivated; they use their knowledge of computer systems to engage in disruptive activities on the Internet in the hopes of drawing attention to some political cause. These disruptions take many different forms, from 'denial of service' (DoS) attacks that tie up Web sites and other servers, to posting 'electronic graffiti' on the home pages of government and corporate Web sites, to the theft and publication of private information on the Internet. Crackers hack with the intent of stealing, altering data, or engaging in other malicious damage (see National Communications System 2000, 40). Former or disgruntled employees carry out a significant amount of cracking against businesses.

The term 'hacker' was originally applied to those early pioneers in computer programming who continually reworked and refined programs. This progressed, as Sprague explains, to the "displaying of feats of ingenuity and cleverness, in a productive manner, involving the use of computer systems" (as quoted in Duff & Gardiner 1996, 215). Gaining unauthorised access to computer networks was one way of displaying such expertise. This original generation of hackers developed a code of practice, which has come to be known as the Hacker Ethic (see Nissenbaum 2004, 197-198; Whittaker 2004, 281-283). It was premised on two principles, namely the free sharing of information and a prohibition against harming, altering, or destroying any information that was discovered through this activity. Over the course of time, however,

> a new generation appropriated the word 'hacker' and with help from the press, used it to define itself as password pirates and electronic burglars. With that the public perceptions of hackers changed. Hackers were no longer seen as benign explorers but malicious intruders (as quoted in Chandler 1996, 232).[26]

Hackers as Terrorists

Much has been made of the similarities between profiles of terrorists and those of hackers. Both groups tend to be composed primarily of young, disaffected, males (Soo Hoo, Goodman & Greenberg 1997, 144-145; Rattray 2001, 89). In the case of computer hackers, a distinct psychological discourse branding them the product of a pathological addiction to computers has emerged. In fact, a large number of hackers who have been tried before the criminal courts for their exploits have successfully used mental disturbance as a mitigating factor in their defence, and have received probation with counselling instead of jail time (Chandler 1996, 242-246; Duff & Gardiner 1996, 223; Skibell 2002, 342). These young men have allowed themselves to be portrayed as personal and social failures: computer-dependent individuals, vulnerable to the personal

[26] According to James Adams, in 2001 there were as many as 30,000 Web sites that posted hacker codes (p.99).

and professional frustrations that have been found to underlie anti-social behaviour. Commonly depicted as socially isolated and lacking in communication skills, their alleged anger at authority is said to reduce the likelihood of their dealing with these frustrations directly and constructively. In addition, the flexibility of their ethical systems; lack of loyalty to individuals, institutions, and countries; and lack of empathy for others are said to reduce inhibitions against potentially damaging acts. At the same time, their description as lonely, socially naïve, and egotistical appears to make them vulnerable to manipulation and exploitation (CSIS 1998, 15). Arising out of this discourse, the possibility of terrorist groups employing the services of hackers to carry out attacks has received growing attention.

Some hackers have demonstrated a willingness to sell their skills to outsiders. The most famous example is the Hanover Hackers case. In 1986, a group of hackers in Hanover, Germany, began selling information they obtained through unlawfully accessing the computer systems of various states' departments of Energy and Defence, a number of defence contractors, and the US Space Agency NASA, to the Soviet KGB. Their activities were discovered in 1988, and the group were finally identified and apprehended two years later (see Stoll 1991). A similar incident occurred during the first Gulf War when, between April 1990 and May 1991, a group of Dutch hackers succeeded in accessing US Army, Navy, and Air Force systems. They sought to sell their skills and sensitive information they had obtained via the intrusions to Iraq, but were apprehended by police in the Netherlands (see Brock 1991).

According to Gregory Rattray, a majority of the analyses of hackers-for-hire--what he calls 'cybersurrogates' for terrorism--generally stress the ease (see Rathmell *et al* 1997, 4) and advantages of such outsourcing. These analysts presume that terrorist groups will be able to easily contact hackers-for-hire, while keeping their direct involvement hidden through the use of cut-outs and proxies. The hackers could then be employed to reconnoitre enemy information systems to identify targets and methods of access. Furthermore, it is posited that if hacker groups could be employed to actually commit acts of cyberterrorism, terrorist groups would improve their ability to avoid culpability or blame altogether. Rattray does flag the important risks and disadvantages to such schemes, however. First, seeking to employ hackers to commit acts not just of

disruption, but of significant destruction that may involve killing people would in all likelihood prove considerably more difficult than buying information for the purposes of intelligence gathering. Second, simply contacting, never mind employing, would-be hackers-for-hire would subject terrorists to significant operational security risks. Third, terrorist organisations run the risk of cybersurrogates being turned into double agents by hostile governments. All three scenarios, Rattray admits, weigh heavily against the employment of cybersurrogacy as a strategy (2001, 87-88).

And these are not the only risks faced by terrorists planning to employ IT to carry out attacks. In their 1997 paper 'The IW Threat from Sub-State Groups: An Interdisciplinary Approach' (1997), Andrew Rathmell, Richard Overill, Lorenzo Valeri, and John Gearson point out that should the terrorists themselves lack sufficient computer expertise, there is the likelihood that they would recruit hackers who would prove insufficiently skilled to carry out the planned attacks (see also Giacomello 2004, 401; McKay 1998b). In addition, Rathmell *et al* concur with Rattray that there is a strong case to be made for such hackers changing sides. This is because the primary motive of the hacker-for-hire is financial gain; thus, given sufficient monetary inducement, such individuals are unlikely to object to reporting to other than their original 'employer' (1997, 5). Finally, Giampiero Giacomello raises, but dismisses, the idea of terrorists coercing computer scientists to aid in attacks:

> Clearly, a terrorist organisation would have little moral scruples and could resort to kidnapping computer scientists. Such an alternative, however, would probably be more problematic than it would be worth. First, the kidnapping itself, especially if it is repeated, may alert intelligence services that would increase surveillance of the terrorist group and, possibly, activate a search by law enforcement agencies. Second, it might prove problematic for terrorists to coerce the kidnapped computer scientist to collaborate with them...they would not have a way to guarantee that the person is working for them or simply sending signals to law enforcement officers somewhere (2004, 406-407 fn.61).

David Tucker also has some interesting insights into the hacker-for-hire scenario. Based on a simulation in which he took part, which involved a hacker and members of a number of terrorist organisations,[27] Tucker foresees potential organisational problems for any hacker-terrorist collaboration. He points out that on those occasions when hackers aren't acting alone, they operate in flat, open-ended associations. This is the opposite of many terrorist groups, which are closed hierarchical organisations. There is certainly the potential for clashes between these different organisational styles, developed in different operating environments and derived from different psychological needs. Tucker reports that a former member of ETA who was involved in the simulation repeatedly stressed the need to belong and the strength of attachment to the group as characteristic of members of clandestine organisations (2000, 16). This is not a character trait typically associated with hackers. In fact, in the simulation in which Tucker took part, the hacker and the terrorists involved disagreed over tactics and had difficulty communicating. Eventually, these difficulties became so great that it resulted in a breakdown in the simulation group. The hacker and the terrorists were simply not able to work together. Tucker observes that if the breakdown can be generalised, it would have obvious consequences for hacker-terrorist collaboration (2000, 14-16)

The only likely scenario, given the above, is cyber attacks carried out by terrorists with hacking skills (Embar-Seddon 2002, 1037). This is not impossible. "The current trend towards easier-to-use hacking tools indicates that this hurdle will not be as high in the future as it is today, even as it is significantly lower today than it was two years ago" (Soo Hoo, Goodman & Greenberg 1997, 141). According to William Church, a former US Army Intelligence Officer:

> If you look at the Irish Republican Army, which was probably the closest before they made peace, they were on the verge of it. They had computer-oriented cells. They could have done it. They were already attacking the

[27] Of the terrorists who took part in the conference/simulation that Tucker attended, one was a member of the Palestinian Liberation Organisation (PLO), two were members of Basque Fatherland and Liberty (ETA), one from the Liberation Tigers of Tamil Eelam (LTTE), and one from the Revolutionary Armed Forces of Colombia (FARC).

> infrastructure by placing real or phoney bombs in electric plants, to see if they could turn off the lights in London. But they were still liking the feel of physical weapons, and trusting them (Borland 1998; see also Rathmell 1997, 43-44 & Rathmell *et al* 1997, 7-8).

Terrorists are generally conservative in the adoption of new tools and tactics (Lesser *et al* 1999, 126; Rattray 2001, 89; Stern 1999, 74; Valeri & Knights 2000, 20). Factors influencing the adoption of some new tool or technology include the terrorist group's knowledge and understanding of the tool, and their trust in it. Terrorists generally only put their trust in those tools that they have designed and built themselves, have experimented with, and know from experience will work. It's for this reason that weapons and tools generally proliferate from states to terrorists (Borland 1998).

O'Brien and Nusbaum make an interesting point when they assert that:

> As IT capabilities continue to proliferate, merging advances in computing with telecommunications and related technologies, both the amount of information and the types of information readily available from open sources are greater than ever before. It is, therefore, ironic that, although there has been a great deal of theorising regarding the potential for terrorist groups to use [Information Warfare], there has been little open-source research on this subject. Open source intelligence (OSINT) is definitely a key asset for monitoring potential threats by cyberterrorists, especially as information concerning Western IT programmes, weaknesses and vulnerabilities can easily be drawn from open sources (2000b, 53; see also National Communications System 2000, ES-3, 30 & 44).

O'Brien and Nusbaum suggest that intelligence agencies should utilise online chat forums, hacker Web sites, etc. to gather intelligence on contemporary asymmetric threats. They suggest that most hackers possess a large degree of hubris with regards to their hacking knowledge and abilities as a result of which such "threat-savvy users" could be coaxed into revealing vulnerabilities they had discovered on the Net, as well

as boasting about their own abilities and exploits (2000b, 53). [28] This position is endorsed by Soo Hoo, Goodman, and Greenberg:

> Foreign Bases of operation might be useful for intelligence-gathering activities, but again, they are not required for IT-enabled terrorism...[I]nformation about various systems' vulnerabilities is often shared online between hackers on computer bulletin boards, Web sites, news groups and other forms of electronic association, and this information can be obtained without setting foot in the target country (1997, 143).

It seems unlikely, however, that professional hackers or cyber mercenaries would engage in the cavalier behaviour described above:

> While amateur hackers receive most publicity, the real threat are the professionals or 'cyber mercenaries.' This term refers to highly skilled and trained products of government agencies or corporate intelligence branches that work on the open market.
>
> The Colombian drug cartels hired cyber mercenaries to install and run a sophisticated secure communications system; Amsterdam-based gangs used professional hackers to monitor and disrupt the communications and information systems of police surveillance teams (O'Brien & Nusbaum 2000a, 53; see also Kaihla 2002).

A 2001 article about Russian hackers reported that fifteen to twenty hackers were available for hire in Moscow, and around ten in St. Petersburg.[29] The cost of hiring one

---

[28] David Smith, the man responsible for transmitting the Melissa virus, helped the FBI bring down several major international hackers. Smith used a fake online identity to communicate with and track other hackers from around the world. His intelligence gathering resulted in the arrest of both Jan DeWit, the author of the Anna Kournikova virus, and Simon Vallor, the author of the Gokar virus (see Mendoza 2003).

[29] In the early days of the Web, it was quite difficult for non-English language speakers to find hacking information, because most online material related to hacking was written in English. Increasingly, however, hacking instruction guides and tools are being translated into many different languages and posted to the Net (see Garrison and Grand 2001a, 5-6).

of these individuals was estimated to be as low as $100 per hack. Russian hackers are also increasingly involved in cybercrime, and a number are thought to have been recruited by the Russian intelligence services (Alvey 2001; see also Garrison & Grand 2001a, 5-6). There is no evidence of such mercenaries having carried out attacks under the auspices of known terrorist organisations, however.

The US Department of Justice labelled Kevin Mitnick, probably the world's most famous computer hacker, a "computer terrorist" (Christen, Denney, & Maniscalco 2002, 194). On his arraignment, Mitnick was denied access not only to computers, but also to a phone, "the judge believing that, with a phone and a whistle, Mitnick could set off a nuclear attack" (as quoted in Skibell 2002, 342).[30] Incredulity aside, hackers are unlikely to become terrorists, because their motives are divergent.

> Despite the personality similarities that can be drawn between terrorists and present-day hackers, the fact remains that terrorism is extreme, and far more aberrant than prankish hacking. And, although hackers have demonstrated that they are willing to bring down computer networks to cause functional paralysis and even monetary loss, this propensity for expensive mischief is not conclusive evidence that they would be willing to jeopardise lives or even kill for a cause. One would hope that the threshold for wilfully causing deaths is high enough that the vast majority of, if not all, hackers would refrain from such behaviour (Soo Hoo, Goodman & Greenberg 1997, 145).

[30] Before all-digital switches made it possible for telephone companies to move them out of band, one could actually hear the switching tones used to route long-distance calls. 'Phreaking' is the term used to describe the art and science of cracking the phone network. Early phreakers built devices called `blue boxes' that could reproduce these tones, which could be used to commandeer portions of the phone network. The reference above is to an early phreaker who acquired the sobriquet `Captain Crunch' after he proved that he could generate switching tones with a plastic whistle pulled out of a box of Captain Crunch cereal! But at no time did he seek to set off any nuclear device using this method.

Hacktivism versus Cyberterrorism

Hacktivism[31] grew out of hacker culture, although there was little evidence of sustained political engagement by hackers prior to the mid-1990s (see Harmon 1998 & McKay 1998a, also Thomas 1998). Nineteen ninety-eight is viewed by many as the year in which hacktivism really took off (McKay 1998a; Samuel 2001, 7; Wray 1998).[32] It was in '98 that the US-based Electronic Disturbance Theatre (EDT) first employed it's FloodNet[33] software in an effort to crash various Mexican government Web sites to protest the treatment of indigenous peoples in Chiapas and support the actions of the Zapatista rebels. Over 8,000 people participated in this, one of the first digital sit-ins.[34] It was also in '98 that JF, a young British hacker, accessed about 300 Web sites and replaced their home pages with anti-nuclear text and imagery. At that time, JF's hack was the biggest political hack of its kind. 'Hacktions' also took place in Australia, China, India, Portugal, Sweden, and elsewhere in the same year (see Harmon 1998 & McKay 1998a). Michael Vatis, one-time Director of the FBI's National Infrastructure Protection Center (NIPC), has labelled such acts as cyberterrorism (Vatis 2001, 4).

Tim Jordan identifies two different types of hacktivism: Mass Virtual Direct Action (MVDA) and Individual Virtual Direct Action (IVDA). According to Jordan

> Mass Virtual Direct Action involves the simultaneous use, by many people, of the Internet to create electronic civil disobedience. It is named partly in homage

---

[31] Members of Cult of the Dead Cow (cDc) hacktivist network claim they invented the term in 1998 (see Delio 2004; Ruffin 2004).

[32] Probably the first incidence of hacktivism took place in 1989 when hackers with an anti-nuclear stance released a computer worm into NASA's SPAN network. The worm carried the message "Worms Against Nuclear Killers...Your System has Been Officially WANKed...You talk of times of peace for all, and then prepare for war." At the time, anti-nuclear protesters were seeking to stop the launch of the shuttle that carried the plutonium-fuelled Galileo probe on the first leg of its voyage to Jupiter (Denning 2001b & 1999, 25-26).

[33] FloodNet is a Java applet that, once the launching page has been accessed, repeatedly loads pages from targeted networks. If enough people participate in a FloodNet attack (i.e. access the launching page at a given date and window of time), the targeted computer will be brought to a halt, bombarded by too many commands for it to process. The FloodNet software is available at http://www.thing.net/~rdom/ecd/floodnet.html.

[34] Probably the very first such demonstration was carried out against the French government. On 21December 1995, a group called Strano Network launched a one-hour Net'Strike attack against Web sites operated by various French government agencies. It was reported that as least some of the sites were inaccessible during that time (Denning 2001b).

> to the dominant form of offline protest during the 1990s, non-violent direct action or NVDA (2001, 8).

The FloodNet attack on the Mexican government Web sites described above was an example of MVDA as was the action against the 1999 World Trade Organisation (WTO) conference in Seattle. The organisers of the latter event, the UK-based Electrohippies,[35] estimated that over 450,000 people participated in their sit-in on the WTO Web site. In contrast to MVDA, IVDA utilises classical hacker and/or cracker techniques and actions for attacking computer systems, but employs them for explicitly political purposes. Jordan makes the point that the name IVDA does not mean the actions are necessarily undertaken by those acting alone, but instead that the nature of such actions means that they must be taken by individuals (i.e. they in no way rely on mass action), although they may be taken by many individuals acting in concert (2001, 9). JF's anti-nuclear protest described above was an example of IVDA, which generally consists of infiltration of targeted networks and semiotic attacks (i.e. Web site defacements). The major difference between MVDA and IVDA, apart from those already described, is that MVDA activists rarely seek to hide their identities--through the use of pseudonyms (handles), for example--or cover their tracks. Advocates of MVDA seek to gather together large groups of people to take part in hacktions and thus to inspire public debate and discussion, and maintain that they have a right to protest even if some of those protests are illegal or bordering on same. Many of those using IVDA, on the other hand, act alone and prefer to remain anonymous, which raises issues of representativeness, authenticity, etc (Wray 1998, 7). Finally, there are also differences between those hacktivists who are devoted to the classical hacking ideal of free flow of information and therefore view DoS attacks as wrong in principle and those who view MVDA as both direct non-violent action and important symbolic protest (see Jordan 2001, 11 & Wray 1998, 11).

It is the disruptive nature of hacktions that distinguishes this form of 'direct action Net politics' or 'electronic civil disobedience' from other forms of online political activism. E-mail petitions, political Web sites, discussion lists, and a vast array

[35] http://www.fraw.org.uk/ehippies/index.shtml

of other electronic tools have been widely adopted as recruitment, organising, lobbying, and communicating techniques by social movements and political organisations of all sorts. Stefan Wray has described this type of use of the Internet by political activists as 'Computerised Activism' (1998, 3; see also Denning 1999 & Jordan 2001, 10). The hacktivist movement is different, because it does not view the Internet simply as a channel for communication, but also crucially as a site for action. It is a movement united by its common method as opposed to its common purpose (Samuel 2001, 4).[36] Those political causes that have attracted hacktivist activity range from campaigns against globalisation, restrictions on encryption technology, and political repression in Latin America to abortion, the spread of electronic surveillance techniques, and environmental protection. Hacktivists are, therefore, arrayed across a far wider political spectrum than the techno-libertarian agenda with which committed 'netizens,' including the hacker fraternity, are often identified.

Hacktivists, although they use the Internet as a site for political action, are not cyberterrorists. Their actions do not even minimally comply with the 'break things and kill people' rule. They view themselves as heirs to those who employ the tactics of trespass and blockade in the realm of real-world protest. They are, for the most part, engaged in disruption not destruction. According to Carmin Karasic,[37] the software engineer who designed the FloodNet program: "This isn't cyberterrorism. It's more like conceptual art" (as quoted in Harmon 1998). Ronald Deibert is correct when he states that while Dorothy Denning's definition of cyberterrorism is accurate and illuminating, her portrayal of hacktivism in her article 'Activism, Hacktivism, Cyberterrorism' is misleading. It employs the typical practice of conflating hacking with criminal activity. This is an association that not only ignores the history of hacking, but what many view as the positive potential of hacking as a tool for legitimate citizen activism (Deibert 2003, 19 fn.64; Denning 1999).[38] Denning appears to have adopted a more moderate position in her later work (see Denning 2000a); Michael Vatis, on the other hand,

---

[36] For a discussion of the various tools and tactics commonly employed by hacktivists and accompanying examples, see Denning 1999.

[37] Karasic's home page is at http://custwww.xensei.com/users/carmin/aboutme.htm.

[38] Chris Hables Gray, on the other hand, believes that "this type of electronic civil disobedience is not good politics" (see Gray 2001, 42-44).

continues to view hacktivists as perpetrators of low-level cyberterrorism (see also National Communications System 2000, 31-32).

Cybercrime versus Cyberterrorism

The issue of computer crime was first raised in the 1960s, when it was realised that computers could easily be employed to commit a variety of frauds. Cyber crime is a more recent phenomenon,[39] which was enabled with the introduction of the modem and the ability to remotely access computer systems, the explosion of e-commerce, and the resultant increase in financial transactions taking place via the Internet (Parker 1998). Attempts to conflate cyberterrorism and cyber crime were inevitable. A UN manual on IT-related crime recognises that, even after several years of debate among experts on just what constitutes cyber crime and what cyberterrorism, "there is no internationally recognised definition of those terms" (Mates 2001). Nevertheless, it is clear that while cyberterrorism and cyber crime both employ information technology, their motives and goals do not coincide. Cyber criminals have financial gain as their primary motive.

> [W]e have entered a new age of computer crime. With the rise of E-commerce, the development of the Net as a commercial entity, and unparalleled media attention, the profit motive for computer crime has entered the stratosphere. Recently, Janet Reno[40] dubbed it a 'huge growth industry.' She's probably not wrong. What Reno and other agents of law enforcement are talking about is not hacking, it is crime. It is the kind of crime where people are hurt, money is stolen, fraud is committed, and criminals make money. It is not the grey area of electronic trespass or rearranged Web pages. It is not the world of electronic civil disobedience and 'hacktivism'...In short, it [is] about money, and that makes it a different kind of crime (Thomas 2000).

[39] For a good recent introduction to cybercrime and related issues, see Sieber 2005.
[40] At the time Thomas wrote this paper, Janet Reno was Attorney General of the United States.

Areas in which individual criminals and criminal organisations have proven proficient in cyberspace include: the theft of electronic funds,[41] the theft of credit card information, extortion, and fraud (see National Communications System 2000, 36-39). It is estimated that worldwide cybercrime cost $1.6 trillion in 2001 (Whittaker 2004, 233).

Secondary to financial gain is the acquisition of information that can underpin the operations associated with making money. It is for this reason that transnational crime syndicates are probably more interested in maintaining a functioning Internet than attacking Internet infrastructures. In other words, organised crime groups view the Net as a tool, not a target. This is because many such organisations employ the Internet--and the public telecommunications network generally--as a vehicle for intelligence gathering, fraud, extortion, and theft (CSIS 1998, 3). For example, as banks and other financial institutions increasingly rely on the Internet for their daily operations, they become more attractive targets for criminal activity. Having said that, criminal groups, such as drug traffickers, may seek to penetrate information systems to disrupt law enforcement operations or collect information on operations planned against them (National Communications System 2000, 35).

None of this means that the proceeds of cyber crime may not be used to support terrorism, but only that were this to occur it ought not to be classed as cyberterrorism *per se*. There are differences of opinion on this issue also, however.

COMPUTER AS TARGET VERSUS COMPUTER AS TOOL

In a probing article simply entitled 'Cyberterrorism?' (2002), Sarah Gordon and Richard Ford draw the reader's attention to the differences between what they call "traditional cyberterrorism" and "pure cyberterrorism." According to Gordon and Ford, traditional cyberterrorism features computers as the target or the tool of attack while pure cyberterrorism is more restricted as it is limited to attacks against computers,

[41] In China, a convicted hacker, one Shi Biao, was executed in 1993 for the theft of £122,000 from the Agricultural Bank of China (Whittaker 2004, 238).

networks, and information (2002, 636-637 & 641). The author's point out that both the media and the general public favour the definition encapsulated in the term "traditional cyberterrorism" while the focus in academia is on "pure cyberterrorism." So while conceding Denning's--and thence Pollitt's--definition is "solid," Gordon and Ford find the definition less than comprehensive:

> First, [Denning] points out that this definition is usually limited to issues where the attack is against 'computers, networks, and the information stored therein,' which we would argue is 'pure cyberterrorism.' Indeed, we believe that the true impact of her opening statement ('the convergence of terrorism and cyberspace') is realised not only when the attack is launched against computers, but when many of the other factors and abilities of the virtual world are leveraged by the terrorist in order to complete his mission, whatever that may be. Thus, only one aspect of this convergence is generally considered in any discussion of cyberterrorism-- an oversight that could be costly. Second, it is very different from the definition that appears to be operationally held by the media and the public at large (2002, 637).

A number of authors agree with Gordon and Ford that cyberterrorism should encompass any act of terrorism that utilises "information systems or computer technology as either a *weapon* or a *target*" (Mates 2001, 6). Nelson *et al* include physical attacks upon information infrastructures in this category (1999, 9-10). However, the same authors disagree with Gordon and Ford on the issue of leveraging the abilities of the virtual world to complete a terrorist mission. Gordon and Ford seek to place the latter activity squarely in the category of cyberterrorism whereas Nelson *et al* emphatically reject this approach. They identify two new categories into which this type of activity may be placed: 'cyberterror support' and terrorist 'use' of the Net. "Cyberterror support is the unlawful use of information systems by terrorists which is not intended, by itself, to have a coercive effect on a target audience. Cyberterror support augments or enhances other terrorist acts." On the other hand, "terrorist use of information technology in their support activities does not qualify as cyberterrorism"

(1999, 10; see also Garrison & Grand 2001b, 2). For now it is sufficient to flag these distinctions, which will be returned to in Chapter Three.

CONCLUSION

Although the body of academic literature devoted to cyberterrorism is small, large amounts of confusion and disagreement exist within it. Despite the routine employment of the term 'cyberterrorism' by academics--along with journalists, opinion leaders, and legislators--to refer to instances of low-level computer abuse, this does not mean, as has been suggested, that the term is "for all practical purposes, useless for researchers" (Giacomello 2003, 5). The academic research and writing produced in this area certainly needs more rigour, particularly with regard to definition. As it stands, there is very little agreement among scholars on what precisely constitutes cyberterrorism: the question 'What is Cyberterrorism?' is therefore particularly difficult to answer. But throwing the baby out with the bathwater is totally unwarranted. It is suggested that, in the future, researchers concern themselves with separating the hype surrounding the issue of cyberterrorism from the more prosaic reality.

This is more difficult than it may at first appear, however. Ralf Bendrath has identified three major stumbling blocks (2003, 51-52). First, this debate is not simply about predicting the future, but is also about how to prepare for it (i.e. the future) in the present. The problem is that those involved in the debate cannot draw on either history or experience to bolster their positions, as a major cyberterrorist incident has never yet occurred. For this reason different scenarios or stories about the possible course of future events are providing the grounds on which decisions must be made. The upshot of this is that the various actors (i.e. government and opposition, the computer security industry, the media-entertainment complex, scholars, and others) with their various, and often times divergent, interests are competing with each other by means of their versions of the future, which are particularly subject to political exploitation and instrumentation (Deibert 2002, 118).

A second, and related, problem is the nature of the space in which a cyberterrorist attack would occur:

> In the physical landscape of the real world, any action has its constraints in the laws of nature...Cyberspace, in contrast, is a landscape where every action is possible only because the technical systems provide an artificial environment that is built to allow it. The means of attack therefore change from system to system, from network to network. This makes threat estimation and attack recognition much more difficult tasks (Bendrath 2003, 51).

Bendrath's final point relates to the highly technical nature of the new threat and the constraints this places on social scientists and their ability to estimate the magnitude of that threat. His solution is for social scientists to draw conclusions by looking at how the threat is perceived: "The way a problem is framed normally determines or at least limits the possible solutions for it" (2003, 52). The next chapter seeks to do this by describing and analysing the cyberterrorist threat image amplified in the US media.

2

THE MEDIA AND CYBERTERRORISM: A STUDY IN THE CONSTRUCTION OF 'REALITY'

"[Cyberterrorism] isn't so much a threat to national security as a threat to civilisation"

- Paul Vixie, *Newsweek* (2003)[42]

"More cyberterroristic than the cyberterrorists themselves, the cyberterror-inducing media have the information world at their mercy"

- François Debrix (2001)

INTRODUCTION

Why is it that some threats take on huge political salience and others do not? Cyberterrorism is thus far noticeable by its absence. Nonetheless, a central element of the post 9/11 'War on Terror' and related efforts to beef-up US 'homeland security' has been an almost paranoid emphasis on the potentially catastrophic threats posed by cyberterrorism. A vast array of political, military, business, academic, and media commentators have appeared on television and been quoted in newspapers predicting deadly attacks by terrorists on the computerised infrastructures that now constitute the structures of everyday American urban life. This depiction of computerised systems as

[42] Vixie was, at that time, president of the Internet Software Consortium (an industry group). See Adams & Guterl, 2003.

the Achilles heel of advanced industrial societies was further fuelled by the use of everyday urban infrastructures as weapons of mass murder on 9/11 itself (Graham 2004).

Following the collapse of the USSR, a number of events occurred that highlighted the growing influence of information technology in the realms of both national and international security. Examples include the high level of IT capability manifested by US troops in the first Gulf War (1990-1991), the increasingly global nature of media coverage as demonstrated in the Somali (1993) and Balkan conflicts (1992-1998), and increased systems failures resulting from the activities of hackers. These and other events highlighted states', particularly the United States', growing dependence on information technology thus ushering in fears of a radically new security threat: the possibility of information systems serving as both a weapon and a tool of attack. This cyber threat became the object of increased attention from the US federal government in the 1990s. A particular concern was that enemies of the United States, unable to emerge successfully from an encounter with American forces on the conventional battlefield, would pursue alternative approaches to inflicting damage on the sole remaining superpower (Pollard 2004, 43). The events of 9/11 were therefore doubly shocking for many US government officials: not only were the attacks appalling in themselves, but the conventional nature of the attacks was also completely unexpected.

Far from reducing the fear of cyber attack however, for many the 9/11 attacks only served to increase the credibility of the cyber threat.

According to a study released in June 2001, seventy-five percent of Internet users worldwide now believe in cyberterrorism. The survey conducted in nineteen major cities around the world found that forty-five percent of respondents agreed completely that "computer terrorism will be a growing problem," while thirty-five percent of respondents agreed somewhat with the same statement (Poulsen 2001). In a July 2002 survey conducted by the American Business Software Alliance, eighty-two percent of information technology professionals were said to believe that US businesses were ill equipped to deal with cyberterrorism (King 2002). A more recent survey carried out by *Federal Computer Week* and the Pew Internet and American Life Project

in 2003 found that about half of Americans fear terrorists will launch cyberattacks on those critical infrastructures that operate the banking, electrical, transportation, and water systems, disrupting everyday life and crippling economic activity (Pew Internet and American Life Project 2003).[43] What these statistics show is that cyberterror is in the zeitgeist. What this chapter seeks to do is to show how it took root there.

THEORETICAL UNDERPINNINGS: THREAT POLITICS

Traditional security studies views threat images as relatively unproblematic and assumes that real threats--out in the world--are directly reflected in security policy. In the last decade or so, practitioners of so-called 'new security' approaches have argued, on the contrary, that there exists no natural or self-evident conformity between the substance of a threat image and whether it has an impact on the political agenda (see Buzan 1991, Buzan *et al* 1998). The analytical approach adopted here is informed by the framework laid out by Barry Buzan, Ole Wæver and others, who are collectively known as the Copenhagen School,[44] which is closely identified with 'new' security studies.

The Copenhagen School approach to security may be described as broadly constructivist. One of the major issues addressed by Buzan *et al* in their seminal text *Security: A New Framework for Analysis* (1998) is "what quality makes something a security issue in international relations?" (Buzan, Wæver, & de Wilde 1998, 21). The answer, they say, can be found in the traditional military-political understanding of security. According to Buzan *et al*, things are generally designated as security issues because it can be argued that these things are more important than others and should therefore be given absolute priority. The evidence for such prioritising often takes the form of a statement such as "If we do not tackle this problem, everything else will be irrelevant (because we will not be here or we will not be free to deal with it in our own

[43] This survey was conducted before the blackout across the northern United States and eastern Canada on 14 August, 2003.

[44] Many of the figures associated with this approach were employed at the Copenhagen Peace Research Institute (COPRI) before it was closed on 31 December 2002.

way)" (Buzan *et al* 1998, 24 & 36). In this way, the securitizing actor claims the right to break the normal political rules of the game. It is for this reason that constructivists view 'security' as a self-referential practice, because it is in this practice that issues become 'security issues' (i.e. not necessarily because a real existential threat exists, but because X issue is presented as such a threat).[45] "Thus the exact *definition* and *criteria* of securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects" [italics in original] (Buzan *et al* 1998, 25). Cyberterrorism, it is argued here, has taken on such saliency. As a terrorism subset, it sits atop the US political agenda.[46]

The formation of agendas depends, unsurprisingly, on power and politics. But while this may appear obvious, it is actually perceived as controversial by many in the community of traditional security studies researchers. Olav Knudsen has even suggested that research that investigates how the security policy agenda is set diverts attention away from 'real' problems (2001, 359-61). Security policy researchers rarely have a problem identifying the 'real' threats, but oftentimes these threat images receive very little substantive political attention. The inability of these researchers to get environmental problems taken seriously as a security issue is a case in point. There is thus a very real need for research and analysis which explores why different actors often perceive the same issue in radically different ways, as well as why certain threat images take on political salience and others do not (Eriksson & Noreen 2002, 1).

According to researchers working at the Scandinavian Threat Politics project,[47] to understand the politics of threat one must be concerned with how threat images are created and become part of the political agenda. In the opinion of the Scandinavian researchers two types of studies need to be undertaken in order to understand the politics of threat:

---

[45] For an analysis of the exaggeration of the threat posed by the Soviet Union to the US during the Cold War and a comparison with the current levels of alarm over the threat posed by international terrorism, see Mueller 2005.

[46] A number of authors have recently suggested adopting a constructivist approach to analysing the cyberterror threat, see Dunn 2004; Eriksson & Giacomello 2004. For a brief (but friendly) critique of this approach see Deibert 2002, 116-117.

[47] The Threat Politics project is a research project funded by the Swedish Emergency Management Agency in conjunction with the Swedish Institute of International Affairs, Uppsala University, and Södertörns University College. The project Web site is available in English and Swedish and may be accessed online at http://www.threat-politics.net/.

1. Studies that focus on specific substantive issues that, at different times, are either included or dropped from the agenda as threat images.
2. Studies that take as their starting point specific political arenas and how threat images are emphasised or downplayed within them.

The present chapter seeks to combine both types of study. The Copenhagen approach to security distinguishes among three types of units: referent objects, securitizing actors, and functional actors. 'Referent objects' are those things that are seen to be existentially threatened and that have a legitimate claim to survival. Those actors who securitize issues by declaring something (the referent object) existentially threatened are known as 'securitizing actors,' while those actors who affect the dynamics of a sector without being the referent object or the actor calling for security on behalf of the referent object, but who nonetheless significantly influence decisions in the field of security are designated 'functional actors' (Buzan et al 1998, 36). In the present analysis, the American state--conceived of as the nexus between US territory, government and society--is the referent object: the thing that is claimed to be threatened by cyberterrorism.[48] The US government is the securitizing actor and the American media establishment is the major functional actor. The goal of this chapter is to present a unified analysis of the politics of the cyberterrorist threat by focusing on cyberterrorism as a specific substantive threat image and tracing how it has been portrayed in the specific political arena occupied by the American media.

Threat Framing

The process of formulating problems, finding scapegoats, and coming up with solutions has been identified in different contexts as 'speech acts,' 'problem definition,' and 'framing.' The problem is to depict an issue--something that is perceived as threatening, for example--in such a way that others listen and are convinced (or are at

[48] For a thorough analysis of 'National security and the nature of the state,' see Buzan 1991, Ch. 2; Buzan 1995.

least persuaded to pay attention to the issue). The term framing is employed here; for Robert Entman,

> [t]o frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described (1993, 52).

Framing is a verbal expression of thought. Individuals perceive and interpret events; events are never simply given. Perception and interpretation are most often followed by verbalisation: that is to say, actors give verbal form to their conceptions of threats and risks. The movement is thus from thought to speech and from the individual to the collective level of analysis. Generally, the choice of "speech costume" has a major impact on whether an issue makes it onto the political agenda (Eriksson & Noreen 2002, 10).

One of the most significant forms of 'threat framing' or 'costuming' is to identify something as a 'security' threat. In the literature, this behaviour has come to be called 'securitization.' Security policy is often regarded as having precedence over all other politics, while national security policy is invariably viewed as the foundation of all security policy: as already pointed out, no other societal goals may be achieved unless society's existence may be guaranteed (Wæver 1995, 49). The upshot of this is that security policy and associated threat images are extremely loaded issues (Deibert 2002, 115). Exploitation of the politically loaded concepts of security and threat may, therefore, make it easier to insert an issue onto the political agenda.

Threats and vulnerabilities that are securitized in this manner must meet certain criteria that distinguish them from the normal run of the merely political. What are these criteria?

> [S]ecurity is about survival. It is when an issue is presented as posing an existential threat to a designated referent object...The special nature of security threats justifies the use of extraordinary measures to handle them.

> The invocation of security has been the key to legitimising the use of force, but more generally it has opened the way for the state to mobilise, or to take special powers, to handle existential threats. Traditionally by saying 'security,' a state representative declares an emergency condition, thus claiming a right to use whatever means are necessary to block a threatening development (Buzan, Wæver, & de Wilde 1998, 21; see also Wæver 1995).

This is what, in language theory, is called a speech act. It is the utterance itself that is the act; by saying the words, something is done. A successful securitizing speech act is a combination of language and society: that is of both intrinsic features of speech and the collectivity that authorises and recognises that speech.

A securitizing speech act has both internal and external conditions. The most important internal conditions are to follow the security form, the grammar of security, and construct a plot that includes existential threat, point of no return, and a possible way out. There are two main conditions attaching to the external conditions of a speech act. The first is the social capital of the speaker (i.e. the securitizing or functional actor) who must hold a position of authority. The second condition has to do with threat: it is more likely that one can conjure a security threat if certain objects can be referred to that are generally held to be threatening. These objects do not, in themselves, necessarily result in securitization, but instead act as facilitating conditions (Buzan *et al* 1998, 33). Importantly, an issue is securitized only if and when the target audience accepts it as such.[49]

Agenda Setting

"There is no tradition of International Relations scholarship that takes communications *per se* as its central focus" (Deibert 1997, 4). There is certainly no distinct 'school' or

[49] A discourse that seeks to present something as an existential threat, but without evidence of audience acceptance is known as a 'securitizing move' (Buzan *et al* 1998, 25). For details of failed securitization projects (undertaken on behalf of the state), see Marsh 1995.

'paradigm' of communications within the field.[50] Having said that, a significant amount of the work that mixes International Relations theory and communications is focused on the facilitative use of media and communications technologies in furtherance of political goals. A considerable body of work takes up issues related to propaganda as an instrument of foreign policy, for example. Harold Lasswell was particularly concerned in his work with the way states manipulate messages to garner international support and/or undermine foes (see Lasswell 1971 [1927]; Lasswell & Lerner 1965; Lasswell, Lerner & Speier 1980) while, more recently, Philip Taylor has contributed a number of monographs that speak to the same issues (see Taylor 1992, 1995, 1997,1999). Other relevant studies have focused on media representations or the 'framing' of international events, as mentioned above (see Dorman & Farhang 1987; Entman 1991; Seib 1997).

A related area of study is that surrounding issues of control. The agenda-setting model of the media posits that the mass media have an influence on what the public recognises as important issues, and the theory has been supported by a wealth of empirical studies. There are two main approaches in this area: one that focuses on elites and the other pluralist-based. The elite approach focuses on formal political power and highly-placed decision-makers, the second approach broadens the concept of the 'political agenda' to include such factors as the agenda(s) of the media. As already indicated, it is the role of the latter that is explored here, although it must be emphasised that issues that receive attention in the media, but not the attention of decision-makers will not appear on the political agenda. Nevertheless, the media remains a central player because it is able, among other things, to influence public opinion: an issue that achieves salience in societal debate may be expected to make its mark on the political agenda (Eriksson & Noreen 2002, 4).

The contention here is that the American news media act as the main source of political information for mass publics--both within the United States, but increasingly, due to the spread of satellite television and the Internet, also abroad--and as the primary 'transmission belt' communicating public fears and desires to political elites and

[50] There are few IR theorists of communications at all; the important exception being Karl Deutch. Deutch's work focused on communication flows and the importance of communicative interaction in the explanation of political behaviour. See Deibert (1997, 19-21) for a brief rundown of Deutch's contribution to IR.

government actors. The "media establishment" has been described as a "major power broker" which exerts "unprecedented power over the dissemination of news" (West 2001, viii). In fact, Timothy Cook identifies the news media as a political institution in itself because it "engages, along with other political institutions, in the authoritative allocation of values in American society" (1998, 85-86). Not only does it act as an intermediary between the mass public and the government, but also within and among branches of government. Gronke and Cook go even further when they posit that "in a system of declining rates of affiliation with political parties and falling levels of participation in community, civic, and other political organisations, it is not unreasonable to suggest that the news media is *the* dominant intermediary organisation in American democracy" (2002, 1). As a functional actor, therefore, the media is unparalleled; it is, in Nye's terms, a major--perhaps *the* major--purveyor of soft power in our society.

Methodology

Buzan *et al* advise that the way to study securitization is to study discourse and political constellations (1998):

> [A] threat image first appears in the mind, whether it is a reaction to something real or merely a work of the imagination. Human cognitive and memory functions play a role in this context. One's conception of a threat may, of course, stop with the thought. In such case, the threat image becomes neither an object for framing nor political action. In other words, it is impossible for a threat image to gain salience if it has not been given some sort of form for decision-makers. It is not sufficient merely to think about threats. They must also be talked about or written about in order to draw attention to them. The way in which this is done has an impact on their success; that is, their effects on the agenda (Eriksson & Noreen 2002, 18).

Threat is first constructed in the individual consciousness; individuals view something as a threat. The next step is for actors in the threatened society to give form to the threat by talking or writing about it in public fora. That is, the threat assumes the trappings of language and is transformed into a topic of public debate through the dissemination of newspaper stories, magazine articles, television documentaries, and eventually mass-market books and movies. Opinion polls are an important source for determining public responses to the threat image as amplified in the latter.[51] Should public debate reach a high enough level of saliency, the threat will become part of the political agenda and an object of political consideration and action. Once the threat becomes the object of government reports and legislation, the threat has effectively been securitized.

FEAR OF TECHNOLOGY, FEAR OF TERRORISM

Frequently, it is our basic perceptions that determine how we conceive of an issue, which is filtered through our prism of preconceived notions. A large amount of social psychological research has found that the uncertain and the unknown generally produce fear and anxiety. This is the psychological basis of the classic ghost story: the fear is greatest when you suspect something, but you're not certain what it is (Eriksson & Noreen 2002, 8). The term cyberterrorism unites two significant modern fears: fear of technology and fear of terrorism. Both of these fears are evidenced in this quote from Walter Laqueur, one of the most well known figures in terrorism studies: "The electronic age has now made cyberterrorism possible. A onetime mainstay of science fiction, the doomsday machine, looms as a real danger. The conjunction of technology and terrorism make for an uncertain and frightening future" (Laqueur 1999, 254). As significant uncertainties or unknowns, therefore both technology and terrorism are perceived as more ominous than known threats (Embar-Seddon 2002, 1034).

[51] However, for some of the pitfalls in relying on opinion polls, see Bennett & Entman 2001, 5-6; Entman 2000, 19-23.

Fear of terrorism,[52] conceived of as random, incomprehensible, and uncontrollable violence, may strike one as relatively 'normal,' fear of technology as perhaps less so. However, as Mark Pollitt points out, for those unfamiliar with high technology, it is arcane, complex, abstract and indirect in its impact on individuals. And "because computers do things that used to be done by humans, there is a natural fear related to a loss of control. People believe that technology has the ability to become the master, and humanity the servant." Couple this relatively new fear with the age-old fears associated with apparently random violence and the result is a truly heightened state of alarm. Pollitt contends that the media have further upped the ante by hyping the concept of convergence:[53]

> According to the press, one is led to believe that all of the functions controlled by individual computers will all converge into a singular system. Further support for this scenario is the increase in 'connectivity.' Many people conclude that the entire world will soon be controlled by a single computer system (1991, 8).

The convergence represented by the reliance on uninterrupted systems of electrically powered computer networks to support all other infrastructures makes attacks on the electrical power grid particularly fearful. The result is that many people now feel themselves "hostages to electricity" (as quoted in Graham 2004, 8). These feelings are reinforced by the prevalence of so-called 'shut-down-the-power-grid scenarios' in the mass media.[54] Two of the most well known scenarios[55] are those designed by John

---

[52] See Homer-Dixon (2002, 57-58) for an interesting take on the fears exploited by the 9/11 attackers and how the "neural network" compounded these.

[53] The Oxford English Dictionary (2003) defines convergence as "The process by which originally distinct technologies may become more compatible or integrated as they develop, so that an increasing number of devices (esp. in electronics, computing, and telecommunications) are multifunctional and interoperable."

[54] A number of academic analyses of cyberterrorism also include such scenarios, see Collin 1998; Devost, Houghton, and Pollard 1996 & 1997. Thomas Homer-Dixon, writing in *Foreign Policy*, introduces his comments with a brief shut-down-the-power-grid scenario, although his is not cyber-based, but involves only physical attacks (2002, 52-53).

[55] Postmodernists prefer the term 'simulations' (see Baudrillard 1983).

Arquilla of the Naval Postgraduate School in Monterey, California[56] and technology journalist Dan Verton.

Shut-Down-the-Power-Grid Scenarios

John Arquilla's 'The Great Cyberwar of 2002' first appeared in *Wired* magazine in February 1998. In the scenario "Liddy Dole faces the biggest crisis of her presidency: the first global cyberwar, where the enemy is invisible, the battles virtual, and the casualties all too real" (Arquilla 1998). The electric grid is one of the first infrastructures to be targeted by the attackers:

> Power outage!....The latest TV news reports indicate that three 500-kilovolt transmission lines extending from hydroelectric dams along the West Coast [*sic*] were knocked out, interrupting electricity and phone service throughout California and Oregon. The executive director of the Western Systems Coordinating Council reported that the problem has cascaded throughout the grid, knocking power plants offline in Rock Springs, Wyoming, in Hells Canyon, Idaho, and in Brush, Colorado, causing outages in several western US states. Reports by noon or so also indicate that no signs of sabotage have been detected. That means no physical destruction of the system (Arquilla 1998).

The body count escalates rapidly caused by everything from traffic accidents to the explosion of a chemical plant. Who are the perpetrators of this mayhem, according to Arquilla's scenario? A group known as the Dove of Jihad claim responsibility, but this is quickly dismissed; China and Russia are then held responsible, followed by a shadowy figure operating out of Afghanistan(!). Eventually, however, the perpetrators

[56] Together with his collaborator David Ronfeldt of Rand, Arquilla is a prominent analyst of information warfare. Arquilla and Ronfeldt are perhaps best known for their development of the concepts of Netwar and cyberwar. Many of their publications are available for download from the Rand Web site at http://www.rand.org.

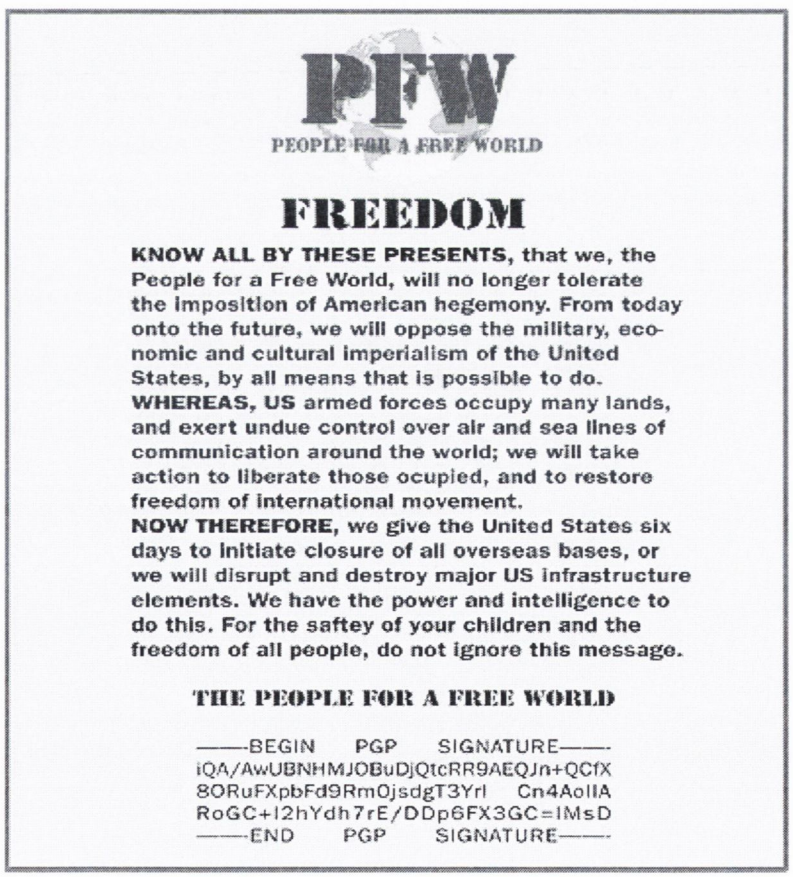
are identified as a coalition of states including North Korea, Vietnam, Iraq, and Libya, aided by the Cali cartel in Colombia and various Asian triads.

Arquilla's scenario is somewhat tongue-in-cheek, and he eventually--the scenario runs to over twenty printed pages--identifies a coalition of states, and not terrorists, as those responsible. This outcome is foreshadowed by the scenario's title: 'The Great Cyberwar.' Arquilla, and his collaborator David Ronfeldt, distinguish in their work between cyberwar and Netwar; cyberwar is the domain of states, while cyberterrorism may be viewed as a category of Netwar, which is the domain of non-/sub-state actors (Arquilla & Ronfeldt 1993, 1996a). Nonetheless, there is a cyberterror component to the scenario in that a number of real and fictional terrorist groups are mentioned, and the coalition of states that are eventually found to be behind the attacks seek to conceal themselves by dubbing their group People For a Free World (see figure 2.1), which is reminiscent of the names of a number of terrorist organisations, including the Weather People and the New People's Army, amongst others.

François Debrix's choice of Fox TV documentary *Dangers on the Internet Highway: Cyberterror* (broadcast in the US in Autumn 1999) to illustrate his argument regarding the hype surrounding the subject of cyberterrorism is interesting from our perspective because the programme is developed around the scenario of "the world's first cyber or Netwar." The programme-makers argue that America's reliance on ICTs is the country's "Achille's Heel," insisting that "the cyber frontier is the next venue for war" and that "cyberwarfare is taking the Internet to its most lethal level" (2001, 154). Various info-war specialists, including John Arquilla, sketch the impacts of a supposed series of escalating cyber attacks: the collapse of air traffic control systems resulting in multiple airplane crashes, overloaded digital networks resulting in collapsed finance and e-commerce networks, collapsed power grids, non-functioning telephone networks, widespread car and train crashes, and nuclear meltdowns. In the television scenario, even the US's ability to fight a conventional war is wiped out due to the coordinated hacker attacks. "Meanwhile, the perpetrators of the war remain undetected behind their distant, encrypted terminals, free to bring the world's mightiest nation to its knees with a few keystrokes in total impunity" (Graham 2004, 18).

Fox TV's scenario bears some striking resemblances to Arquilla's contribution to *Wired* just a few months earlier, but there are also some striking differences. On the one hand, the described outcomes of the cyber attack(s) are strangely similar. On the other, while cyberterrorism is explicitly referred to in the programme's title, the perpetrator of the attacks is unveiled as a little-known country previously thought to have little IT capacity. This does not square with Arquilla's academic analyses of potential cyber threats, which make an explicit distinction between the activities of hostile states (cyberwar) and those of sub-state organisations (Netwar, a subset of which is cyberterrorism).

Figure 2.1 Graphic Accompanying 'The Great Cyberwar of 2002'
***Wired* 6(2), 1998**



Over the course of the next few years, the emphasis in terms of the cyber threat image shifts from states to terrorists and back again.[57] Nobody's quite sure whom they ought to be more afraid of: states or terrorists? Many journalists mix their message and warn that both types of actors are equally threatening.[58] In May 2001, no less august a publication than the *New Yorker* assured its readers that "sophisticated terrorists (or hostile governments) now have the ability to crash satellite systems, to wage economic warfare by unplugging the Federal Reserve system from Wall Street, even to disrupt the movements of ships at sea" (Specter 2001). While in June 2001 an article in *USA Today* entitled 'Cyberspace: The Next Battlefield,' asserted "an adversary could use...viruses to launch a digital blitzkrieg against the United States. It might send a worm to shut down the electric grid in Chicago and air traffic control operations in Atlanta, a logic bomb to open the floodgates of the Hoover Dam and a sniffer to gain access to the funds-transfer networks of the Federal Reserve" (Stone 2001). Post 9/11, however, the spectre of cyberterror took on a new urgency.

In 2003, Dan Verton, a technology journalist,[59] contributed *Black Ice: The Invisible Threat of Cyberterrorism*, an analysis of the cyberterrorist threat aimed at the mass-market. The first chapter of Verton's book describes a coordinated series of cyber and physical attacks on critical infrastructures in the US's Pacific Northwest (2003, 1-16). The attackers carry out a series of suicide bombings using conventional explosives and anthrax-laced powder, they unleash malicious software code which targets Internet root servers and mobile phones, they deface the Web pages of a number of major news

---

[57] In his article 'The American Cyber-Angst and the Real World' (2003), Ralf Bendrath traces the course of the cyber threat image between c. 2000 and 2003 from cyberterrorists to states, back to cyberterrorists and, perhaps, back to states again.

[58] In June 2001, Lawrence K. Gershwin, a top CIA official, took a similar stance in a statement to the Joint Economic Committee of the US Congress. Gershwin told the Committee that foreign governments, rather than terrorists, were the most significant threat to US computers for the next five to ten years. "Terrorists really like to make sure that what they do works....They do very nicely with explosions, so we think largely that they're working on that." Nonetheless, Gershwin warned that a terrorist organisation could surprise intelligence officers and mount a cyber attack within the following six months (see Associated Press 2001b; Joint Economic Committee 2001, 6-10).

[59] This is not to suggest that all journalists, without exception, are guilty of hyping the cyberterrorist threat. It is possible to point to the efforts of some journalists--technology journalists, in particular--to desecuritize cyberterrorism. See, for example, Declan McCullagh's contributions to *Wired* and *C|Net News*; Thomas C. Greene and others in *The Register*; Bruce Schneier in his books, articles, and *Cryptogram* newsletter (http://www.schneier.com/crypto-gram.html); and a goodly amount of the commentary on cyberterrorism produced by *ZDnet* ('Information Resources for IT Professionals').

organisations, and they set off an electromagnetic pulse (EMP) bomb. Verton is clear as to the perpetrators; a collection of sub-state actors comprising a core group of al-Qaeda members, aided by Russian hackers and a number of disgruntled energy company employees with rightwing sympathies. The effects of the attacks are described thus:

> The power outages last for weeks, in some areas, for months. System failures begin to cascade out of control and are felt as far south as California....Medical facilities quickly enter crisis mode as they are forced to rely on back-up power generators for critical care systems....[T]he lack of telecommunications makes coordinating medical emergencies and sharing data on the possible biological or chemical cases nearly impossible. Businesses, banks, government offices, industrial plants, and manufacturing firms are also starved of connectivity. Some will be forced to close their doors for good...Failures and disruptions ripple through potable water control systems, the computers that manage sewage treatment plants, and chemical and oil refineries (Verton 2003, 14-15).

One sceptical reader describes Verton's contribution as "paranoid speculation," and lambastes Verton for his contention that "we can safely discard the opinions of those who argue that cyberterrorism....is impossible" (Greene 2004; Verton 2003, 96).[60] However, such contentions are accepted/acceptable because events in our media-saturated world are allowed to be at one true and false, real and fictional. Verton concludes his scenario with the following observation:

> This is the face of the new terrorism. It is a thinking man's game that applies the violent tactics of the old world to the realities and vulnerabilities of the new high-tech world. Gone are the days when the only victims are those who are unfortunate enough to be standing within striking distance of the blast.

[60] For an article which takes many of the incidents outlined in the scenarios above, interrogates the likelihood of their successful occurrence, and finds them wanting, see Cohen 2003.

> Terrorism is now about smart, well-planned indirect targeting of the electronic sinews of a nation (Verton 2003, 15-16).

He thus transforms his imaginings from prediction to reality. In a similar fashion, the narrator of Fox TV's *Dangers on the Internet Highway* assures viewers that the information contained therein "is not science fiction" (Debrix 2001, 154), intimating that it is thus 'science fact.' Jean Baudrillard, has labelled this condition of undecidability of the event and uncertainty of meaning "hyperreal" modernity. Hyperreality occurs when the media uses its technological capabilities to paint something as more true to life than the object it is purporting to represent (Baudrillard 1983;see also Der Derian 1995, 37-41).

François Debrix suggests that Verton's and Arquilla's musings along with other, similar scenarios give the impression that:

> [T]he next Pearl Harbor will be both everywhere and nowhere at the same time. It's targets will not be the US military or defence system but, instead, the US public and its post-industrial and highly informatized lifestyle. What is now a tool for comfort, an object of leisure, or a necessary support for work....will become the world's deadliest weapon (2001, 156).

Debrix notes that popular fears have taken on a new gravity and emergency responses have become everyday realities in media-saturated societies. This is perhaps especially true in post-9/11 America. Debrix suggests that:

> In a generalised context of uncertainty, common anxiety and more or less planned strategies of emergency give rise to social epiphenomena like cyberterror, its at once real and imagined dangers, and its often paranoid responses. In a context where information becomes knowledge, there is no way of distinguishing cyberterrorism from its representations (on TV, in security literatures, as hypertext on the Web) (Debrix 2001, 153).

The exaggerated nature of the scenarios imagined by Verton, Arquilla, and others is further highlighted when one considers that blackout, failure, and accident are part of the normal operating environment of networked computer and infrastructure systems. It is worth keeping in mind that "water system failures, power outages, air traffic disruptions, and other cyberterror scenarios are routine events that do not always affect national security. System failure is a routine occurrence" (as quoted in Graham 2004, 21). In a relatively sober analysis that appeared in *Jane's Intelligence Review* in 1999, it was observed that:

> There is undoubtedly a lot of exaggeration in this field. If your system goes down, it is a lot more interesting to say it was the work of a foreign government rather than admit it was due to an American teenage 'script-kiddy' tinkering with a badly written CGI script. If the power goes out, people light a candle and wait for it to return, but do not feel terrified. If their mobile phones switch off, society does not instantly feel under attack. If someone cracks a web site and changes the content, terror does not stalk the streets (Ingles-le Noble 1999).

Thus far, cyber-error has proved more frequent and more debilitating than cyberterror. In terms of electrical power, most outages occur due to natural phenomena such as severe weather. In August 2004, Hurricane Charlie ravaged parts of the American state of Florida and it was reported that "it will be weeks rather than days before the most storm-ravaged parts of [Florida] have electricity." This is because the damage was so severe that parts of the power system had to be rebuilt. Indeed when Hurricane Andrew devastated the Miami Area in August 1992, it was fully five weeks before power was restored to all the local supplier's customers (Mayk 2004; Wald 2004; see also Giacomello 2004, 400).

REASONING BY ANALOGY

The importance of basic conceptions is illustrated, within cognitive research, by explanation by analogy, which is a problem-solving method in which knowledge of previous problems with allegedly similar structures is used to find the best way to solve current problems. Within the cyberterror threat discourse the most prevalent analogy is the possibility of an 'electronic Pearl Harbour.' The comparison of so-called 'weapons of mass disruption' with 'weapons of mass destruction' (WMD) is another popular play on words.

Electronic Pearl Harbour

Winn Schwartau of infowar.com first used the term 'Electronic Pearl Harbour' in testimony before the US Congress as early as 1991 (see Schwartau 1994, 43).[61] This analogy links the cyber security debate to a 'real' and successful surprise attack on critical US military infrastructures during World War II while, at the same time, warning against the idea of American invulnerability due to its geographical position. The Pearl Harbour analogy is used with startling frequency in the media as a shorthand description of the likely consequences of a cyberterrorist attack on the United States. A Lexis-Nexis search of major world newspapers found 105 mentions of this and related terms[62] in the ten years between 1994 and 2004.

The term 'electronic Waterloo' has found less favour in the media: a Lexis-Nexis search of major world newspapers found just eight mentions of this and related

---

61 Ralf Bendrath describes Schwartau as "the rock manager turned preacher of 'information warfare'" (2003, 49). In the aftermath of 9/11, Schwartau re-released his 1991 novel *Terminal Compromise* under the new title *Pearl Harbour Dot Com*. The following description of the novel is provided on Amazon.com: "It used to take an entire nation to wage a war. Today it takes only one man. Taki Homosoto survived the hell of Hiroshima. Now, more than 50 years later, the time has come for the Americans to feel the flames of his revenge, using his personal army of terrorists and intelligence agents. The US Government and a network of somewhat reluctant allies - invisible and anonymous hackers join forces to battle this powerful enemy. The devastating climax of this one man's plan...this powerful, bitter survivor of ayamachi, The Great Mistake, is certain to bring global chaos and economic meltdown. A terrifying thought provoking tale."

62 The search was undertaken on 18 August 2004 and used the terms 'electronic Pearl Harbour' (68), 'digital Pearl Harbour' (35), and 'cyber Pearl Harbour' (2).

terms between 1998 and 2004.[63] Just one of these appeared in a US newspaper (*The New York Times*), the rest appeared in British (4) and Canadian (3) publications, whose readers may be expected to be more familiar with said battle.[64] Nevertheless, it has been asserted that the Waterloo analogy is the more accurate of the two. This is because the visions conjured up by reference to an 'electronic Pearl Harbour' are of a sudden crippling blow against critical infrastructures resulting in chaos and destruction. However, it has been argued that this "bolt-out-of-the-blue scenario" is not the most significant cyberwarfare threat to the United States. The greater danger, according to analysts at the Centre for Strategic and International Studies, is a meticulously planned, carefully executed campaign by a focused adversary with a thorough grounding in information warfare techniques. The most important feature of such a strategy, according to the CSIS document, would be its contribution to important strategic goals as part of a larger-scale, possibly long-term strategy. It would not, in other words, be intended simply to gain the public spotlight, create havoc, or win a temporary edge in battle.

> Although the attack on Pearl Harbour precipitated major strategic change, the attack itself was a single blow that failed to achieve Japan's strategic objective, which was to force the United States to an accommodation more favourable to Japan's then expansive foreign policy. The more significant information warfare threat would likely resemble not Pearl Harbour but instead Waterloo, where technology, planning, and careful execution were used as part of a long-range plan aimed at altering the world's political, military and economic order (CSIS 1998, 2).

---

[63] The search was undertaken on 18 August 2004 and used the terms 'electronic Waterloo' (5), 'digital Waterloo' (3), and 'cyber Waterloo' (0).

[64] The Battle of Waterloo was fought thirteen kilometres south of Brussels, Belgium between the French, under the command of Napoleon Bonaparte, and the Allied armies commanded by the British Duke of Wellington and Prussian General Blücher. The French defeat at Waterloo drew to a close twenty-three years of war beginning with the French Revolutionary wars in 1792 and continuing with the Napoleonic Wars from 1803. Napoleon's final defeat at Waterloo marked the end of the Emperor's final bid for power, the so-called 'One Hundred Days', and the final chapter in his remarkable career.

The almost complete absence of references to an 'electronic Waterloo' in the US media is an indication of the necessity for threat images and related analogies to have immediate resonance and attract wide understanding. Their aim is not actually to explain anything about cyberterrorism, but to manufacture fear and to do so in the simplest and most direct way possible.

Weapons of Mass Disruption

In the wake of 9/11, threats to the integrity of America's information infrastructure have been ascribed a level of urgency analogous to nuclear and biological threats, which has galvanised the relationship between IT and security as a primary policy consideration in the United States (Yould 2003, 75). In September 2002, Richard Clarke, former Special White House Adviser for Cyberspace Security, told ABC News: "[Cyberterrorism's] much easier to do than building a weapon of mass destruction. Cyberattacks are a weapon of mass disruption, and they're a lot cheaper and easier" (Wallace 2002). Howard Schmidt, Clarke's one-time deputy, has also repeatedly referred to the threat from 'weapons of mass disruption' (see, for example, McGray 2003). But even before 9/11 the American "cyber-angst" was palpable (Bendrath 2003).[65] As early as 1999, Congressman Curt Weldon (R-Pennsylvania) placed cyberterrorism at the top of his list of modern threats to the American way of life. Speaking at the InfoWarCon conference to an audience of uniformed military personal, corporate IT managers, computer security consultants, and at least one screenwriter,[66] Weldon said "In my opinion, neither missile proliferation nor weapons of mass destruction are as serious as the threat [of cyberterrorism]" (Poulsen 1999). In May 2001, Senator Robert Bennett (R-Utah), stated "[Attacks against the US banking system] would devastate the United States more than a nuclear device let off over a major city" (Porteus 2001). At around the same time, Michael Specter (2001), author of *The New Yorker* article alluded to above, predicted: "The Internet is waiting for its

[65] François Debrix uses the term "e-anxiety" (2001, 165).

[66] In an article for *Foreign Policy* magazine, Thomas Homer-Dixon claims that the US Army enlisted the help of some of Hollywood's top screenwriters and directors--including the creators of *Die Hard* and *McGyver*--to dream up possible scenarios for future terrorist attacks (2002, 61).

Chernobyl, and I don't think we will be waiting much longer." Such predictions are not limited to US commentators. A 2003 *Newsweek* article quoted John Naughton, described as "an Internet expert at Britain's Open University," as saying "If I were Al Qaeda, I wouldn't waste time with nuclear weapons. I'd be going to Microsoft training courses" (Adams & Guterl 2003)

In her seminal article on the role of linguistic metaphors, puns, and acronyms in the field of nuclear defence strategy, Carol Cohn demonstrated how specific uses of language were used to de-dramatise the actual threat (see Cohn 1987). With regard to the cyberterrorist threat, exactly the opposite is happening. Far from de-realising the threat, the discourse of cyberterrorism mobilised by the media and assorted 'experts' makes the threat seem real and palpable. Mediatized discussion of just about any topic fosters the formulation of buzzwords and catchy phrases. The designation of cyber threats as 'weapons of mass disruption' directly analogous to 'weapons of mass destruction'--that is nuclear, biological, or chemical weapons--is, however, both inaccurate and unhelpful in terms of advancing ideas about the relationship between national security and IT. This is true whether one believes such threats are imminent (see Yould 2003, 84-88) or one is sceptical of the cyberterrorist threat. For sceptics, equating the effects of a cyber attack on the US banking system with the effects of the Chernobyl disaster is not only an exaggeration that defies corroboration, but is extremely disingenuous suggesting as it does that the physical (and continuing) death of not just large numbers of people, but literally the whole of a vast territory, is less significant than its digital disconnection (see Cohen 2003, 9-10). The functions of such comparisons are clear however: "Urgency; state power claiming the legitimate use of extraordinary means....*Survival* might sound overly dramatic but it is, in fact, the survival of the unit *as* a basic political unit--a sovereign state--that is the key" [italics in original]. Public perceptions are thus massaged, so that issues such as cyberterrorism, portrayed as having this "undercutting" potential are accepted as having to be addressed prior to all others because, if they are not, the state will cease to exist as a sovereign entity, and all other questions will thus be irrelevant (Wæver 1995, 51 & 53).

IDENTIFYING ANTAGONISTIC ACTORS

The securitization of cyberterrorism is also about specific hostile actors. Traditionally, the focus in security policy analysis has been on potentially threatening states or governments, but in debates about terrorism and information warfare it has been emphasised that non-state actors too may pose a threat. The idea that anonymous adversaries may attempt to penetrate information systems from anywhere in the world breaks with the traditional understanding of security--that the identity, location, and goals of the enemy are known--and increases the sense of fear and insecurity. "The introduction of non-state enemies in security thinking implies opening up Pandora's box, as the number of potential enemies in 'cyberspace' is virtually unlimited" [italics in original] (Eriksson 2001, 218). In terms of IT security, Denning has posited five different types of antagonistic actors: insiders, hackers, criminals, corporations, governments, and terrorists (1999, 26-27). The media have concerned themselves, for the most part, with just two of these: hackers and terrorists.

Terrorist Hackers

In the cyberterror scenarios described here, governments and terrorists were portrayed as the main threats, but hackers were also mentioned. Previous to 9/11, the media were fixated on hackers as antagonistic actors. A reliance on cyberterror simulations alone would have made it difficult to securitize the cyberterrorist threat. This was unnecessary however, because hackers, conceived of as computer abusers, had a history of demonisation in movies, on TV, and in the press. Being "familiar, even archetypal characters" (Entman 2000, 15), when the cyberterrorist threat image was being constructed, they were the perfect candidates for identification as potential perpetrators. It is the classic case of the emergence of "the worst-case result [out] of a dialectic between what is observed and what is imagined" (Lipschutz 1995, 2).

The threat of hackers infiltrating the world's most sensitive military systems is one of the most enduring and popular themes associated with hacking. It was first brought to the public's attention by the 1983 film *War Games*. In the film, a teenage

boy hacks into the computer that monitors and controls the US nuclear and defence system. Believing that it is simply a game-playing machine, the teenager begins a game with the computer. However, the computer believes the game is 'real' and begins the countdown to WWIII.

Wigan (FBI): The Kid Claims he was looking for a toy company. Ha! Ha! That's great!

McKittrick (System Manager): There is no way a high school punk can put a dime in a telephone and break into our systems. He has got to be working for someone else. He's got to be!

Wigan: He does fit the profile perfectly: he is intelligent but an underachiever, alienated from his parents, has few friends, a classic case for recruitment by the Soviets. Now what does this say about the state of our country? Have you got any insight into why a bright boy like this would jeopardise the lives of millions?

FBI Agent: No, Sir, he says he does this sort of thing for fun! (*War Games* 1983)

This scenario resonated deeply with the US public. As mentioned in Chapter One, on his arraignment on charges related to hacking Kevin Mitnick was denied access not only to computers, but also to a phone, because the judge believed that, with the aid of a phone, Mitnick could set off a nuclear attack (see also Ryan 2004, 8-9).

In his book *Hackers*, Paul Taylor describes a 1991 episode of the US chat show *Geraldo* (1999, 178-179). The show's introduction featured excerpts from the film *Die Hard II*, in which terrorists take over the computers of an airport, while the studio section of the show included an interview with Craig Niedorf (aka Knight Lightning), who was the subject of a US court case for having allegedly received the source code of the emergency services telephone computer programs. During the course of the program Geraldo repeatedly referred to Niedorf as the 'Mad Hacker.' The prosecuting

attorney in Niedorf's case also appeared on the show. Below is an excerpt of the dialogue that ensued:

> Geraldo: Don, how do you respond to the feeling among so many hackers that what they're doing is a public service; they're exposing the flaws in our security systems?
>
> Prosecutor: Right, and just like the people who rape a co-ed on campus are exposing the flaws in our nation's higher education security. It's absolute nonsense.

And on the issue of punishment of hackers:

> Prosecutor: I don't think they're being punished very much at all. We're having trouble even taking away their gear. I don't know one of them [who] has done hard time in a prison....even Mitnick who is a real electronic Hannibal Lecter....did not get near any of the punishment that what he was doing entitled him to (as quoted in P.A.Taylor 1999, 178).[67]

At the very end of the show, Geraldo asks the prosecutor to give a brief worst-case scenario that could result from the activities of hackers. He replies: "They wipe out our communications system. Rather easily done. Nobody talks to anyone else, nothing moves, patients don't get their medicine. We're on our knees" (as quoted in P.A. Taylor 1999, 179).

Hackers get a lot of bad press, some of it deserved, some less so. In terms of the securitization of the cyberterrorist threat, the portrayal of hackers as potential adversaries was not restricted to film and television, they were repeatedly identified in the press as the most likely threat actors. The following quote from a 2003 *Newsweek* article entitled 'Bringing Down the Internet' is typical:

---

[67] In the movie *Silence of the Lambs* (1991), Hannibal Lecter (as played by Anthony Hopkins) is a respected psychiatrist turned murderous cannibal.

> If you wanted to write a science-fiction thriller about the day the Internet crashed, you'd start with a computer geek. Armed with nothing but a laptop and a high speed Internet connection, he releases a fast spreading computer virus that in a matter of minutes gives him control of thousands, perhaps millions, of personal computers and servers throughout the world. This drone army launches a silent and sustained attack on computers that are crucial for sending around the billions of packets of data that keep e-mail, the Web and other, more basic necessities of modern life humming. At first the attack seems to be an inconvenience--e-mail traffic grinds to a halt, Web browsing is impossible. But then the problems spread to services only tangentially related to the Internet: automated-teller machines freeze up, calls to emergency numbers fail to get routed to police stations and ambulance services, airport- and train-reservation systems come down. After a few hours, the slowdown starts to affect critical systems: the computers that help run power grids, air-traffic control and telephone networks (Adams & Guterl 2003).

According to the authors of this particular scenario, the cascading failures are not just regional or national in scope, but global. And within a few lines of text the perpetrators morph from "hackers" to "geeks" to "terrorists." The problem, as identified in Chapter One, is that even if 'hackers' managed such a feat, it's not cyberterrorism unless they engaged in the act for political purposes. Most journalists are either unaware of, or ignore, this caveat. They're equally ignorant of the BTKP rule. Chris Hables Gray has observed of war: it "is about killing and maiming human bodies, and if that does not happen, it is not war. Information can serve these ends, as has been recognized since Sun Tzu, but it cannot replace the macabre role of embodiment" (2001, 61). The same may be said of terrorism: it is about killing and maiming human bodies, and if that does not happen, it is not terrorism.

In June 2001 a headline in the *Boston Herald* read 'Cyberterrorist Must Serve Year in Jail' (Richardson 2001). The story continued: "Despite a Missouri cyberterrorist's plea for leniency, a Middlesex Superior Court judge yesterday told the wheelchair-bound man 'you must be punished for what you've done' to Massachusetts

schoolchildren and ordered him to serve a year in jail." The defendant pleaded guilty to "launching a campaign of terror via the Internet" from his Missouri home, including directing Middle School students to child pornography Web sites he posted, telephoning threats to the school and to the homes of some children, and posting a picture of the school's principal with bullet holes in his head and chest on the Net.

In December 2001 a headline in the *Bristol Herald Courier*, Wise County, Virginia, USA read 'Wise County Circuit Court's Webcam "Cracked" by Cyberterrorists' (Still 2001). The webcam, which allowed surfers to log on and watch the Wise County Circuit Courts in action, was taken offline for two weeks for repairs. "(Expletive Deleted) the United States Government" was posted on a web page, but the defaced page could only be seen by the Court's IT contractors. Internet surfers who logged on could only see a blank screen. The 'attack' was thought to have originated in Pakistan or Egypt, according to the report. "This is the first cyberterrorism on the court's Internet technology, and it clearly demonstrates the need for constant vigilance," said Court Clerk Jack Kennedy. "The damage in this case amounted to a $400 hard drive relating to the Internet video server. The crack attack has now resulted in better software and enhanced security to avoid a [*sic*] further cyberterrorism." According to the Court Clerk, Kennedy, cracking can escalate to terrorism when a person cracks into a government- or military-maintained Web site; he said cyberterrorism had increased across the United States since the events of 9-11 and law enforcement had traced many of the attacks to Pakistan and Egypt.[68]

The press have labelled some unlikely acts of computer abuse as 'cyberterrorism.' According to reports, sending pornographic e-mails to minors, posting offensive content on the Internet, defacing Web pages, using a computer to cause $400 worth of damage, stealing credit card information, posting credit card numbers on the Internet, and clandestinely redirecting Internet traffic from one site to another all

---

[68] It was predicted that an escalation in hack attacks would occur in the aftermath of 9-11 (ISTS 2001). However, the predicted escalation did not materialise. In the weeks following the attacks, Web page defacements were well publicised, but the overall number and sophistication of these remained rather low. One possible reason for the non-escalation of attacks could be that many hackers--particularly those located in the US--were wary of being associated with the events of 9/11 and curbed their activities as a result.

constitute instances of cyberterrorism. And yet none of it could be described as terrorism--some of it not even criminal--had it taken place without the aid of computers (see Ross 2000, 255). Admittedly, terrorism is a notoriously difficult activity to define; however, the addition of computers to plain old criminality it is not. So what are the functions of these sorts of reports? They result in a widening of the category of cyberterrorism, which is crucial, as no 'true' act of cyberterrorism, narrowly defined, has ever yet occurred. In order to make the cyberterrorist threat image credible therefore the cyberterror scenarios must be represented as paroxysmal versions of a cyberterror that starts all the way from the teenage hacker.

It seems that even hackers themselves--albeit probably of the script kiddy variety--have begun to be influenced by their portrayal in the media. The anonymous defacement of two US government Web sites, carried out in late November 2001, read as follows: "we are not hacker, we are just cyberterrorist." Elsewhere the defacers referred to themselves as "mujihadeens" and threatened "the greatest cyberterrorist attack against American government." The culprits were almost certainly neither mujihids nor terrorists. It is almost unheard of for a terrorist organisation to refer to themselves as such. In fact many groups use the term 'army' in their self-descriptions as evidence of the legitimacy of the group and their cause (e.g. Irish Republican Army, Irish National Liberation Army, New People's Army, etc.). The perpetrators of the 'attack' described above, on the other hand, are evidently more familiar with media portrayals of cyberterrorism than with any 'real' cyberterrorists (2001a).

It has been observed that all the various ways of abusing computers and IT can hardly be deemed existential threats to sovereign states (Erikkson 2001, 218). Nonetheless,

> The rhetoric surrounding computer hacking consistently reinforces the potentially catastrophic economic and national security threats posed by malevolent intruders, and at the same time attaches the subject of this threat to young obsessive, self-trained computer aficionados. This raises the fundamental question: how can self-trained teenagers be a match for the security devised by governments and corporations that are literally willing to spend billions of

> dollars safeguarding computer systems and cracking down on computer criminals? (Skibell 2002, 336)

In fact, recently the media have reassessed the hacker-as-terrorist discourse, which had begun to appear increasingly unconvincing. In the wake of 9/11, this discourse has been superseded by the terrorist-as-hacker approach.

Hacker Terrorists

The 9/11 attacks resulted in a complete change in threat perceptions, both in terms of the threat from conventional terrorism and its cyber dimension. Ralf Bendrath details how, in the immediate aftermath of the attacks, newspaper articles addressing the threat of cyberterrorism proliferated (2003, 59-60). A Lexis-Nexis search of major US newspapers showed that in the US newspapers of record, the *Washington Post* and *New York Times*, mentions of cyberterrorism doubled in the aftermath of 9/11 (see Table 2.1). This upswing of interest in cyberterrorism was not limited to the US press, a similar trend was noticeable in British newspapers (see Table 2.2). At that time, the question on many people's lips was 'Is Cyber Terror Next?' (Denning 2001a).

Once Osama bin Laden and Al-Qaeda had been fingered as the perpetrators of the 9/11 attacks, a steady stream of newspaper articles began to appear suggesting that the latter were now engaged in planning a major cyberterrorist attack.

> Though nobody really knew how sophisticated Al Qaeda's computer literacy was, more and more people were afraid of them. This created a kind of vicious circle, with the media dramatising the intelligence estimates and politicians in turn picking up media quotes. It was only a question of time before the plain fear would turn into bold forecasting (Bendrath 2003, 63).

In November 2001, an article appeared in *Information Security* magazine that made the jump from "might" or "could" to "will certainly":

> Though we have yet to see terrorist groups--such as Hizbollah, HAMAS, Abu Nidal and Al Qaeda--employ hacking or malware to target critical infrastructures, their reliance Ion information technology and acquisitions of computer expertise are clear warning signs. While damage caused by hacktivists--and even cyberterrorists--has been minimal thus far, security experts predict that the nation's IT infrastructure *will certainly* be a target in the future [my italics] (McAlearney 2001).

While in May 2002 an article in *Newsweek* was headlined 'Islamic Cyberterror: Not a Matter of If, But of When' (Hosenball 2002).

In late June 2002, Roger Cressey, who was at that time Chief of Staff of the President's Critical Infrastructure Protection Board, made a (remarkably) similar claim: "Al Qaeda spent more time mapping our vulnerabilities in cyberspace than we previously thought. An attack is a question of when, not if" (Borger 2002; Gellman 2002a & 2002b). This statement resulted in a deluge of press reports musing upon Al Qaeda's alleged cyber attack plans:

- 'Report: US Fears Possible Al Qaeda Cyber Attacks.' *Reuters*, 27 June
- 'Cyber-Attacks by Al Qaeda Feared.' Barton Gellman in the *Washington Post*, 27 June
- 'US "Fears al-Qaeda Hack Attack."' Kevin Anderson in *BBC News Online*, 27 June
- 'Qaeda Cyberterror Called Real Peril.' Barton Gellman in the *International Herald Tribune*, 28 June
- 'US Fears al-Qaida Will Hit Vital Computer Networks.' Julian Borger in *The Guardian* (UK), 28 June
- 'Al Qaeda Cyber Alarm Sounded.' William Mathews in *Federal Computer Week*, 25 July[69]

[69] In *The Register*, Thomas C. Green contributed, the tongue-in-cheek, 'Soon Al-Qaeda Will Kill You on the Internet' (2002).

Table 2.1
Cyberterrorism in US Newspapers Before and After September 11, 2001

Newspaper	Pre 9/11*	Post 9/11**	Total
	(N)	(N)	(N)
Washington Post	19	41	60
New York Times	15	30	45
Philadelphia Inquirer	10	5	15
Miami Herald	4	7	11
International Herald Tribune	5	3	8

* From first recorded mention in June 1996 to 10 September, 2001.
** 11 September, 2001 to August 2004.
N = Number of articles mentioning the search words
Source: Compiled from Lexis-Nexis archives using the search words 'cyberterrorism,' and 'cyber terrorism.'

Table 2.2
Cyberterrorism in UK Newspapers Before and After September 11, 2001

Newspaper	Pre 9/11*	Post 9/11**	Total
	(N)	(N)	(N)
Financial Times	16	20	36
Guardian	11	20	31
Times	10	8	18
Independent	7	10	17
Mirror	3	10	13

* From first recorded mention in June 1996 to 10 September, 2001.
** 11 September, 2001 to August 2004.
N = Number of articles mentioning the search words
Source: Compiled from Lexis-Nexis archives using the search words 'cyberterrorism,' and 'cyber terrorism.'

William Matthews article in *Federal Computer Week* included a prediction by Congressman Lamar Smith (R-Texas) that "There is a 50 percent chance that the next time al Qaeda terrorists strike in the United States, their attack will include a cyberattack." Finally, on 11 September 2002, a German news agency even went so far

as to quote "military sources in Berlin" who allegedly stated that Al Qaeda "might very well be capable of even preventing a possible US attack on Iraq."

> A Bundeswehr intelligence expert asked: 'What if the Islamists manage to enter the command and control networks of the US Army and mess up everything?' Fighter jets and war ships would receive false instructions and commands, troops would be sent in the wrong direction, bombs would not hit the Iraqi positions they were meant for. This conceivable scenario would lead to a 'military disaster' (DPP News Agency 2002).

The switch in the cyberterrorist threat image, from 'terrorist hackers' to 'hacker terrorists,' highlights two things: first, guarding against, as well as combating, security threats is clearly made easier if one is able to identify the actors responsible. It is suggested that the process of introducing a threat image onto the political agenda is facilitated by the ability to identify the actor or actors constituting the threat (Livingston 1994, 4). Structurally based threats have greater difficulty attracting attention than those portrayed as actor-based (Eriksson & Noreen 2002, 5-6). So while the identification of the cyberterrorist threat with the amorphous category such as that represented by 'hackers' is preferable to the latter, the ability to identify Osama bin Laden and/or Al Qaeda as the source of the cyberterrorist threat is clearly preferable to both of these. Second, certain dramatic events may also have an impact on the resonance of a threat image. The events of 9/11 acted as a trigger factor, revitalising the cyberterrorist threat discourse and the idea of the 'hacker terrorist' in particular.

EMERGENCY MEASURES

Wæver's securitization thesis requires one to study the media more from the perspective of their effects than from their inherent meanings. The purpose of this section is, therefore, to study the effects of the various scenarios, analogies, and general threat images described in this chapter which, because they are presented as 'real,' and

the dangers they display as supposedly immediate, are aimed at convincing the American public that cyberterrorism is imminent and will be extremely destructive, and thus emergency measures are called for. In other words, this 'worst case' portrayal of a threat generally results in a disproportionate response, in which the imagined threat is used to introduce 'real' powers backed up by 'real' legislation that in turn is intended to convey certain imagined scenarios in the mind of, in this case, both hackers and terrorists.

The Pre-9/11 Environment

After the Oklahoma City bombing in 1995, then US President Clinton established the Critical Infrastructure Working Group to address both physical and cyber threats, which eventually gave rise to the Presidential Commission on Critical Infrastructure Protection (PCCIP). The PCCIP's report *Critical Foundations: Protecting America's Infrastructures* (1997) was the first comprehensive description and analysis of the cyber threat to the US national infrastructure. The report highlighted a number of the possible targets for cyberterrorism, including Supervisory Control and Data Acquisition (SCADA) systems, which govern the distribution of telecommunications, electric power, and other infrastructure-based services, which subsequently led to the issuing of Presidential Decision Directive 63 (commonly referred to as 'PDD 63'). "PDD 63 prompted federal agencies to develop critical infrastructure protection plans and encouraged a strategy to protect the nation from cyberattacks" (Raghavan 2003, 302). Various government agencies also began churning out reports addressing the cyberterrorist threat (see Table 2.3). More serious measures were not put in place until after 9/11, however.

The risk of a massive *conventional* terrorist attack on the United States was emphasised by a number of academics and others before the events of 9/11, but was dismissed by the media (see Nacos 2002, 1-2), which chose to focus on cyberterrorism instead. Central decision-makers were therefore much more attuned to the latter threat

than the former. Marcus Sachs,[70] who served in the White House Office of Cyberspace Security and was a staff member of the President's Critical Infrastructure Protection Board, had this to say in 2003:

> We were very shocked in the federal government that the attack didn't come from cyberspace....Based on what we knew at the time, the most likely scenario was an attack from cyberspace, not airliners slamming into buildings....We had spent a lot of time preparing for a cyber attack, not a physical attack (Poulsen 2003).

The Post-9/11 Environment

Previous to 9/11, if one successfully infiltrated a federal computer network, one was considered a hacker. However, following the passage of the PATRIOT Act,[71] which authorised the granting of significant powers to law enforcement agencies to investigate and prosecute potential threats to national security, there is the potential for hackers to be labelled cyberterrorists and, if convicted, to face up to 20 years in prison (NIPC 2001b; see also Middleton 2002; Levin 2002, 984-985). The law gives government investigators broad powers to track wireless phone calls, listen to voicemail, intercept e-mail messages, and monitor computer use. It also criminalizes break-ins into any computer outside of the United States "that is used in a manner that affects inter-state or foreign commerce or communication of the United States" (USA PATRIOT Act, Section 814). Ralf Bendrath identifies this as the cyber equivalent of the US government's 'War on Terrorism,' as it systematically expands the US's cyber reach beyond its territory (2003, 61).

---

[70] Sachs collaborated on a fiction book entitled *Zero-Day Exploit* (2004) detailing yet another cyberterror scenario. This time a 0-day vulnerability in a particular line of SCADA Master products that are widely used in petrochemical facilities is exploited by attackers resulting in gas stations running out of gas, followed shortly by freight carriers, private individuals, and local police and fire departments. Disaster can only be prevented by Reuben, an elite cyber-security researcher who stumbles across the plot while contracting for the federal government (from Amazon.com product description).

[71] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act was signed into law by US President George Bush in October 2001.

Table 2.3
US Government Documents: Cyberterrorism and Critical Infrastructure Protection, 1998-2004*

Prepared By	Year	*Title*
White House	1998	*Presidential Directive 63: Critical Infrastructure*
General Accounting Office	1999	*Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations*
General Accounting Office	1999	*Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences*
White House	2000	*Defending America's Cyberspace: National Plan for Information Systems Protection*
Department of Justice	2000	*Assessment of the Increased Risk of Terrorist or Other Criminal Activity Associated with Posting Off-Site Consequence Analysis Information on the Internet*
General Accounting Office	2000	*Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination*
General Accounting Office	2001	*Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities*
General Accounting Office	2001	*Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*
General Accounting Office	2001	*Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks*
General Accounting Office	2001	*Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities*
National Infrastructure Protection Centre	2001	*Cyber Protests: The Threat to the US Information Infrastructure*
General Accounting Office	2002	*Critical Infrastructure Protection: Significant Homeland Security Challenges Need to be Addressed*
General Accounting Office	2002	*Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*
Congressional Research Service	2003	*Critical Infrastructures: What Makes an Infrastructure Critical?*
General Accounting Office	2003	*Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*
General Accounting Office	2003	*Potential Terrorist Attacks: Additional Actions Needed to Prepare Critical Financial Markets*
White House	2003	*The National Strategy to Secure Cyberspace*
White House	2003	*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*
General Accounting Office	2003	*Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*
General Accounting Office	2003	*Information Security: Progress Made, but Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*
Congressional Research Service	2003	*Terrorism and Security Issues Facing the Water Infrastructure Sector*
White House	2003	*Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.*
General Accounting Office	2004	*Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems.*
General Accounting Office	2004	*Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*
General Accounting Office	2004	*Technology Assessment: Cybersecurity for Critical Infrastructure Protection*

* All documents are available in full on the Internet.
Source: Compiled from list available at Web site of National Memorial Institute for the Prevention of Terrorism (MIPT) http://www.mipt.org and Internet searching.

It is not the PATRIOT Act, however, but the massive 500-page law establishing the US Department of Homeland Security that has the most to say about terrorism and the Internet. The law establishing the new department envisions a far greater role for the United States' government in the securing of operating systems, hardware, and the Internet in the future. In November 2002, US President Bush signed the bill creating the new department, setting in train a process that would result in the largest reshuffle of US bureaucracy since 1948. At the signing ceremony, Bush said that the "department will gather and focus all our efforts to face the challenge of cyberterrorism" (as quoted in McCullagh 2002b).

The Department of Homeland Security merges five agencies that shared responsibility for critical infrastructure protection in the United States: the FBI's National Infrastructure Protection Center (NIPC), the Defense Department's National Communications System, the Commerce Department's Critical Infrastructure Office, the Department of Energy's analysis center, and the Federal Computer Incident Response Center. The new law also creates a Directorate for Information Analysis and Infrastructure Protection whose task it will be to analyse vulnerabilities in systems including the Internet, telephone networks, and other critical infrastructures, and orders the establishment of a "comprehensive national plan for securing the key resources and critical infrastructure of the United States" including information technology, financial networks, and satellites. Further, the law dictates a maximum sentence of life-imprisonment without parole for those who deliberately transmit a program, information, code, or command that impairs the performance of a computer or modifies its data without authorisation, "if the offender knowingly or recklessly causes or attempts to cause death." In addition, the law allocates $500 million for research into new technologies, is charged with funding the creation of tools to help state and local law enforcement agencies thwart computer crime, and classifies certain activities as new computer crimes (Krebs 2002; McCullagh 2002a; Poulsen 2002).

European Union governments also moved to counter computer-assisted terrorism in the wake of 9/11. The Council of Europe rushed through its Convention on Cybercrime in response to the attack, and the UK parliament passed the Anti-Terrorism, Crime and Security Act 2001 (ACSA), broadening the definition of terrorist

organisations to include cyberterrorists for the first time, defining these as persons who disrupt or interfere with electronic systems.

CONCLUSION

Policymakers define security on the basis of a set of assumptions regarding vital interests, possible scenarios, and plausible enemies, which grow out of the specific historical and social context of a particular country and some conception of what is "out there" (Lipschutz 1995, 10). As we have seen, the media plays a key role in shaping these assumptions, constructing these scenarios, and generally informing us as to what is "out there." It is thus infused with massive soft power in terms of the process of defining security. The end of the Cold War provided an unprecedented window of opportunity for the movement of a wide range of non-military issues into the realm of security policy. With the aid of the mass media, cyberterrorism came to be viewed as the 'new' security threat *par excellence*.

We cannot predict who will voice security concerns; only with hindsight can we see how much legitimacy an actor *did* possess. Every day some actor seeks to speak security, but the attempt becomes consequential only when society more or less actively backs up the speaker(s). People's sense of what issues are of political relevance is always an ongoing process, which requires an emphasis on how threat images are discursively constructed, maintained, and altered. Particular emphasis needs to be placed upon the processes whereby national security issues communicatively emerge, and the central role of the media in such emergences, because the political communication/threat image environment shapes both the information available and the ways ordinary people use it in thinking about politics and national security.

Demonstrating the effects of the media's influence on decision-making is always difficult due to the indirect and complex dynamics involved. Clearly though the American media has been highly successful in 'speaking' cyberterrorism into existence. Their reliance on "(hyper-)reality-producing dramas" (Debrix 2001, 153), Pearl Harbour analogies, comparisons of the effects of cyberterrorism with those of WMD,

portrayal of hackers as a menace to national security, and general widening of the concept of cyberterrorism, in conjunction with the policy window opened by the events of 9/11 and, consequently, the ability to pinpoint Osama bin Laden and Al Qaeda as certain future cyberterrorists has resulted in the enactment of a raft of emergency measures as detailed in the USA PATRIOT Act and the Homeland Security Act.

It may be that these emergency measures are uncalled for, however. François Debrix suggests that all of the various apocalyptic scenarios, televised simulations, and musings as to the greater lethality of cyber than nuclear attack have ensured that the next Pearl Harbour will never materialise. Why? Because the fear of cyberterrorism has been spread so widely and with such success that should a 'real' attack ever occur it couldn't match these.

> Being conditioned to such a degree of generalised panic, any real cyberterrorist attack that does not follow the simulated scenario and produce the anticipated amount of casualties will fall short of being worthy of people's attention and worry (Debrix 2001, 156).

The question that then arises is whether the--for the most part--American-constructed cyberterrorist threat image has resonance beyond the borders of the United States?

"Traditionally, the US has been the dominant actor in IT issues. The US is and has been a 'sender' of ideas to other states about how to comprehend IT problems and their solutions" (Holmgren & Softa 2003, 15). That is one of the reasons why this chapter is focused upon the US case. Nonetheless, threat images are constructed and responded to differently in different countries and regions. This raises a number of questions. Are we, for example, moving toward a converged perception of the cyberterrorist threat in the United States and Europe, or are the images in these different territories more divergent than similar? It is not only national political agendas that ought to be of interest. The description and analysis of how the cyberterrorist threat is being discussed and created within the European security community, particularly within the framework of a EU common foreign and security

policy and within NATO, is also an avenue for future research. These are not the avenues further explored in the present project, however.

What this chapter has sought to show is how the cyberterror threat has been amplified in the US media. It is generally difficult to unravel how news frames shape the social construction of reality from the 'actual' reality of events. This is especially true in cases where the 'events' do not yet have a reality, as is the case with cyberterrorism, and presents particular difficulties if a "consensual interpretation" (Kern, Just, Norris 2003, 281) predominates so that a one-sided frame becomes uncritically taken for granted by politicians, journalists, and the public. 'Terrorism' is generally conceived as physical acts of violence intended to produce fear, and conjures up images of exploding bombs and mutilated bodies. The cyberterror threat image builds upon this aspect of terrorism by seeking to convince the public that cyberterrorism will ultimately result in mass casualties. There is another dimension to terrorism, however: the information dimension. And terrorists exploit it every bit as much as the physical. Death and destruction is not terrorists' ultimate goal; it is power and influence. Terrorists seek political and social change, and their objective is to influence populations in ways that support that change. To accomplish this, they engage not just in physical, but also information operations, and the integration of these.

Up until very recently, cyberterrorism was presented as the sole intersection of terrorism and the Internet, even in the face of contrary independent evidence. The one-sided nature of the analysis only became apparent to many when, in a little over four weeks in April and May 2004, one Abu Musab-al Zarqawi "rocketed to worldwide fame, or infamy, by a deliberate combination of extreme violence and Internet publicity" (Eedle 2004). In early April 2004, Zarqawi posted online a thirty minute audio recording which explained who he was, why he was fighting, and details of the attacks for which he and his group were responsible. Paul Eedle (2004) has described the latter as "a comprehensive branding statement":

> The Internet gave Zarqawi the means to build a brand very quickly. Suddenly the mystery man had a voice, if not a face, and a clear ideology which explained

> his violence... But what is the point of an insurgent group building a brand, establishing a public profile in this way? The answer is to magnify the impact of its violence.

Prior to the instigation of his Internet-based PR campaign, each of Zarqawi's attacks had to kill large numbers of people in order to get noticed in the chaos and mounting daily death toll in Iraq. By going online, however, Zarqawi was able to both control the interpretation of his violent message and achieve greater impact with smaller operations. By the end of April 2004, his group were regularly issuing communiqués via the Net. The first claimed responsibility for a suicide speedboat attack on Iraq's offshore oil export terminal in the Gulf which, although the operation failed, still shook oil markets because of Zarqawi's efforts at publicising the attack through the Internet.

In May 2004 Zarqawi took things a step further when he used the Internet's force multiplying effect to the maximum effect for the first time when

> ...he personally cut off the head of an American hostage live on video, and had the footage posted on the Internet....The entire purpose of the beheading was to video it, to create images that would grip the imaginations of friends and enemies alike. It worked. Zarqawi risked almost nothing in this operation; but he started a withdrawal of foreign contractors which has paralysed reconstruction in Iraq and done as much if not more to undermine US plans as a bomb that killed 100 people in Najaf. And he made himself a hero to jihadis across the world (Eedle 2004).

The free availability of this and other grisly 'snuff movies' on the Internet led to a realisation that the most important aspect of the terrorism-Internet relationship was not the much vaunted 'cyberterrorism,' but those more mundane and everyday terrorist uses of the Net, from information provision to recruitment, which have a pedigree stretching back for many years before Zarqawi's appearance on the online scene. The remainder of this project is concerned with describing and analysing these.

PART II

ON TERRORIST 'USE' OF THE NET

"Terrorists use the Internet just like everybody else"

- Richard Clarke (2004)

3

TERRORIST 'USE' OF THE INTERNET AND FIGHTING BACK

"There is a free wheeling political life on the Net, but it is mostly an extension of political life off the Net"

- Resnick 1999, 60

INTRODUCTION

In 1995, there were just twenty million individuals worldwide with access to the Internet. Nonetheless, in the same year, Charles Swett, a US Department of Defense employee, produced his *Strategic Assessment: The Internet*[72] in which he details how political processes were moving onto the Internet, both within the United States and internationally, despite the relatively low numbers of Internet users globally. In his assessment, Swett points to the way in which the Internet played important roles in contemporary conflicts such as Desert Storm, the Tiananmen Square massacre, the attempted coup in Russia, the conflict in the former Yugoslavia, and in the challenge to government controls in Iran, China, and other authoritarian states (pp.'s 9-15). This led Swett to envisage that, in the future, the Internet would play an increasingly significant role in international conflict (pp.'s 16-17). "While there is already a great deal of political use of the Internet domestically and internationally, there is likely to be a

[72] A revised version of this text was subsequently published in the online journal *First Monday* (see Swett 1996).

significant increase in the scale and sophistication of such use in the coming years," he forecast (p.17). Though some of Swett's other predictions fall somewhat wide of the mark,[73] his conviction that the Internet would prove a boon to international conflict actors has certainly come to pass.

More recently the impact of new media has been developing as an area of interest within IR. The relationship between NGOs and these new communications technologies has generated a particularly large body of work. Much of this research was inspired by the Zapatista insurgency in Chiapas in southern Mexico, which was hailed as the world's first postmodern movement. The EZLN (*Ejército Zapatista de Liberación Nacional* or Zapatista Army of National Liberation) was not a 'wired' indigenous army; its members did not have their own laptop computers, Internet connections, fax machines, or mobile telephones. These information-age capabilities were in the hands of a large number of transnational and some Mexican NGOs. And they used them to stunning effect for conveying both the Zapatista's and their own views, for communication and coordination purposes, and creating an extraordinary mobilization of support as laid out in numerous conference papers, journal articles, chapters, and books (Arquilla & Ronfeldt 2001b; Bob 2001; Castells 1997, Ch. 2; Cleaver 1998; Collier 1999; Garrido & Halavais 2003; Hayden 2002; Holloway, Pelaez & Pelaez 1998; Ronfeldt, Arquilla, Fuller, & Fuller 1998).

Another dramatic example of the 'new' activism was the so-called 'Battle of Seattle' in 1999, in which mass demonstrations against the World Trade Organization disintegrated into violent clashes between the police and demonstrators. The Seattle demonstrations and other similar protests in Prague in 2000 and Genoa in 2001 employed the Internet in a more indirect, but no less constructive manner, than the EZLN insurgency. The 'anti-globalization' protests involved a disparate range of environmental, development, ethnic nationalist, anarchist, and revolutionary socialist groups, with the Internet and mobile phones providing the principal means of

[73] In addition to his prediction about the future utility of the Internet in international conflict, Swett also accurately predicted that members of the US Congress and federal agency officials would inexorably be drawn to the Internet and, eventually, the Internet would be used as a tool of statecraft by national governments (1995, 16). However, predictions that have not yet materialized include the emergence of new political parties operating solely through the Internet, the erosion of the monopoly of the traditional mass media, and the replacement of text-oriented e-mail by video messaging (1995, 15-16).

organization and communication, both in the lead-up to and on the streets during the demonstrations (de Armond 2001; Van De Donk, Loader, Dixon, & Rucht 2003; Sullivan 2001; Vegh 2003). Research has also been undertaken on the use of information technologies by more institutionalized NGOs such as Amnesty International, Oxfam, and others (see Hajnal 2002), but the emphasis on so-called 'grass roots' organizing in this area of research is still strong (see Bennett 2003b; Leizerov 2000; Lin & Dutton 2003).

Given the above, and with over 600 million Internet users worldwide in 2005, today the Internet is recognized as a powerful political instrument. David Resnick has identified three types of Internet politics:

1. Politics Within the Net: This refers to the political life of cyber-communities and other Internet activities that have minimal impact on life off the Net.
2. Politics Which Impacts the Net: This refers to the host of public policy issues raised by the Internet both as a new form of mass communication and a vehicle for commerce.
3. Political Uses of the Net: This refers to the employment of the Internet by ordinary citizens, political activists, organised interests, governments, and others to achieve political goals having little or nothing to do with the Internet *per se* (i.e. to influence political activities offline) (1998, 55-56).[74]

This chapter is centrally concerned with 'Political Uses of the Net,' specifically the use(s) made of the Internet by terrorist groups, a subject that to date has been the focus of only a very small amount of substantive social science research.

[74] Kumiko Aoki (1994) divides the study of virtual communities into three separate categories in a similar fashion.

CONCEPTUALISING TERRORIST ACTIVITY ON THE NET

The 'Use' Approach

In Chapter One it was suggested that differences exist between what's been called "traditional cyberterrorism" and "pure cyberterrorism." According to Gordon and Ford, traditional cyberterrorism features computers as the target or the tool of attack while pure cyberterrorism is more restricted: it is limited to attacks against computers, networks, and information (2002, 636-637 & 641). However, Gordon and Ford believe that the true impact of the convergence of terrorism and cyberspace is realised not only when the attack is launched against computers, but when many of the other factors and abilities of the virtual world are leveraged by terrorists in order to carry out their attacks (2002, 637). Nelson *et al* emphatically reject this approach however. They identify two new categories into which this latter type of activity may be placed: 'cyberterror support' and terrorist 'use' of the Net. "Cyberterror support is the unlawful use of information systems by terrorists which is not intended, by itself, to have a coercive effect on a target audience. [It] augments or enhances other terrorist acts." On the other hand, terrorist 'use' of computers as a facilitator of their activities, whether for propaganda, communication, or other purposes, is simply that: 'use;' and, crucially, does not qualify as cyberterrorism (1999, 10). This approach to terrorist use of the Internet, which fits with Resnicks more general category, is also that employed by Kent Anderson, who has devised a three-tiered schema for categorizing fringe political activity on the Internet.

Anderson, formerly senior vice-president of IT Security and Investigations for information security firm Control Risks Group, utilizes the terms 'Use,' 'Misuse,' and 'Offensive Use,' to distinguish between different types of Internet-based political activism.

> Use is simply using the Internet/WWW to facilitate communications via e-mails and mailing lists, newsgroups and websites. In almost every case, this activity is simply free speech...Misuse is when the line is crossed from

> expression of ideas to acts that disrupt or otherwise compromise other sites. An example of misuse is Denial-of-Service (DoS) attacks against websites. In the physical world, most protests are allowed, however, [even] if the protests disrupt other functions of society such as train service or access to private property...The same should be true for online activity. Offensive use is the next level of activity where actual damage or theft occurs. The physical world analogy would be a riot where property is damaged or people are injured. An example of this type of activity online is the recent attack on systems belonging to the World Economic Forum, where personal information of high profile individuals was stolen[75] (Weisenburger 2001, 2).

Combining Anderson's categorization with the definitions of cyberterrorism outlined by Pollitt (1998) and Denning (2000a) in Chapter One it is possible to construct a four-level scale of the exploitation of the Internet for political activism by unconventional actors, ranging from 'Use' at one end of the spectrum to 'Cyberterrorism' at the other (see Table 3.1). Unfortunately, such a schema has not generally been employed in the literature or in the legislative arena. This is particularly disquieting given that the vast majority of terrorist activity on the Internet is limited to 'Use.'

What Makes the Internet Different?

Thomas Friedman has argued that contemporary globalization "goes farther, faster, cheaper, and deeper" (as quoted in Nye 2002, 85; see also Nye 2004, 31). He might have been describing the Internet. The Internet is a powerful tool, which is used and manipulated by actors to accomplish a wide variety of tasks. The networked nature of the Internet allows users to access a nearly limitless supply of information and data that can be shared across the network. People can use the Internet to educate themselves, to entertain themselves, to conduct business, to shop, or to engage in political action.

---

[75] In May 2001, protesters obtained 80,000 pages of classified data belonging to the high-profile attendees of the 30th Annual World Economic Forum in Davos, Switzerland. The data, including the names, addresses, user names, passwords, payment information, and other details belonging to as many as 27,000 attendees was burned to a CD-ROM and passed to a journalist affiliated with a Swiss newspaper.

Table 3.1. Typology of Cyber Activism and Cyber Attacks

Action	*Definition*	*Source*	*Tactical Objective*	*Example*
Use	Using the Internet to facilitate the expression of ideas and communication(s)	Internet Users	Communication	Emails, mailing lis newsgroups, websites
Misuse	Using the Internet to disrupt or compromise Web sites or infrastructure	Hackers, Hacktivists	Disruption	Denial-of-Service (DoS) attacks
Offensive Use	Using the Internet to cause damage or engage in theft	Crackers	Exploitation	Stealing data (e.g. credit card details)
Cyberterrorism	An attack carried out by politically-motivated actors either via the Internet or targeting the Internet that results in violence against persons or severe economic damage	Terrorists	Destruction	A terrorist group using the Internet to carry out a major assault on the New York Stock Exchange, the North American electricity grid, etc.

There is no *a priori* reason, however, why actors should use the Internet to engage in these activities over any other potential tool that will garner the same result. Three conditions must therefore generally be met for actors to view the Internet as a source of instrumental power. First, the Internet must offer advantages greater than other tools. As with any tool, the Internet does not exist in a vacuum; rather, actors are presented with different options and make choices based on relative advantages. If actors are to use the Internet, it must offer relative advantages over other potential tools. If no such comparative benefit exists, actors will see no utility in using the Internet, opting instead for some other, more effective, option. There are nine key properties of the Internet that render it different from traditional media and a key instrumental power source:

(a) Volume: far larger volumes of information can be transferred easily compared with previous modes of communication.

(b) Speed: the ability to compress data and more space for transmitting data decrease the amount of time it takes to exchange information.

(c) Format: the ability to combine text, graphics, audio, and video means that in-depth, dynamic, and visually stimulating communication is possible simultaneously.

(d) Direction: the possibilities for two-way interactive communication are greatly expanded on the WWW as a result of the greater space and speed, but also due to the enhanced horizontal or lateral links arising out of hypertext linkage between sites.

(e) Individual Control: the opening up of control over direction in the sending and receiving of information means that power is decentralized to the individual user who has the choice of not only what to view, but also what to publish.

(f) Anonymity: Internet users enjoy a large measure of anonymity. There are numerous information security applications that allow customers to conceal their identity, the content of their communications, or the details of their transactions. These include free e-mail services, electronic remailers,[76] anonymizers,[77] and widely available encryption and steganographic tools.

(g) Evasion of Government Control: the primary way in which actors may evade government control is through operating their Web site(s) in jurisdictions with high levels of free speech protection. The various tools identified in (f) above may also be used to avoid censorship.

(h) Reduced Transaction Costs: registering a Web site costs less than US$50 and many Internet sites allow users to create Web sites at no cost at all. Free e-mail

---

[76] Anonymous electronic remailers allow e-mail messages to be sent without the receiver ever knowing the sender's identity although the recipient is usually able to reply to and correspond with the sender of such a message. Many remailers also provide encryption services. Popular remailers are those maintained by HushMail (http://www.hushmail.com) and ZipLip (http://www.ziplip.com).

[77] Internet anonymizers retransmit Internet content to users, thereby protecting users personal information. Anonymizer services protect users' personal computers' identifying information while surfing, enabling users to remain one or more steps removed from the sites they access. Anonymizers come in two types: networked designs, where users communications are routed through a network of other computers, and single-point designs, where communications are anonymized through a single site. The Electronic Frontier Foundations Tor (http://tor.eff.org/) is an example of the former while the free service available at http://www.anonymizer.com/ is an example of the latter.

services are commonplace on the Internet while newsgroups and message postings are likewise available at no cost.

(i) Globality: perhaps more importantly, these low-cost Internet technologies allow users to transmit and share information globally nearly instantaneously. The networked structure of the Internet finds the quickest and most effective route for information flows. Web sites from anywhere in the world take only seconds to load while e-mails can circle the globe in an instant (Dartnell 1999, 124-125; Gibson & Ward 2000, 304; Hinnen 2004, 5; McLaughlin 2003, 4; Swett 1995, 3; Wall 2002, 27; Weimann 2004a, 3).

In summary, then, Web-based communication has the potential to be a more immediate, individual, dynamic, in-depth, interactive, anonymous, unedited, cheaper, and far-reaching process than is possible in conventional media.

In terms of viewing the Internet as an instrumental power source, the second condition that must be met is that potential users have access to the Net. If actors are to capitalize on the advantages of the Internet, they must be able to access and use the technology. Assessing user access requires going beyond pure numbers; statistics about the number of computers or Internet hosts in a given population provide only a basic understanding of potential access. Internet access also depends on other context-dependent factors: issues such as the security environment and government censorship can directly impact how or even whether specific actors are able to utilize the Internet. While Internet access may be considered a given in the United States and Western Europe, user access in many parts of the world is subject to many constraints. Third, and related to actor access, use of the Internet also requires audience access. The Internet is, to a large extent, an interactive technology. Actors create Web sites for one or more audiences, be they local, regional, national, or global in scale. The Internet offers little utility if Web sites go unvisited, messages unread, and e-mails unchecked. The effective use of the Internet therefore requires that potential audiences have access to the technology. As with actor access, context-dependent factors can and do influence the ability of messages to reach their intended audiences (McLaughlin 2003, 4).

With this understanding of the utility of the Internet in mind, it is possible to delineate the current and potential uses of the Internet by terrorist actors.

Why Terrorists are Launching Into Cyberspace

What are terrorist groups attempting to do by gaining a foothold in cyberspace? In 1997, Wayne Rash, in his *Politics on the Nets*, posited eight uses of the Net that he foresaw political groups adopting. He described these as tactical communications, organization, recruitment, fundraising, strategic positioning, media relations, affinity connections, and international connections (1997, 176-177). Although Rash did not identify terrorists as a specific political Internet user group, his list of uses is broadly similar to those later developed by authors concerned with the narrower issue of terrorist use of the Net (see Table 3.2). In 1999, for example, Steve Furnell and Matthew Warren described the core terrorist uses of the Net as propaganda/publicity, fundraising, information dissemination, and secure communications (1999, 30-32). Fred Cohen presents his readers with a broadly similar list of uses (2002, 18-19). Timothy L. Thomas, on the other hand, presents a more detailed rendition of terrorist uses of the Net. In his article 'Al Qaeda and the Internet: The Danger of "Cyberplanning,"' which appeared in the US Army journal *Parameters* in 2003, Thomas discusses some sixteen potential uses of the Internet by terrorists (pp.'s 114-122). These include using the Internet to put together profiles (p.114), to help poorly funded groups to raise money (pp.'s 116-117), to gather information on potential targets (p.118), to disrupt business (p.120), and to mobilize a group or diaspora (pp.'s 120-121). Thomas does not adopt the use paradigm but refers instead to what he dubs "cyberplanning"--"the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed" (2003, 113)--which nonetheless shares sufficient similarities with the use approach as to be almost indistinguishable from it. Finally, in a recent report for the United States Institute of Peace entitled *WWW.terror.net: How Modern Terrorism Uses the Internet* (2004a), Gabriel Weimann identifies eight different ways in which, he says, terrorists currently use the Internet. These are psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, information sharing, and planning and coordination (pp.'s 5-11).

Table 3.2 Terrorist Uses of the Net

Author(s)	*Furnell & Warren (1999)*	*Cohen (2002)*	*Thomas (2003)*	*Weimann (2004a)*
Uses	-Propaganda & Publicity - Fundraising - Information Dissemination - Secure Communications	- Planning - Finance - Coordination & Operations - Political Action - Propaganda	- Profiling - Propaganda - Anonymous/Covert Communication - Generating "Cyberfear" - Finance - Command & Control - Mobilisation & Recruitment - Information Gathering - Mitigation of Risk - Theft/Manipulation of Data - Offensive Use - Misinformation	- Psychological Warfare - Publicity & Propaganda - Data Mining - Fundraising - Recruitment & Mobilisation - Networking - Sharing Information - Planning & Coordination

There is considerable overlap amongst the terrorist uses of the Net identified by the different authors in Table 3.2.[78] While twenty-two different categories of use are mentioned; often, authors are simply using different terms to refer to the same issues. This is clearest in terms of the identity shared by the concepts 'fundraising' and 'finance,' but also relates to the concepts 'information gathering' and 'data mining,' for example. Given such overlaps, the analysis below relies on what have been determined to be the five core terrorist uses of the Internet: information provision, financing, networking, recruitment, and information gathering. Each of the uses identified in Table 3.2 fits into one of these categories or its sub-categories.[79] All four authors mentioned identify resource generation along with information provision, particularly propaganda, as primary terrorist uses of the Internet. I have subsumed a number of

[78] Such overlaps are not just evident amongst those who adopt a use paradigm, but are shared with those who adopt an Information Operations (IO) approach (see Denning 2004; Emery Early, & Buettner 2004; O'Brien & Lev 2002).

[79] For information regarding the placement of each of the issues identified in Table 3.2, see Appendix C.

other issues, including secure communication and planning, under the heading 'Networking.' Finally, although recruitment is mentioned by just two of the authors discussed here (Thomas 2003; Weimann 2004a), there is evidence to support the view that the Internet has been utilized to promote participation in terrorist activity and it is thus included as a core use here. Each of the five core terrorist uses of the Internet is explained and analyzed in more detail below.

FIVE TERRORIST USES OF THE NET

Information Provision

This refers to efforts by terrorists to engage in publicity, propaganda and, ultimately, psychological warfare. The Internet, and the advent of the World Wide Web in particular, have significantly increased the opportunities for terrorists to secure publicity. This can take the form of historical information, profiles of leaders, manifestos, etc. But terrorists can also use the Internet as a tool of psychological warfare through spreading disinformation, delivering threats, and disseminating horrific images, such as the beheading of American entrepreneur Nick Berg in Iraq and US journalist Daniel Pearl in Pakistan via their Web sites (Weimann 2004a, 5). These functions are clearly improved by the Web's enhanced volume, increased speed of data transmission, low-cost, relatively uncontrolled nature, and global reach.

Until the advent of the Internet, terrorists' hopes of winning publicity for their causes and activities depended on attracting the attention of television, radio, or the print media. As Weimann points out, "these traditional media have 'selection thresholds' (multistage processes of editorial selection) that terrorists often cannot reach" (2004a, 6). The same criteria do not, of course, apply to the terrorists' own websites. The Internet thus offers terrorist groups an unprecedented level of direct control over the content of their message(s). It considerably extends their ability to shape how different target audiences perceive them and to manipulate not only their own image, but also the image of their enemies. Although, for many groups, their target

audience may be small, an Internet presence is nonetheless expected. Regardless of the number of hits a site receives, a well-designed and well-maintained Web site gives a group an aura of legitimacy. David Resnick sums this up well:

> Traditionally, mass media serve a mass public, while specialized media serve select audiences. The Web is a hybrid, both a specialized medium and a mass medium. There is room for groups and causes which appeal to narrow constituencies. A presence on the Web could greatly increase the exposure of a narrow interest group both to its own potential constituency and to the public at large. Small relatively obscure interest groups probably have more to gain by going online than mainstream well-established groups which are skilled at using traditional mass media. Because of the hypertext linkages which permeate the Web even a very specialized interest can be categorized in more general terms and become linked to more popular sites. In any case, no matter how obscure or outré the cause, if it has a Home Page it can probably be located by employing a search engine (1998, 66).

Most Internet sites of terrorist groups seek to advance the organization's political and ideological agenda. Terrorists' use of the Net for publicity purposes, particularly the content and value of dedicated Web sites established by particular groups, is one that will be treated at length in Chapters Five to Seven. For now, it is sufficient to draw the reader's attention to this aspect of terrorist use of the Net and to introduce the idea that it is this facet of terrorist Net use that is currently most important.

Financing

This refers to efforts by terrorist groups to raise funds for their activities.[80] Money is terrorism's lifeline; it is "the engine of the armed struggle" (Napoleoni 2004, 1).[81] The

[80] For information about terrorist financing in general, see Ehrenfeld 2003; General Accounting Office 2003; Napoleoni 2003.

[81] Plainly, sources of funding are numerous and vary substantially between groups, while sources for financing depend on the needs of the organization. "A group like the FARC in Colombia, obviously

immediacy and interactive nature of Internet communication, combined with its high-reach properties, opens up a huge potential for increased financial donations as has been demonstrated by a host of non-violent political organizations and civil society actors.[82] Terrorists seek financing both via their Web sites and by using the Internet infrastructure to engage in resource mobilization using illegal means. They also use the Internet to transfer funds.

Direct Solicitation Via Terrorist Web Sites

Numerous terrorist groups request funds directly from Web surfers who visit their sites. Such requests may take the form of general statements underlining the organizations' need for money, more often than not however requests are more direct urging supporters to donate immediately and supplying either bank account details or an Internet payment option. While at one time the Ulster Loyalist Information Service, which was affiliated with the Loyalist Volunteer Force (LVF), and accepted funds via PayPal, invited those who were "uncomfortable with making monetary donations" to donate other items, including bulletproof vests (see Figure 3.1). A second, and related, fundraising method is to profile site visitors by employing user demographics (yielded, for example, from identifying information entered in online questionnaires or order forms) and to contact those whose profiles indicate they are potential financial supporters, a function which may be carried out by proxies, according to Tibbetts:

---

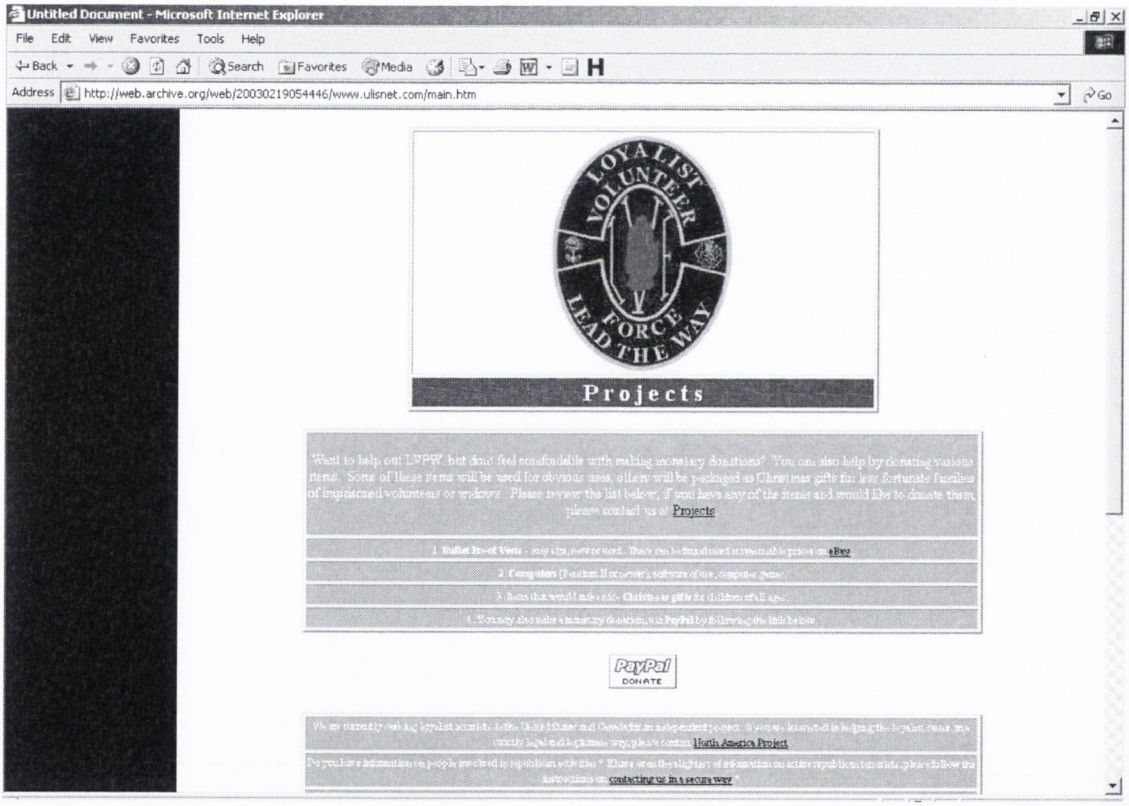
needs to generate large amounts of money in order to support a large and relatively expensive infrastructure. In contrast some paramilitary groups in Northern Ireland have financial requirements under US$ 1 million per annum. The September 11 attacks have been estimated as costing less than US$500,000" (Hinnen 2004, 8; Noble 2003).

[82] For example, the Internet provided a channel, not just for the American public, but publics worldwide, to reach out financially to those affected by the events of 9-11. The day before the attacks, the American Red Cross's Web site had 20, 959 visitors and gathered $1,024. On the day of the attacks, the number of visitors skyrocketed to 243,974 with people making contributions at the rate of one per second. More than $1 million was contributed in the space of twelve hours, and the American Red Cross went on to raise $39.5 million in the following seven days. The most the organisation had managed to raise online previously was $2.5 million, in response to the earthquakes in India and Central America earlier in 2001. A number of Internet companies also banded together to raise money for charities aiding victims of the attacks, more than $57 million was raised in the first week alone on the websites of six companies: Amazon.com, AOL Time Warner, Cisco Systems, eBay, Microsoft, and Yahoo.

> As Internet user demographics become clearer and better defined, terrorist groups -- either themselves, or through proxies with plausible deniability -- will be able to target those users who have demonstrated sympathy or sensitivity to certain particular causes or social issues, and solicit private donations from individuals fitting the right 'profile' whenever they desire (2002, 20).

A third way in which groups raise funds is through the establishment of online stores and the sale of items such as books, audio and video tapes, flags, t-shirts, etc.[83]

Figure 3.1 Ulster Loyalist Information Service Web Site (March 2003)



[83] In July 2003, Sinn Féin were forced, under intense pressure from both sides of the Atlantic, to remove a t-shirt bearing the slogan 'Sniper at Work'--referring to the infamous IRA marksman who operated in South Armagh at the height of the conflict in Northern Ireland--from their official Web site's online store. A range of other items remain for sale on the site at http://www.sinnfeinbookshop.com/ including t-shirts bearing the slogan 'IRA: Undefeated Army' and others bearing the Sinn Féin emblem along with the URL of the official Web site.

Exploitation of E-Commerce Tools & Entities

The Internet facilitates terrorist financing in a number of other ways besides direct solicitation via terrorist Web sites. According to Jean-Francois Ricard, one of France's top anti-terrorism investigators, many Islamist terror plots are financed through credit card fraud (Thomas 2003, 117).[84] Imam Samudra, sentenced to death for his part in the Bali bombing of 2002, has published a prison memoir of some 280 pages, which includes a chapter that acts as a primer on 'carding.' US and Indonesian cybercrime experts have described the information contained in the latter as rudimentary: Samudra directs aspiring 'carders' to specific Indonesian-language Web sites that provide instructions and advises learning about hacking by finding mentors through online chats, listing six chat rooms as sources. Samudra's laptop computer revealed an attempt at carding, though it is unclear whether he succeeded in actually raising funds in this manner. "If you succeed at hacking and get into carding, be ready to make more money within three to six hours than the income of a policeman in six months. But don't do it just for the sake of money. Remember, the main duty of Muslims is jihad in the name of God, to raise arms against the infidels, especially now the United States and its allies," Samudra tells his readers (Sipress 2004, A19).[85] He is thought to be among the most experienced IT users in Jemaah Islamiah.

According to Dutch experts, there is strong evidence from international law enforcement agencies such as the FBI that at least some terrorist groups are financing their activities via advanced fee fraud, such as Nigerian-style scam e-mails. To date, however, solid evidence for such claims has not entered the public realm (Libbenga

---

[84] In the wake of the 9/11 attacks, the American Red Cross (ARC) warned Internet users to beware of a credit-card-stealing Trojan horse program that was made to look as though it came from the disaster relief organization. According to the ARC, the fraudulent program arrived as a large executable file in an e-mail attachment that presented a form bearing the Red Cross logo and requesting the users address and credit card details when activated. After a victim completed the form and clicked the 'Donate Now' button, the data was uploaded to a third party site unaffiliated with the ARC. This is not to suggest that the perpetrators of this fraud were terrorists or in any way associated with a terrorist group The ARC warning is available at http://www.redcross.org/press/other/ot_pr/011018virus.html.

[85] In 2000, five individuals associated with Hizbollah were charged in the US with obtaining a false drivers license that was used to submit fraudulent credit card applications. One individual used various aliases to obtain additional fraudulent credit cards while another bribed an employee of First Union National Bank to reactivate a closed account of an individual who had left the U.S. to execute a check fraud scheme (Emerson 2002, 18).

2004b). There is ample evidence, however, to support the contention that terrorist-affiliated entities and individuals have established Internet-related front businesses as a means of raising money to support their activities.[86] For example, in December 2002, InfoCom, a Texas-based ISP, was indicted along with its individual corporate officers on thirty-three counts relating to its provision of communication services, in-kind support, and funds to terrorist organizations including Hamas and its affiliate the Holy Land Foundation for Relief and Development (HLFRD). InfoCom's capital was donated primarily by Nadia Elashi Marzook, wife of Hamas figurehead Mousa Abu Marzook (Hinnen 2004, 18; see also Emerson 2002, 11-12 & 16). In March 2000, Japan's Metropolitan Police Department reported that a software system they had procured to track 150 police vehicles, including unmarked cars, had been developed by Aum Shinryko. The Aum cult gassed the Tokyo subway in 1995, killing twelve people and injuring 6,000 more. In addition to the difficulties inherent in the Japanese police 'financing' a terrorist group in this fashion, at the time of the discovery, the cult had received classified tracking data on 115 police vehicles. The cult had also developed software for at least eighty Japanese companies and ten government agencies and had worked as subcontractors for other firms. Dorothy Denning (2001a) points out that the cult could have installed Trojan horses[87] in software to launch or facilitate cyber attacks at a later date.

Exploitation of Charities and Fronts

Terrorist organizations have a history of exploiting not just businesses, but also charities as undercover fundraising vehicles. This is particularly popular with Islamist terrorist groups, probably because of the injunction that observant Muslims make regular charitable donations. In some cases, terrorist organizations have actually established charities with allegedly humanitarian purposes. Examples of such undertakings include Mercy International, Wafa al-Igatha al-Islamiya, Rabita Trust, Al

[86] IT businesses may also be terrorist targets, however. For example, India's IT software and services outsourcing industry is thought to be a possible target of Lashkar-e-Tayyiba (LeT). Documents seized from three members of this groups killed in an encounter with Indian police in March 2005 revealed that LeT planned to carry out suicide attacks on software companies in Bangalore (Ribeiro 2005).

[87] A Trojan horse is a destructive program that masquerades as a benign application.

Rasheed Trust, Global Relief Fund, Benevolence International Foundation, and Help The Needy. Along with advertising in sympathetic communities' press, these 'charities' also advertised on websites and chat rooms with Islamic themes, pointing interested parties to their Internet homepages.

For example, Al-Rashid Trust, a Pakistan based, al-Qaeda affiliated charity described itself as "[a] prestigious welfare organization whose comprehensive services are benefiting all the Muslims of the world." The Trust's website solicited donors with an impressive list of humanitarian accomplishments and a promise that "[m]ore attention shall be given to the departments of health, food, education, and employment."[88] Days after 9/11, however, President Bush signed an executive order identifying the Trust as a financial conduit for the Taliban and al-Qaeda and freezing its U.S. assets. In fact, visitors to the former Taliban Web site were greeted with a sleek pop-up appeal to donate to Al-Rashid.[89] The appeal was directed at Taliban supporters in the UK and the US, listing two wire account numbers in Pakistan: one for dollars and one for pounds-sterling (Emerson 2002, 23). The Benevolence International Fund (BIF) provides another example of how terrorists can simultaneously raise funds and avoid scrutiny by obtaining charitable status. In 1993, the United States Internal Revenue Service (IRS) granted BIF tax-exempt status under 26 U.S.C. § 501(c)(3) (2000). In the 1990s, BIF raised millions of dollars, in part by accepting donations on its website.[90] The US authorities have uncovered evidence that BIF transferred money to al-Qaeda, and the US Treasury Department has listed BIF as a financier of terrorism. In October 2002, BIF's leader, Enaam Arnaout, was indicted for, among other things, providing material support to terrorist organizations, including al-Qaeda. In 2003, Arnaout pled guilty to lesser charges involving diversion of charitable contributions to groups in Bosnia and Chechnya engaged in political violence (Hinnen 2004, 16-17; Weimann 2004a, 8).

---

[88] This site is no longer operational. However, the relevant page may be accessed via the Internet Archive at http://web.archive.org/web/20030608204207/http://www.ummah.net.pk/dharb/services.htm.

[89] The Taliban Web site at http://www.dharb-i-mumin.com is no longer operational, but may be accessed via the Internet Archive.

[90] http://www.benevolence.org. It should be noted that this URL appears to have changed hands some time between April and July 2003 and appears to no longer be associated with BIF.

Terrorists have also infiltrated branches of existing charities to raise funds clandestinely. Many such organizations provide the humanitarian services advertised: feeding, clothing, and educating the poor and illiterate, and providing medical care for the sick. As Todd Hinnen has pointed out, "it is important not to presume that charitable organizations have terrorist affiliations simply because they serve regions or religious or ideological communities with which terrorism may be associated" (2004, 17; see also Emerson 2002, 3). For example, Rachel Ehrenfeld (2004) and others (see, for example, Emerson 2002, 25) have claimed that the most active Hamas front organization worldwide is the London-based Palestinians Relief and Development Fund (Interpal). [91] In 2003 alone, according to Ehrenfeld, this organization sent more than $20 million to different Hamas organizations in the Palestinian territories.[92] Recently, however, the UK's Charity Commission has cleared this charity of any wrongdoing (UK Charity Commission 2004). As a result, Interpal's trustees have said that they will now seek to have their organization removed from the US Treasury Department's list of terror organizations. Nonetheless, some such organizations, in addition to pursuing their publicly stated mission of providing humanitarian aid, also pursue a covert agenda of providing material support to militant groups. These organizations' publicity materials may or may not provide hints as to their secret purposes.

The Qatar Charitable Society (QCS) provides an example of how a terrorist organization can infiltrate a legitimate charity and exploit its supporters. At the trial of the conspirators who planned the bombings of the U.S. Embassies in Kenya and Tanzania, a former al-Qaeda member and QCS employee identified QCS as an al-Qaeda front and a financial conduit for militant jihadists around the globe. The mission statement on its website did not indicate any such activity: "QCS aims to offer relief and help to orphans, victims of war and disasters by supporting them financially, socially and culturally up to the age of 18. QCS aids widows to meet living expenses particularly those who lost all relatives and friends" (Emerson 2002, 9-11; Fritz, Harris

[91] http://www.interpal.org/index.html.
[92] According to the UK Charity Commission, Interpal's income for 2001 was around £4 million.

et al 2004, 14; Hinnen 2004, 17-18).[93] Terrorist exploitation of such charities ought to be of particular concern to US authorities because they operate under tax-exempt status in the United States. This has meant that the U.S. government, and thus all U.S. taxpayers, has indirectly financed organizations that actively fund terrorist activities abroad (Emerson 2002, 4; Herzfeld 2003, 875).[94]

Internet Banking

Todd Hinnen identifies and describes three primary ways in which terrorists may use the Internet to transfer funds. First, they use Internet banks, online banking, and other financial services. Second, they use Internet-based alternative value transfer systems, such as Internet payment services and so-called 'ecash.' Third, terrorists may communicate over the Internet regarding the movement of funds (2004, 27-35). Terrorist use of online banking services is facilitated in part by banks that have links to terrorist groups. Hinnen cites the example of Al-Taqwa Bank, founded by the Muslim Brotherhood in the Bahamas in 1988, which maintained branches in Algeria, Liechtenstein, Italy, Malta, Panama, and Switzerland, and provided banking services to al-Qaeda and Hamas until it was shut down by sanctions in the wake of 9/11. Similarly, Hamas established Al-Aqsa Bank in 1997 (2004, 28; see also Emerson 2002, 19-22).

As the LVF and InfoCom examples show, the support sought by and provided to terrorist organizations may not always be in the form of cash. Terrorist groups use the Internet to solicit other fungible goods, to accumulate supplies, and to recruit foot soldiers. According to Todd Hinnen, "[t]errorists have used identities they have stolen

---

[93] The QCS's Web site at http://www.qcharity.org is no longer operational, but may be accessed via the Internet Archive. The above quotation is available at http://web.archive.org/web/20010224172507/qcharity.org/qenglish/index.html.

[94] The same is true in Britain. According to the UK Charity Commission, it "is alert to the possibilities of charities being used to further or support terrorist activities [and] will deal with any allegation of potential links between a charity and terrorist activity as an immediate priority...The Commission's own work reveals that connections or links between registered charities in England and Wales and terrorist organizations are very rare. However, any links between charities and terrorist activity are totally unacceptable and corrosive of public confidence in charities. 'Links' in this case might include fundraising or provision of facilities, but also include formal or informal links to organizations 'proscribed' under the Terrorism Act 2000, and any subsequent secondary legislation" (Charity Commission 2004).

through online fraud schemes to obtain cover employment within the United States, access to bank and credit card accounts, and even entry into secure locations" (2004, 22). In this chapter, however, the term 'financing' has been used in its narrow sense to mean the remittance of money. Nonetheless, it may also be used as shorthand for the accumulation of any of the material resources necessary for terrorists to maintain their organizations and carry out operations.

Networking

This refers to groups' efforts to flatten their organizational structures and act in a more decentralized manner through the use of the Internet, which allows dispersed actors to communicate quickly and coordinate effectively at low cost. The Internet allows not only for intra-group communication, but also inter-group connections. The Web enhances terrorists' capacities to transform their structures and build these links because of the alternative space it provides for communication and discussion and the hypertext nature of the Web, which allows for groups to link to their internal sub-groups and external organizations around the globe from their central Web site.

Transforming Organizational Structures[95]

Violent dissidents can overcome state barriers to Internet use by adjusting organizationally. Faced with centrally organized state apparatuses, terrorist groups may move towards more networked forms of organization. These networked forms of organization offer terrorist groups advantages over the hierarchical structure of states. The horizontal structures associated with networked organizations make it more difficult for centrally organized states to counter terrorist activities. The networked structure of the Internet is an important enabler in becoming increasingly networked. The international scope of the Internet allows violent actors to network themselves on a global scale, which allows them to conduct operations outside the sovereign territory of

[95] For a brief introduction to organizational network analysis, see Arquilla & Ronfeldt 2001c & 2001d, 319-323.

certain states. The organizational changes wrought by the Internet are particularly potent for terrorists as it allows these groups to operate transnationally and thus overcome the constraints of internal censorship and infrastructure limitations prevalent in some regions (McLaughlin 2003, 11).

Rand's John Arquilla, David Ronfeldt, and Michele Zanini have been pointing to the emergence of new forms of terrorist organization attuned to the information age for some time. They contend, "terrorists will continue to move from hierarchical toward information-age network designs. More effort will go into building arrays of transnationally internetted groups than into building stand alone groups" (Arquilla *et al* 1999, 41). This type of organizational structure is qualitatively different from traditional hierarchical designs. Terrorists are ever more likely to be organized to act in a more fully networked, decentralized, 'all-channel' manner. Ideally, there is no single, central leadership, command, or headquarters. Within the network as a whole there is little or no hierarchy and there may be multiple leaders depending upon the size of the group. In other words, there is no specific heart or head that can be targeted. To realize its potential, such a network must utilize the latest information and communications technologies. The Internet is becoming an integral component of such organizations, according to the Rand analysts (Arquilla *et al* 1999, 48-53; Arquilla & Ronfeldt 2001a).[96]

Arquilla, Ronfeldt, and Zanini have also pointed to the way in which difficulties coping with terrorism will increase if terrorists move beyond isolated attacks towards new approaches that emphasize campaigns based on swarming. They point out that while little analytic attention has been paid to swarming, it is likely to be a key mode of

---

[96] The militias or patriot movement in the United States are known to have adopted inter-networked forms of organization similar to those outlined above. While the anonymity of the Internet is seen as fuelling the conspiracies of the militias, for the groups themselves access to such new technologies is seen as a vital tool for recruitment and funding (in a similar way to terrorist organizations). The Internet has enabled the militias to spread their ideas worldwide. There are militias in Australia and Canada, and it has been suggested that the Far Right in Europe has adopted the idea of 'leaderless resistance' via the Internet (Mulloy 1999, 16). Activists within the patriot movement have repeatedly urged their compatriots, not only to organize themselves along networked lines, however, but also to opt out of other more pervasive networks that are viewed as dangerously perceptible to attack: "We need to set up our own cashless societies, our own barter networks, and unhook from the grid, to become self-sufficient, away from the power company, the gas company, and the water company" (Mulloy 1999, 324; see also Arquilla & Ronfeldt, 2001a). At the same time that the militias are unhooking from the grid, however, it is asserted that terrorist groups are more networked than ever before.

conflict in the information age (Arquilla *et al* 1999, 41; see also Zanini 1999, 250). In their *Countering the New Terrorism* (1999), Arquilla *et al* describe this new technique thus:

> Swarming occurs when the dispersed nodes of a network of small (and perhaps some large) forces converge on a target from multiple directions. The overall aim is the sustainable pulsing of force or fire. Once in motion, swarm networks must be able to coalesce rapidly and stealthily on a target, then dissever and redisperse, immediately ready to recombine for a new pulse. In other words, information age attacks may come in 'swarms' rather than the more traditional 'waves' (pp.'s 53-54).

This device points to the adaptable, flexible, and versatile nature of offensive networks with regard to opportunities and challenges. The fact that the 9-11 hijackers employed a technique similar to the one described above has given the Rand analysts' work a far higher profile than might otherwise have been expected.

Planning and Coordination

"[The] proliferation of cheap, dual-use software allows entities with otherwise modest means to conduct command and control globally, in real time, and with considerable security" (Tibbetts 2002, 6). As early as 1996, Manuel Castells, pointed out that due to such proliferation networks were spreading and gaining in strength as a distinct form of organization:

> Our exploration of emergent social structures across domains of human activity and experience leads to an overarching conclusion: as a historical trend, dominant functions and processes in the information age are increasingly organized around networks. Networks constitute the new social morphology of our societies...While the networking form of social organization has existed in other times and spaces, the new information technology paradigm provides the

material basis for its pervasive expansion throughout the entire social structure (p. 469).

"Many terrorist groups share a common goal with mainstream organizations and institutions: the search for greater efficiency through the Internet" (Margulies 2004, 2). Several reasons have been put forward to explain why modern IT systems, especially the Internet, are so useful for terrorists in establishing and maintaining networks. As already discussed, new technologies enable quicker, cheaper, and more secure information flows. In addition, the integration of computing with communications has substantially increased the variety and complexity of the information that can be shared (Weimann 2004a, 9).

This led Michele Zanini to hypothesize that "the greater the degree of organizational networking in a terrorist group, the higher the likelihood that IT is used to support the network's decision making" (1999, 251). Zanini's hypothesis appears to be borne out by recent events. For example, many of the terrorists indicted by the United States government since 9/11 communicated via e-mail. The indictment of four members of the Armed Islamic Group (Gama'a al-Islamiyya) alleges that computers were used "to transmit, pass and disseminate messages, communications and information between and among IG leaders and members in the United States and elsewhere around the world."[97] Similarly, six individuals indicted in Oregon in 2002 allegedly communicated via e-mail regarding their efforts to travel to Afghanistan to aid al-Qaeda and the Taliban in their fight against the United States.[98] In addition, Mukhtar al-Bakri, indicted in 2002 for training with al-Qaeda with a view to carrying out attacks against the United States, allegedly e-mailed his co-conspirators to discuss and plan acts of terrorism;[99] while four members of a Colombian terrorist organization,

[97] Indictment, United States v. Sattar, No. 02-CRIM-395, 11 (S.D.N.Y Apr. 9, 2002). Available online at http://news.findlaw.com/hdocs/docs/terrorism/ussattar040902ind.pdf.
[98] Indictment, United States v. Battle, No. CR 02-399 HA, 5 (D.Or. Oct. 2, 2002). Available online at http://news.findlaw.com/hdocs/docs/terrorism/usbattle100302ind.pdf.
[99] Criminal Complaint, United States v. Al-Bakri, No. 02-M-108, 8 (W.D.N.Y. Sept. 13, 2002). Available online at http://news.findlaw.com/hdocs/docs/terrorism/usal-bakri091302cmp.pdf.

the United Self-Defense Forces of Colombia (AUC), indicted in November 2002, allegedly used e-mail to broker a guns-for-drugs deal[100] (Hinnen 2004, 38).

The Internet has the ability to connect not only members of the same terrorist organizations but also members of different groups. For example, hundreds of so-called 'jihadist' sites exist that express support for terrorism. According to Weimann, these sites and related forums permit terrorists in places as far-flung as Chechnya, Palestine, Indonesia, Afghanistan, Turkey, Iraq, Malaysia, the Philippines, and Lebanon to exchange not only ideas and suggestions, but also practical information about how to build bombs, establish terror cells, and ultimately perpetrate attacks (2004a, 9). Complementing this notion of simultaneity is the Internet's facilitation of asynchronous interactions: visitors to a Web site need not communicate in real-time; instead they can send messages that will be read and responded to at the convenience of other users, but without the transmission delays of older communication modes like 'snail mail.' The Internet also facilitates the automatic, increasingly sophisticated, and user-accessible archiving of material--including site updates and new forum posts--awaiting the visitor's attention. The temporal versatility of the Internet, in conjunction with its geographic reach, is thus another enabling factor for networked groups (Margulies 2004, 37).

Mitigation of Risk

As terrorist groups come under increasing pressure from law enforcement, they have been forced to evolve and become more decentralized. This is a structure to which the Internet is perfectly suited. The Net offers a way for like-minded people located in different communities to interact easily, which is particularly important when operatives may be isolated and having to 'lie low.' Denied a physical place to meet and organize, many terrorist groups are alleged to have created virtual communities through chat rooms and Web sites in order to continue spreading their propaganda, teaching, and training. Clearly, "information technology gives terrorist organizations global

[100] Criminal Complaint, United States v. Varela, No. H-02-1008M, 9-10 (S.D.Tex. Nov. 1, 2002). Available online at http://news.findlaw.com/hdocs/docs/terrorism/usromero110102cmp.pdf.

power and reach without necessarily compromising their invisibility" (Tibbetts 2002, 5). Timothy L. Thomas contributes the following re. risk mitigation and terrorist use of the Internet:

> *The Internet puts distance between those planning the attack and their targets.* Terrorists planning attacks on the United States can do so abroad with limited risk, especially if their command and control sites are located in countries other than their own. Tracing the route of their activity is particularly difficult. The Net provides terrorists a place to plan without the risks normally associated with cell or satellite phones [italics in original] (2003, 119).

Clearly, the issue of risk mitigation is closely associated with that of secure communication.

Secure Communication

Secure communications are of utmost importance to terrorist groups and their operatives. The capacity to communicate securely is also an enabler of networked forms of organization. The use of e-mail by terrorists has already been mentioned in this section. Swapping plaintext e-mails is not a very secure form of communication in and of itself; however, there are a number of tools available via the Internet that enable secure communications. According to Michael Whine, numerous Islamist Web sites provide password-protected areas on their sites accessible only to members and known sympathizers. Whine provides the example of the United Islamic Students Association in Europe, which maintained a members only site. This level of secrecy, Whine suggests, may indicate that instructions for militant activity were included on the site (1999, 234).[101] Other, more technologically sophisticated, fixes are also available to ensure Internet communications remain secure. The use of cryptography and, in

[101] The site at http://www.tawheed.org is no longer operational nor are its previous contents accessible via the Internet Archive.

particular, steganography by terrorist groups has received massive amounts of media attention since 9/11. Chapter Four discusses terrorist use of such applications at length.

Recruitment

This refers to groups' efforts to recruit and mobilize sympathizers to more actively support terrorist causes or activities. The Web offers a number of ways for achieving this: it makes information gathering easier for potential recruits by offering more information, more quickly, and in multimedia format; the global reach of the Web allows groups to publicize events to more people; and by increasing the possibilities for interactive communication, new opportunities for assisting groups are offered, along with more chances for contacting the group directly. Finally, through the use of discussion forums, it is also possible for members of the public--whether supporters or detractors of a group--to engage in debate with one another. This may assist the terrorist group in adjusting their position and tactics and, potentially, increasing their levels of support and general appeal (Gibson & Ward 2000, 305-306; Soo Hoo, Goodman & Greenberg 1997, 140; Weimann 2004a, 8).

Online recruitment by terrorist organizations is said to be widespread. As Kathryn Fritz and her colleagues point out, such recruitment is

> ...often conducted in a manner similar to that of any other business. For example, both groups use their websites to present themselves in a way that encourages 'applicants' to choose their organization over that of a rival...Well-designed sites allow potential applicants to peruse mission statements, as well as testimonials from current (and sometimes 'former') 'employees' (often with photographs), thereby providing the data necessary for the applicant to make an informed decision. In addition, applicants can link to contact information (designed for both the applicant and the general public), scan the 'about us' and 'what's new' sections to see how active the organization has been in recent events, download multimedia, and purchase items from the online store. Online forms streamline the application process. (Fritz, Harris *et al* 2004, 7).

Harris *et al* provide the example of an Iranian site that boasts an application for suicide bombers guaranteeing that the new 'martyr' will take seventy relatives with him into heaven. If the recruit is unsure about joining, or if the group is unsure about the recruit, he is directed to a chat room where he is 'virtually' vetted. If he passes muster, he will be directed to another chat room for further vetting, and finally contacted personally by a group member. This process is said to be aimed at weeding out 'undesirables' and potential infiltrators (2004, 9).

It is more typical, however, for terrorist groups to actively solicit for recruits rather than waiting for them to simply present themselves. Weimann suggests that terrorist recruiters may use interactive Internet technology to roam online chat rooms looking for receptive members of the public, particularly young people. Electronic bulletin boards could also serve as vehicles for reaching out to potential recruits. The SITE Institute, a Washington, D.C.-based terrorism research group that monitors al Qaeda's Internet communications, provides details of a high-tech recruitment drive launched in 2003 to recruit fighters to travel to Iraq in order to attack U.S. and coalition forces there. Potential recruits were allegedly bombarded with religious decrees and anti-American propaganda, provided with training manuals on how to be a terrorist, and--as they were led through a maze of secret Internet chat rooms--given detailed instructions on how to make the journey to Iraq. Weimann details one exchange in a secret Al Qaeda chat room in early September 2003 where an unknown Islamic fanatic (alias 'Redemption Is Close') wrote "Brothers, how do I go to Iraq for Jihad? Are there any army camps and is there someone who commands there?" Four days later he received a reply from 'Merciless Terrorist': "Dear Brother, the road is wide open for you--there are many groups, go look for someone you trust, join him, he will be the protector of the Iraqi regions and with the help of Allah you will become one of the Mujahidin." 'Redemption Is Close' then presses for more specific information on how he can wage jihad in Iraq. 'Merciless Terrorist' sends him a propaganda video and instructs him to download software called Pal Talk, which enables users to speak securely over the Internet (2004a, 8).

Violent political actors have a history of seeking to recruit online. Right wing extremists, in particular, have been known to use the Internet to attract 'more

sophisticated' recruits (Stern 1999, 150). The late William Pierce, a physicist and former leader of the US neo-Nazi group National Alliance, also authored *The Turner Diaries*, a novel in which a group of right-wing extremists use CBRN weapons to take over the world.[102] Pierce believed that he could attract more intelligent members to the Alliance over the Internet than over the radio or through distributing leaflets. According to Jessica Stern, he explicitly attempted to recruit military personnel, presumably because they have access to higher technology weapons than would ordinarily be available to the public (1999, 74). Other population segments targeted for recruitment by terrorist groups include women and children. Details about the way in which the Internet has been utilized in the recruitment of these is detailed in Chapter Six. For now it is sufficient to observe, "terrorists are tech-savvy enough to take advantage of the computer (and by extension, the Internet) as the 'great equalizer.' Disenfranchised youth around the world are flocking to sites that offer the opportunity to become involved in [your cause here]" (Fritz, Harris *et al* 2004, 9).

In a twist on the recruitment angle, Dan Verton details how a would-be terrorist used the Internet to in effect 'advertise' himself to interested groups. In 1995, Ziyad Khalil enrolled as a computer science major at Columbia College in Missouri. According to Verton, Khalil became a Muslim activist on the campus, developing links to several radical groups and operating a website that supported Hamas. Thanks in large part to his Internet activities; he came to the attention of bin Laden and his lieutenants ultimately becoming al Qaeda's procurement officer in the United States. Khalil arranged the purchase of satellite telephones, computers, and other electronic surveillance technologies and helped bin Laden communicate with his followers and operatives (Verton 2003, 88-91; Weimann 2004a, 8).

Information Gathering

This refers to the capacity of Internet users to access huge volumes of information, which was previously extremely difficult to retrieve as a result of its being stored in widely differing formats and locations. Today, there are literally hundreds of Internet

[102] His *nom de plume* was Andrew Macdonald.

tools--many of them available for download from the Net at no charge--that aid in information gathering; these include a range of search engines, millions of subject-specific email distribution lists, and an almost limitless selection of esoteric chat and discussion groups. Indeed, so vast are many of these information repositories that a growing number of Web sites offer customized search tools for extracting information from databases on their sites. In 1999, Jessica Stern observed that "right-wing extremists and other groups are using the Internet not just to attract 'more sophisticated' recruits but also discuss grand strategy, 'swap anthrax recipes,' and plan operations. Some foreign extremist groups with representatives in the United States are also using the Internet" (p.150). One of the major uses of the Internet by terrorist organizations is thought to be information gathering. Unlike the other uses mentioned above terrorists' information gathering activities rely not on the operation of their own Web sites, but on the information contributed by others to "the vast digital library" that is the Internet (Weimann 2004a, 6). There are two major issues to be addressed here. The first is termed 'data mining' and refers to terrorists using the Internet to collect and assemble information about specific targeting opportunities.[103] The second issue is 'information sharing,' which refers to more general online information collection by terrorists.

Data Mining

In January 2003, US Defence Secretary Donald Rumsfeld warned in a directive sent to military units that too much unclassified, but potentially harmful material was appearing on Department of Defence (DoD) Web sites. Rumsfeld reminded military personnel that an al-Qaeda training manual recovered in Afghanistan states: "Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty percent of information about the enemy." He went on to say, "at more than 700 gigabytes, the DoD Web-based data makes a vast, readily available source of

[103] Others exploring terrorist use of the Net have employed the term 'data mining' in a less expansive fashion to refer to the systematized analysis of large bodies of data using specialist computer software (see Denning 2004; Fritz et al 2004, 26-32). For an introduction to the latter, see De Rosa 2004; Two Crows 1999. Two companies that advocate the adoption of data mining techniques to explore the relationship between terrorism and the Internet are Decision Support Systems Inc (http://www.metatempo.com) and 7-Seas Global Intelligence (http://www.7-seas.net).

information on DoD plans, programs and activities. One must conclude our enemies access DoD Web sites on a regular basis" (McCullagh 2003).

In addition to information provided by and about the armed forces, the free availability of information on the Internet about the location and operation of nuclear reactors and related facilities was of particular concern to public officials post 9/11. Roy Zimmerman, director of the Nuclear Regulatory Commission's (NRC) Office of Nuclear Security and Incident Response, said the 9/11 attacks highlighted the need to safeguard sensitive information. In the days immediately after the attacks, the NRC took their Web site entirely off line. When it was restored weeks later, it had been purged of more than 1,000 sensitive documents. Initially, the agency decided to withhold documents if "the release would provide clear and significant benefit to a terrorist in planning an attack." Later, the NRC tightened the restriction, opting to exclude information "that could be useful or could reasonably be useful to a terrorist." According to Zimmerman, "it is currently unlikely that the information on our Web site would provide significant advantage to assist a terrorist" (Ahlers 2004).

The measures taken by the NRC were not exceptional. According to a report produced by OMB Watch,[104] since 9/11 thousands of documents and tremendous amounts of data have been removed from US government sites. The difficulty, however, is that much of the same information remains available on private sector Web sites (McCullagh 2003; Bass & Moulton 2002). Patrick Tibbetts points to the Animated Software Company's Web site which has off-topic documents containing locations, status, security procedures and other technical information concerning dozens of U.S. nuclear reactors,[105] while the Virtual Nuclear Tourist site contains similar information. The latter site is particularly detailed on specific security measures that may be implemented at various nuclear plants worldwide[106] (Tibbetts 2002, 15).

Also, freely available on the Net are 3-D models of the exterior and limited portions of the interior of the Citigroup Inc. headquarters building in Manhattan, along with details of the building's history of structural design weaknesses, including its

---

[104] Office of Management and Budget (OMB) Watch is a watchdog group based in Washington DC. Their home page is at http://www.ombwatch.org.

[105] See http://www.animatedsoftware.com/environm/no_nukes/nukelist1.htm.

[106] See http://www.nucleartourist.com/.

susceptibility to toppling over in high winds, the construction of its central support column, and the fire rating of the materials used in the building. The Citigroup building is one of the sites specifically named in the August 2004 terror advisory issued by the US Department of Homeland Security.

Many people view such information as a potential gold mine for terrorists.[107] Their fears appear well founded given the capture of al-Qaeda computer expert Muhammad Naeem Noor Khan in Pakistan in July 2004, which yielded a computer filled with photographs and floor diagrams of buildings in the U.S. that terrorists may have been planning to attack (Jehl & Johnston 2004; Verton & Mearian 2004). The Australian press has also reported that a man charged with terrorism offences there had used Australian government Web sites to get maps, data, and satellite images of potential targets. The government of New South Wales was said to be considering restricting the range of information available on their Web sites as a result (ABC 2004).

Terrorists can also use the Internet to learn about antiterrorism measures. Gabriel Weimann suggests that a simple strategy like conducting word searches of online newspapers and journals could allow a terrorist to study the means designed to counter attacks, or the vulnerabilities of these measures. Weimann provides the example of newspaper articles detailing attempts to slip contraband items through airport security. He mentions a report, which noted that at Cincinnati airport, contraband slipped through over fifty percent of the time. "A simple Internet search by terrorists would uncover this shortcoming, and offer the terrorists an embarkation point for their next operation" (2004b, 15). A number of authors have also lambasted reports on various online news sites which noted that US law enforcement agencies were tracing calls made overseas to Al Qaeda cells using phone cards, cell phones, phone booths, or Internet-based phone services. These authors were concerned that exposing the targeting techniques of law enforcement agencies would allow the terrorists to alter

[107] See Chapter Six of Dan Verton's *Black Ice* (2003), which is entitled 'Web of Terror: What al-Qaeda Knows About the US.' The chapter provides a wide-ranging, though somewhat breathless, survey of the potential dangers posed by Web-based information. At one point, for example, Verton observes: "many corporate Web sites contain messages supporting globalization. Unfortunately, this is a particular message that has been known to stimulate portions of the al-Qaeda organization and could make these companies a potential target" (p.121).

their operating procedures accordingly (Andrew 2001, 2-3; Thomas 2003, 114; Weimann 2004b, 15).

Sharing Information

Policymakers, law enforcement agencies, and others are also concerned about the proliferation of 'how to' Web pages devoted to explaining, for example, the technical intricacies of making homemade bombs. Many such devices may be constructed using lethal combinations of otherwise innocuous materials; today, there are hundreds of freely available online manuals containing such information. As early as April 1997, the US Department of Justice had concluded that the availability of this information played a significant role in facilitating terrorist and other criminal acts:

> It is readily apparent from our cursory examination that anyone interested in manufacturing a bomb, dangerous weapon or weapon of mass destruction can easily obtain detailed instructions for fabricating and using such a device. Available sources include not only publications from the so called underground press but also manuals written for legitimate purposes, such as military, agricultural, industrial and engineering purposes. Such information is *also readily available to anyone with access to a home computer equipped with a modem* [italics mine] (US Department of Justice 1997, 15-16).

Jessica Stern provides details of one such manual, *Bacteriological Warfare: A Major Threat to North America* (1995), which is described on the Internet as a book for helping readers survive a biological weapons attack and is subtitled 'What Your Family Can Do Before and After.' However, it also describes the reproduction and growth of biological agents and includes a chapter entitled 'Bacteria Likely To Be Used By the Terrorist.' The text is available for download, in various edited and condensed formats, from a number of sites [108] while hard copies of the book are available for purchase over the Internet from sites such as Barnesandnoble.com for as little as $13. Its author is one

[108] See, for example, http://www.uhuh.com/reports/harris/book.htm.

Larry Wayne Harris, a microbiologist and former neo-Nazi, who at one time purchased three vials of the bacterium that causes bubonic plague (Stern 1999, 51).

More recently, an Al Qaeda laptop found in Afghanistan had been used to visit the Web site of the French Anonymous Society (FAS) on several occasions. The FAS site publishes a two-volume *Sabotage Handbook* that contains sections on planning an assassination and anti-surveillance methods amongst others (Thomas 2003, 115; Weimann 2004a, 9).[109] Another manual, *The Mujahadeen Poisons Handbook* (1996), authored by Abdel-Aziz is available via the Hamas-Palestinian Information Center's Arabic-language Web site. The 'handbook' details in twenty-three pages how to prepare various homemade poisons, poisonous gases, and other deadly materials for use in terrorist attacks. A much larger manual, nicknamed *The Encyclopedia of Jihad* and prepared by al Qaeda, runs to thousands of pages; distributed via the Web, it offers detailed instructions on how to establish an underground organization and execute terror attacks (Weimann 2004a, 9; see also Smolla 2002). Further, BBC News reported that at least one jihadist Web site posted careful instructions on how to use mobile phones as detonators for explosives prior to the Madrid train bombings, the perpetrators of which subsequently employed this method of detonation (Corera 2004).

This kind of information is sought out not just by sophisticated terrorist organizations but also by disaffected individuals prepared to use terrorist tactics to advance their idiosyncratic agendas. In 1999, for instance, right-wing extremist David Copeland planted nail bombs in three different areas of London: multiracial Brixton, the largely Bangladeshi community of Brick Lane, and the gay quarter in Soho. Over the course of three weeks, he killed three people and injured 139. At his trial, he revealed that he had learned his deadly techniques from the Internet by downloading copies of *The Terrorist's Handbook* and *How to Make Bombs: Book Two.* Both titles are still easily accessible (Weimann 2004a, 10). According to the US Bureau of Alcohol, Tobacco, and Firearms, federal agents investigating at least thirty bombings and four attempted bombings between 1985 and June 1996 recovered bomb-making literature that the suspects had obtained from the Internet. None of these were

[109] The two-volume handbook is available for download from a number of Internet sites including http://sabotage.org/handbook/.

terrorism-related, but many involved minors (ADL 1998). Gabriel Weimann provides the example of a further deadly bomb attack, which occurred in Finland in 2002, and was also carried out by a minor. The brilliant chemistry student, who called himself RC, spent months discussing bomb-making techniques with other enthusiasts on a Finnish Web site devoted to bombs and explosives. RC posted numerous queries on topics like manufacturing nerve gas at home. And he often traded information with the site's moderator, who used the screen name Einstein and whose postings carried a picture of his own face superimposed on Osama bin Laden's body, complete with turban and beard. Then RC exploded a bomb that killed seven people, including himself, in a crowded Finnish shopping mall. The sites sponsor, a computer magazine called *Mikrobitti*, immediately shut down the Web site used by RC, known as the Home Chemistry Forum. However, a backup copy, with postings by teenagers who used aliases like Ice Man and Lord of Fire, was immediately reposted, on a read-only basis (Weimann 2004b, 15).

The Open Source Threat?

The threat posed by the easy availability of bomb-making and other 'dangerous information' is a source of heated debate. Patrick Tibbetts warns against underestimating the feasibility of such threats. He points out that captured Al Qaeda materials include not only information compiled on 'home-grown explosives,' but also indicate that this group are actively pursuing data and technical expertise necessary to pursue CBRN weapons programs. According to Ken Katzman, a terrorism analyst for the Congressional Research Service, much of the material in these captured documents was probably downloaded from the Internet (Tibbetts 2002, 17). As a result, many have called for laws restricting the publication of bomb-making instructions on the Internet, while others have pointed out that this material is already easily accessible in bookstores and libraries (ADL 1998). In fact, much of this information has been available in print media since at least the late 1960s, with the publication of William Powell's *The Anarchist Cookbook* and other, similar titles.

Jessica Stern has observed: "In 1982, the year of the first widely reported incident of tampering with pharmaceuticals, the Tylenol case, only a few poisoning manuals were available, and they were relatively hard to find" (1999, 50). This is doubtless true; they were hard to find, but they *were* available. As Stern herself concedes, currently how-to manuals on producing chemical and biological agents are not just available on the Internet, but are advertised in paramilitary journals sold in magazine shops all over the United States (Stern 1999, 51). According to a US government report, over fifty publications describing the fabrication of explosives and destructive devices are listed in the Library of Congress and are available to any member of the public, as well as being easily available commercially[110] (US Department of Justice 1997, 5). Ken Shirriff sums up this point well:

> Note that *The Anarchist Cookbook* is available from nearly any bookstore in the U.S. These dangerous institutions will also sell you Nazi and hate literature, pornography, instructions on growing drugs, and so forth. For some reason, getting this stuff from a bookstore is not news, but getting it over the Internet is (Shirriff 2001).

Despite assertions to the contrary (Weimann 2004a, 9), the infamous *Anarchist Cookbook* (1971) is not available online, although it is easily purchased from bookstores or from Amazon.com. According to Ken Shirriff, author of 'The Anarchist Cookbook FAQ,' there are various files available on the Internet that rip off the name 'Anarchist Cookbook' and have somewhat similar content, but they are not the real *Anarchist Cookbook*. There are other files that do contain parts of the content from the original *Anarchist Cookbook*, often mixed with other material, but the whole publication unedited and in its entirety is unavailable online. The original author, William Powell, had this to say in 2001:

---

[110] The same report mentions that one Kansas bomber got his bomb instructions from the August 1993 *Reader's Digest* (1997, 6-7).

> The book, in many respects, was a misguided product of my adolescent anger at the prospect of being drafted and sent to Vietnam to fight in a war that I did not believe in. I conducted the research for the manuscript on my own, primarily at the New York City Public Library. Most of the contents were gleaned from Military and Special Forces Manuals (Shirriff 2001).

The anonymous authors of Web sites claiming to post the *Cookbook* and similar texts often include a disclaimer that the processes described should not be carried out. This is because many of the 'recipes' have a poor reputation for reliability and safety. One author had this to say about the contents of *The Mujahideen Poisons Handbook* mentioned above:

> The quality of the text is so poor it would be humorous if it were not attached to a preface which puts on the airs of a sinister man confessing a wish to pass on an esoteric and dangerous technical capability to sympathizers. (Indeed, since the material is shaky it cannot be entirely ruled out that it was fabricated as a hoax or written by a total know-nothing simply wishing to create an impression of menace...) (Smith 2004b).

Smith goes on to point out that at least one of the recipes for poison gas contained in the same handbook was nothing more than the standard procedure for making a stink bomb (see also Smith 2004a).

In terms of obtaining information about the construction of CBRN weapons from the Internet, it is generally agreed that much of this type of information is also flawed, while some is, in fact, pure imagination. Although, some relatively accurate information on the construction of such weapons *is* available online, raw data on such a process is not particularly valuable. Putting together a terrorist operation requires elaborate planning, as demonstrated by the 9/11 hijackers. Organizations with the structure and control over their members required for such planning might also be expected to have the resources for developing and distributing their own proprietary

tactical materials. As, indeed, Al Qaeda has done.[111] However, even when a terrorist outfit draws inspiration and data from materials published on the Internet, these materials often duplicate other materials already available in other public fora. In addition, while on the surface information about scientific processes may be more technical than information regarding terrorist tactics, the same analysis ultimately applies. Actually utilizing a formula for poison gas or a nuclear device, for example, requires not only the cultivation of a body of knowledge and professional judgment, but also the financial resources to build and maintain a physical plant for the manufacture and distribution of the weapon. Developing the expertise and the infrastructure to exploit the information gathered thus demands a significant investment of time and money. Individuals with sufficient skills and resources to exploit the information are unlikely to need the published formula to carry out their plans. Similarly, persons lacking such expertise cannot benefit from the information even when it is published on the Internet or elsewhere. The upshot of this is that attempts to stop the flow of 'harmful' information have no useful purpose and would doubtless inspire, what Peter Margulies has termed, "an endless virtual fun-house of mirror sites" in any case (2004, 74-76).

Perhaps the most likely 'recipes' to be of use to terrorists are those related to hacking tools and activities. Such information is also likely to be considerably more accurate than bomb making information, for example; this is because the Internet is both the domain and tool of hackers. In testimony before the US House Armed Services Committee in 2003, Purdue University professor and information assurance expert, Eugene Spafford said bulletin boards and discussion lists teach hacking techniques to anyone: "We have perhaps a virtual worldwide training camp," he testified (Spafford 2003, 31). Terrorists have been known to exploit this resource. Imam Samudra's instructions regarding the use of chat rooms favored by hackers to obtain information about 'carding' have already been mentioned. In 1998, Khalid Ibrahim, who identified himself as an Indian national, sought classified and unclassified US government software and information, as well as data from India's Bhabha Atomic Research Center,

[111] Portions of an Al Qaeda Training Manual are available via the US Department of Justice's Web site at http://www.usdoj.gov/ag/trainingmanual.htm.

from hackers communicating via Internet Relay Chat (IRC).[112] Using the online aliases RahulB and Rama3456, Ibrahim began frequenting online cracker hangouts in June 1998. In conversations taken from IRC logs, Ibrahim claimed to be a member of Harkat-ul-Ansar,[113] a militant Kashmiri separatist group. Confirming Ibrahim's true identity was difficult; the most compelling evidence that he was acting on behalf of Harkat-ul-Ansar was a US$1,000 money order he sent to a teenage hacker in the US in an attempt to buy stolen military software. Although he used several anonymous Hotmail accounts to send his emails, Ibrahim always accessed the Net from an Internet service provider in New Delhi. He approached members of various cracking teams, including the Masters of Downloading, the Noid, and Milw0rm, looking for sensitive information. Members of the cracking group Noid said that Ibrahim asked them for help gaining access to the SIPRNET, the Pentagon's secure Internet protocol network used for the exchange of classified information and email by the military and intelligence communities. In one transcript of an Internet chat conversation between Ibrahim and crackers, Ibrahim threatens to have the youths killed if they reported him to the FBI. In the event, it appears that almost all of Ibrahim's efforts to buy information were rebuffed (McKay 1998b).

Finally, it is important to keep in mind that removal of technical information from public Web sites is no guarantee of safeguarding it. In essence, this effort is akin to 'closing the barn door after the horse has bolted.' Intelligence and technical data obtained by terrorist operatives prior to 9/11 can be archived, stored and distributed surreptitiously irrespective of government or private attempts to squelch its presence on the Internet in 2005. Indeed, these materials can be loaded onto offshore or other international Web servers that cannot be affected by US legislation, rendering any attempt to halt their spread outside the reach of American law enforcement (Tibbetts 2002, 17). This point is made in a recent Rand report whose authors believe that the threat posed by open source data is small. The 2004 report advises that federal officials should consider reopening public access to about three dozen Web sites withdrawn from the Internet after the 9/11 attacks because the sites pose little or no risk to US

[112] IRC is a text-based network where real world identities are routinely concealed or forged. IRC 'conversations' are logged, but transcripts are easily tampered with and are therefore unreliable.
[113] Harkat-ul-Ansar is on the State Department's list of FTOs.

national security. Baker *et al* report that the overwhelming majority of federal Web sites that reveal information about airports, power plants, military bases and other potential terrorist targets need not be censored because similar or better information is easily available elsewhere. Rand's National Defense Research Institute identified 629 Internet-accessible federal databases that contain critical data about specific locations. The study, conducted between mid-2002 and mid-2003, found no federal sites that contained information a terrorist would need to launch an attack. It identified four databases where restricting access probably would enhance national security; none remain available to the public. These included two Web sites devoted to pipelines, one to nuclear reactors, and one to dams. The researchers recommended that officials evaluate sixty-six databases with some useful information, but they did not anticipate restrictions would be needed, because similar or better data could be easily obtained elsewhere (Baker *et al* 2004a & 2004b).

OTHER TYPES OF USE

So far this chapter has focused on terrorists' use of the Internet as a facilitator of their activities. This section will provide a brief introduction to both terrorist misuse of the Net and their offensive use of same.

Misuse

The term 'misuse' refers to using the Internet to disrupt or compromise Web sites or infrastructure. Its purpose is disruption, and it is usually undertaken by hackers or hacktivists. The 'misuse' category is obviously a very large one, so the comments here are restricted to misuse carried out in conjunction with terrorist groups or activities.

A number of US government agencies have pointed to an 'e-mail bombing' by the Tamil Tigers as the first known act of cyberterrorism. The 'bombing' consisted of about 800 e-mails a day for approximately two weeks. The messages read "We are the

Internet Black Tigers and we're doing this to disrupt your communications." William Church, a former US Army intelligence officer, observed that

> The Liberation Tigers of Tamil Eelam are desperate for publicity and they got exactly what they wanted...Considering the routinely deadly attacks committed by the Tigers, if this type of activity distracts them from bombing and killing then [I] would like to encourage them, in the name of peace, to do more of this type of 'terrorist' activity (as quoted in Denning 2001b).

Instead of an act of cyberterrorism, the Tigers 'bombing' campaign is more accurately described as terrorist misuse of the Net. "It was e-mail attacks. That is harassment, that is not terrorism" (Borland 1998).

In May 2001 'cyberterrorism' reared its head once again when supporters of the terrorist group Laskar Jihad (Holy War Warriors) hacked into the websites of the Australian embassy and the Indonesian national police in Jakarta to protest against the arrest of their leader. The hackers intercepted users logging on to the Web sites and redirected them to a site containing a warning to the Indonesian police to release Ja'far Umar Thalib, the group's leader. Thalib was arrested in connection with inciting hatred against a religious group and ordering the murder of one of his followers. According to police, the hackers, the self-styled Indonesian Muslim Hackers Movement, did not affect police operations while the Australian embassy said the hackers did not sabotage its Web site, but only directed users to the other site (Anonymous 2001).

Numerous instances of misuse were evidenced in the wake of the 9/11 attacks. A group of Muslim hackers who attacked the Web site of a group of pro-US hackers indicated they stood by Bin Laden, even as they condemned the 9/11 attacks. "Osama Bin Laden is a holy fighter and whatever he says makes sense," the group known as GForce Pakistan wrote on the defaced site. The group also posted warnings that it planned to hit major US and British military Web sites and claimed to have "some very high confidential US data," which it threatened to reveal to officials of Al-Qaeda should the US fail to meet several demands including the removal of US troops from Saudi Arabia and the cessation of bombing in Afghanistan. Another GForce

defacement contained similar sentiments and included images of badly mutilated children who, the group claimed, had been killed by Israeli soldiers (Denning 2001a; NIPC 2001c). GForce also proclaimed an 'Al-Qaeda Alliance Online,' other members of the 'alliance' included the Anti-India Crew (AIC) and Pakistan Hackerz Club. In early December 2001, AIC breached five Internet servers operated by the US General Accounting Office. The compromised systems included two servers that handle the accounting office's e-mail, as well as a file transfer system and two Web servers. The agency's main site was not affected[114] (NIPC 2001a). Other US Web sites, including those of World Trade Services, the National Oceanic and Atmospheric Agency, and the National Institute of Health were also defaced in the aftermath of 9/11.

...And Offensive Use

The term 'offensive use' refers to using the Internet to cause destruction and/or engage in theft. Its purpose is exploitative. For instance, in November 2000 an attack originating in Pakistan was carried out against the American Israel Public Affairs Committee, a US lobbying group. The group's site was defaced with anti-Israeli commentary.[115] The attacker also stole some 3,500 e-mail addresses and 700 credit card numbers, sent anti-Israeli diatribes to the addresses and published the credit card data on the Internet. The Pakistani hacker who took credit for the crack, the self-styled Dr. Nuker, said he was a founder of the Pakistani Hackerz Club, the aim of which was to "hack for the injustice going around the globe, especially with [*sic*] Muslims" (Schwartz 2000).

---

[114] For more information on these and other hack attacks conducted in the wake of the terrorist attacks in New York and Washington, see ISTS 2001.

[115] The defacement may be viewed online at http://www.attrition.org/mirror/attrition/2000/11/02/www.aipac.org/.

FIGHTING BACK

At the beginning of this chapter, Charles Swett's 1996 Internet assessment was mentioned. In that document Swett suggested, as more foreign officials, military officers, business people, and journalists got e-mail addresses, the Internet could be used as a medium for psychological operations campaigns. The Internet, he said, could rapidly convey the official government perspective on a host of important issues to a wide and influential audience. To date, however, most official government Web sites are limited to routine public affairs whereas it is commonplace on the Web to see public diplomacy conducted on behalf of a host of political dissenters, including terrorists. Nonetheless, use of the Internet is a double-edged sword for terrorists. They are not the only groups 'operating' the Net (Rogers 2002, 191), which can act as a valuable instrumental power source for anti-terrorist forces also. The more terrorist groups use the Internet to move information, money, and recruits around the globe, the more data that is available with which to trail them. (Although, it must be said, the practical difficulties of collecting and exploiting that data are probably greater than commonly understood). Since 9/11 a number of groups have undertaken initiatives to disrupt terrorist use of the Internet, although a small number of such efforts were also undertaken previous to the attacks. Law enforcement agencies have been the chief instigators of such initiatives, but they have been joined in their endeavours by other government agencies as well as concerned individuals and various groups of hacktivists.

The Role of Law Enforcement and Intelligence Agencies

Investigators turned to Internet tools in their investigation of the 9/11 attacks as never before. What role did the Internet play in the investigation of the attacks? Importantly, what could be done online to track the group depended in large part on what the group did online. In a briefing given in late September 2001, FBI Assistant Director Ronald

Dick, head of the United States National Infrastructure Protection Center (NIPC),[116] told reporters that the hijackers had used the Net, and "used it well."

In the immediate aftermath of the 9/11 attacks US federal agents issued subpoenas and search warrants to just about every major Internet company, including America Online, Microsoft, Yahoo, Google, and many smaller providers. It is known that the hijackers booked at least nine of their airline tickets for the four doomed flights online at least two to three weeks prior to the attacks. They also used the Internet to find information about the aerial application of pesticides. Investigators have in their possession hundreds of e-mails linked to the terrorists in English, Arabic and Urdu. The messages were sent within the United States and internationally. According to the FBI, a number of these messages include operational details of the attacks. Some of the hijackers used e-mail services that are largely anonymous-- Hotmail, for example--and created multiple temporary accounts. A number of them are known to have used public terminals, in libraries and elsewhere, to gain access to the Net, whereas others used privately owned personal or laptop computers to do so (Cohen 2001; Fallis & Cha 2001, A24; O'Brien 2001, 52).

Also in the immediate aftermath of 9/11, the FBI were involved in the official closure of what appears to be hundreds--if not thousands--of Internet sites. For instance, several radical Internet radio shows, including *IRA Radio*, *Al Lewis Live* and *Our Americas*, were pulled by an Indiana ISP in late September 2001 after the FBI contacted them and advised that their assets could be seized for promoting terrorism. The New York-based *IRA Radio* was accused of raising funds for the Real IRA. The site contained an archive of weekly radio programmes said to back the dissident Irish republicans (Cobain 2001, 8). The archive of political interviews from the programme *Al Lewis Live*, hosted by iconoclastic actor/activist Lewis,[117] drew some 15,000 hits a day. *Our Americas* was a Spanish-language programme about rebels in Latin America

[116] The Clinton administration spearheaded the first major US effort to upgrade computer security in government and business against cybercrime. President Bill Clinton issued an order in May 1998 establishing the National Infrastructure Protection Center, a collaboration between law enforcement, military, and intelligence organizations to increase defenses against computer crime. The center also developed an information-sharing network with major industrial sectors.

[117] Formerly Grandpa on the 1960s hit TV show 'The Munsters'!

(Kornblum 2001, 3D).[118] Others voluntarily purged sites perceived as terrorist. For example, Yahoo! pulled dozens of sites in the *Jihad* Web Ring, a coalition of 55 *jihad*-related sites, while Lycos Europe established a twenty-person team to monitor its Web sites for illegal activity and to remove terrorist-related content (Gruner & Naik 2001; Scheeres 2001b).

Intelligence Gathering

The bulk of this chapter has been concerned with showing how the Internet can act as a significant source of instrumental power for terrorist groups. Use of the Internet can nonetheless also result in significant undesirable effects for the same groups. First, unless terrorists are extremely careful in their use of the Internet for e-mail communication, general information provision, and other activities, they may unwittingly supply law enforcement agencies with a path direct to their door. Second, by putting their positions and ideological beliefs in the public domain, terrorist groups invite opposing sides to respond to these. The ensuing war of words may rebound on the terrorists as adherents and potential recruits are drawn away (Soo Hoo, Goodman & Greenberg 1997, 140). Perhaps most importantly, however, the Internet and terrorist Web sites can serve as a provider of open source intelligence for states' intelligence agencies. In 1996, Swett noted: "The Internet is a potentially lucrative source of intelligence useful to the DOD. This intelligence can include...information about the plans and operations of politically active groups." Swett even foresaw the Internet being used for counter-intelligence, although he added a cautionary note that if it became known that the DOD was monitoring the Internet for intelligence or counter-intelligence purposes, then Internet users might start to post false information, and "our analysis function would need to account for this."

Swett's predictions about the intelligence gathering opportunities provided by the Internet have proved accurate. Although spy agencies are loath to publicly admit it,

[118] Al Lewis Live can still be heard on Pacifica Radio in the United States. The IRA Radio site was allowed back online in March 2002 at http://www.iraradio.com. However, it appears to have closed down again some time after February 2003. Site archives are available via the Internet Archive. The other sites mentioned remain offline.

it is generally agreed that the Web is playing an ever-growing role in the spy business. According to the 9/11 Commission's *Staff Statement No. 11*, "open sources--the systematic collection of foreign media--has always been a bedrock source of information for intelligence. Open source remains important, including among terrorist groups that use the media and the Internet to communicate leadership guidance" (2004, 9). By the 1990s the US government's Foreign Broadcast Information Service (FBIS) had built a significant translation effort as regards terrorism-related media.[119] Thus many now believe that terrorists' presence on the Internet actually works against them. "A lot of what we know about al-Qaida is gleaned from [their] websites," according to Steven Aftergood, a scientist at the Federation of American Scientists in Washington, D.C., and director of the nonprofit organization's Project on Government Secrecy.[120] "They are a greater value as an intelligence source than if they were to disappear" (as quoted in Lasker 2005). For example, Web sites and message boards have been known to function as a kind of early warning system. Two days before the 9/11 attacks, a message appeared on the popular Dubai-based Alsaha.com discussion forum proclaiming that "in the next two days," "a big surprise" would come from the Saudi Arabian region of Asir. The remote province adjacent to Yemen was where most of the nineteen hijackers hailed from (Bradley 2004). In another example, intelligence officials issued warnings in the days previous to the November 2003 attacks in Riyadh, Saudi Arabia that killed eighteen people and wounded 120 others. The warnings were allegedly based on information they obtained from anonymous postings on Arabic Web sites and other forms of Internet 'chatter' (Warner 2003).

Innovations such as the FBIS, while useful, do not tell the whole story, however.[121] The problem begins with the sheer volume of information floating about in cyberspace. According to the 9/11 Commission's *Staff Statement No. 9*, prior to 9/11 the FBI did not have a sufficient number of translators proficient in Arabic and other relevant languages, which by early 2001 had resulted in a significant backlog of

---

[119] An example of open source intelligence that remained unacted upon was the al-Qaeda interview conducted by an Italian newspaper in 2000 in which the interviewee stated that he and others were being trained as pilots to conduct kamikaze attacks (Verton 2003, 177-178).

[120] The project's Web site is online at http://www.fas.org/sgp/.

[121] For an analysis of pre-9/11 intelligence failures (for which the author blames the Clinton administration) and the impact of IT in the US intelligence community, see Chapter Eight ('Intelligence: Stopping the Next Attack') of Verton's *Black Ice* (2003).

untranslated intelligence intercepts.[122] In addition, prior to 9/11, the FBI's investigative activities were governed by Attorney General Guidelines, first put in place in 1976 and revised in 1995, to guard against the misuse of government power. The Guidelines limited the investigative methods and techniques available to FBI agents conducting preliminary investigations of potential terrorist activities. In particular, they prohibited the use of publicly available source information, such as that found on the Internet, unless specified criteria were present (2004, 8). These guidelines have since been modified and terrorist Web sites are thought to be under increased surveillance since 9/11, especially by Western intelligence agencies (Verton 2003, 220). This task remains gargantuan, however; information gleaned from the Net must be corroborated and verified before it can be added to the intelligence mix. This requires significant input of operatives and resources. And still intelligence agencies simply cannot monitor the entire Internet all of the time as, for the present at least, this remains an impossible undertaking.

Technological Fixes

Given the above, it is unsurprising that many US officials and commentators are recommending that any additional funds that become available to the intelligence agencies be spent on human intelligence capabilities, rather than new technology. Others, however, are convinced that new technologies need to be developed and deployed in the fight against terrorism. They bemoan the fact that prior to 9/11, "Signals intelligence collection against terrorism, while significant, did not have

[122] The shortage of qualified language specialists is an ongoing problem for US intelligence and law enforcement agencies. The 9/11 Commission's *Staff Statement No. 12* had this to say about the shortage and its impact upon the translation of intercepts: "While highest priority cases are supposed to be translated within 24 hours, the FBI cannot translate all it collects. According to a recent report by the Department of Justice Inspector General, 'the FBI shortages of linguists have resulted in thousands of hours of audiotapes and pages of written material not being reviewed or translated in a timely manner.' The choice is between foregoing access to potentially relevant conversations and obtaining such conversations that remain untranslated. Despite the recent hire of 653 new linguists, demand exceeds supply. Shortages of translators in languages such as Arabic, Urdu, Farsi, and Pashto remain a barrier to the FBI's understanding of the terrorist threat" (2004, 4). The French authorities, on the other hand, are said to have separate translating units for the twenty Algerian dialects alone.

sufficient funding within the NSA. The NSA's slow transformation meant it could not keep pace with advances in telecommunications" (Staff Statement No. 11 2004, 10). Although DCS-1000--more commonly known as Carnivore--the FBI's e-mail packet-sniffer system has not been employed since 2002, Bureau officials have instead employed commercially available monitoring applications to aid in their investigations. And US law enforcement agencies are not the only ones employing high-tech surveillance methods. The Pakistani authorities have made a number of significant terror-related arrests since 9/11, which have resulted from the interception of e-mail messages. Intelligence agencies are also said to be deploying the classic spy tactic of establishing so-called 'honey pots' with a high-tech twist: in this case, setting up bogus Web sites to attract those people they are seeking to monitor (Warner 2003; see also Associated Press 2002). Numerous other technological fixes are also in the works.

For example, US computer scientists are at work developing optical character recognition software to scan Arabic documents, even handwritten ones, for specific words or phrases. It is hoped the software will expand access to both modern and ancient Arabic texts, while also acting as an aid in intelligence gathering. The researchers, at the University of Buffalo, have received $240,000 in funding from the federal Director of Central Intelligence Postdoctoral Research Fellowship Program for the project, which will eventually allow Arabic documents to be digitised and posted on the Web (Thompson 2005).[123] The CIA is also partly funding research into surveillance of Internet chatrooms with a view to creating "new capabilities to combat terrorism through advanced technology." Researchers at the Rensselaer Polytechnic Institute in Troy, New York, received funding for the development of "a system to be deployed in the background of any chatroom as a silent listener for eavesdropping...[which] could aid the intelligence community to discover hidden communities and communication patterns in chatrooms without human intervention" (McCullagh 2005; see also Associated Press 2004). With regard to Web sites, researchers in the Department of Information Systems Engineering at Ben-Gurion University of the Negev in Israel, in collaboration with a colleague at the University of South Florida, reported in August

[123] There are many sites offering translation services via the Web. In terms of Arabic to English translation, probably the best-known site is Ajeeb.com, which has been providing free machine-based translation services since 2001.

2004 that they had developed a system that could identify ninety-five percent of Internet pages containing terrorism-related content. The experimental system is based on the recognition of patterns in texts with terror content, based on examples from existing Internet sites. It uses these patterns to identify 'hits' by surfers on other Web sites with similar characteristics, in order to locate users affiliated with terror organizations and new sites set up by terrorist elements, amongst other things (Dror 2004; Elovici *et al* 2004).

Other Innovations

It should be clear at this stage that the events of 9/11 impacted intelligence and law enforcement agencies not just in the United States, but around the world. On this side of the Atlantic, MI5 took the unprecedented step of posting an appeal for information about potential terrorists on dissident Arab websites. The message, in Arabic, was placed on sites that the authorities knew were accessed by extremists, including 'Islah.org,' a Saudi Arabian opposition site, and 'Qoqaz.com,' a Chechen site which advocated *jihad.*[124] The message read:

> The atrocities that took place in the USA on 11 September led to the deaths of about five thousand people, including a large number of Muslims and people of other faiths. MI5 (the British Security Service) is responsible for countering terrorism to protect all UK citizens of whatever faith or ethnic group. If you think you can help us to prevent future outrages call us in confidence on 020-7930 9000.

MI5 were hopeful of eliciting information from persons on the margins of extremist groups or communities who were sufficiently shocked by the events of 9/11 to want to contact the agency. The agency had intended to post the message on a further fifteen

[124] Hamburg resident Said Bahaji, a suspected accomplice of the 9/11 hijackers, was on the mailing list of 'Qoqaz.net' (Gruner & Naik 2001; Liu 2001, 62).

sites known to be accessed by radicals, but many of these were shut down by the FBI in the aftermath of the attacks (Gruner & Naik 2001; Norton-Taylor 2001).

The events of 9/11 prompted numerous states' intelligence agencies to reappraise their online presence. Since 2001, MI5 has substantially enhanced its Web site.[125] The evolution of the site from December 1998 to the present is depicted in Figure 3.2. The new site is divided into five major sections. A section entitled 'The Threats' provides details on the current threats to UK national security, including a summary of the threat from international terrorism. Anyone with information they think might help protect national security is invited to contact the Service directly via a secure page on the website in a section called 'How You Can Help'.[126] Expert advice to help businesses to protect themselves against security threats was added in April 2004. The new 'Security Advice' is aimed principally at businesses and staff in organizations with responsibility for the safety of others. It was compiled by the Security Service's National Security Advice Center (NSAC), which works to protect key government assets and businesses vital to the UK's Critical National Infrastructure. The 'About MI5' section of the site contains a brief history of the service, it's organizational structure, and other details. In February 2004 the Home Office announced additional funding for the Security Service to increase staff by fifty per cent in the next few years; there is a prominent link to the site's recruitment section from the top page. In order to build on the co-operation of the Muslim community, the site is also available in Arabic. (Additional languages will be added in due course).

Also in 2004, Israel's Mossad spy agency launched a Web site aimed at recruiting staff. Advertised vacancies ranged from computer security specialists to English-speaking waiters and agents for "special tasks." The site, which is available in both Hebrew and English and replaces a rudimentary single-page site, includes a short history of the agency, a mission statement, and an online employment application

---

[125] The information is complementary to that provided on www.homeoffice.gov.uk/terrorism, which is aimed at the general public, and www.ukresilience.info, which provides information for emergency planners and local authorities.

[126] In addition to the new web form, anyone with information they want to pass on to the Security Service can call the public telephone number 020 7930 9000 in confidence.

form.[127] Obviously as interested in gathering intelligence as in recruiting new staff, the 'Contact Us' page invites users to submit "information that could be useful" to the agency while promising to protect tipsters' anonymity (Harris 2004).

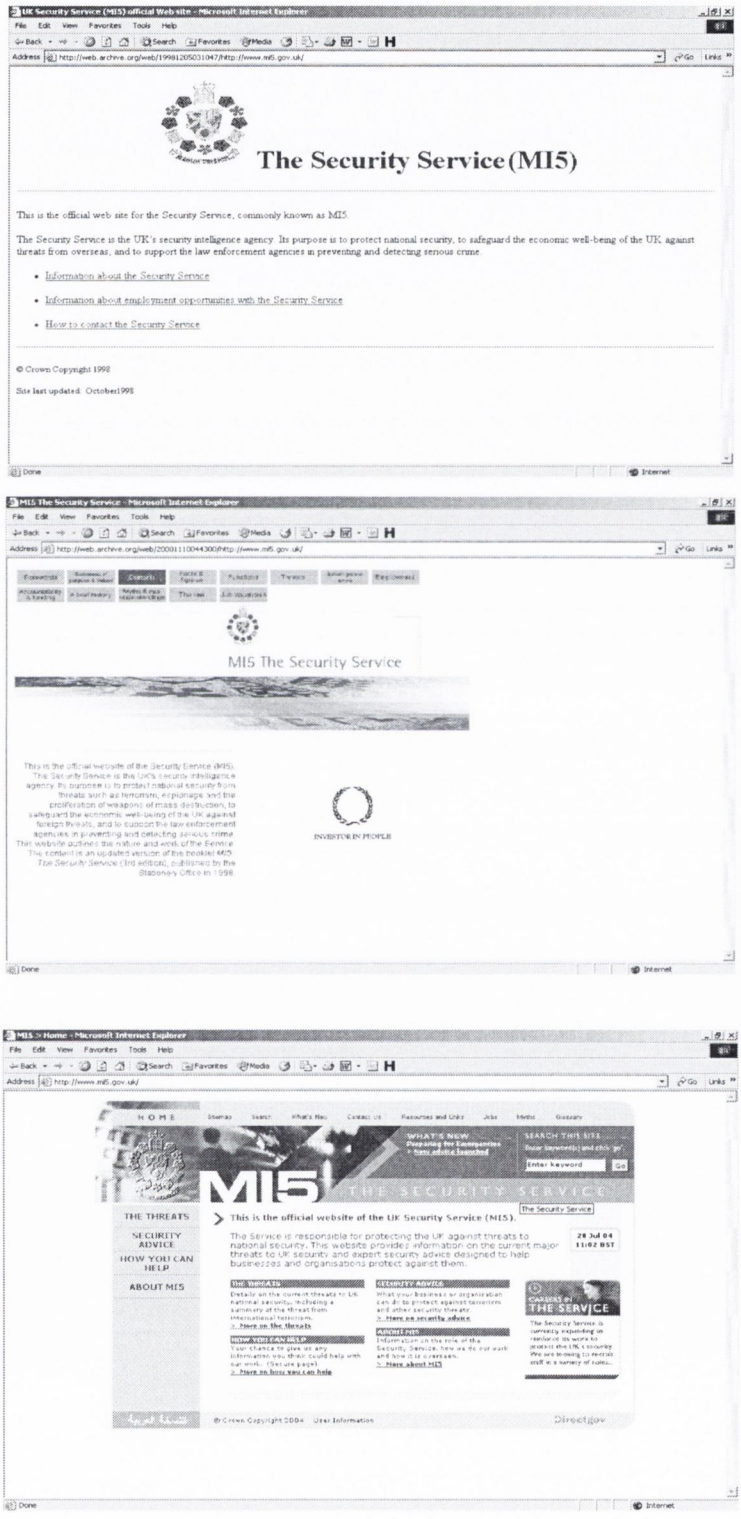
Other Agencies: Sanitising Government Sites

US government Web sites were vital repositories of information for Internet users in the days and weeks following the 9/11 attacks (see Table 3.3). The sites became important venues for those both directly and indirectly affected by the events of 9/11, members of the public wishing to donate to the relief efforts, and the various agencies' own employees, some of whom were victims of the attacks (or later of the anthrax scares) (see Pew 2002, 33-37).

While some agencies were uploading information onto the Net, however, others were busy erasing information from their sites. To avoid providing information that might be useful to terrorists planning further attacks, federal agencies, as well as some state and private Web page operators, took large amounts of material off the Internet in the wake of the 9/11 attacks. Some of the erasures were voluntary; others were carried out following requests from US government departments. As mentioned earlier the Nuclear Regulatory Commission, which regulates American nuclear power plants, closed its Web site down for a period following a request from the Department of Defence that it do so. Although no other agency removed its entire site, pages were erased from the Web sites of the Department of Energy, the Interior Department's Geological Survey, the Federal Energy Regulatory Commission, the Environmental Protection Agency, the Federal Aviation Administration, the Department of Transportation's Office of Pipeline Safety, the National Archives and Records Administration, the NASA Glenn Research Centre, the International Nuclear Safety Centre, the Los Alamos National Laboratory, the Bureau of Transportation Statistics' Geographic Information Service, and the National Imagery and Mapping Agency

[127] The Mossad's English language Web site may be accessed at http://www.mossad.gov.il/Mohr/MohrTopNav/MohrEnglish/MohrAboutUs/.

Figure 3.2 Evolution of MI5 Web Site, December 1998 to December 2004



(Dalglish, Leslie & Taylor 2002, 25; Pew 2002, 8-9; see also Baker *et al* 2004).

What sorts of information was removed from the sites? The Environmental Protection Agency (EPA) removed thousands of chemical industry risk management plans dealing with hazardous chemical plants from its site. More sensitive information about 'worst case' chemical accidents is kept in special reading rooms located around the country. The Office of Pipeline Safety removed several pages, including those with maps that it said illustrated places where hazardous liquid pipelines flowed through unusually sensitive environmental areas. Department of Transportation officials removed pipeline mapping information as well as a study describing risk profiles of various chemicals, while the Bureau of Transportation Statistics removed the National Transportation Atlas Databases and the North American Transportation Atlas, which environmentalists had used to assess the impact of transportation proposals. The Center for Disease Control and Prevention removed a *Report on Chemical Terrorism* that described industry's shortcomings in preparing for a possible terrorist attack (Dalglish, Leslie, & Taylor 2002, 2; Gugliotta 2001, A29; Pew 2002, 8-9; Scheeres 2001b). Many of the agencies posted notices that the information had been removed because of its

Table 3.3 Increasing Use of Government-Related Web Sites Post 9/11

Site	% Increase in Unique Visitors: Sept. 11-12
panynj.gov (New York/New Jersey Port Authority)	7,715%
disasterrelief.org (a disaster relief portal run by the Red Cross)	2,342%
redcross.org	1,494%
fbi.gov	1,306%
nyc.gov (municipal site)	787%
whitehouse.gov	433%
fema.gov (the federal disaster relief agency)	173%
cia.gov	129%
state.gov (US State Department)	83%
navy.mil	61%

Source: Pew Internet and American Life Project 2001b, 8.

possible usefulness to terrorists.[128]

On 17 October 2001, in a separate move to limit information available under US freedom of information (FOI) laws, Attorney General John Ashcroft ordered federal agencies to review more closely which documents they release. The new policy allows officials to withhold information on any 'sound legal basis.' Under less stringent policies issued in 1993, agencies could only hold back information in order to prevent 'foreseeable harm.' Ashcroft cited the 9/11 attacks as reasons for the change, which will almost certainly affect what documents are publicly available online from now on thus contravening the spirit of the Electronic FOI Act of 1996, which encouraged agencies to post information on their Web sites (Bridis 2001, A27; Dalglish, Leslie & Taylor 2002, 21-22).

States have been eager to follow in the footsteps of the federal government in this regard. The state of Florida now prevents online access to information on crop dusters and certain driver's license information. The state of New Jersey removed chemical storage information from the Net, and the state of Pennsylvania is withholding certain information pertaining to the environment from Net users (Pew 2002, 9). In New York, the director of the Office of Public Security, James K. Kallstrom, and the director of the Office of State Operations, James G. Natoli, sent a jointly authored confidential memorandum to the heads of all state agencies requesting them to re-evaluate all sensitive information they possessed. The memorandum directed agencies to remove all sensitive information from the Internet and to exempt it from FOI disclosures. Kallstrom and Natoli defined sensitive information as "information related to systems, structures, individuals and services essential to the security, government, or economy of the state" (Dalglish, Leslie & Taylor 2002, 28).

Senator Patrick Leahy of Vermont, a strong advocate of open government, wrote to the General Accounting Office--the investigative arm of Congress--regarding Ashcroft's order, that the new memorandum replaces a policy that "favored openness" and "encouraged a presumption of disclosure" with a policy that encourages denials

[128] The Electronic Frontier Foundation maintains a tally of sites that have been shut down or restricted since 9/11. The EFF list is available at http://www.eff.org/Privacy/Surveillance/Terrorism/antiterrorism_chill.html. In addition, the National Coalition Against Censorship's site on 'Free Expression After 9/11' can be found at http://www.ncac.org/issues/freeex911.html.

even when "there is doubt whether an exemption applies" and there is "no foreseeable harm" from disclosure (as quoted in Dalglish, Leslie & Taylor 2002, 21-22). However, survey data suggests that the American public are willing to give their government considerable leeway in deciding what information may be provided on agency Web sites if officials argue that some information might be useful to terrorists: 69% believe the US government should do everything it can to keep information out of terrorists' hands, even if that means that the public will be deprived of information that it needs or wants. Stemming from this, 67% of Americans say that the government should remove information from its Web sites that might potentially help terrorists, even if the public has a right to access that information. In addition, two-thirds of the US public believes businesses and utility companies should not put sensitive information on their Web sites.

Yet even as they concede a willingness to cede non-disclosure powers to government officials, a significant number of Americans are sceptical that erasing information from the Internet will make a difference in the fight against terrorism: 47% say that withholding or removing information from government Web sites will *not* make a difference in battling terrorism, while 41% believe that taking information off these sites *will* hinder terrorists. Interestingly, a survey carried out in summer 2002 found that just 25% of Americans (28% of Internet users) were aware that government agencies had erased information from Web sites. Further, only 5% of Internet users said they had noticed that information they expected to be available on a government site was missing (Pew 2002, 9-10).

Hackers and Hacktivists

Hackers also took to the Net in the aftermath of the terror attacks, some to voice their rage, others to applaud the attackers. A group calling themselves the Dispatchers proclaimed that they would destroy Web servers and Internet access in Afghanistan and also target nations that support terrorism. The group of sixty people, led by a 21-year-

old security worker from Ohio, proceeded to deface hundreds of Web sites[129] and launch Distributed Denial of Service (DoS) attacks[130] against targets ranging from the Iranian Ministry of the Interior to the Presidential Palace of Afghanistan. Another group, known as Young Intelligent Hackers Against Terror (YIHAT) claimed, in mid-October, to be negotiating with one European and one Asian government to 'legalize' the groups hacking activities in those states. The group's founder, Kim Schmitz, claimed the group breached the systems of two Arabic banks with ties to Osama Bin Laden, although a spokesperson for the bank denied any penetration had occurred. The group, whose stated mission is to impede the flow of money to terrorists, issued a statement on their Web site requesting that corporations make their networks available to group members for the purpose of providing the "electronic equivalent to terrorist training camps." Later, their public Web site was taken offline, apparently in response to attacks from other hackers[131] (Denning 2001a, 1; NIPC 2001c).

Not all hacking groups were supportive of the so-called 'hacking war.' On 14 September 2001, the Chaos Computer Club, an organization of German hackers, called for an end to the protests and for all hackers to cease vigilante actions. They called instead for global communication to resolve the conflict: "we believe in the power of communication, a power that has always prevailed in the end and is a more positive force than hatred" (as quoted in Hauss & Samuel 2002). A well-known group of computer enthusiasts, known as Cyber Angels, who promote responsible behaviour, also spoke out against the hacking war. They sponsored television advertisements in the US urging hackers to help gather information and intelligence on those who were participating in this hacktivism (Hauss & Samuels 2002; NIPC 2001). In any event, the predicted escalation in hack attacks (ISTS 2001) did not materialize. In the weeks

---

[129] Web defacement is one of the most popular tools at the disposal of hackers. 'Attrition.org,' which at one time mirrored and collected statistics on defacements, recorded over 5,800 defacements in 2000, up from 3,700 in 1999. The group ceased collecting such data in May 2001 by which time over 5,300 defacements had already taken place.

[130] Distributed Denial of Service (DDoS) attacks are actions by distributed computers that prevent any part of another computer system from functioning in accordance with its intended purpose. DDoS attacks generally employ armies of 'zombie' machines taken over and controlled by a single master to overwhelm the resources of a target with floods of packets (ISTS 2001, 7 & 11).

[131] The site was located at http://www.kill.net. This URL now takes one to Kim Schmitz's homepage, also at http://www.kimble.org. (Kimble is Schmitz's *nom de guerre*). Schmitz's site contains a brief flash movie detailing YIHAT's 'mission.'

following the attacks, Web page defacements were well publicized, but the overall number and sophistication of these remained rather low. One possible reason for the non-escalation of attacks could be that many hackers--particularly those located in the US--were wary of being negatively associated with the events of 9/11 and curbed their activities as a result.

It's never been all plain sailing for terrorist users of the Net, even prior to 9/11. Their homepages have been subject to intermittent DoS and other hack attacks and there have also been strikes against their Internet Service Providers (ISPs) that have resulted in more permanent difficulties. In 1997, for example, an e-mail bombing was conducted against the Institute for Global Communications (IGC),[132] a San Francisco-based ISP, hosting the Web pages of the *Euskal Herria* or *Basque Country Journal,* a publication edited by supporters of the Basque group Homeland and Liberty (ETA). The attacks against IGC commenced following the assassination by ETA of a popular town councilor in northern Spain. The protestors wanted the site pulled from the Internet. To accomplish this they bombarded IGC with thousands of spurious e-mails routed through hundreds of different mail relays, spammed IGC staff and customer accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against other organizations using IGC services. IGC pulled the *Euskal Herria* site on 18 July 1997, but not before archiving a copy of the site enabling others to put up mirrors. Shortly thereafter, mirror sites appeared on half a dozen servers on three continents. Despite this, the protestors e-mail action raised fears of a new era of censorship imposed by direct action from anonymous hacktivists. Furthermore, approximately one month after IGC pulled the controversial site off its servers, Scotland Yard's Anti-Terrorist Squad shut down Internet Freedom's U.K. Web site for hosting the journal. Scotland Yard claimed to be acting against terrorism (Denning 1999, 270-71).[133] The so-called 'cyberwar' that raged between Israelis and

[132] Online at http://www.igc.org/igc/gateway/index.html.

[133] For more information on the e-mail bombing and IGC's response to it see http://www.igc.apc.org/ehj/. Also the press release issued by Internet Freedom UK in response to the shutting of their operations by Scotland Yard: http://www.fitug.de/debate/9709/msg00018.html. The group's Web site is located at http://www.netfreedom.org.

Palestinians and their supporters in 2000 was a mere nuisance in comparison with such targeted and sustained campaigns.[134]

Since 9/11 a number of Web-based organizations have been established to monitor terrorist Web sites. One of the most well-known of such sites is Internet Haganah,[135] self-described as "an internet counterinsurgency." Also prominent is the Washington DC-based Search for International Terrorist Entities (SITE) Institute[136] that, like Internet Haganah, focuses on Islamic terror groups. Clients of SITE's fee-based intelligence service are said to include the FBI, Office of Homeland Security, and various media organizations. But what are the goals of these private organizations? SITE is a for-profit concern while Internet Haganah survives on donations and advertising revenue. SITE's co-founder and director, Rita Katz, has commented: "It is actually to our benefit to have some of these terror sites up and running by American companies. If the servers are in the US, this is to our advantage when it comes to monitoring activities" (as quoted in Lasker 2005). While Aaron Weisburd, who runs Internet Haganah out of his home in Southern Illinois, says his goal is to keep the extremists moving from address to address: "The object isn't to silence them--the object is to keep them moving, keep them talking, force them to make mistakes, so we can gather as much information about them as we can, each step of the way" (as quoted in Lasker 2005; see also Bunt 2003, 24 & 93). On the Haganah Web site, the mark of victory is a little blue graphic of an AK-47 assault rifle, each of which represents another terrorist Web site put out of commission (at least temporarily). Weisburd's *modus operandi* is to first research a site, he then makes a 'whois' inquiry. If there is evidence of extremism, he contacts the hosting company and urges the host to remove the site from its servers. If successful, Internet Haganah may purchase the domain name so the address can never be used again. Since its inception in 2003, Internet Haganah has taken credit for or assisted in the shutdown of more than 600 sites it claims were linked to terror.

---

[134] The so-called 'Interfada' is discussed in Chapter Seven.
[135] In Hebrew, 'Haganah' means defense. Internet Haganah is online at http://www.haganah.org.il/haganah/index.html.
[136] The SITE Web site is at http://www.siteinstitute.org/.

CONCLUSION

Researchers are still unclear whether the ability to communicate online worldwide has resulted in an increase or a decrease in terrorist acts. It is agreed, however, that online activities substantially improve the ability of such terrorist groups to raise funds, lure new faithful, and reach a mass audience (Arquilla *et al* 1999, 66; Piller 2001, A1). The most popular terrorist sites draw tens of thousands of visitors each month. Obviously, the Internet is not the only tool that a terrorist group needs to 'succeed.' However, the Net can add new dimensions to existing assets that groups can utilize to achieve their goals as well as providing new and innovative avenues for expression, fundraising, recruitment, etc. At the same time, there are also tradeoffs to be made. High levels of visibility increase levels of vulnerability, both to scrutiny and security breaches. Nonetheless, the proliferation of official terrorist sites appears to indicate that the payoffs, in terms of publicity and propaganda value, are understood by many groups to be worth the risks. Details of the contents, functioning, and effectiveness of these sites are provided in part three of this text. Before describing and analysing this most important aspect of terrorist Net use however, Chapter Four explores the use of the Internet for secure terrorist communications.

4

TERRORIST USE OF DIGITAL STEGANOGRAPHY: REAL OR IMAGINED?

INTRODUCTION

Perhaps when you were a child you used lemon juice to write on paper then allowed the paper to dry, which resulted in the disappearance of your text. Your writing would magically reappear on the apparently blank sheet of paper when you heated it.[137] This is an example of steganography: the science of secret writing or the art of hiding messages within other messages.

"Steganography...has until recently been the poor cousin of cryptography" (Sellars 1999, 1). Although steganography is related to cryptography, they are not the same. The goal of steganography is to hide the existence of a message; the goal of cryptography is to scramble a message so that it cannot be understood, although its existence may be detected (Karp 2002). The advantage of steganography over cryptography is that it can be employed to secretly transmit messages without the fact of the transmission being discovered. In fact, it is common for steganographers to encrypt their hidden message before placing it in the cover message, although it should be noted that the hidden message does not have to be encrypted to qualify as steganography. A message can be in plain English (or any other language for that matter) and still constitute a hidden message. Nonetheless, those that employ steganography in their communications are generally careful to make use of the extra layer of protection that encryption provides. This is because covert information is not

[137] Many organic fluids, including urine, behave in this fashion because they are rich in carbon and therefore char easily (Singh 2001, 10).

necessarily secure, just as secure information is not necessarily covert (Cochran 2000, 15).

Steganography hit the headlines when, between February and July 2001, *USA Today* reported that terrorists were using steganography to hide their communications from law enforcement agencies.[138] According to the articles' author, Jack Kelley, the messages were being hidden in images posted on the Internet. Kelley gave the example of images posted on the Internet auction site eBay. Very little evidence to substantiate these claims was provided in the newspaper articles; nonetheless, in the wake of 9/11, media outlets worldwide picked up the story.

This chapter explores the plausibility of widespread terrorist use of steganography and concludes that in a similar fashion to the cyberterrorist threat image described in Chapter Two, Kelley's articles initiated the rapid emergence of a "consensual interpretation" (Kern *et al* 2003, 81) of steganography as a tool of terrorists, which ultimately became uncritically taken for granted by politicians, journalists, scholars, and the wider public. This chapter investigates how and why such a one-sided frame met with such rapid and widespread success while also contributing a number of reasons for reappraising same. The chapter is divided into five sections. In an effort to raise the level of discussion on this issue that has taken place thus far, section one details the historical background to steganography, while section two outlines some of the technical details pertaining to digital steganography. The third section describes the alleged use of steganography by terrorists as reported in newspapers and magazines, while the situating of Jack Kelley as an information entrepreneur who was later removed from his position at *USA Today* due to irregularities in his reporting is also at issuance here. Steganalysis is the science of detecting hidden messages and is one of the reasons why terrorists might be unwise to use steganography to conceal their communications; this process and its efficacy are described and discussed in section four. Finally, section five is devoted to an analysis of alternative methods of clandestine communication via the Internet terrorists might employ instead. The basic argument advanced here is that terrorists are unlikely to be

[138] "The tabloid *USA Today* is probably the best indicator for the general threat perception in the mass media" (Bendrath 2003, 54).

employing digital steganography to facilitate secret intra-group communication as Kelley and others have claimed. This is mainly because terrorist use of digital steganography is both technically and operationally implausible; terrorists are therefore more likely to employ low-tech steganography, such as semagrams and null ciphers, instead.

A BRIEF HISTORY OF STEGANOGRAPHY

Steganography means covered or secret writing in Greek.[139] It is a form of information-hiding that has a long and established pedigree. The earliest known examples of steganography were recorded by the Greek historian Herodotus and date back to ancient times. The Greek tyrant Histaeus was held prisoner by King Darius in Susa during the 5th century BC. Histaeus wanted to send a message to his son-in-law Aristagoras in Miletus, so he shaved the head of a slave and tattooed a message on his scalp. When the slave's hair grew long enough to conceal the message/tattoo, he was dispatched to Miletus (Singh 2001, 9).[140] Herodotus provides us with another example of steganography from antiquity: the Greeks often communicated by writing on wax-covered tablets; when the Greek, Demeratus, needed to secretly notify the Spartans that Xerxes intended to invade Greece, he scraped the wax off of a tablet and wrote the message on the wood underneath. He then recovered the wooden tablets with wax. On inspection, the tablets appeared blank and unused, thus ensuring that Demeratuses message remained undiscovered (Cochran 2000, 12; Sellars 1999, 4; Singh 2001, 8).

Invisible inks are not simply children's playthings; they have been a popular method of chemical steganography for centuries. The ancient Romans would write between the lines of a text using invisible inks concocted from such readily available substances as fruit juices, urine, and milk. In fact, invisible inks were used in military conflict as recently as World War II (Sellars 1999, 4; Singh 2001, 10).

---

[139] Cryptography means 'secret writing.'

[140] Astonishingly, this method was still used by some German spies at the beginning of the twentieth century.

Gaspari Schotti was the author of the earliest book on steganography. His four hundred-page tome, entitled *Schola Steganographica*, was published in 1665. Schotti drew extensively upon the work of Johannes Trithemius (1462-1526), a German monk and early researcher in steganography and cryptography. Steganographic research continued to develop in the fifteenth and sixteenth centuries. Bishop John Wilkins--later the master of Trinity College, Cambridge--devised a number of steganographic processes that ranged from coding messages in sheet music and string knots to invisible inks. Auguste Kerckhoff's *Cryptographie Militaire* appeared in 1883 and was followed by Charles Briquet's *Les Filigraines* (1907), a historical dictionary of watermarks (Cochran 2000, 11-12; Sellars 1999, 4-5).

It was during the twentieth century that steganography came into its own, however. The British employed Lord Robert Baden-Powell, the founder of the Boy Scout movement, as a scout during the Boer War (1899-1902). His job was to record the location of Boer artillery positions. To avoid suspicion were he captured, Baden-Powell worked his maps into drawings of butterflies. On casual inspection the drawings appeared innocuous; however, certain markings on the wings actually indicated the positions of enemy installations. World War II ushered in a period of intense research and experimentation in steganography and associated fields. Invisible inks were employed in the early war years; later, null ciphers (i.e. unencrypted messages) were used to convey secret messages. The null cipher, which had the appearance of an innocent message about everyday occurrences, was thought unlikely to arouse suspicion and therefore to be less prone to interception. Both Duncan Sellars and Gary Kessler give the example of the following message sent by a German spy during WWII:

> Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Decoding this message (by lifting the second letter in each word) reveals the following secret text: Pershing sails from New York June 1 (Kessler 2004; Sellars 1999, 5-6).

Document layout was also used to conceal secret information: by modulating the position of lines[141] and words,[142] messages could be marked and identified. In addition, techniques such as writing messages in typewriter correction ribbon, and using pin punctures to mark selected letters were also popular (Sellars 1999, 6; Stallings 1998, 27).

J. Edgar Hoover, the director of the FBI, dubbed the German invention of the microdot "the enemy's masterpiece of espionage" (Dembart 2001). Microdots are photographs reduced to the size of a period, which have the clarity of standard sized typewritten pages. Using microdots, secret messages could be photographically reduced and affixed as the dot for the letter 'i' or other punctuation on any document containing text. Microdots permitted the secret transmission of large amounts of data, including technical drawings and photographs. The existence of the micro-dot was discovered by the Allies in 1941 on a typed envelope carried by a German agent. At that time, fears about the transmission of secret messages were so intense that, in the United States, the international mailing of postal chess games, knitting instructions, newspaper clippings, and children's drawings were banned. It was also illegal to send cables requiring that specific types of flowers be delivered on a specific date, and eventually the US and British governments banned international flower deliveries altogether (Byte 1997/8; Johnson 1995; Sellars 1999, 6).

During the 1980s, the then-British Prime Minister Margaret Thatcher became so angered at press leaks of cabinet documents that she had the word processors in Westminster programmed to encode ministers' identities in the word spacing, so that those responsible for leaks could be identified (Anderson 1996, 39-40; Anderson & Petitcolas 1998, 474). More recently, the digital age has revolutionised steganography. In fact, according to some, the Internet has become the modern version of the 'dead drop,' a slang term describing the location where Cold War-era spies left maps,

---

[141] This is known as line-shift coding. In this method, text lines are vertically shifted to encode the document uniquely. This method is probably the most visible text coding technique to the reader, however (see Sellars 1999, 7).

[142] This is known as word-shift coding. In this method, code words are included in a document by shifting the horizontal locations of words within text lines, while maintaining the appearance of natural spacing (see Sellars 1999, 8).

pictures, and other information, for collection by their handlers (Denning & Baugh 2001, 133; Kelley 2001a & 2001b).

DIGITAL STEGANOGRAPHY

The classic model for invisible communication in the modern scientific literature has been traced to G.J. Simmon, who in 1983 formulated it as the 'Prisoners Problem.' The scenario is this: Alice and Bob[143] are in jail, and wish to concoct an escape plan. However, all their communications pass through the warden, Willie; if Willie detects any encrypted messages, he will negate their plan by restricting them to solitary confinement. The upshot of this is that Alice and Bob must find some way of hiding their ciphertext in an innocent-looking covertext; they must establish a subliminal channel, in other words (Anderson 1996, 39; Anderson & Petitcolas 1998, 474; Katzenbeisser 2000, 17-19). Alice could, for example, create a picture of a purple horse grazing in a red meadow and send this piece of modern art to Bob. If successful, Willie will have no idea that the colours of the objects in the drawing transmit information.

Computer-based (i.e. digital) steganography is a relatively new process. Its usefulness is based on two simple principles. The first is that the files that contain digitised images or sounds may be subtly altered without compromising their functionality. The second principle rests on the inability of minor changes in colour or sound quality to be distinguished by humans (Johnson & Jajodia 1998, 273). Digital steganography is usually based on randomness. There are many occurrences of randomness in computer-based information. Steganographic data can be hidden in this random information or noise. The merits of a steganographic method are judged on whether the addition of the steganographic data changes the randomness (Ballard *et al* 2002, 996; Davern & Scott 1996, 279).

---

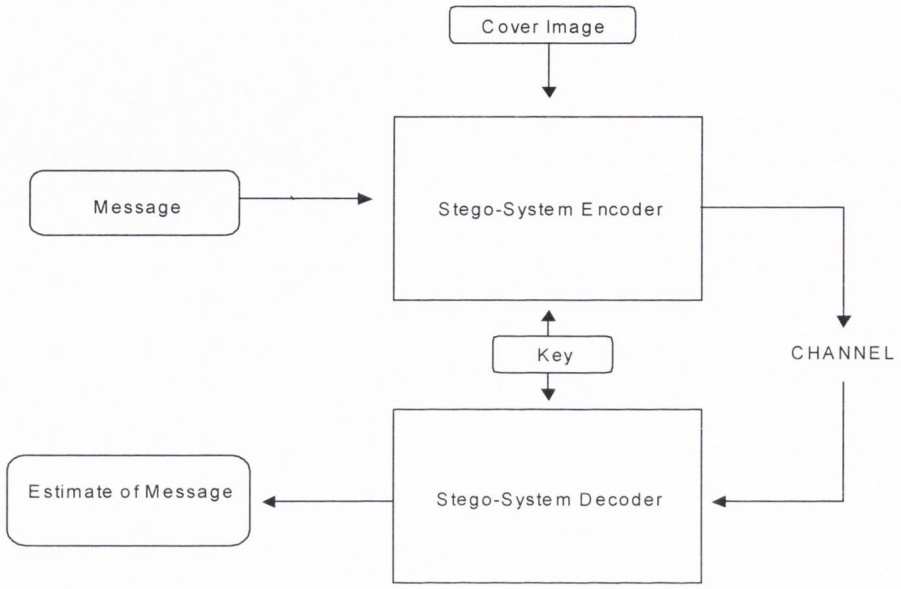
[143] In the field of cryptography, communication protocols usually involve two fictional characters named Alice and Bob. The standard convention is to name the participants in the protocol alphabetically (Carol and Dave often succeed Alice and Bob in a multi-person protocol), or with a name whose first character matches the first letter of their role (e.g. Willie the warden).

Digital steganography schemes can be characterised using theories of communication. The parameters of information hiding, such as the amount of data bits that can be hidden, the perceptibility of the message, and its robustness to removal can be related to the characteristics of communications systems: capacity, signal-to-noise ratio (SNR), and jamming margin. The notion of capacity in digital steganography indicates the total number of bits hidden and successfully recovered by the stego-system. The SNR serves as a measure of detectability. In this context, the message one is seeking to conceal (i.e. the embedded signal) represents the information-bearing signal, and the cover image is viewed as noise. Contrary to typical communication scenarios where a high SNR is desired, a very low SNR for a stego-system corresponds to lower perceptibility and therefore greater success when concealing the embedded signal. The measure of jamming resistance describes the level of robustness to removal or destruction of the embedded message, whether intentional or accidental (Marvel *et al* 1998, 48).

All digital steganographic schemes/tools employ the same basic principles. Let us assume that one wishes to hide a secret message in an image: the message is embedded in a digital image by the stego-system encoder, which uses a key or password, the resulting stego-image is transmitted in some fashion over a channel (e.g. the Internet) to an intended recipient, where it is processed by the stego-system decoder using the same key (see Figure 4.1).[144] During transmission, unintended or hostile viewers may monitor the stego-image, but they should observe only the transmittal of the innocuous image without discovering the existence of the hidden message (Ballard *et al* 2002, 998; Katzenbeisser 2000, 18-19; Marvel *et al* 1998, 49).

[144] The terminology employed here was decided upon at the First International Workshop on Information Hiding which was organized by Ross Anderson and took place at Cambridge University, UK, in 1996 (see Pfitzmann 1996, 347-350).

Figure 4.1 Overview of Generic Steganographic Scheme*



*Adapted from Marvel *et al* 1998, 50. See also Shin 2000, 19.

The possible covers for hidden messages are innocent looking carriers; in terms of digital steganography, these will be images, audio, video, text, or some other digitally representative code, which will hold or cover the hidden information. A message is the information hidden and may be plaintext, ciphertext, images, or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier. Hiding information may require a stego-key, which is additional secret information (e.g. a password) required for embedding the information. When a secret message is hidden within a cover image, the resulting product is a stego-image (Johnson & Jajodia 1998, 275). According to Mercer *et al*, to be useful, a steganographic system/tool must provide a method to:

(a.) Embed data invisibly,

(b.) Allow the data to be readily extracted,

(c.) Promote a high information rate or capacity, and

(d.) Incorporate a certain amount of robustness to removal (Mercer *et al* 1998, 49).

The remainder of this section is concerned with data encoding in still digital images. This is because the media attention surrounding terrorist use of steganography has focused on the latter.

Image steganography has made great strides in recent times with the development of fast, powerful graphical computers. Images provide excellent carriers for hidden information and many different techniques and tools have been developed for just this purpose.[145] These can be categorised into two groups: those in the Image Domain and those in the Transform Domain. *Image domain* tools encompass bit-wise methods that apply least significant bit (LSB) insertion and noise manipulation. These approaches are common in steganography and may be characterised as 'simple systems.' Typically, the image formats used in such steganography methods are lossless and the data can be directly manipulated and recovered. The *transform domain* grouping of tools include those that involve manipulation of algorithms and image transforms such as Discrete Cosine Transformation (DCT) and wavelet transformation. These methods hide messages in more significant areas of the cover and may manipulate image properties (e.g. luminance). These techniques are generally far more robust than bit-wise techniques. However, a trade-off exists between the amount of information added to the image and the robustness obtained. JPEG images use the DCT to achieve image compression (Johnson & Jajodia 1998, 276-277; see also Sellars 1999, 9-13 & Wayner 1996, Ch. 9).

There are a large number of stego-tools freely available on the Internet: Neil Provos' OutGuess is a universal steganographic tool that allows the insertion of hidden information into the redundant bits of data sources. It is freely available for download from http://www.outguess.org/. Another freely available steganography tool is Spammimic, which is available for download from http://www.spammimic.com: this site, developed by *Disappearing Cryptography* (1996) author Peter Wayner, gives you access to a program that will encrypt a short message into spam (see Kessler 2004). Similarly, a program known as Snow hides information by adding extra white space at the end of each line of a text file or e-mail message. Steghide embeds messages in

[145] To view examples of 'before' and 'after' images (i.e. an image containing a hidden message and the same image with no hidden data contained in it), see Johnson 1995; Marvel *et al* 1998, 58.

.bmp, .wav, and .au files, while MP3Stego does the same for MP3 files (McCullagh 2001a). These tools are surprisingly easy to use (see Karp 2002). And it is precisely this ease-of-use that has led many people to view steganography as an ideal terrorist tool.

> Basically, all a terrorist needs to do is choose a tool, 'stego' a message, and e-mail the message to a friend or post it to a publicly available site. Thereafter, an accomplice can retrieve this container message using the correct pass-phrase and the same software. Because steganography is not widely known, and technologically viable images are prolific on the Internet, it is very likely that the result image will go unnoticed as it reaches its destination (Ballard et al 2002, 998).

STEGANOGRAPHY HITS THE HEADLINES

On 5 February 2001, an article penned by Jack Kelley and headlined 'Terrorist instructions hidden online' appeared in *USA Today*. In the article, Kelley claimed that:

> Through weeks of interviews with US law-enforcement officials and experts, *USA Today* has learned new details of how extremists hide maps and photographs of terrorist targets--and post instructions for terrorist activities--on sports chat rooms, pornographic bulletin boards and other popular Web sites...Officials and experts say the messages are scrambled using free encryption programs set up by groups that advocate privacy on the Internet. Those same programs can also hide maps and photographs in an existing image on selected Web sites. The e-mails and images can only be decrypted using a 'private key' or code, selected by the recipient.

The threat actor is thus immediately identified as all extremists, while their target is identified as not just the US, but also her allies. The blame is then indirectly laid on the privacy advocacy groups who posted the encryption programs allegedly used by the

terrorists. [146] Kelley goes on to quote Ben Venzke, special projects director for iDefense, a cyberintelligence company:

> The operational details and future targets, in many cases, are hidden in plain view on the Internet...Only the members of the terrorist organisations, knowing the hidden signals, are able to extract the information.

The evidence? A quote from CIA Director George Tenet, which does not mention steganography:

> To a greater and greater degree, terrorist groups, including Hezbollah, Hamas, and bin Laden's al Qaida group, are using computerised files, e-mail, and encryption to support their operations.[147]

The next day, 6 February, Kelley followed up with 'Terror groups hide behind Web encryption.' As in the first article, the pornography industry is implicated here also:

> Hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may lie the encrypted blueprints of the next terrorist attack against the United States or its allies.

The evidence? A quote from the FBI Director, Louis J. Freeh, which once again makes no mention of steg:

> Uncrackable encryption is allowing terrorists--Hamas, Hezbollah, al Qaida and others--to communicate about their criminal intentions without fear of outside

---

[146] In Britain, Foreign Secretary Jack Straw provoked a storm of protest by suggesting on the BBC that the media and civil liberties campaigners had paved the way for the terror attacks on America by advocating free speech and favoring publicly available encryption.
[147] From a document Tenet wrote to the US Senate Foreign Relations Committee in March 2001.

> intrusion...They're thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities.[148]

Later in the same article, Kelley identifies a number of locations for online terrorist activities, amongst them regions with little or no public Internet access:

> ... [E]ncryption has become the everyday tool of Muslim extremists in Afghanistan, Albania, Britain, Kashmir, Kosovo, the Philippines, Syria, the USA, the West Bank and Gaza and Yemen, US officials say (Kelley 2001b).

He follows up by insisting that education about online encryption techniques are components of terrorist training courses provided in Afghanistan and Sudan (Kelley 2001b).[149]

Six months later, in July 2001, Kelley penned a further article entitled 'Militants wire Web with links to jihad.' According to Kelley

> Muslim groups are increasingly turning to the Internet to carry on their jihad, or holy war, against the West...The groups use Web sites to plan attacks, recruit members and solicit donations with little or no chance of being caught by the FBI or other law enforcement agencies...Most of the information on the Web sites is written in Arabic and encrypted, or scrambled. The encrypted data is then hidden in digital photographs, which makes it difficult, if not impossible, to find or read...The groups regularly change the addresses of their Web sites to confound officials.

It will be noticed that the threat actor has morphed from the amorphous category "extremists" to "Muslim groups" and jihadists. It is in this article that Kelley charges that al-Qaeda operatives have sent "hundreds of encrypted messages that have been

---

[148] Freeh's testimony was given during a closed-door hearing on terrorism before a Senate panel in March 2001.

[149] Although it is worth pointing out that e-mail, because it uses very little bandwidth, is particularly suitable for communication in areas with slow Internet connections and low-grade infrastructure (Dahan & Sheffer 2001, 96).

hidden in files on digital photographs on the auction site eBay.com." This article differs from the first two not just in its focus on Islamic militants, but also because it contains the first use of the term steganography by Kelley. According to the article

> US officials say that azzam.com contains encrypted messages in its pictures and texts--a practice known as steganography. They say the hidden messages contain instructions for al-Qaeda's next terrorist attacks. Mathematicians and other experts at the National Security agency at Fort Meade, Md., are using supercomputers to try to break the encryption codes and thwart the attacks.

The remainder of the article details the (freely available) contents of a number of Islamist Web sites.

Sandor Vegh describes this series of articles as "one of the most spectacular and edifying examples of threat reporting [in the] offensive against the free use of online encryption" (2002, 10). Approximately three months later, shortly after the attacks of 9/11, the ABC News show *Primetime* dutifully revived the rumour, essentially claiming that it had been substantiated, though no evidence was produced. A stegged photo was shown, but it was a demo, not in any way associated with terrorism (see Ross 2001). Shortly afterwards an Associated Press article entitled 'Bin Laden's cybertrail proves elusive' appeared in *USA Today*. This article comes to rather different conclusions than those reached by Kelley and the producers at ABC. It's opening line reads

> Despite warnings from top government officials that terrorists would use exotic technology to communicate, suspected terrorist mastermind Osama bin Laden instead has used 'no-tech' methods, foiling efforts to track him, former US intelligence officials said.

In fact, according to this article, "Bin Laden relies on human messengers, safe houses and close-knit groups such as family members to send out his directives." Wayne Madsen, a former communications specialist for the National Security Agency, is quoted as saying, "This isn't low tech. You'd have to really call it no-tech" (see also

Manach 2001). In contrast to Bin Laden, Madsen admits that the 9/11 hijackers might have communicated via the Internet. He points to their possible use of seemingly innocuous messages posted on Web sites. For example, some minor change to a Web site might indicate the launch date of an attack, because they knew it in advance (an issue that is discussed in more detail below).

The above notwithstanding, Kelley's original allegations were picked up by *Time Magazine*. Adam Cohen, in his article 'When Terror Hides Online,' suggested that

> A terrorist mastermind could insert plans for blowing up a nuclear reactor in, say, the nose of a puppy on a pet-adoption website. Operatives in the field, told which nose to look at, could then check for their marching orders. Steganography is a fast, cheap, safe way of delivering murderous instructions (Cohen 2001).

Cohen suggests that bin Laden's followers may have learned of steganography "when it burst on the pop-culture scene in recent movies like *Along Came a Spider*." Controversy arose about Cohen's article when Matthew Devost of the Terrorism Research Center charged that the writer had misrepresented him. It appears from the article that Devost believes that terrorists are using steganography on the Internet, but according to Devost: "I do not think that terrorists are using steganography on the Internet and I articulated this belief very clearly to Mr. Cohen."[150]

Finally, in October 2001, an article composed by Reuter's staff, entitled 'Researchers: No secret bin Laden messages on sites,' appeared in *USA Today*. That short piece detailed how computer science researchers at the University of Michigan had written a program to detect messages hidden inside photos on the Web. Peter Honeyman, scientific director of the University's Center for Information Technology Integration, and graduate student Neils Provost, ran a cluster of workstations against more than 2 million images on popular Web sites such as eBay, and attacked the candidates with a dictionary of more than 1.8 million words. They were prompted to do

[150] Devost's comments are posted on his Web site at http://www.devost.net/archives/000036.html.

so by Kelley's original series of articles alleging that terrorists hide secret messages inside innocent-looking photos on the Web. They found nothing (see Provos & Honeyman 2001; also Manjoo 2001). This has not stopped some in the media pointing to terrorist use of steganography as a proven fact (see Friedman 2002; Lyman 2001; McGrory 2001, 11; Soloway, Nordland, Nadeau 2002). A 2003 headline in the *New York Post* read '9/11 Plot Hidden in E-Porn' (Lathem 2003). And *USA Today* persists in revisiting the steganography issue. In August 2004, it published an article entitled 'Look closely: The picture may tell a story,' which basically rehashed the newspaper's original take on steganography as a "covert channel for terrorists around the world" without adding anything new (Berkowitz 2004).

Others are scathing; Ross Anderson of Cambridge University, an expert in information hiding, wrote a letter to *The Times* of London in which he questioned the motives of those "propagating this lurid urban myth."

> Perhaps the goal is to manufacture an excuse for the failure to anticipate the events of September 11th. Perhaps it is preparing the ground for an attempt at bureaucratic empire-building via Internet regulation, as a diversionary activity from the much harder and less pleasant task of going after al-Qaida. Perhaps the vision of bin Laden as cryptic pornographer is being spun to create a subconscious link, in the public mind, with the scare stories about child pornography that were used before September 11th to justify government plans for greater Internet regulation (Anderson 2001).

The argument that newspaper articles such as Kelley's may be linked to government attempts at Internet regulation has been put forward by a number of commentators as the reason for the widespread take-up of the allegations contained in the *USA Today* series (see Leyden 2001; Rosenheim 1997, 170; Vegh 2002). The remainder of this chapter is concerned with describing and analyzing the arguments against widespread terrorist use of digital steganography, which are basically three in number. The first argument focuses on threat image reporting and its effects, and is related not just to Anderson's comments above but also to the analysis of cyberterrorist threat images

contained in Chapter Two. The second argument, which is closely linked to the first, relates not to the content of terrorism threat reporting, but to the originator of the reports, Jack Kelley. The final argument put forward here is somewhat different: in seeking to rebut the assertions about the widespread take-up of digital steganography amongst terrorists made by Kelley and others, the final argument is that terrorist use of digital steganography is both operationally unnecessary and technically risky.

AGAINST TERRORIST USE OF DIGITAL STEG

Jack Kelley as Issue Entrepreneur

How a problem is framed/understood/defined "involves alternative scenarios, each with its own facts, value judgements and emotions" (Edelman as quoted in Livingston 1994, 11), as illustrated throughout Chapter Two. How a particular problem is defined also resonates with practical political consequences. Steven Livingston has identified a number of these. With regard to simplification of the environment, Livingston points out that focusing on specific problem origins eliminates other possible explanations and solutions. In fact, in a case like that of steganography it is not clear that any 'problem' even existed before it was defined as such. The definition of this 'problem' then was very much linked to desired solutions. "Constructions or definitions of problems do not necessarily precede solutions. Rather, problems are often constructed in ways which meet the requirements of desired solutions" (Livingston 1994, 11). The task for those who favour some set of policies over others is to cast about for a problem likely to generate wide fear and attach it to the favoured solution. In terms of investment of authority finally, particular problem definitions invest authority in particular actors and ascribe a variety of deviant roles to others.

Approaches, such as that outlined above, which conceive of political power as issue management need not only concern themselves with the mass media as a unitary actor, but may also benefit from analyses of the content of the reporting of individual issue entrepreneurs. "An issue entrepreneur is a group, administrative agency, or

individual political actor...who encourages the adoption of a particular issue or issue definition rather than some other one" (Livingston 1994, 10). Clearly Jack Kelley acted as an entrepreneur with regard to the issue of terrorist use of steganography. It was his stories that first highlighted the possibility of the latter and, in the wake of 9/11, it was his stories that were repeatedly drawn upon to substantiate the claim that a link existed between terrorism and steganography. This is problematic for two related reasons: Jack Kelley was forced to resign from his position at *USA Today* in January 2004 when it was discovered that a number of his articles for the newspaper were based upon information 'supplied' by fabricated sources (Steinberg 2004). This is relevant because Kelley claimed that his articles about terrorist use of steganography were "based upon weeks of interviews with US law-enforcement officials" (2001a). However, not a single such official is identified by name in the articles which draw heavily upon information allegedly provided by "US Officials," "officials and experts," and "senior US law enforcement officials" (Kelley 2001a, 200b, 2001c). An alternative interpretation portrays Kelley as the dupe--willing or unwilling, it is not clear--of a campaign of misinformation initiated by the US intelligence services (Manach 2001; McCullagh 2001a; see also Deibert 2002, 122).

In any event, in his articles Jack Kelley defined digital steganography as a tool of terrorists and thus set up digital steganographic tools as potential threats to US national--and, indeed, international--security. Kelley thus played directly into the hands of those US lawmakers who favoured restrictions upon the widespread availability of encryption and steganographic tools. Such sensational, high profile reporting of a threat as terrorist serves to build consensus, even active popular enthusiasm, for countermeasures that might have been questioned had the threat not been depicted as terrorist and therefore so immediate and so impervious to less sweeping restrictions. If particular problem definitions serve to rationalise and justify desired solutions, images of enemies serve to focus anxiety on a single dreaded object. Kelley focused in his articles on the activities of Islamic terrorists while also weighing in against the activities of privacy advocates and further invoking what is seen as one of the Internet's major vices: pornography (see Manach 2001).

When a problem is 'securitized' in this fashion, this tends to lead to specific ways of addressing it: threat, defence, and often state-centred solutions (Wæver 1995, 65). In fact, as Murray Edelman has noted, "A central function of some public administrative agencies is the publicising of narratives about threats remote from daily life, for these narratives create the rationale for intelligence organisations, national police agencies, and departments of defence" (as quoted in Livingston 1994, 10). The media may also collude in such processes, however (see Barstow & Stein 2005). As already mentioned, the events of 9/11 resulted in renewed interest in the use of steganography and other encryption technologies online by terrorist organizations. On 25 September 2001, an *ABC News* article pointed the finger for the attacks directly at encryption technologies, the use of which allegedly prevented the NSA from continuing its eavesdropping on Osama bin Laden and his associates. More importantly, the article singled out the freely available encryption tool known as PGP (for 'Pretty Good Privacy') as the greatest concern for law enforcement (Vegh 2002, 12). The *ABC* posting followed a *Washington Post* report four days earlier about the overwhelming grief of Phil Zimmermann, the programmer who invented and made PGP freely available, for having put this powerful technology at the disposal of terrorists (Cha 2001). Zimmermann later stated that he was seriously misquoted in the article and he never regretted PGP (Willan 2003). Moreover, there is no proof that PGP was actually used by the 9/11 terrorists.[151] Sandor Vegh thus accuses the media of twisting stories

> toward supporting an agenda the administration was pushing, namely, a ban on encryption, or a backdoor built in the programs that would enable law enforcement to unlock the code if needed...[As such, Kelley's stories were just] one piece of an elaborate government disinformation campaign aimed at vilifying

[151] PGP has been used by other terrorists, however. In May 2003, for example, Italian police seized at least two handheld devices from Red Brigade members that contained PGP-encrypted information, which was thus rendered unavailable to the authorities (Willan 2003). On the other hand, Phil Zimmermann's Web site, http://www.philzimmermann.com, contains numerous letters of appreciation from human rights organizations that have been able to defy government clampdowns thanks to PGP software.

encryption, in particular, and the Internet, in general, in order to gain public consent for its control (2002, 12-13).[152]

The Internet and the abilities of intelligence officials to eavesdrop on e-mail and phone calls, was supposed to help prevent attacks such as those that occurred in New York and Washington from ever coming to successful fruition. In the event they did not and, as a result, assumptions about the role the Internet could play in fighting terrorism were challenged. Investigators nevertheless relied on Internet tools in their investigation of the attacks as never before (Schwartz 2001). In two successive briefings, however, senior FBI officials stated that the agency had found no evidence that the hijackers used electronic encryption methods to communicate on the Internet. Although many e-mail messages sent to and from key members of the hijack teams were uncovered and studied, none of them, according to the FBI, used steganography. Evidence from questioning terrorists involved in previous attacks, both in America and on American interests abroad, and monitoring their messages revealed that they simply used code words to make their communications appear innocuous to eavesdroppers.[153]

Steganalysis

The third major argument against terrorist use of digital steganography is a technical one. Steganalysis, the science of detecting hidden messages and thence the science of detecting steganography, makes terrorist use of digital steganography tools risky. Just as a cryptanalyst applies cryptanalysis in an attempt to decode or crack encrypted messages, the steganalyst is one who applies steganalysis in an attempt to detect the existence of hidden information (Johnson 2000, 80-81; Johnson & Jajodia 1998, 275).

---

[152] Though Vegh himself points out that Wired magazine's contribution to the terrorism and steganography debate is more balanced than that of the daily newspapers. For example, in a February 2001 article, tech journalist Declan McCullagh actually referred to suggestions that the discourse surrounding steganography is indeed fuelled by the government for a specific agenda: "Some administration critics think that the FBI and CIA are using potential terrorist attacks as an attempt to justify expensive new proposals such as the National Homeland Security Agency or further restrictions on encryption and steganography programs" (McCullagh 2001a; Vegh 2002, 14).

[153] A number of authors persisted in claiming the contrary despite the FBI statements. See, for example, Hosmer & Hyde 2003, 2.

In cryptanalysis, portions of the plaintext (if it is available) and portions of the ciphertext are analysed (see Singh 2001, 19-50). In steganalysis, comparisons are made between the cover object, the stego-object, and possible portions of the message. In cryptography, the end result is the ciphertext; in steganography, the end result is the stego-object. With steganography, the hidden message may or may not be encrypted, as noted earlier. If it is encrypted, then cryptanalysis techniques may be applied to further understand the embedded message on its extraction (Johnson 2000, 81).

Different tools vary in their approaches for hiding information. Without knowing which tool has been employed and which, if any, stego-key has been used, detecting the hidden information may become quite complex. However, some of the tools produce stego-images with characteristics that act as signatures for the steganography method or tool used (Johnson 2000, 80; Johnson & Jajodia 1998, 277). It has always been theoretically possible to produce a completely unbreakable code or completely secret channel, but only at considerable inconvenience. Steganography is not foolproof. [154]

There are two methods of attack on steganography: detection of the embedded message and destruction of the embedded message. Clearly detection defeats the goal of steganography, which is to hide the existence of an embedded message. Destruction advances a step further and prevents the intended recipient of the message from accessing the information contained therein.

Digital images provide excellent covers for hidden information. However, distortions may occur as a result of embedding information. Selecting the optimum combination of steganography tools and covers is key to successful information hiding. Images can become grossly degraded with even small amounts of embedded

---

[154] There are several problems that have arisen when it comes to steganalysis. Since it is a relatively new and growing field, all the problems have not quite been worked out. One of the biggest problems is getting a high number of false positives. This can be attributed to the large amount of images and other kinds of media, and the wide range of sources of these files. A digital camera is a good example of this. There are many different manufacturers of digital cameras, and they all have several models. Between all the different models, from all the different manufacturers, there are over a hundred different formats, using different algorithms for compression. These images can be manipulated by the camera, or image editing programs on the computer. All of this editing and compressing makes it very difficult to determine a 'normal' format against which to compare other images. Monotone pictures and drawings also come up with high false positive rates. In addition, it is extremely hard to detect small messages of fifty bytes or less; the best results, for Stegdetect at least, stem from messages that are 150 bytes or more.

information. This 'perceptible noise' can advertise the existence of hidden information. Characteristics of digital images that point to the existence of hidden information include unusual sorting of colour palettes, relationships between colours in colour indexes, or exaggerated 'noise.' One approach to identifying such patterns is to compare the original cover images with the stego-images and note visible differences. Minute differences are readily noticeable when comparing the cover and stego-images (Johnson 2000, 82). Ross Anderson dismisses most commonly used steganography tools as providing inadequate security. According to Anderson, there are three or four generations of Steganography software available; however, "The stuff you can download is first generation and easily defeated" (McCullagh 2001b).

Neil Johnson, whose work has been utilised extensively in this chapter, is one of a small but growing number of digital detectives working in the field of steganalysis.[155] According to Johnson, his techniques have helped police to take into custody a suspect who raised suspicions after repeatedly e-mailing innocuous photographs to addresses that appeared to be of family members, without ever receiving any replies. "I identified the stego signature that law enforcement used to catch the guy," said Johnson. The US National Security Agency (NSA) and police agencies have underwritten Johnson's research. In fact, the NSA certifies the Centre for Secure Information Systems' graduate program at George Mason from which Johnson obtained his PhD, and the Pentagon funds related research at other institutions.

The United States military also maintains a keen interest in research into new steganography software and applications and the development of new steganalysis tools. The Naval Research Laboratory and the United States Air Force were parties to the fourth, fifth, and sixth annual Information Hiding Workshops, which took place in Pittsburgh in 2001, in the Netherlands in 2002, in Toronto in 2004, and in Catalonia, Spain in 2005 respectively. WetStone technologies based in New York state have also made progress in a tool to detect steganography. Their *Steganography Detection and Recovery Toolkit* is being developed for the US Air Force Research Laboratory in

[155] Steganalysis is a relatively young research field; few articles on the subject appeared before the late 1990s. Gary Kessler (2004) provides some examples of currently available software that can detect the presence of steganography programs, detect suspect carrier files, and disrupt stegged messages. Many more steganalysis programs are listed at http://www.stegoarchive.com.

Rome, New York. The goal of the toolkit is "to develop a set of statistical tests capable of detecting secret messages in computer files and electronic transmissions, as well as attempting to identify the underlying steganographic method." The project arose out of a study the Air Force commissioned from WetStone on forensic information warfare in 1998. At that time, the company was asked to identify technologies that the Air Force needed to guard against and it highlighted steganography as one of these (McCullagh 2001b).

WetStone has also developed a commercially available application known as Stego Suite. The suite includes Stego Watch, Stego Analyst, and Stego Break. Stego Watch allows users to detect digital steganography, or the presence of communications hidden in digital image or audio files, and can extract information that has been embedded with some of the most popular steganography tools using a dictionary attack. Stego Analyst is a full featured imaging tool that allows investigators to search for visual clues that steganography has in fact been utilized in both image and audio files. Stego Analyst combines with Stego Watch to allow individual suspect images to be visually examined. In addition to visual clues, Stego Analyst gives users the ability to examine characteristics such as color palettes, hue, intensity, used colors, and their red-green-blue (RGB) values. Finally, Stego Break is an application designed to obtain the password that has been used on a file found to contain steganography. Currently, Stego Break can crack passwords for JP Hide 'n Seek, F5, JSteg and Camouflage steganography embedding applications. This program continuously scans a web domain for the presence of hidden data. Stego Suite can be purchased from WetStone technologies for approximately US$2,000. The other well-known steganalysis tool is StegDetect, which was developed by OutGuess creator Niels Provos. It is capable of detecting several different steganographic methods for embedding hidden information in JPEG images. Currently, the detectable schemes are Jsteg, Jphide, Invisible Secrets, Outguess , F5 (header analysis), AppendX, and Camouflage. StegDetect is available for free download from the Internet.

Lastly, any cover can be manipulated with the goal of disabling or destroying some hidden information, whether there is an embedded message contained therein or not. While detecting the existence of a hidden message will save time in the disabling

phase by processing only those covers that contain hidden information, detection is not a bar to disablement. Consider the scenario mooted by Kelley in his July 2001 article: an individual wishes to covertly communicate by hiding messages in images on public Internet sites. Suppose all image files uploaded by this individual, say Alice, pass through some gateway, perhaps a computer server, which is under the control of Bob. Bob wants to automatically introduce noise into *all* image files passing through the gateway in order to disrupt any such covert communication. Bob need not examine the files individually to try to find hidden information. Rather, the disruption may be completely automated (Ettinger 1998, 321). So, reverting to Kelley's assertion that terrorists are hiding instructions for attacks on sites such as eBay and, presuming that this were actually taking place, eBay and other similar sites would have at their disposal a fairly simple means of stamping out such practices. Terrorists ought therefore to utilise low-tech steganographic methods instead.

ALTERNATIVE SECURE COMMUNICATION METHODS

Low-Tech Steg

There is ample evidence supporting the assertion that terrorists employ encryption on files stored on their computers' hard drives and in their electronic communications. According to Denning and Baugh, some terrorist groups are employing high-frequency encrypted voice and data links to communicate with their state sponsors. They also state that Hamas is using encrypted Internet communications to transmit maps, pictures, and other details pertaining to terrorist attacks[156] (Denning & Baugh 2001, 117; see also Jolish 2002). The FBI located encrypted files on the laptop computer of Ramsey Yousef, a member of the group responsible for the original attack on the World Trade Centre in 1994 and a Philippine airliner in late 1995. On decryption these files were found to contain information detailing further plans to blow up eleven US-owned

[156] According to Denning and Baugh, the Israeli General Security Service believes that most of the data is being sent to the Hamas worldwide centre in Great Britain (2001, 117).

commercial airliners in the Far East. Much of this information was also available in unencrypted documents, but successful decryption of electronic records can be important to an investigation. This was the case when Japanese authorities seized the computers of the Aum Shinrikyo cult. Aum had stored encrypted information on the computers; the authorities were able to decrypt the files after finding the key on a floppy disk. According to Denning and Baugh, the files contained evidence that was crucial to the investigation (Denning & Baugh 2001, 120).

There have been a small number of reported cases of criminals using steganography to facilitate their crimes. For example, a credit card thief used it to hide stolen card numbers on a hacked Web page. He replaced bullets on the page with images that appeared the same, but that contained the credit card numbers, which he then offered to associates (Denning & Baugh 2001, 133; see also Libbenga 2004a). There is no substantiated evidence of terrorists employing the same techniques, however.[157] A majority of the media accounts detailing terrorist use of steganography draw heavily on the original unsubstantiated assertions made by Jack Kelley in *USA Today*. It has become an article of faith that bin Laden and his associates routinely communicate through stegged messages posted on pornographic Web sites.[158] The following statement by US Army Lt. Gen. Joseph Kellogg Jr., Director of Command, Control, Communications, and Computers for the Joint Staff, is fairly representative: "They are hiding stuff in pictures and embedding them in places we can't get to...like porn sites" (Caterinicchia 2003). Which raises the question, if you cannot get to them, how you know they're there? By reading *USA Today* perhaps?

---

[157] To date, the only comment from a government official implying a direct connection between terrorists and digital steganography has come from an unnamed source formerly connected to the French Ministry of Defence. The source, as noted in an October 30, 2001 article in the *New York Times*, claimed that a terrorist suspect named Jamal Beghal used the technique to plan a failed suicide bomb attack on the U.S. embassy in Paris. "The terrorists were instructed that all their communications were to be made through pictures posted on the Internet, the defense official said" (Kolata 2001; see also Erlanger & Hedges 2001). Details about this alleged use of steganography remain scant, however. Beghal and a number of accomplices were convicted of the plot in a French court in March 2005; however, it was Kemal Daoudi and not Jamal Beghal who was convicted of being the group's logistics and communications expert and it remains unclear whether he employed steganography in this role (Associated Press 2005; Benhold 2005).

[158] The frequency of such assertions led one journalist to comment "that the likelihood of Islamic fundamentalists hiding messages in porn is roughly the same as their likelihood of hiding them in pig carcasses" (Greene 2003).

There are those who are sceptical of these assertions, however. Indeed, many analysts believe that al-Qaeda uses prearranged phrases and symbols (i.e. low-tech steganography) and not digital steganography to direct its operatives. With regard to the Internet for example, "an icon of an AK-47 can appear next to a photo of Osama bin Laden facing one direction one day, and another the next. Colours of icons can change as well. Messages can be hidden on pages inside sites with no links to them, or placed openly in chat rooms" (Soloway *et al* 2002). Another suggestion, made by Michael Caloyannides, a computer forensics specialist, which doesn't involve the Internet *per se* but ATM networks instead, involves the simple withdrawal of say £20 from a machine in London, which could serve as an instant message to an accomplice monitoring the account from anywhere in the world (Zeller 2004, C1). Secret communications of this type (i.e. those that are not in written form) are known as semagrams. Similar forms of communication have proved successful in the past.

In 1993, for example, the forces of Somali warlord Mohamed Farah Aidid banged out messages on drums instead of using telephones in order to thwart the efforts of US forces seeking to intercept his communications. While in the 1980s, David O'Connell, the then-Chief of Staff of the Provisional Irish Republican Army (PIRA), gave a television interview in which he announced the commencement of a bombing campaign in Britain, which materialised a week later with the bombing of two bars in Birmingham in which twenty-one people died. The possibility exists, although it cannot be proven, that O'Connell used the television appearance to signal the attacks to PIRA operatives stationed in the UK (Schmid & De Graaf 1982, 43). It was probably similar fears that prompted US National Security Adviser, Condoleeza Rice, to request US television networks not to air the video of Osama bin Laden that was delivered to Al Jazeera television in the wake of 9/11. The US networks declined the request due, they said, to the fact that the video was easily downloadable via the Internet and therefore already freely available. In February 2003, George Tenet, the then-director of the CIA, told the Senate Armed Services Committee, that analysts were examining audio recordings allegedly made by Osama bin Laden, looking for particular phrases or words that might be coded signals to al-Qaeda operatives in the field. In particular, analysts were said to be examining passages of audio that referred repeatedly to al-Qaeda's

efforts to dig "trenches" in Afghanistan and statements urging his followers to "fight in the plains, mountains, farms, and cities." An individual described as a "senior intelligence official" said that analysts had not come to any definitive conclusions, but said that it was possible that the message, taken in its entirety, was a "go signal" (Johnston 2003).

In an interview recounted in London's *Sunday Times* newspaper, two of those involved in the preparations for the 9/11 attacks, Khalid Sheikh Mohammed and Ramzi Binalshibh, revealed to a reporter from Al Jazeera television that Mohammed Atta communicated with Binalshibh in German via the Internet. He posed as a student in America contacting his girlfriend 'Jenny' in Germany. According to Mohammed and Binalshibh, an elaborate code was agreed so that Atta could keep in touch with his al-Qaeda commanders through e-mail and Internet chat rooms. For example, the targets were referred to as university departments: the Twin Towers were the 'faculty of town planning'--Atta's academic speciality; Capitol Hill was the 'faculty of law' and the Pentagon was the 'faculty of fine arts' (Fielding 2002, 1; Fouda 2002, 15-17). Yosri Fouda, the journalist who conducted the interview, reports that he saw the last communication between Atta and Binalshibh, which was conducted in German and took place in an Internet chat room. It read:

> The first semester starts in three weeks. Nothing has changed. Everything is fine. There are good signs and encouraging ideas. Two high schools and two universities. Everything is going according to plan. This summer will surely be hot. I would like to talk to you about a few details. Nineteen certificates for private study and four exams. Regards to the professor. Goodbye (Fouda 2002, 17).

The Indonesian authorities also claim to have intercepted e-mails sent by members of the group Jemaah Islamiyah (JI) which used the phrase "to marry as soon as possible," which the former say was a JI code word meaning to plant a bomb (Aglionby 2003, 17). Such low-tech fixes are similar to those found in the section on secure

communications in the al-Qaeda training manual, some of which methods date back at least fifty to one hundred years (Denning 2004, 12).

Anti-communist terror squads in El Salvador employed a similar strategy in 1977 when on election day they seized the radio station of the National Water Authority and used it to instruct their followers with coded messages. The code word for the opposition votes was 'coffee' and 'sugar' meant votes for the terror squad's own supporters. 'Little birds' were election supervisors and 'giving lessons' meant to intimidate them. 'Put some *Tamales* in the tank' signified filling ballot boxes with fraudulent votes. Those candidates who supported the right-wing terror squads triumphed in the radio-controlled election (Schmid & De Graaf 1982, 26-27).

E-Mail & E-Groups

Of course, the employment of encryption and steganography, whether digital or low-tech, are not the only ways--perhaps not even the best way--to seek to secure one's online communications. Todd Hinnen suggests that a common alternative is to provide the username and password of an e-mail account to all the members of a conspiracy. One member drafts, but does not send, an e-mail message. He then exits the e-mail account. His co-conspirators can log on to the same account from anywhere in the world, read the draft, and then delete it. Because the draft was never sent, the ISP neither retains a copy nor is there a record of it traversing the Internet. This is because the message never went anywhere: its recipients came to it. Another method for secure online communication described by Hinnen involves providing basic electronic mail services in conjunction with a terrorist(-sympathizer) Web site. Hinnen provides the example of an imaginary Web site www.jihad.com, which is password-secured and supports basic e-mail services. E-mail could be sent from one of the e-mail accounts provided by such a Web site (e.g. johndoe@jihad.com) to another (e.g. janedoe@jihad.com) without ever leaving jihad.com's servers. It could not, therefore, be intercepted or tracked. In fact, intelligence and law enforcement would have no way of ever knowing about such a message unless they obtained access to jihad.com's servers or records (Hinnen 2004, 39; Zeller 2004, C1). Such e-mail accounts then could

be used as effective dead drops to facilitate completely anonymous, asynchronous communications.

Terrorist organizations might also communicate securely using e-groups.[159] A user may register an e-group with only a valid e-mail address. If the user wishes, he can control who joins the group, what messages its readers post for review, and whether its content is publicly available or password protected. E-groups probably appeal to terrorists for a number of reasons. They can be established for free and without providing any authentic identifying information. They facilitate mass communication to geographically dispersed groups: using one e-mail address, an e-group member can reach hundreds or thousands of other members across the globe. E-groups also tend to be available even in countries that strictly limit Internet use because they are established in subdirectories of innocuous Internet services such as Yahoo! Finally, e-groups can be established with built-in security in the form of a password. For these reasons, according to Hinnen, "e-groups may be broadly used by terrorist organizations for everything from ideological indoctrination and the dissemination of *fatwas*, to providing directions to *mujahideen* training camps, to operational planning for future attacks" (Hinnen 2004, 40).

CONTRARY VIEWS

Having described and analysed the inconsistencies contained in Jack Kelley's original series of articles asserting widespread terrorist use of digital steganography to conceal their communications, the increasing availability and sophistication of detection tools, the highly secure nature of many low-tech steganography methods and, finally, the

[159] An e-group is a service offered by an Internet Service Provider through which users with common interests can exchange messages. When the 'owner' of an e-group registers that group, s/he can determine both whether it is public (i.e. open to anyone) or private (i.e. open only to invited users possessing a password) and whether it is moderated (i.e. user messages may only be posted by a moderator who has reviewed the message) or un-moderated (i.e. users may post messages directly, without the intervention of a moderator). Users may elect to receive posted messages either by visiting the e-groups website, where recently posted messages are archived, by receiving each message in their e-mail accounts as it is posted, or by receiving a periodic digest of messages in the same fashion.

availability of reliable alternatives to both encryption and steganography by which terrorists might ensure secure online communication, it would be remiss not to mention that a number of prominent IT security experts remain wedded to the proposition that terrorist use of digital steganography tools is widespread.

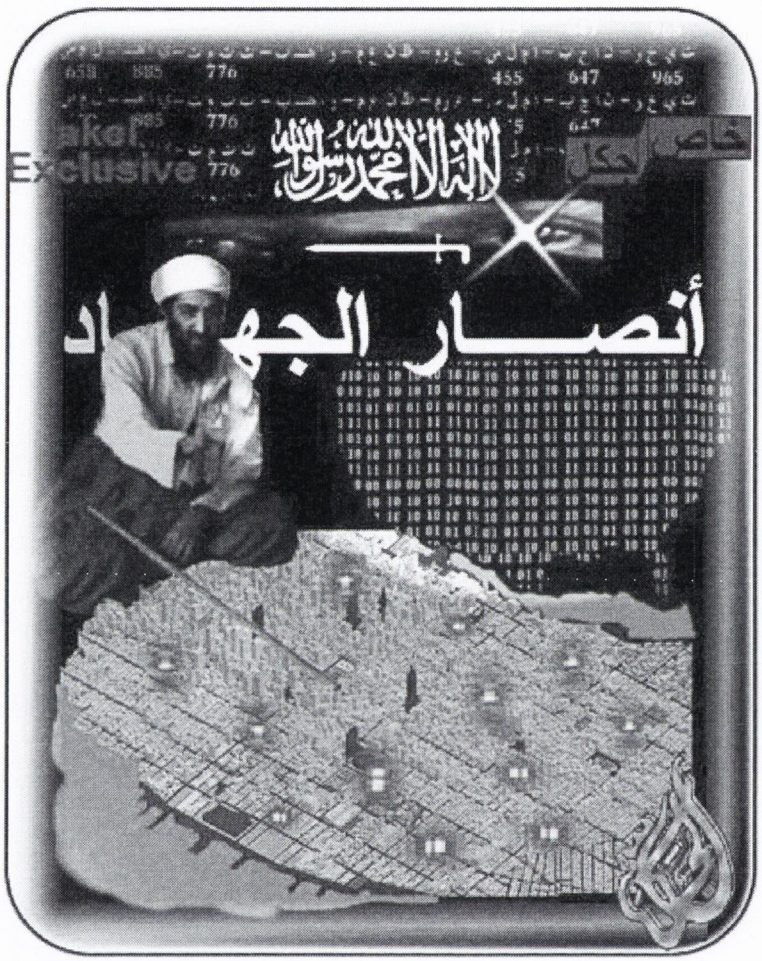
Chet Hosmer, the president and CEO of WetStone Technologies claims to have found stegged images on the eBay auction site. In fact, according to Hosmer, "Quite an alarming number of [Internet] images appear to have steganography in them." While newspaper reports have claimed that Neil Johnson has become so worried by steganography's potential use by terrorists that he stopped publishing his research on how to detect it, reasoning that if people knew how he detected it, and where, they could devise new methods to thwart detection and/or move their messages to sites he had not checked (Kolata 2001). Bruce Schneier (2001) has also contributed to the debate. "Steganography is a good way for terrorist cells to communicate, allowing communication without any group knowing the identity of the other," according to Schneier, although he provides no evidence in support of this observation. In contrast, Neil Doyle, author of *Terror Tracker* (2004), has pointed to an Islamist Web site that is intermittently available and which shows Osama Bin Laden and a map of Manhattan (see Figure 4.2).

> It contains 'red sites (that) appear to be identifying targets for being attacked,' says Neil Doyle, a new kind of private detective. And what worries [Doyle] about the site, one of thousands he's discovered, are the numbers running across the page. 'The repeated sequence at the top there and it's thought that, well, that does match up to a known al Qaeda cryptography method'...Doyle believes the site's code could be a means of command and control (CBS News 2004).[160]

Dorothy Denning also allows that al-Qaeda operatives may "possibly" be employing steganography based on content contained in the group's online magazine *Al-Battar*

[160] Thanks to Dorothy Denning for drawing my attention to this site.

Figure 4.2 Image from Abualbukhary.net, July 2004



Training Camp. In the sixth issue of this publication, which appeared in March 2004, the use of Web sites as dead drops is advocated (Denning 2004, 12). Denning[161] also sounds a note of caution as to the usefulness of the University of Michigan study (Provos & Honeyman 2001) referred to earlier (see also Kessler 2004). Terrorism scholars who have endorsed the assertion that terrorists routinely employ steganography include Magnus Ranstorp (2004, 62 & 64), Timothy Thomas (2003, 119), and Gabriel Weimann (2004a, 10; 2004b, 16; 2006, 131-132).

[161] Personal e-mail correspondence of 3 December, 2004.

CONCLUSION

At base, steganography is a procedure for hiding information from an enemy's prying eyes and is therefore not a new idea, as illustrated in section one. Digital steganography is a relatively new invention however and section two is devoted to demystifying it. It has been widely reported--in *USA Today*, the *New York Times*, the *Times* of London, *Newsweek*, *Time* magazine, and many other venues--that terrorist groups employ digital steganography to engage in covert communication. In particular, the assertion that Islamist terrorist organizations routinely post secret information and plans on pornographic Web sites is accepted as fact. A large part of this chapter is concerned with showing that this is unlikely to be the case. The argument here is not that terrorists are unfamiliar with technology; clearly they are quite familiar with the Internet and its use(s) as illustrated in Chapter Three, and have shown themselves to be technologically adept in other respects also (see Clarke 2004; Hoffman1998, 180-183; Hoffman 1999, 28-38).[162]

Nor is the argument that terrorists do not employ steganography. Crucially, the argument here is that terrorists are more likely to employ low-tech steg (e.g. null ciphers, semagrams, etc.) than high-tech steg (i.e. digital steganography tools) in their communications. This is because the use of digital steganography by such groups is both technically risky--due to the availability of tools to detect stegged messages--and operationally implausible--due to the availability of low-tech steganography and other secure communication methods the existence of which are difficult to detect and almost impossible to prove. It is submitted that Jack Kelley's reliability as an information entrepreneur is also compromised, however. To conclude: the main problem facing communications intelligence experts is selection (i.e. knowing which of the billions of e-mails or Web images to look at) rather then the possibility that the e-mails or images might be stegged, encrypted, or otherwise camouflaged. A competent opponent is unlikely to draw attention to himself by being one of the relatively few users of digital steganography.

---

[162] The technological prowess of some al-Qaeda members has been questioned, however, due to their use of anonymous Swiss mobile phone SIM cards that they appeared to believe upon insertion actually anonymized mobile handsets (see Lettice 2004; Van Natta & Butler 2004).

PART III

ON TERRORIST WEB SITES

"On the Internet, attention replaces media and mobility replaces space as the primary values and organizing metaphors. It is not important how often you speak or how widely you broadcast it, but how many people listen. Space can be bought at the local computer store, but what counts is how easy it is to access your space. Sometimes this depends on skill with software and access to the best hardware. Technology can therefore produce power, as in the real world, but power has other sources as well. Charisma and knowledge are power in the real world and perhaps even more so in the virtual. On the Net your identity is changeable, produced rhetorically and sustained or deconstructed by manipulating knowledge"

- Chris Hables Gray (2001)

5

TERRORIST WEB SITES: THEIR CONTENTS, FUNCTIONING, AND EFFECTIVENESS

INTRODUCTION

There has been a shift in emphasis in this text from an initial focus on cyberterrorism and its portrayal in the mass media to what has been termed terrorist 'use' of the Net. While the previous chapter focused upon allegations that digital steganography tools have been widely used by terrorists to facilitate intra-group communications, the present chapter revisits a number of the other 'use' issues raised in Chapter Three. Many of these uses rely on a functioning Web site, whether operated by terrorists and/or their supporters to engage in propaganda and raise funds or sites operated by others, but used by terrorists for communication, data mining, or planning and coordination purposes. Four of the five major terrorist uses of the Internet, as identified in Chapter Three, may be pursued by terrorists via their own Web sites. These are information provision, financing, networking, and recruitment. (Clearly, information gathering is, for the most part, reliant not on terrorists' own sites, but the information posted on the Internet by others). The following chapters are therefore centrally concerned with exploring the primary materials provided by modern terrorists in the form of their Web sites, in an effort to map the virtual terrorist presence, with a view to highlighting the increasing role of soft power in our information society and the way in

which Internet-savvy terrorist groups have wielded this. The coding scheme described below is designed to address two questions: Are terrorist Web sites contributing to the four functions identified? How well or effectively are they performing these functions? (Gibson & Ward 2000, 306).

COMPARING TERRORIST WEB SITES: METHODOLOGY

Of the thirty-six organisations that currently appear on the US State Department's list of Designated Foreign Terrorist Organisations, fifteen maintain official sites.[163] Ten of these are available in English, and it is these sites that will be the subject of this analysis.[164] All ten groups, their countries of origin, and the URLs of their Web sites are listed in Table 5.1.[165] The content analysis of the sites closely follows the coding scheme developed by Rachel Gibson and Stephen Ward in their article 'A Proposed Methodology for Studying the Function and Effectiveness of Party and Candidate Web Sites,' which appeared in the *Social Science Computer Review* in 2000. Although Gibson and Ward focus on political party and election candidate Web sites, they foresee their scheme as having broader applicability to the sites of other political actors such as, they say, "Internet groups, municipal governments, and civic or community-based pro-democracy advocates" (Gibson & Ward 2000, 302). Gibson and Ward do not specifically refer to terrorist organisations; nonetheless, their general

---

[163] Some sites are clearly more official than others. There is no doubt, for example, that the Hizbollah Web sites were established and are maintained by the Hizbollah organisation. The same is true of the LTTE site. Other sites were established and are maintained by organisations with close ties to the concomitant terrorist organisation. This is true of the Committee to Support the Revolution in Peru (CSRP) who founded and maintain Sendero Luminoso's Web site. Sites such as the latter are of a quasi-official nature; sites not represented here are those founded and maintained by supporters who appear to have no direct ties to the groups for whom they cheerlead.

[164] All Web sites were downloaded in January 2004 with the exception of the Hamas site, which was downloaded in May 2004. It is worth noting here that the results of this and similar analyses are always provisional because the subject of analysis is impermanent. This is a snapshot of the terrorist presence in cyberspace on given days at given times.

[165] Brief profiles of each of the groups are contained in the US State Department's annual publication *Patterns of Global Terrorism*, which are available online at http://www.state.gov/s/ct/rls/pgtrpt/. See David Whittaker's *Terrorism Reader* (2001) for additional background information on Hizbollah (Ch. 4), the LTTE (Ch. 6), ETA (Ch. 9), Sendero Luminoso (Ch. 11), and FARC (Ch. 12).

Table 5.1 Terrorist Group Web Sites

Terrorist Group	Country/Region of Origin	URL of Web Site
Aleph/Aum Shinrikyo	Japan	http://english.aleph.to
Basque Homeland and Liberty (ETA)	Spain	http://www.contrast.org/mirrors/ehj/aehj/aehj.html
Revolutionary Armed Forces of Colombia (FARC)	Colombia	http://www.farc-ep.ch/pagina_ingles/
Hamas	Israeli-Occupied Territories	http://www.hamasonline.com
Hizbollah	Lebanon	http://www.moqawama.tv/page2/main.htm
Kach/KahaneChai	Israel, USA	http://www.kahane.org/home.html
Liberation Tigers of Tamil Eelam (LTTE)	Sri Lanka	http://www.eelamweb.com
New People's Army (NPA)	Philippines	http://www.philippinerevolution.org
Kurdish Workers Party (PKK)/Kongra-Gel	Turkey	http://www.kongra-gel.org/
Sendero Luminoso	Peru	http://www.csrp.org

schema was judged to be applicable to these sites also. This is because their coding scheme seeks to gather evidence pertaining to basic questions applicable to all political Web sites: a.) what the purpose(s) of the sites are and b.) how effectively they deliver their contents. The scheme facilitates the comparison of sites based on indicators for information and communication flows and those for site delivery.

Functionality

To assess functionality, the coding scheme was organised around Web sites' broad direction of information and communication flow (ICF). Four categories of ICF are identified: downward, upward, lateral (inward or outward), and interactive. The first three categories of ICF are unidirectional (i.e. communication is predominantly one-way); downward from the organisation to the individual user, upward from the user to the organisation, outward from the organisation to other bodies, or inward to internal groupings. The latter two flows may be described as lateral. Interactive ICFs are two-way or multidirectional contacts between groups and individuals whereby there is input

from one side (usually the user) with the expectation of producing a response from the other side. Transactional communications such as donating, where the exchange is non-substantive and one-way, are considered to constitute an upward rather than an interactive ICF. Gibson and Ward draw a distinction between asynchronous or sequential interaction and synchronous or real-time exchanges within the category of interactive ICF. As a result of that distinction, which is maintained here, a search engine was considered an asynchronous interactive mode of communication because a response follows user input after a certain time delay and cannot then be subject to modification, while chat rooms are considered synchronous interactive modes of communication because they allow for free-flowing exchanges in which both inputs and responses are subject to continuous modification (Gibson & Ward 2000, 306).

Table 5.2, 'Information and Communication Flows on Ten Terrorist Web Sites', is divided into five categories. The first category, 'Downward Information Flows', is based largely on word counts of the groups' organisational histories; available documents, such as manifestos, etc.; values or ideologies; organisational structures; details of operations; leader profiles; negative campaigning; and credit claiming. The figures for 'Newsletters' and 'Media releases' refer to the number of each available on the Web site, including archived copies. The availability of a FAQ (i.e. list of Frequently Asked Questions) was coded on a simple 'present/absent' (1/0) basis. The number accompanying the category 'Targeted pages' refers to the number of groups targeted. The second category is 'Upward Information Flows' and refers to the presence or absence of donation mechanisms, merchandise for sale, and cookies coded on a 1/0 basis. Category three, 'Lateral/Horizontal Information Flows,' is focused on sites' link structures, specifically the number of links to groups supportive of the organisation's goals (i.e. 'Partisan Links'), the number of general information sites linked to from the terrorist site (i.e. 'Reference Links'), and the number of sub-organisational groups linked to (i.e. 'Internal Links'). The final two categories deal with 'Interactive Information Flows.' Category four deals with the measure of asynchronous flows (i.e. sequential interaction): the number of opportunities available to download logos, posters, and/or screensavers; the presence or absence of online art galleries, photo archives or galleries, site searches, online games or gimmicks, e-mail lists, and bulletin

Table 5.2 Information and Communication Flows on Ten Terrorist Web Sites

	Aleph	*ETA*	*NPA*	*Hamas*	*Hizbollah*	*Kach*	*PKK*	*LTTE*	*FARC*	*SL*
Downward Information Flows										
Organisational History	1,169	18,791	30,042	18,162	0	0	0	12,844	4,222	8,368
Documents	2,552	3,991	29,823	9,181	0	0	3,842	10,289	8,170	36,803
Values/Ideology	5,238	3,226	19,375	5,184	0	1,550	12,382	2,653	9,376	14,126
Structure	1,596	0	247	0	0	0	0	133	4,617	0
Operations	0	0	0	0	108,896	0	0	5,512	0	8,944
Newsletters	0	0	79	0	0	0	0	0	4	9
Media Releases	13	0	137	615	0	0	1	15	12	0
Leader profile	0	0	14,236	13,035	0	1,237	427	28,261	0	23,255
FAQ	0	0	1	0	0	0	0	1,526	0	0
Negative Campaigning	0	16,951	0	16,515	705,836	0	0	1,156	8,699	24,367
Credit Claiming	0	0	0	0	108,896	0	0	5,682	0	0
Targeted Pages	0	1	0	0	0	0	0	1	0	1
Upward Information Flows										
Donation	0	0	0	0	0	1	0	0	0	0
Merchandise	0	0	0	0	0	1	0	1	0	1
Cookies	0	0	0	0	0	0	1	0	0	0
Lateral/Horizontal Information Flows										
Partisan Links	0	7	6	5	2	19	21	0	0	10
Reference Links	0	15	0	0	0	6	0	3	0	0
Internal Links	12	0	1	2	23	1	1	0	0	0
Interactive Information Flows: Asynchronous										
Download Logos/Screensavers/Posters/Pamphlets	0	0	0	642	0	3	0	10	0	11
Online Art Gallery	0	1	0	0	0	0	0	0	0	1
Online Photo Archive/Gallery	0	1	1	0	1	1	0	1	0	0
Site Search	0	0	0	1	1	1	1	0	0	1
Online Games/Gimmicks	0	1	1	1	1	1	0	1	0	1
E-mail Contact	17	3	2	1	1	1	0	4	1	0
E-Mail Feedback	4	1	4	1	1	4	3	1	3	3
Join E-mail List	0	1	1	1	0	1	0	1	0	0
Bulletin Board	0	0	0	0	0	1	0	0	0	0
Interactive Information Flows: Synchronous										
Chat Room	0	0	0	0	0	0	0	0	0	0

boards; and the number of addresses offered through which to initiate e-mail contact. 'E-mail feedback' is classified using a four-point scale: presence of e-mail address (1), e-mail requesting comments (2), online form/poll (3), no reference (0). The final category, 'Interactive Information Flows: Synchronous' (i.e. real-time exchanges), identifies the presence or absence of chat rooms on the various sites measured on a simple 1/0 basis.

Delivery

The second issue of interest is the success of the terrorist Web sites in delivering the postulated functions. This was divided into six basic components: presentation and appearance, accessibility, navigability, freshness, and visibility.[166] Presentation and appearance refers to the 'glitz factor.' Gibson and Ward break this component down into two sub-categories: flashiness (graphics emphasis) and dynamism (multimedia properties). Basically, site designers endeavour to engage the browser's attention by manipulating font type and size, text spacing, graphics, colours, backgrounds, video clips, sound bits, animation, and interactive gimmicks. The visual appeal and entertainment value that such properties add to a site are considered to make it more effective in delivering its message than, say, purely static, plain-text pages. Research has indicated, however, that although minimal levels of novelty can stimulate and demand attention, extreme novelty leads to over stimulation, cognitive overload, distraction, and ultimately, impaired information processing (Hill & Hughes 1998, 147).

The second component is accessibility. High levels of 'glitz' will be undermined if a site is off-line, takes a long time to load, and various features and/or pages are inaccessible. Third, navigability is an important component of any site. A site that is easy to move around and makes it simple to locate particular information

[166] Gibson and Ward included a seventh category, responsiveness, which tested the speed and quality of the response to an e-mailed request for information. This category was not included in this research as a number of researchers in this area advised me that, based on their experience, responses to such a general request were unlikely to be forthcoming. I will explore the issue of responsiveness in future research nonetheless.

communicates its message more effectively. Site maps and search engines are factors that assist efficient site navigation. Fourthly, freshness is considered key to effective content delivery. Sites that are regularly updated will create more interest than those that are not. Stale sites deter repeat visits. Finally, measures of visibility of the site on the WWW were also included. To deliver its contents, a site must be relatively straightforward to locate. A site that is not visible on the Web is failing to deliver its contents (Gibson & Ward 2000, 308).

Table 5.3, 'Terrorist Web Site Delivery,' explores the effectiveness of terrorist Web sites in terms of their delivery of the functions stated earlier and utilising the categories identified above. 'Flashiness' was measured in terms of the total number of images appearing on the site, including those contained in photo archives and online art galleries. Images appearing on menu bars were counted only once if they were fixed as a frame to reappear on each page. The dynamism of sites was measured in terms of multimedia content using a four-point scale: moving icons (+1), audio (+2), video (+3), live streaming (+4). 'Freshness' was classified on a six-point scale according to whether the site was updated daily (6), every one to two days (5), every three to seven days (4), every two weeks (3), monthly (2), every one to six months (1), or hadn't been updated for more than six months (0). Accessibility was broken down into three categories. A count was made of the number of languages, including English, in which each site was available. The second category explored the sites' accessibility in principle by measuring whether each site had a no-frame option (+1), text-only option (whole site) (+1), text-only documents to download or print (+1), foreign language translation (+1). On a more practical level, a simple 1/0 count was used to record whether a site was working or inaccessible on a given date (a) and a measure of the English home page in Kb was also recorded at that time (b). The number attached to 'Navigability' is based on the following calculation: navigation tips (+1), number of search engines (+n), home page icon on each page (+1), major site area links/menu bar on each page (+1), site map/index (+1). Finally, visibility was measured in terms of an advanced Google search measuring 'links in' both to the top-level English-language page (a) and the home page of the group's main Web site (b), if such existed.

Table 5.3 Site Delivery Indicators for Ten Terrorist Web Sites

	Aleph	*ETA*	*NPA*	*Hamas*	*Hizbollah*	*Kach*	*PKK*	*LTTE*	*FARC*	*SL*
Graphics/Flashiness	117	141	77	679	367		23	588	8	286
Multimedia/Dynamism	0	6	6	6	6	6	0	6	0	5
Freshness	0	0	5	5	5	1	1	1	1	1
Languages	3	3	2	1	2	3	4	1	6	2
Accessibility (in principle)	1	1	1	0	1	1	2	0	1	2
Accessibility (in practice)	(a.) 1 (b) 7Kb	(a.) 1 (b) 45.5Kb	(a.) 1 (b) 21Kb	(a.) 1 (b.) 26Kb	(a.) 1 (b.) 6Kb	(a.) 1 (b.) 55Kb	(a.) 1 (b.) 50.5Kb	(a.) 1 (b.) 23Kb	(a.) 1 (b.) 1Kb	(a.) 1 (b) 8Kb
Navigability	3	1	4	3	3	1	3	2	2	5
Visibility (links in)	(a.) 19 (b.) 27	(a.) 128	(a.) 38	(a.) 26	(a.) 21 (b.) 60	(a.) 5 (b.) 152	(a.) 8 (b.) 43	(a.) 247	(a.) 0 (b.) 72	(a.) 180 (b.) 29

ANALYSIS OF CONTENT

Downward Information Flows

Background Information

So what is the content of terrorist Web sites? A majority of the sites analysed provided historical background on the group and the conflict. This ranged from extensive background on Palestine, the land and its people, on the Hamas site, along with a brief profile of the group (approx. 500 words) to the Aleph site which contained a brief "apology for the Aum Shinrikyo-related incidents" and concise details of "drastic reform" of the organisation. The FARC site contained just a small amount of historical information and had not been updated to reflect the prominently displayed reference to the groups' fortieth anniversary 'celebrations' on their overall homepage. This is in contrast to the large amount of background information to be found on the NPA site, including text and pictures relating to the thirty-fifth anniversary of the group's founding. Just three sites were devoid of substantive historical content; these were the sites maintained by Hizbollah, Kach, and the PKK. Hizbollah maintain a suite of Web sites and extensive background information on the group is provided on their Central Press Office site. The Kach and PKK sites, on the other hand, appeared to be more concerned with current news and events than explanation of their positions based on historical events. The lack of background information may also point to a presumption on the part of these sites' creators that visitors to their sites are already familiar with the groups' origins and the history of the respective conflicts.

'Official' Documentation & Ideological Tracts

Large amounts of 'official' documentation were to be found on the Web sites of the leftist organisations. The Web site of Sendero Luminoso contained a section entitled 'Documents of the Communist Party of Peru,' which included numerous reports and declarations of the group's Central Committee, including the *Programme of the*

Communist Party of Peru (1988). The NPA site also contained extensive documentation including a section entitled 'Peace Talks Documents' (approx. 5,000 words) and another 'Recent Statements,' measuring more than 25,000 words. The LTTE site had available copies of two e-books entitled *Broken Promises* (1995) and *A Struggle for Justice*, the latter of which was advertised as available in hardcopy from the Tiger's International Secretariat in London; however, these offices were closed down by the British government in 2001 (Wayland 2004, 419).

A majority of the sites analysed contained sections or documents dealing with the groups' values or ideology. Once again the leftist groups--the NPA, Sendero Luminoso, PKK, and FARC--devoted large amounts of text to explaining their ideological stance. Hizbollah were the only group to make no overt mention of their values or ideology on the site analysed, but a number of clear statements on these issues were included on their Central Press Office site. Implicitly, however, the contents of the site analysed left one in no doubt as to Hizbollah's political and religious stance. Six of the ten sites in the study contained no information on the group's organisational structure. Two sites, those maintained by the NPA and LTTE, contained very brief references to their groups' organisational configuration. As mentioned previously, the Aleph site contained information about the groups restructuring in the wake of the 1995 sarin gas attack on the Tokyo subway. In a somewhat similar vein, the FARC site contained quite a detailed rundown of their structure in a document that sought to prove the FARC's right to recognition as belligerents pursuant to the Geneva Conventions. In other words, both Aleph and FARC provided information on their organisational structure in order to make claims for legitimacy.

Operational Information

Details of terrorist operations were also absent from a majority of the sites analysed. Just three groups provided information about their operations. The LTTE site provided analysis and photographs of the operation code-named 'Unceasing Waves' that took place from 1996 to 2000 while the Sendero Luminoso site contained a section with text and pictures entitled 'Reports from the Battlefield.' The Hizbollah site stood out,

however, as it contained more than 100,000 words devoted to 'Military Operations.' This section of the Hizbollah site provided a day-by-day accounting of Hizbollah operations from 1997 to the present. The following is a description of events on 6 April 2000:

> 12:00- The IR team of martyrs Mohammad Hassan Ghaddar and Hassan Abbas El-Haj attacked Aramta position with the rocket-propelled grenades striking its northern fortification and inflicting those who were inside it. 6:35- The fighters of Lebanese Resistance Brigades (LRB) targeted Rshaf position with the machine guns and rocket-propelled grenades scoring accurate hits. Meanwhile, another group of LRB was falling upon the positions of Hemayed and Jamoussa with the suitable arms. Direct goals were chalked up, the fighters told.

The Hizbollah site also contained a gallery of photographs of dead 'martyrs' numbering 153. While the Hamas site does not provide text relating to their operations, the site contained fourteen 'martyrdom videos,' that is video footage of persons taken previous to their engaging in suicide bomb attacks.

Newsletters

Just three of the Web sites had newsletters available on their sites. Three copies of the newsletter *Resistencia* were available on the FARC site (Vol.s 26, 29, 30). Issues of politics, economics, and culture were addressed in each issue. These included articles entitled 'Variations on Plan Colombia,' 'Women and Their Struggle,' 'The Left and the Elections in the Dominican Republic,' 'Remembering History,' and 'Venezuela and Colombia: Two Brother Peoples that are Resisting the Imperialist Offensive Together.' Nine issues of *Peru Action and News* were available in HTML format on the SL Web site. The earliest available issue dated from Summer 1997 and the most recent available issue appeared in Winter 2002. Each newsletter was six to ten pages in length and contained political commentary, statements of the Committee to Support the Revolution in Peru (CSRP), news, and other information. The NPA site had the most

extensive collection of newsletters with seventy-nine copies available, all were downloadable in both HTML and PDF formats. These dated from 1998 to 2004. The site described the newsletter as follows:

> *Ang Bayan* is the official news organ of the Communist Party of the Philippines issued by the CPP Central Committee. It provides news about the work of the Party as well as its analysis of and standpoint on current issues. *AB* comes out fortnightly. It is published originally in Pilipino [*sic*] and translated into Bisaya, Ilokano, Waray, Hiligaynon and English.

Subscriptions to *Ang Bayan* were also available via e-mail. A number of other sites also provided e-mail newsletters; these included ETA, Hamas, Kach, and the LTTE. None of these newsletters were posted online.

Leadership Information

Clifford Bob has pointed to the way in which the Zapatistas benefited from the personal charisma of their major spokesperson Subcomandante Marcos. Fluent in Spanish and English, prolific in written communication, and attuned to contemporary cultural events, Marcos quickly became an internationally recognised symbol of the Zapatistas who responded to and skilfully exploited the significant interest in him shown by the Western media and civil society. Asked in an interview whether the EZLN had become too closely associated with him, Marcos asserted: "I don't gain anything personally. It is the movement that benefits, because this way more people pay attention to the issue" (as quoted in Bob 2001, 324; see also Brysk 1995, 563). Six of the ten sites analysed here contained a profile of their group's leader. Some of these, such as those that appeared on the Sendero Luminoso and LTTE sites, were quite extensive.

The Tamil Tiger leader, Veluppillai Prabhakaran, received extensive coverage on the LTTE site. The 'National Leader' section of the site contained eight interviews with Prabhakaran, 'Speeches and Messages' dating from as far back as 1984, a selection of twenty quotes, a five-second video clip, and a selection of twenty-seven

portrait photographs. The SL leader, Dr. Abimael Guzmán (aka Chairman Gonzalo), has been imprisoned by the Peruvian government since 1992. The SL site had a large section devoted to the activities of the International Emergency Committee to Defend the Life of Dr. Abimael Guzmán (IEC) which contained reports, conference proceedings, published advertisements, leaflets, and emergency bulletins (1995-2001), while elsewhere on the site the text of Dr. Guzmán's 1992 'Speech from a Cage' was reproduced along with accompanying photographs.[167] The Hamas site had a prominent link on its top page to a section of the site devoted to memorialising the group's deceased leader, Sheikh Achmed Yassin (1938-2004). This section contained a biography of Yassin, a selection of quotes, the text of five of Yassin's speeches, and a selection of reactions to his killing from around the globe. The leaders of both Aleph and Hizbollah have their own personal Web sites.[168] Neither the ETA nor the FARC Web sites identified or discussed the leadership of their organisations.

FAQs

Only two of the ten sites displayed a list of Frequently Asked Questions (FAQ). The LTTE FAQ related to the group and its origins as opposed to the Web site. The list of questions addressed in the FAQ were as follows:

1. What is Tamil Eelam ?
2. Why did Tamils in Sri Lanka want Tamil Eelam ?
3. Who is the leader of Tamil Eelam ?
4. Is Tamil Eelam a communist idea ?
5. What is the present state of Tamil Eelam ?
6. Is there religious freedom in Tamil Eelam ?
7. Can any one travel to Tamil Eelam ?

---

[167] Former Peruvian president (1990-2000), Alberto Fujimori, also maintains an online presence via his Web site http://www.fujimorialberto.com, which he maintains from exile in Tokyo. The site is available in Spanish, English, and Japanese.

[168] Joyu Fumihiro's official site is online at http://www.joyu.to. Nasrollah's personal homepage may be accessed at http://www.nasrollah.org.

8. Who is LTTE ?
9. Where can I find more information ?

The NPA FAQ (entitled 'Q&A and located on the menu bar in the top right of each page), on the other hand, dealt with technical issues such as downloading and unzipping files.

Negative Campaigning

Those sites that show a '0' in the 'Negative Campaigning' section of Table 6.2 were not sites that were free of negative comments regarding their foes. Instead negative comments were spread haphazardly throughout these sites and were therefore not conducive to measurement in the same way as the negative campaigning on some of the other sites that was located in special sections or documents and therefore easily identified and measured. The ETA site, for example, contained numerous documents detailing instances of torture, unlawful killing, and multiple other human rights abuses allegedly carried out by the Spanish authorities. In a similar vein, a large part of the SL site was taken up with criticism of the Peruvian government and its officials and their actions against SL members and supporters. The Hamas site had a section devoted to 'Zionist Crimes,' which contained sixty-one separate articles detailing alleged Israeli mistreatment of Palestinians. A sampling of article titles:

'Occupation Forces Fire at Worshipers During Prayer'

'Zionist Terrorist Forces Wound Palestinian Baby'

'Palestinian Mother Arrested to Blackmail her Wanted Son'

'Zionist Terrorist Sniper Paralysis [*sic*] Palestinian Child'

The same section of the Hamas site also contained four videos entitled 'Zionist Crimes on Video' (2 mins 36 secs), 'Zionist Heli [*sic*] Bombing Ambulance' (25 secs), 'Zionist Terrorists Beating Child' (13 secs), and 'Zionists Terrorise Palestinians' (2 mins 40 secs).

By far the largest amount of negative campaigning was carried out on the Hizbollah site. A section entitled 'Israeli Aggressions' contained hundreds of pages--over 700,000 word--detailing what appeared to be every act of Israeli aggression against the Lebanese since 1998. Below is one of the two reports filed on 15 January 2002:

> Eight "Israeli" warplanes violated Lebanese airspace on Monday, a statement issued by the Army Command said. The warplanes roared over the country, breaking the sound barrier over Beirut and Tripoli in separate sorties. The statement said the planes also swooped over south Lebanon and the Bekaa Valley. In a separate statement, the United Nations condemned similar violations, which occurred on Sunday after a lull that lasted 10 days. According to the statement, Staffan de Mistura, the UN secretary-general's personal representative for southern Lebanon, called upon "Israel" to cease such air violations across the UN-delineated Blue Line.

The list of alleged 'aggressions' was enormous incorporating not just violations of airspace, but torture, unlawful detentions and killings, shootings, bombings, deportations, destruction of crops and livestock, beatings of women and children, etc.

The figure occupying Hizbollah's entry for 'Credit Claiming' in Table 6.2 is the same as the figure for 'Operations.' This is because detailing operations was judged to be a method of credit claiming. The LTTE entry for 'Credit Claiming' is a composite figure made up of the figure for 'Operations' with the addition of a small amount of text (approx. 170 words) that was deemed 'credit claiming' and was found linked from the 'LTTE' icon on the navigation bar at the top of the page. None of the other sites analysed were judged to contain significant amounts of overt credit claiming.

Targeted Pages and Sites

Just two of the sites analysed contained pages targeted at a specific demographic. In both cases, this was women. The women's section of the ETA site was divided into four sections: 'How Are We Doing?,' 'Some Facts,' 'Leaders and Fighters,' and 'Documents.' The text of 'How Are We Doing?' (approx. 3,000 words) dated from early 1999 and addressed issues relating to women's human rights, both globally and in the Basque Country specifically; violence against women and government responses to same; the right of Basque women to abortion services; women and work; and the impact on Basque women of European integration. The 'Leaders and Fighters' page contained brief profiles of thirteen female Basque leaders and fighters who lived from the middle ages to the late twentieth century, while the 'Documents' section contained just five documents relating to the role of women in Basque society, the most recent of which dated from 2002. The LTTE site also had a page, linked from the Web sites top page, dedicated to 'Women Fighters.' This page was composed of an essay produced in 1990 by a female LTTE member along with a selection of links to other relevant areas of the site. The 1990 essay entitled 'Freedom Birds of Tamil Eelam' opened as follows:

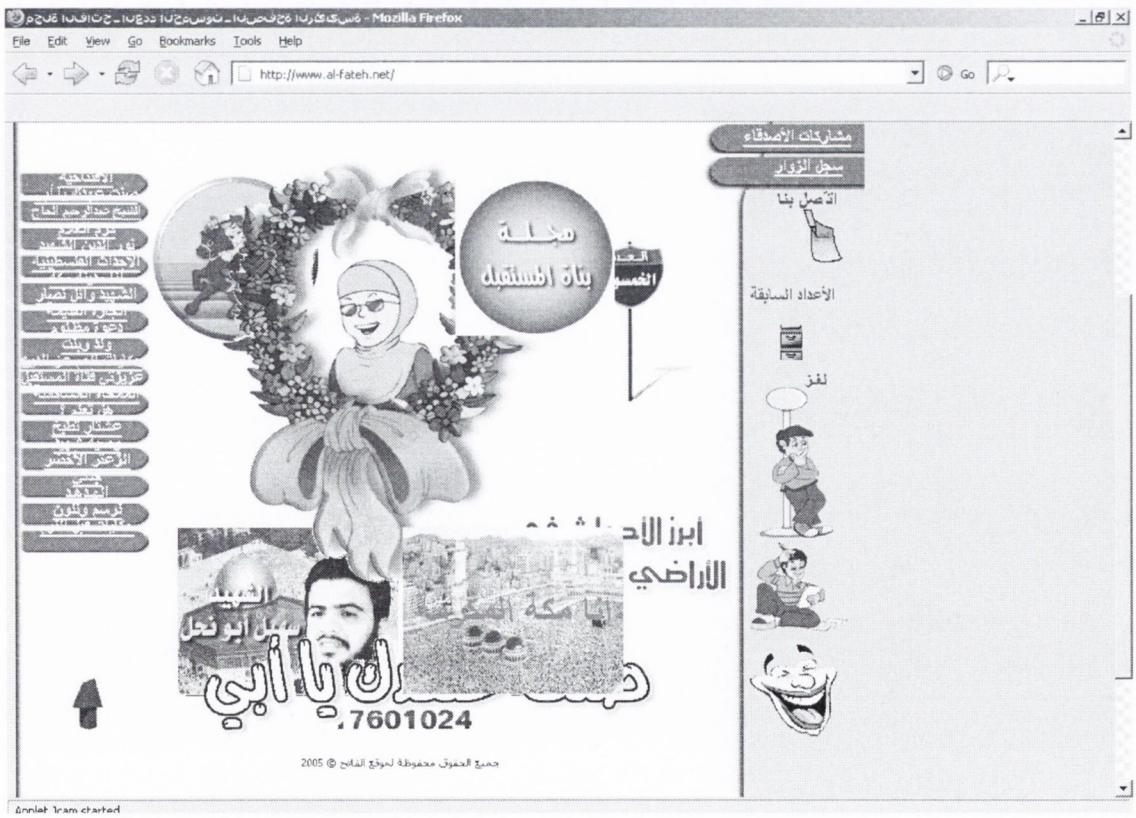
> Women, Tamil women, have been long subject to oppression of a dual nature. On the one hand, women... have borne the brunt of the national oppression...On the other hand, women have been subject to an internal form of social oppression rising out of male chauvinism. This form of oppression is reinforced by the conservative traditions and some of the cultural norms inherent in the Tamil community...Also, caste oppression finds its virulent expression when relating to women. This brief article will however deal with one aspect namely the impact of the war on Tamil women. It will, in particular, trace the development of the "birds of freedom," the women military wing of the LTTE.

Along with this text, links to the LTTE leader's International Women's day messages from 1992, 1993, and 1996, and a link to the National Heroes Day section of the site

were also provided. Women were also quite prominent in the images available in the site's e-card database and there was a link to this section of the site from the women's page also. Finally, although the Hizbollah site analysed here does not contain specific pages targeted at women, Hizbollah maintains a separate Web site devoted to 'women's issues.'[169]

It's worth noting that, although none of the ten sites focused on here contain pages targeted at children, terrorist groups have been known to take advantage of young people's familiarity with the Internet. The Hamas organization actually maintains a separate children's Web site. The top page of this site features a Western-looking boy sitting atop a horse and wielding a large sword, which is a symbol of Hamas (see Figure 5.1). The site includes many cartoon images, stories, games, and jokes. At one time, for example, it featured two smiling cartoon skyscrapers giving

Figure 5.1 Top Page of Hamas Children's Site (al-fateh.net)



[169] The Hizbollah Women's Organization Web site was at http://www.alaaleb.org, but no longer seems to be accessible.

each other a 'high-five,' as though they were happy to have been destroyed. Hamas's children's site also allows visitors to post e-mails and participate in bulletin boards and chat rooms, which are presumably monitored in the search for promising young recruits (Fritz, Harris *et al* 2004, 9-10; see also Denning 2004, 5 & ITIC 2004). The site is only available in Arabic.[170]

Upward Information Flows

A number of sites solicited financial contributions, but none provided online donation facilities, such as a credit card payment option. A number of the sites that requested donations also had merchandise for sale. The Kach Web site had numerous requests for donations, including a pop-up box on the top page that read as follows:

> Make Donations. Israel needs you now more than ever. Support Kahane.org the only organisation that has a program that could save Israel. Help us legalise the Kahane views in Israel. Only one answer, and it is not fences or Oslo. All hostile Arabs who wish to destroy Israel must be removed from Israel.

Clicking on the pop-up brought one to a page requesting donations by mail to an address in Brooklyn, New York. A telephone number was also provided. The Kach site also had a 'Shopping Centre'. For sale were books, videotapes, audiotapes, t-shirts, jewellery, Israeli and Kahane Chai flags, and stickers. To purchase, one was requested to print out the order form provided and send it, along with a check or money order in US dollars, to the organization's Brooklyn, New York address.

---

170 In February 2004, a British Muslim rapper produced an English-language rap video touted by the media as a tool for recruiting young people into al-Qaeda. The rapper, who identified himself in the video as Sheikh Terra, is accompanied by Soul Salah Crew (presumably a twist on the name of the British rap group So Solid Crew). He is seen to have a copy of the Koran in one hand and a pistol in the other. The rap video is entitled 'Dirty Kuffar' ('infidel'), and was produced by Digihad Productions. Sample lyrics: "Peace to Hamas and the Hizbollah, OBL [Osama bin-Laden] pulled me like a shiny star, like the way we destroyed them two towers ha-ha. The minister Tony Blair, him a dirty Kuffar. The one Mr. Bush, him a dirty Kuffar. The video is available online at http://www.ratatak.com/modules/mydownloads/singlefile.php?lid=14.

There was a 'Contributions' button located on the top page of the Hizbollah site, but this was not operational at the time the site was downloaded for analysis. A request for financial contributions was at one time included on Hizbollah's Al-Manar TV site and was accompanied by an account number for a bank in Beirut, Lebanon. However, all such requests for contributions now appear to have been scrubbed from Hizbollah's English-language Web sites. None of the Hizbollah sites provide items for sale.

The following request for support appeared on the top page of Sendero Luminoso's site:

> We're all-volunteer, from our national office staff to our student agitators -- we rely on yearly membership dues, material purchases and contributions to pay our office rent, phone, postage and printing expenses. If you want to hook up with, support and/or join us, please contact us today by phone, fax or postal mail.

The 'Materials' section of the site offered numerous items for sale including copies of the group's newsletter *Peru Action and News*, books and pamphlets, VHS videotapes, stickers, magnets, t-shirts, pins and buttons, and music CDs. To purchase, one was requested to print out the order form provided and send it, along with a check or money order in US$ made out to CSRP, to the organisation's Berkeley, California address. "Volume discounts (up to 40% off) are available to bookstores, teachers, and to supporters for use in community outreach." A calculator was provided at the bottom of the page to help with the math.

The LTTE's 'Online Store' had similar sorts of items for sale and operated in much the same manner as its Kach and SL equivalents, one's check or money order to be posted to an address in Toronto, Canada. The Aleph site had no items for sale, but requested that those who wished donate to the charities established to aid victims of the 9/11 terrorist attacks in the US. None of the other Web sites analysed contained either requests for donations or merchandise for sale.

Just two of the ten sites analysed installed cookies.[171] They were the Hamas and PKK sites.

Hyperlink Analysis: Lateral/Horizontal Information Flows

Links Out

Hyperlink analysis has two measures: the number of links from a site and the number of citations linking to a site. The sites analysed addressed special interests and many of them were therefore relatively self-contained or 'close-ended' meaning that the sites generally did not offer extensive external links of either a partisan or non-partisan nature. The FARC site, for example, was entirely self-contained. It offered no external links whatsoever, to the extent that once one had entered the English- language section of the site there was no clear way of navigating back to the site's top page as the 'Home' link only returned one to the top English-language page. The rationale for such design, it is assumed, is that the surfer is 'forced' to remain within that group's frame of reference (Deuze 2003, 212; Rogers 2002, 196).

Not all of the ten sites analysed were so close-ended, however. The Kach site had the greatest number of external links. A majority of these were of a partisan nature and appeared in the 'Friendly Sites' section of the sidebar. The Kach site also contained six reference links, which appeared in the 'News Network' section of the sidebar and allowed one to link to the newspapers *Ha'aretz* and the *Jerusalem Post*, among other news sources. The ETA site also had a relatively large number of reference links. However, these differed from those appearing on the Kach site in that they were links not to current affairs sources, but to sites such as the University of Minnesota Human Rights Library, the homepage of the UN High Commissioner for Human Rights, and

[171] Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. They are embedded in the HTML information flowing back and forth between the user's computer and the servers and were devised to allow user-side customisation of Web information. Cookies make use of user-specific information transmitted by the Web server onto the user's computer so that the information might be available for later access by itself or other servers. Web servers automatically gain access to relevant cookies whenever the user establishes a connection to them, usually in the form of Web requests. For more information on cookies, check out http://www.cookiecentral.com.

Amnesty International Spain. None of the other sites analysed adopted a similar linkage practice.

Linking to sites maintained by organisational sub-groups is another practice that is not particularly popular among terrorist Web sites. This may be because a majority of the groups studied are centralised and their Web presence follows the same pattern, but may also stem from the fact that the present research focuses upon the groups' English-language sites and that sub-group sites are only available in indigenous languages. The Aleph site provided links to twelve 'branch' sites throughout Japan, but these were only available in Japanese. The Hizbollah site, on the other hand, provided a links page containing links to the Web sites of some twenty-three constituent organisations and various representatives of the organisation. These included links to Hizbollah's Al-Manar satellite television station, Al-Nour radio,[172] and Al-Ahed magazine;[173] the homepage of the group's Secretary General, Sayed Hassan Nasrollah; and the homepage of the group's Deputy Secretary General, Sheikh Naim Kasem,[174] among others. All of these sites were available in English.

The SL site was the only site to contain any links to information about other, similar groups operating in the same country. The SL site contained information about and demanded that the basic rights of Lori Berenson, an American woman imprisoned in Peru, for her alleged involvement with the Tupac Amaru Revolutionary Movement (MRTA) be respected.[175] Despite the bitter ideological differences between the two groups, the SL site also provided an external link to a Web site maintained by Lori Berenson's supporters, [176] which provides regular updates on her situation.[177]

---

[172] http://www.alnour.net/
[173] http://www.alahed.org
[174] http://www.naimkassem.org
[175] See http://www.csrp.org/alert.htm. Scroll almost to the bottom of the page to view text headed 'Committee to Support the Revolution in Peru Demands Basic Rights for Lori Berenson' (1995).
[176] http://www.freelori.org/
[177] The MRTA's home page is at http://www.nadir.org/nadir/initiativ/mrta/. The site is primarily Spanish-language, but portions of it are available in English translation. It contains a small amount of information about Lori Berenson's situation. For more information about the MRTA and it's Web strategy, in particular, see Dartnell 1999, also Reuters 1997.

Links In

The number of citations to a site is a measure of the extent to which a site is recognised among other sites that deal with the same or similar issues. There are two major ways of determining the 'popularity' of a site. The first is to measure the number of 'hits' on or visits to a site. Many pages offer a 'hit counter' that records the number of times a page has been visited in a given span of time, which number can serve as an indicator of the popularity of the page. This was not a viable method in this research, however, as none of the ten sites analysed provided such a 'hit counter.' This approach is severely disadvantaged in any event as it is relatively simple to manipulate hit counters. Further, the number shown does not indicate the number of visits by different surfers, but is the raw number of hits on the page. The upshot of this is that the page may legitimately have been hit a large number of times, but only by a small number of regular visitors. The second measure of popularity is to measure the number of links to a page from other pages. This was the method employed here. The top English-language page of each of the sites along with the sites' overall home page, if such existed, were subjected to a Google 'Advanced Search' that allows one to find pages that link to specific URLs.[178]

In terms of visibility, some sites were considerably more prominent than others (see Table 6.3). The LTTE site was the most prominent of the ten sites analysed with 240 'links in' in January 2004. The Sendero Luminoso, Kach, and ETA sites were also fairly prominent during the same period. The top English-language FARC page had no direct 'links in,' but the group's Spanish-language homepage acted as a cover page for all of the FARC sites and this page had seventy-two 'links in' in January 2004. The PKK site showed a very small number of 'links in', at just eight, but this was due to the structure of the PKK sites, which did not have a cover page similar to the FARC site.

[178] Google was chosen because it is the world's leading Internet search engine. It ranks Web pages using software called PageRank. PageRank relies on the uniquely democratic nature of the Web by using its vast link structure as an indicator of an individual page's value. In essence, Google interprets a link from page A to page B as a vote, by page A, for page B. But, Google looks at more than the sheer volume of votes, or links a page receives; it also analyses the page that casts the vote. Votes cast by pages that are themselves "important" weigh more heavily and help to make other pages "important." For more, see http://www.google.com/technology/index.html.

However, it was possible to navigate from the top Kurdish-language page, which acted as the site's overall top page, to the top English-language page of the PKK site, and the former had just over forty 'links in' in January 2004.

Hits Returned

The transition from the hit economy to the link economy, in the late 1990s, recognised that an organization's Web reputation no longer derived from its site design but was rather a product of the organisation's showing in reputable spaces (Rogers 2002, 205). As Rogers points out, the 'chaos' of the Internet may be viewed as a product of the lack of source authority in an information free-for-all. Let's take the example of the NPA. With some 25,000 pages with something to say about the NPA, all being listed by engines, returning sites with frequent NPA keywords, one might expect that search engines with link authority logics (such as Google) would return www.philippinerevolution.org at the top of the returns. However, while search engines such as Google have to some extent resulted in "a new form of basic Web epistemology" by providing an indication of the status of information according to measurable reputability dynamics as determined by the Web (Rogers 2002, 200), this works less well in terms of searches for terrorist sites as opposed to sites containing more mainstream views. Instead of the NPA themselves being viewed by Internet users as the most reliable source of information about their group therefore, the US government is instead seen to be the most reputable source of information about the organisation, and the same is true of a number of the other groups discussed in this chapter (see Table 5.4).

Interactive Information Flows

Some sites were highly interactive while others were much less so. Just half of the sites analysed provided site search facilities. The Kach site had the most interactive features, including a site search. There were posters and flyers for download, thousands of photographs (of the Kahane family, protests, parades, funerals, etc.), cartoons, jokes,

Table 5.4 Google Search for Terrorist Group Information (10 April 2005)

Search Term(s)	No. of Hits Returned	Top Returned Site
"Aum Shinrikyo"	79,300	Apologetics Index http://www.apologeticsindex.org/a06.html
"Basque Homeland and Liberty"	370	Profile, International Policy Institute for Counter-Terrorism (Israel) http://www.ict.org.il/inter_ter/orgdet.cfm?orgid=8
"Revolutionary Armed Forces of Colombia"	94,300	Profile, International Policy Institute for Counter-Terrorism (Israel) http://www.ict.org.il/inter_ter/orgdet.cfm?orgid=37
"FARC"	919,000	FARC Official Site
"Hamas"	2,340,000	Hamas Official Site
"Hizbollah"	188,000	Hizbollah Official Site
"Kahane Chai"	16,500	Profile, International Policy Institute for Counter-Terrorism (Israel) http://www.ict.org.il/inter_ter/orgdet.cfm?orgid=19
" LTTE"	436,000	LTTE Official Site
"New People's Army"	25,000	'Philippines' NPA Redesignated as Terrorist Group' (US Embassy, Japan) http://japan.usembassy.gov/e/p/tp-20040811-11.html
" PKK"	1,410,000	Profile, US Department of State http://library.nps.navy.mil/home/tgp/kurds.htm
"Kongra-Gel"	47,300	Kongra-Gel Official Site
"Sendero Luminoso"	94,600	Library Guide to SL, University of North Carolina http://ils.unc.edu/~marsc/sendero.htm
"Shining Path"	120,000	Council on Foreign Relation's (USA) Terrorism Q&A http://cfrterrorism.org/groups/shiningpath.html

'pre-state underground music,' etc. Contact information was provided in the form of an e-mail address and a telephone number. The site also contained an online poll. In addition, the Kach site was the only site with an online gaming section, which contained five games in which players were supposed to kill Ehud Baraq, Shim'on Peres, and Yasir Arafat, amongst others. The aim of one of the games, entitled 'Escape of the Oslo Criminals,' was described as follows:

> The year is 2010. Red Alert ! Red Alert ! The insane and dangerous Oslo Architects have escaped from their High Security Mental Asylum and are

> heading towards PA! You must stop them from reaching the safety of their friends of the PLO and prevent the Israeli citizens from lynching them.

When challenged by a reporter about the games, David Ha'ivri, a Kach member, replied: "Each week, Jews are murdered. There are more dangerous things than this game. The people who appear in the games gave weapons to the terrorists who murder Jews. It's just a game for children on the Internet" (FBIS 2002b).

While none of the sites investigated had chat room facilities, the Kach site was the only site with a bulletin board forum. This forum was quite active with 610 members, 578 separate topics, and over 5,800 posts.

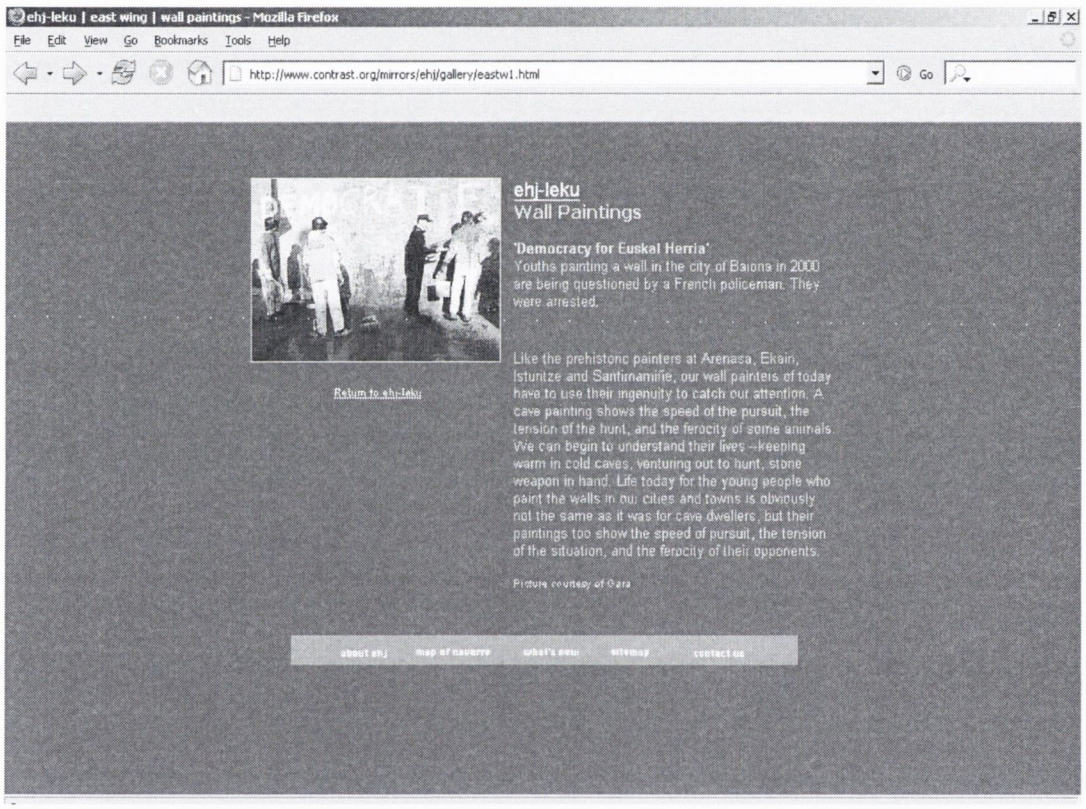
The Hamas sites had the most items available for download with an archive of over 600 screensavers available. Artistic renderings have long been important propagandistic devices (see Johnson-Cartee & Copeland 2004, 141-142); this is reflected not just in the Hamas screensavers, but the online art galleries contained on two of the sites. There are twenty-nine separate art works displayed on the SL site, mainly paintings, line drawings, and a small number of wall murals. A majority of these were colourful, but crude posters with slogans such as 'Break the chains! Unleash the fury of women as a mighty force for revolution!' and 'Long live the invincible People's War!' They were contained in the sections 'Art in Support of the Revolution' and 'Revolutionary Art of Peru.' Many of the images were also available as fridge magnets. According to the site's creators:

> The art displayed here was mainly created by imprisoned fighters and supporters of the PCP. The materials to produce these artworks had to be smuggled into the prisons by friends and family. The art has since made its way around the world. Many of the artists were killed in the prison massacres of June 1986 and September 1992.

The ETA site also had an online art gallery. However, this 'virtual gallery' was a great deal more sophisticated than its SL equivalent. It contained ten video installations and photomontages with audio, accompanied by information about the various artists. One

of the montages, 'The Liberation of Navarre,' featured a naked woman in grainy black and white curled in the foetal position, slowly unfolding the length of her body, only to find herself in an enclosed space, unable to escape. The gallery also contained a montage of photographs of wall murals, from scrawled words to complex paintings, accompanied by a short explanation of this practice (see Figure 5.2).

Figure 5.2 Page from ETA Site's Online Art Gallery



Five of the sites analysed had online photo galleries or archives. As mentioned earlier, the Kach site contained thousands of images of the Kahane family, the funerals of murdered Israelis (including the Kahanes), etc. The Hizbollah site contained over 150 photos of dead 'martyrs' along with an archive of some 200 still-images from Al-Manar television. The LTTE site also had an extensive photo archive containing over 400 images. This archive was searchable by both category and key word. Some of the categories included 'Warrior Statues' (19 photos), 'Elephant Pass Victory' (287 photos), 'Tamil National Leader' (27 photos), 'Liberation Tigers' (49 photos) and

'Tiger Operations' (26 photos). These categories were then divided into sub-categories. So, for example, 'Liberation Tigers' was divided into 'Black Tigers' (7 photos), 'General Photos' (12), 'Men Fighters' (11 photos), 'Sea Tigers' (7 photos), and 'Women Fighters' (12 photos). There was also the facility to send these images as e-cards.

As mentioned, the Kahane site was the only site with an online gaming section, but a number of the other sites included less sophisticated games and gimmicks. The ETA site contained a clickable map of the Basque country and an interactive map of the city of Pamplona, along with real-time information on the weather in the area. This site also contained a Basque language primer. The Hamas site contained thirteen poems linked from the site's top page;[179] the NPA site also included poetry and two albums of 'revolutionary' music. Like the NPA site, both the LTTE and SL sites also contained music recordings. The Hizbollah site contained four cartoons, while the Kach site contained eighty-four. A majority of the latter were pro-Israel/anti-Arab, while some twenty-four were anti-Semitic cartoons that had appeared in the Arab press. In addition to the musical offerings and e-cards mentioned above, the LTTE site also had clickable maps, an online quiz, and a 'Memory of the Day' section, while the SL site offered free stickers and/or a free newsletter to anybody who wished to post the CSRP a stamped, self-addressed envelope.

The Aleph site had the most e-mail contacts, with seventeen addresses listed. The LTTE provided four separate e-mail addresses, ETA supplied three, and the NPA two. The Hamas, Hizbollah, Kach, and FARC sites each provided one e-mail address. The PKK and SL sites were the only sites not to provide e-mail contact details. Instead, the SL site invited visitors to contact them via postal mail, phone, or fax. In addition to e-mail contact details, a number of the sites also provided online forms or polls. Sites soliciting such feedback included both SL and the PKK, along with Aleph, the NPA, Kach, and FARC. Half of the sites analysed offered visitors the opportunity to sign-up

[179] The Hamas charter states that "the book, the article, the bulletin, the sermon, the thesis, the popular poem, the poetic ode, the song, the play and others" are all important vehicles for ideological mobilisation. Hamas even supports singing troupes that praise Hamas and espouse its ideology. In one case, three of the Hamas operatives who carried out the suicide bombing at the Park Hotel in Netanya, Israel on Passover in April 200--including the suicide bomber--were members of a Hamas singing troupe (Levittt 2005).

for e-mail newsletters.[180] However, these newsletters were not archived on any of the five sites--ETA, NPA, Hamas, Kach, LTTE--that offered this facility and so their content remains unknown.

The least interactive sites were those maintained by FARC and the PKK. These sites had no items for download, neither online art nor photo galleries, no games or gimmicks, and no e-mail lists. While the PKK site had a search facility, the FARC site did not even include this basic feature.

Terrorist Web Site Delivery

Half of the sites investigated could be described as 'glitzy.' The Kach site, due to its very large number of images, was the flashiest of the sites analysed. Other sites containing large numbers of images were the Hamas, LTTE, Hizbollah, and Sendero Luminoso sites. With just eight images, the FARC site was the least glitzy of all.[181] Regarding the second component of the glitz factor, audio and video were available on six of the sites: ETA, NPA, Hamas, Hizbollah, Kach, LTTE, and SL. All of these sites, excepting the SL site, also contained moving icons. The Aleph, PKK, and FARC sites contained neither audio nor video, nor moving icons.

The NPA, Hamas, and Hizbollah sites were the most up-to-date. All three had new material added every one to two days. The Aleph and ETA sites, on the other hand, had not been updated for more than six months. In fact, most of the material on these sites appeared to date from 2001. The remaining sites had been updated at various points in the preceding six months.

Eight of the sites analysed were available in more than one language. The Hamas and LTTE sites were only available in English. However, there are other Web sites associated with these groups available in an assortment of other languages, including Arabic and Tamil respectively. The FARC site had the most translations. It

---

[180] The FARC maintain a Spanish-language Yahoo! Newsgroup, although this is not mentioned on their English-language site. The news service (access via http://mx.groups.yahoo.com/group/farc-info/) distributed communiqués on a monthly basis during a six-month period in 2001-2002, but has not been used since (see Scheeres 2001a & 2002).

[181] There are a number of limitations to using the raw number of graphics to judge flashiness (see Gibson and Ward 2000, 313).

was available in English, Spanish, Italian, Portuguese, Russian, and German. However, the Portuguese and German sites were inaccessible at the time this research was undertaken. The PKK site was available in four languages: English, German, Kurdish, and Turkish. The Aleph, ETA, and Kach sites were all available in three languages. All three sites were available in English, while the Aleph and Kach sites were also available in Russian and the groups' native languages, Japanese and Hebrew respectively. The ETA site, while predominantly in English, also had Spanish and Basque language components. Three further sites were available in both English and the groups' native language. These were the NPA (Pilipino), Hizbollah (Arabic), and Sendero Luminoso (Spanish) sites.

The top mark a site could have scored in terms of accessibility was four. However, none of the Web sites performed well in this category, and the top mark actually scored was two, by the PKK site, which had both foreign language translations and text-only documents for printing. The Hamas and LTTE sites, because they did not have foreign language translations, performed very poorly, receiving zero points, while the remainder of the sites scored just one point (for foreign language facilities). None of the sites were offline during January 2004, the period during which the sites were downloaded for study.

Gibson and Ward adopt a sensible rule of thumb when it comes to the time it takes for a home page to load. They say that a home page size greater than 30Kb will mean the page contains multiple graphics and will therefore take a long time to load for the average home user (Gibson & Ward 2000, 313). Just three of the sites investigated had homepages greater than 30Kb. The largest of these was the Kach site at 55Kb, followed by the PKK site at 50.5Kb, and lastly the ETA site at 45.5 KB. The FARC homepage at just 1Kb loads instantly,[182] as do the Hizbollah (6Kb) and Aleph (7Kb) pages.

If accessibility was not a top priority on any of the sites, navigability was an issue that received more attention. The top-scoring site was that maintained by the CSRP for Sendero Luminoso. The SL site included a search capacity, navigation tips, a

[182] The top FARC page (i.e. the Spanish-language homepage from which all the other sites were linked) was slightly more graphical at 14Kb.

home page icon on each page, a menu bar on each page, and a sitemap linked from the top page. The NPA site was also easily navigable due to the provision of navigation tips, a home page icon on each page, major site area links, and a site map linked from the top page. The most difficult sites to navigate were the ETA and Kach sites. The ETA site had a menu bar on each page, but no search facility or navigation tips, while the Kach site provided a search facility, but no site map or navigational tips, which would have increased the user-friendliness of this very large site.[183]

CONCLUSION

Overall, then, how well did these Web sites deliver the functions postulated at the beginning of the chapter? In terms of information provision, the sites were an unmitigated success. A majority of the sites contained large volumes of information about the groups' history, heroes, founders, mindsets, and motivations that would be difficult for many people to access without the aid of the Internet. If information provision was clearly the primary function of the sites, then promotion of participation was a close second. In this instance, this refers less to the recruitment of persons to take part in terrorist activities than to the mobilisation of supporters and sympathisers to more actively support the terrorists' causes whether through linking from their own sites to the terrorist sites, printing out and pasting-up the posters supplied for download on a number of the sites in their local areas, or contacting the groups via the various avenues highlighted on the Web sites and getting more directly involved. Funnelling money to terrorist groups is also a form of participation, of course. A number of the sites analysed sought to raise funds for their activities via their Web sites either through directly soliciting donations or offering merchandise for sale. Perhaps the least satisfactory aspect of the Web sites analysed, in terms of their postulated functions, was the use of the sites for networking purposes. Most of the sites analysed were quite centralised and provided little or no links to either sub-groups within the organisation

[183] 'Visibility,' the final site delivery variable, was addressed in the *Hyperlink Analyses* section above.

or to other, perhaps similar or sympathetic, groups around the globe. Having said that, some of the sites were linked to by quite a large number of other sites.

In terms of delivery, the sites differed quite markedly. A number of the sites were quite glitzy and had significant multimedia content, while others were static and dull. While a small number of the Web sites were updated regularly, many were updated only intermittently, and two had not been updated for more than a year.[184] Many of the sites were available in more than one language, thus giving them a global reach. The sites scored low on other measures of accessibility however, such as the availability of text-only documents for printing. Nonetheless, easy navigation was a hallmark of a significant number of the sites, which provided search capacities, site maps, homepage icons on each page, and major site area links.

Two sites stand out in terms of their functioning and effectiveness. These were the Kach and NPA sites. The Kach site, although its design was somewhat amateur, delivered very effectively on the functions postulated. It was crammed with information and commentary; contained thousands of photographs of the aftermath of attacks on Israelis, the funerals of those killed in attacks, etc, all meant to serve as evidence of the rightness of the groups ideological position; had an online gaming section and numerous other gimmicks, including an online store; and was the only site to have a functioning discussion forum. The NPA site, on the other hand, was considerably smaller than the Kach site, contained considerably less images, and had neither an online store nor a discussion forum. Nonetheless, the NPA site was remarkably well designed, both in terms of appearance and navigability, and was updated regularly. The site contained large amounts of information about the NPA and its activities; had a 'Culture' section including musical recordings and poetry; contained copies of the group's newsletter stretching back a number of years; and provided numerous ways of contacting the organisation, including the mobile phone number of the NPA Press Officer. According to research carried out at Stanford University, the appearance of a Web site--its design look--is a major factor for many Internet users in judging a site's

[184] It is impossible to deduce from simply looking at these sites what explains the significant differences in delivery referred to. The only definitive way in which to address this analytical deficiency would be to make direct contact with sites' Webmasters and solicit information about their reasoning with regard to the delivery issues highlighted; this is therefore a matter for future consideration and research.

credibility. The professional appearance of the NPA site may be expected therefore to lend credence to the site's content due to the Stanford researchers' finding that the appearance of a Web site influenced Internet users credibility rating of sites more strongly than any other factors, including the source of the information and its accuracy (Denning 2005, 7).[185]

The FARC site was in marked contrast to the Kach and NPA Web sites. This site was amateurish both in its appearance and overall structure. It had not been updated for some time, was difficult to navigate, and contained only a small amount of information about the FARC and its activities. (In contrast to the English-language pages analysed here, however, the FARC's Spanish-language site had a professional appearance, was regularly updated, chockfull of information, and easily navigated).[186] The remainder of the sites analysed met with varying, but generally high, levels of success in terms of their functioning and effectiveness.

To sum up then: the importance of information and communication technologies to war and conflict is well established. What is less well understood is how new global technologies, such as the Internet, are changing the dynamic of conflicts as communicative and information power is decentralised down to the sub-state level and its reach extends beyond the confines of local territorially-defined boundaries. Can a well-designed and well-considered presence on the Internet play an important role in politics in a conflict situation? This chapter has been concerned with exploring the functions of terrorist Web sites, particularly as these relate to the major terrorist uses of the Net, as laid out in Chapter Three. It is posited that the chapter successfully illustrated that a majority of the sites investigated made an effective contribution to terror groups' financing, networking, recruitment and, particularly, information provision functions, essentially providing a considerable soft power return on a relatively small original resource input. With this in mind, the next chapter is

---

[185] The home page of the Stanford Web Credibility project is at http://www.webcredibility.org.

[186] The Colombian military responded to the FARC's information campaign by establishing their own Web site which contains, amongst other things, photographs of the hundreds of soldiers and police kidnapped and killed by the rebels, a multimedia presentation of the campaign to stamp out the FARC, an online employment application form, and a discussion forum. Portions of this primarily Spanish-language site located at http://www.fuerzasmilitares.mil.co/ are also available in English, German, and French translation (see Scheeres 2002).

devoted to a more detailed description of the information provided and rhetoric employed on terrorist sites, along with an analysis of the audience(s) for same.

6

THE DISCURSIVE STRUCTURING OF TERRORIST WEB SITES: NARRATIVES OF RELIGION, REVOLUTION, & RIGHTS

INTRODUCTION

One of the purposes of the previous chapter was to illustrate how the changing technological landscape has transformed the means and media by which violent political movements can create and contest their respective 'images.' The effectiveness of political movements relies not only upon their political activity and its theoretical conception, but also upon their cultural representation and aesthetics. Some terrorist Web sites are 'better' than others as Chapter Five shows. This is because appearance affects the perceived credibility of information:"[P]ower in the area of appearance depends on having knowledge about how appearance impacts an audience, and what styles are most effective with a particular culture or group. It also depends on having the skills and resources needed to make information appear in a particular manner" (Denning 2005, 5).

Appearance is not everything however; the contents of any given Web site are also of vital import. Building upon the description of the components and appearance of terrorist Web sites contained in Chapter Five, the primary purpose of the present chapter then is the fleshing out of the discursive structuring of the same sites. Firstly though, a crucial question that has not yet been addressed is 'Who is the audience for these sites?' Clearly, for soft power resources to have an effect they must have a 'real world' impact. For most public messages, there will be multiple audiences and so it is with terrorist Web sites whose audiences are identified and discussed below. An additional reason for the analysis of audience(s) is on the basis that effective message generators recognise that their rhetoric must be created for and targeted at a specific audience or audiences. Before examining appeals contained in the message proper, therefore, one must begin with a description and analysis of what and who the audience is as "considerations of audience drive the creation of effective persuasive messages in the first place" (Tuman 2003, 72).

INCREASING THE SCOPE OF CONFLICT

According to E.E. Schattschneider, the "most important strategy in politics is concerned with the scope of conflict" (1960, 3). The reason for this is that "conflicts are frequently won or lost by the success that the contestants have in getting the audience involved in the fighting or in excluding it" (Schattschneider 1960, 4). Historically, each innovation in communication technology has resulted in changes to the communication patterns of political violence groups. Given that the means to gather and disseminate information are more pervasive today then ever before, it is no surprise that the visibility of violent conflicts has increased, particularly online. This in turn has meant that more people, in more places, have the potential to become involved in such conflicts. This is not to suggest that technology determines the pattern of politics, but given Schattschneider's understanding of politics as fundamentally conflictual behaviour, that violent political actors have taken advantage of contemporary technological innovations ought perhaps to be the least remarkable of information age innovations (Adams 1996, 423; Brown 2002, 266-67).

Schattschneider's theory suggests that groups that are disadvantaged in terms of the scope of politics have the tendency to embrace new technologies with the

capability of enlarging that scope. In this respect, terrorism has always been about communication. In fact, "Without communication there can be no terrorism" (Schmid & De Graaf 1982, 9). The Russian terrorists of the late nineteenth century were as anxious to communicate directly with the outside world as their modern counterparts. In the late nineteenth century, the Narodnaya Volya (People's Will)[187]

> Decided to organize abroad the propaganda of its actual aims...and to enlist the sympathies of European society by acquainting it with the domestic policy of our government. Thus, while shaking the throne by the explosions of our bombs within the Empire, we might discredit it from without and possibly to the diplomatic interference of a few countries which had been enlightened as to the international affairs of our dark tsardom. For this purpose we had at our disposal those revolutionary forces that had been lost to the movement in Russia, that is the emigrants (Vera Figner,[188] as quoted in Rapoport 1988, 35).

The Narodnik's efforts met with a high level of success. Their famous letter to Alexander III, justifying the assassination of his father, was calculated to woo liberal sentiment. Karl Marx declared the letter one of 'cunning moderation,' and Vera Figner employed similar language saying that its great "moderation and tact...won the sympathetic approval of all Russian society." The letter, which carried no reference to the terrorists' revolutionary aspirations, caused a sensation upon it's publication in the European press, to the extent that a number of conservative periodicals admitted their approval of the *Narodniks* demands (Rapoport 1988, 36; see also Geifman 1993, 36).

Now, thanks to the Internet, for the first time terrorists are equal communication partners in the electronic agora. It is the unmediated nature of the

---

[187] The Narodnaya Volya has been described as "the first modern terrorist organization in the world" (Geifman 1993, 3), and was involved in numerous terrorist actions in Russia in the 1870s. The most famous of these was the assassination of the Tsar in 1878. The group was disbanded in 1881, by which time it had been decimated by the mass arrest of many of its members and the self-imposed exile of others.

[188] Vera Figner, the daughter of prosperous parents, was born in Kazan, Russia, in 1852. Upon finishing school, Figner moved to Zurich in Switzerland to begin training as a doctor. In Geneva she met Russian political exiles and was converted to revolutionary socialism. After her medical training Figner returned to Russia where she worked as a medical aide. She joined the *Narodniks* in 1879 and became the leader in 1881. She was involved in planning several acts of terrorism including the assassination of Alexander II. She remained at large until being arrested in 1883 and the following year was sentenced to death. This was eventually commuted to life imprisonment in Siberia. Figner was released in 1904 and died in 1943.

Internet, in conjunction with high levels of connectivity, which renders it a communications medium unlike any other. There is a tendency in newspapers and on television for the primary sources of political information to be those who represent authority or who are members of the existing power structure. The British scholar Stuart Hall distinguishes between these 'primary definers' (e.g. politicians, police spokesmen, government officials), and what he calls 'secondary definers' (e.g. political or social activists, 'reformers,' terrorists) who reside outside the existing power structure. The latter are used much less frequently by the media than are primary definers, according to Hall (Crelinsten 1987, 420). So while modern terrorists can manipulate the media into devoting newsprint and airtime to their activities, political claims, and demands, the media in turn manipulates the terrorists: "The insurgent terrorist messages are transported to the public mainly by the media and the message is thereby almost invariably abbreviated, distorted or even transformed" (Schmid & De Graaf 1982, 110). Journalists and TV presenters achieve this by playing up the violent spectacle at the expense of analysis, in order to attract consumers, thus undermining the terrorists' claim to legitimacy by depicting them as merely violent--oftentimes irrational and perhaps even psychotic--and therefore not political (Crelinsten 1987, 421). With the advent of the Internet, however, the same groups can disseminate their information undiluted by the media and untouched by government sensors. Indeed the importance of communication, and thence communications technologies, to terrorism is one of the basic premises upon which this text is based.

As regards audience(s), Schattschneider goes on to say that

> Every fight consists of two parts: (1) the few individuals who are actively engaged at the centre and (2) the audience that is irresistibly attracted to the scene. The spectators are as much a part of the over-all situation as are the overt combatants. The spectators are an integral part of the situation, for, as likely as not, the *audience* determines the outcome of the fight. The crowd is loaded with portentousness because it is apt to be a hundred times as large as the fighting minority, and the relations of the audience and the combatants are highly unstable [italics in original] (Schattschneider 1960, 2).

Certainly, significant imbalance exists in the relationship between "combatants" and Internet audiences. Two concepts commonly characterise the idea of the Internet audience: that it is global, whether potentially or actually; and that it is knowable. The idea that the Internet audience is global is founded on the understanding of the Internet as a borderless medium. The act of establishing a Web site therefore is often loosely deemed equivalent to communicating--potentially, at least--with the world.

Internet audiences may therefore be conceived of as 'imagined communities' (Anderson 1983), in the sense that they are geographically dispersed groups of people who are presumed to share similar tastes and interests. Indeed, Internet audiences are often portrayed as existing independently of the Net: the Web merely facilitates something that they would already have wanted to be involved with. On this analysis, the Internet becomes just another communications tool, which may be drawn upon by pre-existing communities with pre-existing needs (Hine 2001, 192). This may be less true of the international audiences for terrorist Web sites, however. It is submitted that instead of these having an existence independent of the Internet, it is the goal of the designers of terrorist Web sites to essentially construct or create their audiences by connecting people through information and images to their political projects.

'Audience' is a complex category that ought to be at the heart of any Web site production process. Organizations produce Web sites for multiple reasons however, many of which they may poorly understand themselves. In many cases, the Web site becomes an organisational necessity for reasons as much to do with fear of not having a Web presence as the benefits of having one. In other words, many organizations feel that they must have a Web site, independent of any particular ideas of its use or audience (Hine 2001, 184 & 189). This is because having a Web site, especially one that is conceived of as 'good,' either in terms of content or presentation, can be seen as enhancing organizational status both online and off. In extreme cases, the Web site is established so that the site address may be included in printed literature; the tracking of Web site use or the tailoring of the site to a particular audience is secondary to what the site comes to stand for: a competent organization, IT-savvy, and 'on the ball' (Hine 2001, 191). While terrorist groups are probably as concerned with appearing Net-savvy and forward-looking as other types of organizations, it appears also to be the case that those terrorist groups who take the time and trouble to establish an official Web site are, for the most part, highly audience aware.

Domestic vs. International Mobilization

One of the major functions of terrorist groups is to mobilize other key actors in support of their political objectives. Terrorists' mobilizational goals are generally twofold. First, groups seek to increase their overall power base in order to increase their access to resources. Efforts at domestic recruitment are designed to move from an initial core group of active supporters to larger groups of adherents or sympathizers.

> The first individual likely to become involved in an issue as it expands beyond the immediate initial participants are the members of the *identification group*, those people who feel strong ties to the originators of an issue and who see their own interest as tied to that of those raising the issue. The members of the identification group are not only the first to be mobilized but are also most likely to support the position of the originators. At the same time, the identification group is not likely to be particularly large, and success in reaching the public agenda usually requires further issue expansion. A typical example of the expansion of an issue to members of an identification group is the definition of a controversy in terms of regional, ethnic, or religious interest (Cobb, Ross & Ross 1976, 128).

For example, many national-separatist and ethnic terrorist groups recruit from amongst large, often dispersed, ethnic populations who identify with their goals. Increasing their power base to larger and more powerful segments of domestic and international society gives non-state actors access to resources that can then be used to exert political pressure on the 'enemy,' generally embodied by a state or states (Adams 1996, 423-424).

The second step in the mobilization process involves rallying the established power base behind the terrorist groups' specific political objectives. The recruitment phase gives non-state actors access to financial and material resources, but it is the rallying phase that seeks to 'cash in' those assets and produce tangible political change. This component of mobilization generally includes calls for financial support along with calls for political support. A terrorist group backed with financial resources and having the support of key domestic and international actors is well

equipped to exert political pressure on a state. It is such political pressure that can directly influence the policies of governments.

In Sean McLaughlin's (2003) analysis of largely non-violent dissident actors operating in the Middle East, the latter direct this type of political action at two important actors: domestic elites and society at large. Elites are clear targets for mobilization because, he says, they possess considerable resources, both financially and politically. McLaughlin points to Denoeux's (1993) work on urban unrest in the Middle East, which demonstrated the disruptive power that 'counter elites' possess within that region. In the aggregate, society at large likewise controls significant resources. Again within the Middle East, the 1979 Iranian Revolution demonstrated the power of a society mobilized for political purposes. The cumulative power of these two domestic actors gives non-state dissidents good reason to recruit and mobilize them. According to McLaughlin, successful mobilization of one or both of these groups can help to tip the relative balance of power in favour of non-state dissidents.

McLaughlin goes on to point out that internationally focused forms of political action were largely ignored by the groups he studied. Rather, dissident actors focused their attention towards domestic audiences indicating, he says, that dissident actors seeking to engage in Internet-based political action favour political fungibility over audience accessibility. It is true that in the case of the Middle East and other areas with low rates of domestic Internet diffusion, international audiences, particularly those in Europe and the United States, present themselves as more readily accessible audiences. However, despite this high level of accessibility, international audiences offer limited political utility when compared with local domestic audiences that can more readily impact political realities on the ground within their own locales, according to McLaughlin. He concludes therefore that dissidents appear willing to devote significant resources to reaching audiences with limited Internet accessibility, but high political utility in preference to those international audiences with high Internet accessibility, but what is viewed as insignificant political utility. This leads McLaughlin to aver that it remains too soon to dismiss Appadurai's (1996) argument that political activity remains rooted in local realities.

Doubtless, Appadurai is correct; the terrorist groups with which the present research project is concerned, for example, are primarily interested in drawing attention to and instigating action on their own behalf and that of their local

'constituents' against the policies and actions of the representatives of territorially bounded states. The point is that the IT tools that they employ are emphatically global in nature; while the Internet may be used for domestic mobilization, it is clearly it's transnational mobilizing capacities that render it a strategic communicative instrument unlike any other. Terrorists' establishment of Web sites not just in their native languages, but also in English and a host of other tongues demonstrate the fact that terrorists are seeking to use the Net as not just another tool for domestic communication, but as the centerpiece of their international information strategies. This chapter will show that the discursive structuring of terrorists' English-language Web sites is further evidence of their targeting not just of domestic audiences, but also global publics.

TERRORIST WEB SITES' AUDIENCES

The major question to be addressed in this section is not who are the audiences for terrorist Web sites but, more specifically, who are the audiences for English-language terrorist sites?

The Internet and Domestic Mobilization

The reduced transaction costs associated with the Internet offer clear advantages for terrorist groups seeking to mobilize domestically. Since mobilization focuses on the organization of resources within states, the Internet provides an avenue for groups to broadcast their message(s) to entire populations at limited cost while e-mail offers a low-cost and convenient way to disseminate recruitment messages and symbols to a targeted audience. E-mail is particularly useful in this respect as it is a low-bandwidth activity and may increasingly be composed and/or accessed not just using personal computers, but mobile telephones and other types of personal organisers also.

In areas where Internet access is limited, efforts at mobilization through the Internet may 'piggyback' on other pre-existing communication networks within the state. By directing Internet-based mobilization at key nodal actors within pre-existing communication networks, terrorists' messages can be passed on through these pre-existing connections including low-tech channels such as telephone, fax, and

photocopying or, indeed, no-tech methods such as word-of-mouth (McLaughlin 2003, 6). In the same way that taped sermons from the exiled Ayatollah Khomeini were circulated through pre-existing religious connections in Iran (see Sreberny-Mohammadi & Mohammadi 1994, 119-121), Internet-based messages need only reach certain key actors in order to be circulated more widely. In this way, each and every Internet user has the capacity to become an information source.

Because of the focus in this text on English-language Web sites, this chapter is less concerned with domestic audiences than international audiences. Nonetheless, an important point in this regard is that the Internet does indeed allow for the targeting of different messages at different audiences, particularly when those audiences speak different languages. While the hyperlinked structure of the Internet may make it appear difficult to segment information for different audiences, this task is greatly simplified when linguistic differences distinguish potential audiences. The profound linguistic differences between Arabic and English allow a group such as Hamas to present itself one way to its local and regional audiences and in quite another to its Israeli and 'Western' audiences. Clearly, this ability is not limited to Arabic and English, but can be generalized to any sufficiently dissimilar languages. In fact, the Hamas portal at http://www.palestine-info.info points visitors to six sites hosted on servers in different countries and available in six different languages. According to researchers at the US Naval Postgraduate School, "although the sites usually have similar headline stories, they often vary in perspective, structure, and content" (Emery, Earl, Buettner 2004, 20). This is an important enabling factor in terms of Internet-based dissidence, allowing a single group to present multiple messages to various audiences by allowing editorial discretion and customized messages based on the audience, which in turn affords terrorists greater flexibility in the prosecution of their information war arising out of a greatly expanded potential support base (McLaughlin 2003; Tibbetts 2002, 35).

Not all groups build on this opportunity, however. In terms of the description and analysis of the FARC's Internet site contained in Chapter Five, the group does seek to gain international support, though this goal is clearly secondary to its domestic focus. The fact that the FARC provides a significant amount of non-Spanish content indicates that the group is directing some of its message towards international publics. Ultimately, however, the poorly defined nature of FARC's international audience and the static quality of its English content, in particular, limit FARC's attempts at

international support erosion. Although it is worth pointing out that, because Central and South America are largely Spanish-speaking, FARC's impressive Spanish-language site is targeting not just domestic, but also large regional audiences and not forgetting Spanish speakers in the United States and Europe.

International Audiences & Their Role(s)

The Internet offers unparalleled access to the international community. The Internet's ability to limit transaction costs over huge distances makes the technology an appealing one for non-state actors seeking to gain access to international audiences. Web sites are simple and cost-effective ways of providing information to world publics, giving the international community the ability to access information from anywhere in the world at any time. E-mail lists and message boards likewise provide instant access to potentially global audiences. It is therefore no surprise to find that many terrorist groups have established Web sites and use e-mail to generate international support.

Internet technologies allow dissidents to communicate with established supporters across long distances instantaneously. This ensures that supporters receive political messages quickly, enabling political support to be activated in limited timeframes. By internationalizing a conflict or political dispute, non-state actors seek to access a broader range of resources not available domestically. These resources can include financial and other types of material support, but also include intangible assets such as political support and sympathy. The sheer size of the international community makes internationalization an appealing strategy for terrorist groups. As with domestic mobilization, internationalization involves both recruiting and then rallying supporters. Sean McLaughlin (2003) identifies five different types of actors at which international mobilizing efforts may be directed.[189] First, non-state actors could focus upon other states within the international community, although the difficulties associated with this type of internationalization make it rare, particularly for terrorist groups. Communication between states and violent non-state actors is constrained because it must take place outside the normal channels of inter-state communication

[189] Gabriel Weimann identifies broadly similar audiences for terrorist sites in his USIP report. These are current and potential supporters, international public opinion, foreign journalists, and enemy publics (2004a, 4-5).

and generally in secret. Given the Internet's open architecture, it is a venue unlikely to be employed for this purpose.

Much more likely is that internationalization efforts will be directed at societies within other countries. Society-directed internationalization seeks to bypass the problems linked to direct communication with states. By mobilizing transnational populations, non-state actors can indirectly pressure foreign governments and seek to have their objectives included on the international agenda. Terrorists may also be able to garner material support from individuals within other states. The Zapatistas, benefited greatly from their ability to ally themselves with powerful societal actors within the United States, such as student and faculty organizations, which were able to publicize and support the Zapatistas' objectives.

Third, non-state actors can focus internationalization attempts at diaspora populations. In terms of nationalist-separatist terrorist groups, this audience may be particularly germane owing to the large and influential communities of expatriates such conflicts often give rise to. Gaining access to these populations allows terrorist groups to tap into the financial resources of the diaspora community. Indeed many terrorist groups have been linked to international charities that tap directly into diaspora populations for financial support as discussed in Chapter Three. Diaspora communities may also be able to influence the domestic environment by demonstrating support for the terrorist group to relatives and friends who remain in the homeland.[190]

Fourth, internationalization can seek to involve what has come to be called 'transnational' or 'global' civil society. These terms, which are often used interchangeably, most often refer to the networks of international non-governmental organizations (INGOs) that have become truly established in the last decade or so. The resources offered by INGOs are rarely financial but instead take the form of political support. INGOs are increasingly powerful players in the international community because of their ability to exert political pressures on states. INGOs can directly change state policies or can influence states indirectly, by altering public perceptions and opinions. INGOs are therefore a potentially powerful ally in non-state

[190] It's worth noting that "ICT-amplified diasporic discourse," particularly that supportive of politically violent groups, almost certainly does not represent the entirety of any particular community. When confronted with extremely polemical online narratives, it is perhaps easy to fall into the trap of ascribing those views to an entire population, yet this type of political communication represents only a portion of the views of any given group and, with regards to the Internet, only those with Web access at that (Kalathil 2002, 353; see also Appadurai 1996, 197).

actors' efforts to balance the power of states. By gaining access to the political resources of global civil society, non-state actors improve their chances of directly influencing state behaviour and also tap into a larger network of INGO supporters. Again the Zapatistas were able to tap into a variety of human rights INGOs that sent representatives to Chiapas as political observers, and who successfully constrained the Mexican government from using violence against the indigenous people.

Finally, terrorist groups can focus internationalization efforts at the media. The media provides a multi-faceted way for terrorists to have their messages broadcast to potentially huge audiences. Mass-media attention provides benefits beyond publicising acts of violence, including a degree of legitimacy and the forced attention of large differentiated publics. In terms of terrorist Web sites, it also provides the opportunity for mention of these and sometimes the publication of their URLs. Soo Hoo, Goodman & Greenberg have observed that, "for terrorists, using IT is not a perfect substitute for international news-media coverage and may even have negative consequences" (1997, 140). Increasingly however terrorist IT use and an increased focus on terrorist Web sites, in particular, are themselves garnering terrorists publicity.

It is also worth underlining that

> The importance of the digital public sphere for contesting media power would be far less if it were sealed off from other communication channels in society. However...the different media spheres are becoming increasingly porous. Researchers are beginning to pay attention to the pathways from micro-to-middle media that bring important messages in contact with mass media gatekeepers. The distributed property of the Web makes it difficult for news organizations to close the gates on tempting stories that competitors will be tempted to report if they don't. The rise of 24/7 cable news operations makes the demand for novel information high (Bennett 2003a, 32).[191]

Newspaper reports and television broadcasts, whether regional or international, have the ability to reach policymakers, societal actors, diaspora populations, and INGO

[191] For an analysis of the impact of Web logs (i.e. 'blogs') on foreign policy, particularly their use as source material by professional journalists, see Reynolds 2004.

activists simultaneously. Media coverage is therefore a powerful political resource for terrorists, enabling their messages to reach multiple audiences with minimal effort.

The disposition of each of the audiences identified to the terrorist message or the message generator can be expected to differ dramatically. The message generator must clearly be concerned therefore with the following audience-centred questions: How is each audience likely to feel about the message the specific terrorist site is presenting? And what is its likely disposition towards the terrorist group as a whole? There are three broad categories into which audience 'feeling' is generally classified:

- *Hostile*: audience members cannot be persuaded because they are so opposed to what is being said or to the speaker personally.
- *Sympathetic*: audience members are, in effect, already persuaded because of their support, agreement, etc. with the message or message generator from previous experience.
- *Neutral*: audience members have no firm disposition towards either message or message generator; the audience is yet to be either persuaded or dissuaded.

Theoretically, it is possible for an entire audience to fall into one or other of these categories; more commonly, however, elements of all three classifications may be found in an audience. For Internet-based messages, in particular, there are certain to be multiple audiences, which may be divided along these lines. Prior awareness of this aids the message generator in shaping particular messages for particular audiences (Tuman 2003, 74-75). Tibbetts has this to say about terrorists' tailoring of messages for different audiences:

> [T]errorist propaganda on the Web takes many forms, and can be tailored to a variety of audiences. For example, content can be targeted specifically at those who are already 'true believers': that is, those whose perception of the organization is already positive, whose perception of the 'enemy' is already negative, or both. Propaganda on such sites can be intended to reinforce that belief. On other sites, content can be oriented more toward persuading 'unbelievers' of the correctness of the terrorists' point of view. Although inducing a radical change of belief on the part of an opponent would obviously be beneficial, the chief benefit from these sites would be convincing the 'fence-

sitters': those who have not formed an opinion, or who have mixed feelings about issues important to the terrorists. For example, it may be easier to persuade educated Western audiences with facts rather than with imagery. If the goal is to recruit suicide bombers, images of graphic violence interspersed with half-truths and religious dogma may be more appropriate (Tibbetts 2002, 36).

Those responsible for the discursive structuring of the ten English-language sites analysed herein appear to have been particularly cognisant of their educated, liberal, Western audience(s).

THE DISCURSIVE STRUCTURING OF TERRORIST SITES

Now that the composition of the audience has been addressed, the next issue to consider is the actual content of the terrorists' cyber-messages. This is because however useful the Internet is as a political tool and in providing a political space, "all the channels of communication in the world are no substitute for a language, a political discourse that is accessible" (Sreberny-Mohammadi & Mohammadi 1994, 105). Thus the focus of the remainder of this chapter is a more detailed examination of the content of the most prominent narratives appearing in the ten terrorist Web sites explored here.

Efforts at both domestic and international mobilization are generally accompanied by efforts at support erosion. Support erosion is a political activity that seeks to erode public support for an opposing actor in a conflict. Whereas mobilization and internationalization are focused on the positive accumulation of resources for dissidents, support erosion seeks to break down the resource and power base(s) of states. By eroding support for the state, terrorists hope to limit the financial and political resources at a state's disposal thus improving the relative balance of power of the terrorists' *vis-á-vis* the state. Processes of domestic and international mobilisation cannot generally be separated from efforts at support erosion: messages designed to increase support for terrorists are almost always coupled with information aimed at damaging support for the state. Basically, terrorists seek to 'level the playing field' with states by improving their own relative power while, at the same time, decreasing that of the state. Since support erosion is closely linked to both

mobilization and internationalization, the audiences for this type of information can also be both domestic and transnational. Dissidents seek to exert political pressure on the state by eroding popular domestic support for state policies or the governing regime itself and thus undermining overall regime stability. In a similar fashion, the erosion of international backing for a government or its policies can further weaken a regime's legitimacy within the international community (McLaughlin 2003, 8).

In terms of the international dimension, a central plank of many such strategies is

> the shift from the 'self-interest' politics that dominates the domestic agenda to a 'moral' and 'ideological' politics...The battle for the middle class was and is about securing the moral and ideological 'high ground'...the tactics of grassroots movements are designed for one specific purpose; to alter the 'balance of power' between the decisionmakers and the general public, thereby discrediting the claims of the former" (Marsh 1995, 136-137).

Since support erosion is focused on denying resources to the state, the messages and symbols associated with it are expected to be negative. With regard to domestic populations, terrorists might be expected to employ political and religious motifs to negatively portray the state. For international audiences, support erosion is focused upon broad international norms; terrorists often seek to erode international support for a state by accusing it of oppression or other human rights abuses, for example. Three distinct types of narrative were apparent in the ten sites focused on here; these might be broadly termed narratives of religion, revolution, and rights.

Religious Narratives

A central function of ideology is to elaborate a worldview, but also to construct a collective identity. Religiously inspired narratives played a significant role in the discursive structuring of a number of the Web sites explored here. One reason for this may be that "religious beliefs are shared by *communities*, and community bonds are quite useful for resisting oppression" [italics in original]. In one sense then, religious communities do not have to be constructed, they are already in existence and may be perceived as simply in need of rousing: "A belief system does not simply define

beliefs, it also defines a group, persons who share a perceived common destiny. Such ties help a group to mark time and preserve its anger and identity while waiting for the right moment to rebel" (Adams 1996, 429). Many, indeed most, religious philosophies are eschatological; in other words, they support the denial of what is, for an imagined world that is manifested after death (i.e. 'the next life' or 'future life'). Many political violence groups also have an intense belief in a future imagined differently from their present and may, therefore, find it useful to draw upon eschatological themes such as the annihilation and endurance of the individual (soul), an individual leader or prophet, or even the world itself (Adams 1996, 430).

The Web sites of both Kahane Chai and Hamas evidenced such positions with both groups seeking to invoke religious principles in order to deny the claim of the other to what each views as 'their' land(s). The following is an excerpt from the writings of Rabbi Meir Kahane, which is available on the Kach Web site:

> It is a central tenet of Judaism that G-d wished the Jew to create a unique, total, pure and complete Jewish life, society and state in Eretz Israel. This being so, who can honestly believe that He then sanctioned the democratic right of a non-Jew, who is totally alien and outside the Jewish society and who is free of its religious obligation, to have the slightest say in its workings?...It is not merely that the land belongs to the Jewish people. It is that the land belongs to G-D and which He gave to the Jewish people for a specific reason and under a specific condition... And that is why the non-Jew who wishes to live there can do so only under certain conditions, the most important being that he has nothing to say concerning the state, its character, its workings. This is so for all non-Jews...How much more so for the non-Jewish residents of the Land who lived there BEFORE the L-rd gave it to the Jews. Those residents refuse to recognize such a fact. They believe the land to be theirs and dream of the day when they will regain it. To allow them to remain as proprietors, or even freely living with restrictions, is to ensure not only the general spiritual assimilation that is threatened by any large number of non-Jews, but also the threat of revanchist political and military attack.[192]

[192] From 'The Arabs in Eretz Israel,' available online at http://www.kahane.org/meir/arabs.html.

The 'Covenant' of the Hamas organisation contained a similar undertaking in the section entitled 'Strategies of the Islamic Resistance Movement: Palestine Is Islamic Waqf':[193]

> The Islamic Resistance Movement believes that the land of Palestine is an Islamic Waqf consecrated for future Muslim generations until Judgement Day. It, or any part of it, should not be squandered: it, or any part of it, should not be given up. Neither a single Arab country nor all Arab countries, neither any king or president, nor all the kings and presidents, neither any organization nor all of them, be they Palestinian or Arab, possess the right to do that. Palestine is an Islamic Waqf land consecrated for Muslim generations until Judgement Day.[194]

Religiously inspired terrorist groups may also portray themselves as expressions of religious faith and their actions as, therefore, a matter of duty. "[B]ecause the realm of the sacred is almost by definition unquestionable and unquestioned, political 'realities' and messages couched in religious terms are all the more persuasive and powerful" (Hegland as quoted in Sreberny-Mohammadi & Mohammadi 1994, 116). The following is an excerpt from an article penned by Rabbi Meir Kahane on the fourth day of the Yom Kippur War (1973) and available on the Kach Web site, which invoked such faithfulness to the 'Jewish G-d of History':

> ...[T]here are practical consequences that are to be drawn and there are very real steps that are forced upon us by the Reality of the Jewish G-d of History. From the existence of this G-d, from both the awesome fear on the one hand and the certain confidence on the other, emerges an inescapable and imperative path. It is the path of Faith and Belief. Faith in the Jewish Destiny and that if only the Jew remains true to His G-d and his heritage he can never be destroyed or overcome. Belief in the Power and Will of his G-d to destroy the enemy of the Jews...Faith and belief that the rational and logical and obvious and pragmatic wither away before the power of the Creator and Destroyer, the G-d who shapes and forms the G-d of

[193] In Islamic countries, the term 'waqf' (also 'wakf') refers to the custom of giving a piece of land, etc., to a religious institution, so that the revenue can be used for pious or charitable purposes; the term can also be used to refer to property given in this way.
[194] Available online at http://www.hamasonline.com/indexx.php?page=Hamas/hamas_covenant.

> History…They mean gazing upon a 'real' world that appears to be fraught with danger and that calls for a rational retreat from duty and Jewish obligation, and to deliberately choose the opposite path, of a seeming madness and irrationality, because it alone is the path of fidelity and faithfulness to Jewish values and because G-d will protect those who have faith in Him.[195]

Similarly, in the section entitled 'The Universality of the Islamic Resistance Movement,' the Hamas 'Covenant' warned those speaking out against the group that they were essentially challenging God:

> He whoever denigrates its worth, or avoids supporting it, and turns a blind eye to facts and is challenging Fate itself, whether intentionally or unintentionally, would awaken to see that events have overtaken him and will find no excuses to justify his position.

Bringing such strong moral, social, and spiritual obligations and sanctions into play acts as a further aid in ensuring that audience members who share the same religious faith as a particular terrorist group will be moved to share their political values and goals also. The employment of religious rhetoric may be viewed then as less about cajoling audiences to accept one's position and more akin to commanding them to do so (Sreberny-Mohammadi & Mohammadi 1994, 111-113).

Religiously inspired terrorist organisations are generally practiced in communicating with ordinary people and further aided by a rhetoric that has been honed over long periods; in the cases of Islam and Judaism, hundreds or thousands of years. This allows such groups to sum up their positions with brevity by drawing upon discourses known to all those who share their religious persuasion (Picard 1997, 216). For example, the Kach slogan "Chosen people-Chosen land-Chosen destiny,"[196] is a clear reference to the Jewish people as 'God's chosen people.' Nor does the Hamas slogan leave one in doubt as to the religious stance of that organisation: "Allah is its goal, the Prophet its model, the Quran its Constitution, Jihad its path and death for the

[195] From 'The G-d of History,' available online at http://www.kahane.org/meir/jewish_g-d.html.
[196] See 'Kahane.org: Principles and Philosophy' at http://www.kahane.org/philosophy.htm.

sake of Allah is the loftiest of its wishes."[197] 'New' religious organisations, on the other hand, may have less of a narrative repertoire upon which to draw, although mixing 'old' and 'new' religious precepts can mitigate this problem. This appeared to be the strategy adopted by Aum Shinrikyo whose 'Five Precepts for Lay Members'[198] read rather like the Ten Commandments and who also drew upon Buddhist and Hindu principles and practices as detailed on their Web site. In terms of the discursive structuring of their site, but also more generally, the Aleph group is somewhat of an outlier. It is unclear, for example, what the group's goals were in carrying out the Tokyo subway attack and the group's Web site did little to enlighten audiences on that score. A majority of religiously inspired terrorist groups are, in contrast, quite clear on their Web sites as to their enemies and goals, as are those groups who espouse revolution.

Revolutionary Narratives

The international class-based language of Marxism was used on a number of the sites to interpolate another already existing community: the worldwide community of leftists. The SL and NPA sites were replete with terms such as 'workers,' 'the masses,' 'people's war,' 'Yankee imperialism,' 'heroic combatants,' 'the revolutionary internationalist movement,' etc. The NPA's commitment to Marxist-Leninist principles was described as follows on their site:

> From the great treasury of Marxism-Leninism, we draw basic principles and historical lessons to shed light on the people's war that we are waging. But these are of general value; they are a general guide to our action. To rest content with them, without integrating them with our concrete practice, is to turn them into lifeless dogma. To dispense with them is to engage in blind action.[199]

In addition to Marxist-Leninists, the SL also described themselves as Maoists.

---

[197] See the Hamas Covenant, as above.

[198] These are as follows: 'Do not kill, do not steal what was not given to you, do not conduct sexual misconduct, do not lie, abstain from alcohol, cigarette [*sic*] and so on.' Available online at http://english.aleph.to/lib/doctrines/basic_d/04-3.html.

[199] From 'Specific Characteristics of Our People's War' (1972). Available online at http://www.philippinerevolution.org/cpp/index.shtml.

> The ideology of the international proletariat arose in the crucible of the class struggle as Marxism, becoming Marxism-Leninism and, finally, Marxism-Leninism-Maoism...These are three stages, periods or milestones in the dialectical process of development of a single unity that in 140 years, beginning with the *Communist Manifesto*, through the most heroic epic of class struggle, through fierce and fruitful two-line struggles within the communist parties themselves, through the tremendous work of giants of thought and action that only the class could have brought forth, with three unfading luminaries standing above the rest--Marx, Lenin and Mao Tsetung--and through great leaps, especially three, has armed us with Marxism-Leninism-Maoism, principally Maoism today. However, while the universal validity of Marxism-Leninism has come to be recognized, Maoism is not broadly recognized as the third stage; thus, while some simply deny it as such, others only go so far as to accept it as 'Mao Tsetung Thought.' Essentially, in both cases, while they clearly have differences between them, they both deny the overall development of Marxism by Chairman Mao Tsetung. Not to recognize Maoism's character as an 'ism' is to deny that it is universally applicable and, consequently, its character as the third, newest and highest stage of the ideology of the international proletariat: Marxism-Leninism-Maoism, principally Maoism, which we uphold, defend and apply.[200]

Marxist-Leninists, Maoists, or both, the Web sites of SL and the NPA tell remarkably similar stories: the instigation of people's war arising out of oppression by local elites acting in tandem with 'Yankee imperialists.'

A crucial element in any political movement is defining the enemy and, in the process, reinforcing the collective 'we' of revolutionary actors. For SL, the 'near' enemy is Peru's "Fascist, Genocidal and Country-Selling Dictatorship" while the 'far' enemy is the US government.[201] Why, SL asked, is the US government so concerned about the revolution in Peru?

---

[200] From 'On Marxism-Leninism-Maoism' (1988). Available online at http://www.csrp.org/pcp-mlm.htm.

[201] Interestingly, al-Qaeda and affiliated organizations portray their enemies in a similar fashion with 'near' enemies identified as assorted state leaders and governments in the Muslim world and the 'far' enemy as variously the United States, the 'West,' and/or the 'Zionist-Crusader alliance' (Burke 2004,

> Simply put, the US ruling class is dependent on dominating and plundering vast areas of the world for its very existance [*sic*]. Latin America is a key part of this US empire, and Peru is a very important country in Latin America--both strategically and economically. So the US rulers fear losing Peru to a Maoist revolution that would rip Peru out of the global web of imperialist exploitation and robbery, a revolution that claims nothing less than to be a Base Area for the advance of the world socialist revolution![202]

In April 2005, the NPA's spokesperson made similar remarks in relation to the situation in the Philippines, as detailed on the NPA Web site: "bootlicking officials of the Arroyo government want to make the Filipino people swallow their national dignity and sacrifice their national sovereignty on the altar of US military interventionism," he said. The spokesperson, Rosal, then called on the Philippine people to reject the "bribes of the US government, oppose the puppetry of the Arroyo regime and fight for Philippine national sovereignty against US military intervention."[203] This is in keeping with the repeated references on the NPA site to the Philippine government, led by Gloria Arroyo, as the "US-Arroyo regime" [204] and the "Arroyo Puppet regime."[205] In a similar fashion, one-time Peruvian president Alberto Fujimori was repeatedly referred to on the SL site as a "US-puppet."[206]

There were also repeated references to the Peruvian and Philippine governments as fascist and their actions as terrorist on both sites. The following are the titles of a number of press statements drawn from the NPA Web site:

2; Gerges 2005), although some divisions have emerged on this score between, in particular, Bin Laden and Abu Musab al-Zarqawi, the alleged leader of 'al-Qaeda in Iraq' (see Eedle 2004; Napoleoni 2005, 40-43).

[202] From section entitled 'The Crimes of the US-Backed Fujimori Regime' at http://www.csrp.org/usint.htm.

[203] Press release entitled '"Project: Bayanihan" is US Bribe in Exchange for Military Intervention, CPP Says.' Available online at http://www.philippinerevolution.org/cgi-bin/statements/releases.pl?date=050413;refer=kr;language=eng.

[204] See, for example, 'Oppose the Media Gag! Oppose the US-Arroyo Regime's Terrorism and Steps Towards Open Fascist rule! (http://www.philippinerevolution.org/cgi-bin/statements/statements.pl?author=cpp;date=050308;language=eng).

[205] See, for example, 'Raise the People's War to a New and Higher Level Against US Imperialism and the Arroyo Puppet Regime (http://www.philippinerevolution.org/cgi-bin/statements/statements.pl?author=cc;date=050329;language=eng).

[206] See, for example, 'Celebrate the Fall of the US-Puppet Fujimori: Support the People's War in Peru!,' online at http://www.csrp.org/cmte/fuji-fall-statement.htm.

- 'On the Arroyo Regime of Terror' (April 2005)[207]
- 'Resist the Terrorism of the US-Arroyo' (March 2005)[208]
- 'CPP Says Arroyo Regime is Veering Towards Open Fascism' (March 2005)[209]
- 'The Macapagal-Arroyo Regime Spews Out Lies Like Goebbels Did' (December 2004)[210]
- 'Arroyo Regime Cannot Defeat People's War Even With US Terrorist Support' (October 2004)[211]

The FARC Web site contained numerous similar comparisons.[212]

On the SL site, a review of John Malkovich's film *The Dancer Upstairs* (2002),[213] which is set in Peru, criticised the negative portrayal of the 'people's war' in the film:

> The 'terrorist' label is quickly stuck on those who rise up to resist their oppression. John Malkovich may claim that his *Dancer* story is fiction, but what purpose does it serve to portray people who are fighting for their liberation as terrorists?[214]

The implicit suggestion here is that it serves the purposes of the Peruvian government and their US ally to portray SL members and their supporters as terrorists so that they may be dealt with more harshly than might otherwise be the case.

Terrorist groups ideologically wedded to Marxism, Leninism, or Maoism, or some combination of these perspectives, might also be expected to address economic issues on their Web sites. And, indeed, this is the case with not just the NPA and SL, but also ETA, who espouse a broadly Marxist-Leninist worldview. A large number of

---

[207] Statement of the CPP, available online at http://www.philippinerevolution.org/cgi-bin/statements/statements.pl?author=cpp;date=050407;language=eng.
[208] Editorial contained in *Ang Bayan*, available online at http://www.philippinerevolution.org/cgi-bin/abshow/abshow.pl?year=2005;month=03;day=21;edition=eng;article=01.
[209] CPP Information Bureau press release, available at http://www.philippinerevolution.org/cgi-bin/statements/releases.pl?date=050311;refer=kr;language=eng.
[210] Statement available online at http://www.philippinerevolution.org/cgi-bin/statements/statements.pl?author=ndfnp;date=041213;language=eng.
[211] CPP Information Bureau press release, available online at http://www.philippinerevolution.org/cgi-bin/statements/releases.pl?refer=kr;date=041021;language=eng.
[212] See http://www.farcep.org/pagina_ingles/articles.html.
[213] The film's official Web site is located at http://www2.foxsearchlight.com/thedancerupstairs/index.html and includes a synopsis of the story, amongst other things.
[214] Drawn from PDF flyer, which is available online at http://www.csrp.org/pdf/dancer.pdf.

the media statements included on the NPA site dealt with issues such as the imposition by the Philippine government, with the support of the US, of new taxes and increased oil prices:

> The Arroyo regime seeks to cow the mass-based forces that stand against the government's moves to increase and impose new taxes, allow the wholesale entry and plunder of foreign mining companies, permit incessant oil price increases and invite the escalation of US military intervention.[215]

A broadly similar analysis was contained in an SL text entitled 'The Reality Behind the So-Called Economic Miracle in Peru' (1996), the opening paragraph of which read as follows:

> The Fujimori regime, under the direct guidance of U.S. imperialism, has launched a new economic program. The imperialists call it a 'free market economy' and 'privatization.' In short, it is about squeezing even more profit out of the Peruvian masses and plundering the country dry. Fujimori's economic plans offer up the Peruvian masses as low-cost wage slaves to the multinational capitalists, and has put the land and resources of Peru on the auction block.[216]

The ETA Web site laid the blame for high rates of unemployment in the Basque territories on centralised European Union policies and also upon the high numbers of multinational corporations that established plants in the region. These concerns were reflected in the following excerpted from an article entitled 'The Multinational Corporation: Navarre's Other Master' (2000) and posted on the ETA Web site:

> ...the multinational corporations impose their dictatorship. The global organization of inequality is not affected by the fact that the Basque territories now export Volkswagens and Mercedes Benzes to Europe and to

---

[215] Excerpted from CPP statement entitled 'Political Assassination Will Not Terrorize the People to Submission,' available online at http://www.philippinerevolution.org/cgi-bin/statements/statements.pl?author=cpp;date=050323;language=eng.

[216] Available online at http://www.csrp.org/stories.htm#real. See also 'Foreign Economic Domination Reaches New Heights' (1994), which is available at http://www.csrp.org/stories.htm#Eco.

> other distant markets. It is the German concerns that have considered it more convenient to export cars to certain markets from its affiliates in southern Europe: the low production costs and disposable labour force are Basque, the high profits are German. The Basque territories compete among themselves for the role of imperialist-investment favourite. They put no limitations on the entrance of foreign capital, its movement within their economy, the export of profits, or the repatriation of capital. Our regional governments lure companies with 'tax relief' and many other 'incentives.' Foreign companies take over local companies encouraged by the governments, and the local capitalist becomes a junior partner or functionary of his conquerors.[217]

Though less dogmatic than their NPA and SL counterparts, the FARC and ETA sites clearly evidenced many of the same concerns and employed many of the same buzzwords.

Rights-Based Narratives

While a number of the Web sites analysed employed religious narratives and others employed revolutionary narratives, by far the most popular approach was what might broadly be termed rights-based narratives. This term encompasses three quite distinct rights-based approaches: claims to recognition based upon historical rights, either to land or a separate identity; claims for recognition based upon international legal rights; and claims that political violence was only undertaken as a last resort of people whose human rights had been systematically abused. Each of the Web sites analysed here employed one or more of these rights-based arguments as detailed below.

Historical Rights

As Gabriel Weimann has observed, and as also mentioned in Chapter Five, "nationalist and separatist organizations generally display maps of the areas in dispute: the Hamas site shows a map of Palestine, the FARC site shows a map of

[217] Available online at http://www.ehj-navarre.org/navarre/na_history_mc.html.

Colombia, the LTTE site presents a map of Sri Lanka, and so forth" (2004a, 4). One of the functions of these graphics is to assert the historical right of the terrorist groups, as representatives of the people who inhabit these territories or some part therefore, to ownership of same. When taken in conjunction with the reconstruction by the political violence groups on their Web sites of an alternative or oppositional history with its own important dates and heroes, the symbolic power of which is also drawn upon to inspire the movement, these maps take on a peculiar resonance. The following, excerpted from an article entitled '36 Years for Peace and National Sovereignty,' is drawn from the FARC Web site and is an example of the former:

> ...turned into an armed revolutionary nucleus infused by our people's tradition of struggle, by the resistance of the natives and the black slaves to the violent and bloody methods used by the Spanish when they came to these lands, by the 1780 Commoner insurrection lead by Jose Antonio Galan, by the valour, courage and dignity of those who liberated our nation from spanish [*sic*] colonialism between 1810 and 1819 and raised the banners of anti-imperialism, social justice and latin american [*sic*] unity, unfurled by the Liberator, Simon Bolivar but brought down and stained by the creole [*sic*] political class. This nucleus took up the echo of pain and anger of those massacred on Dec. 6, 1928 in the 'Banana Region' and made the cherished aspirations of the working class and people its own.[218]

As already mentioned, the top pages of the FARC and NPA sites trumpeted the anniversary celebrations of these groups. A number of the other Web sites also celebrated the longevity of their particular groups' struggle thus underlining their more recent history in addition to what might be termed the groups' pre-historical rights.

[218] http://www.mondofariano.org/pagina_ingles/history/36years.html

International Legal Rights

Also included on the FARC Web site was an open letter, dated November 2001, to the UN representatives to Colombia, Jan Egeland and James Lemoyne, the final paragraph of which read as follows:

> Finally, we want to express to you that we value highly your mediation effort as representatives of the U.N., for the purpose of facilitating the resolution of the process's current difficulties. As soon as the central government removes the measures that in a discriminatory manner restrict the access of some foreigners to the zone, we can hold the meeting you are requesting.[219]

The FARC clearly wished to portray themselves in this letter as supporters and upholders of international law. Indeed a large part of the FARC's English-language site was devoted to lengthy disquisitions on the applicability of international law to the Colombian conflict and, in particular, the FARC's rights under same.[220]

The FARC were not the only group to draw Internet users attention to their rights under international law; the Hizbollah sites also included texts considering their group's position in international law as did the PKK and NPA sites, amongst others. The author of the article '"Israel's" International Responsibility Towards its Continued Aggression on Lebanon,' which was available on the Moqawama site, castigated the Israeli intervention in Lebanon as an international crime[221] while the text entitled 'The Armed Popular Resistance in the International Public Law,' which appeared on the same site, argued that Hizbollah is a legitimate resistance organisation under public international law.[222] The PKK site contained at least one

---

[219] Available online at http://www.mondofariano.org/pagina_ingles/comunics.html.
[220] See, for example, http://www.farcep.org/pagina_ingles/documents/beligerence.html.
[221] The original page from the Hizbollah site is no longer available online. However, the text referred to here originally appeared on the Lebanese Army's Web site and is still accessible at http://www.lebarmy.gov.lb/article.asp?ln=en&id=1180.
[222] This page is no longer available online in its original format, but the original text may be accessed via Google's cache here: http://66.102.9.104/search?q=cache:2qhZKZUZDzwJ:www.moqawama.net/r_resist/armed_po.htm+%22The+Armed+Popular+Resistance+in+The+International+Public+Law%22&hl=en.

similar article.[223] Additionally, on the NPA site the recruitment of children was addressed briefly with the groups' spokesman pointing out that under the Geneva conventions, they could recruit fighters from the age of fifteen up, but that since 1998, the NPA had made eighteen years of age the minimum recruitment age. The NPA spokesman went on to assert that "[t]he consideration is no longer just international law but the need to make sure that those being recruited are not immature in their thinking but are of the right age and level of maturity."[224] A stated respect for international law was in many cases closely bound up with a stated respect for human rights.

Human Rights

One popular way for those who consider themselves disenfranchised to get their concerns on the political agenda is by attaching their issue(s) to legitimate symbols or discourses and thereby redefining, displacing, or enlarging that wider agenda (Brysk 1995, 571). Alison Brysk has pointed out that counter-hegemonic uses of what she calls 'symbolic politics' "generally involve reversal of a canonical narrative, attachment of new characters to an existing narrative, or self-representation by marginalized members of society" (1995, 573). It is submitted that the designers and authors of terrorist Web sites have embraced all three of these approaches: while in the past terrorist groups were reliant on the mass media for their representation, they increasingly employ their Web sites for the purposes of self-representation; in particular, they have taken the discourse of human rights and inserted themselves as new characters within it, which, in turn, has led to the reversal--perhaps, more appropriately, 'inversal'--of the same canonical narrative.

The overarching narrative structures or plots of the Web sites studied herein were remarkably similar: government abuses of the 'people' were followed by appeals for help to domestic elites and/or the international community and, when these were ignored, resort to force of arms was the only remaining mechanism available to the 'people' for redress of their grievances. Both the original abuses and subsequent government crackdowns on the terrorist groups were portrayed on the

[223] See 'Rules for the Conduct of Warfare' at http://www.kongra-gel.com/index.php?option=content&task=view&id=11&Itemid=72.
[224] See http://www.philippinerevolution.org/pib/intrvw/clarifications.shtml#children.

terrorist sites as human rights violations, a discourse that is expected to resonate with global, particularly Western, publics. Employing the discourse of human rights allows for issues and events important to political violence groups to be tied to values that are already widely accepted in the Western world. This does not mean that Western audiences will automatically accept all messages with a human rights component, but instead that such messages will likely be more easily understood and receive more favourable attention than messages reflecting more contested values.

The opening paragraph of Chapter One of the LTTE's e-book *A Struggle for Justice*, entitled 'Why Did the Tamils Take Up Arms?' read:

> The birth and growth of the armed resistance movement should be analysed within the historical development of the Tamil struggle for self-determination. The Tamil struggle for self-determination has an evolutionary history of nearly half a century. It is a history characterized by state repression and resistance by the Tamils. The political struggles in the early periods were peaceful, democratic and non-violent but later assumed the form of armed resistance as the military repression of the state intensified into genocidal proportions.[225]

In the final chapter of the same e-book, the concern of the international community about the human rights situation in Sri Lanka was discussed. According to the text's author(s),

> The present Sri Lankan Government has made a few cosmetic reforms by appointing a human rights task force and commissions of inquiry to hoodwink the international community. But the country continues to be governed by Emergency laws, anti-terrorism acts and military and police tyranny...The military occupied areas in the Northeast have turned into massive concentration camps where Tamils are being subjected to arbitrary arrests, detention without trial, rape, torture and murder.[226]

---

[225] See http://www.eelamweb.com/publication/justice/whydid.shtml.
[226] See http://www.eelamweb.com/publication/justice/hidden.shtml.

The FARC's 'story' of their establishment in the early 1960s followed a similar plotline:

> Faced with the evidence of the coming aggression, and in order to find another way out, the inhabitants made every effort to approach all institutions and organizations susceptible to being motivated, including the parliament, the church and the international community, and have them come to that region and know its situation first hand. The only response was a declaration of solidarity by French intellectuals and Father Camilo Torres' attempt to come to the zone, which was prevented by the army. The President, representing the liberals and conservatives and following the guidance of the yankees [*sic*], gave the military command a free hand. Operation Marquetalia began: 16,000 men supported by the most modern techniques, advised by Pentagon officials and supported by the big print media, initiated the 'patriotic mission' to wipe out that group of Colombians in three weeks. They used every means at their disposal: aerial bombardment, strafing, parachute assaults, encirclements of extermination, bacteriological warfare, torture, summary executions, the buying of consciences and payment of bribes, as well as the jailing and abuse of those who were in solidarity with the 'Resistance of Marquetalia.'[227]

A majority of the other Web sites also employed similar narratives of persecution and rights violations.

While all the groups and sites studied addressed the issue of human rights, not all were willing to concede the importance of this issue to the same extent. For example, those groups with a strong religious component were less concerned with human rights, than historical and legal rights. Having said this, both Hamas and Hizbollah made positive comments about the role of human rights on their Web sites with the authors of the Hamas Covenant asserting "Hamas is a humane movement, which cares for human rights." Sendero Luminoso, on the other hand, was the group least amenable to the human rights discourse, which they portrayed as yet another tool of US imperialism. The following is indicative of their stance:

---

[227] See http://www.mondofariano.org/pagina_ingles/history/36years.html.

> Yankee imperialism, which acts like the gendarme of the world, is a paper tiger trying to prolong its death agony by raising the rotten and washed-out banners of "economic neo-liberalism," "human rights" and "bourgeois democracy," the peace of bayonets and eclectic, idealistic pragmatism because it has nothing new to offer. These paper tigers try to lull and intimidate the masses with a deceitful policy, "human rights." This flag they are waving today refers to the rights of imperialism, the bourgeoisie and world reaction. The puny, fake peace they proffer is an attempt to put the masses' consciousness to sleep in order to impose their hegemony as the world's leading superpower, no matter what it takes. It is the peace of bayonets, of gravediggers, of slavery.[228]

Statements similar to the above were also made in the context of various of the groups' inclusion on the US government's list of FTOs.

RESPONSES TO US TERRORISM DESIGNATION

An issue that was addressed on many of the terrorist Web sites investigated here was the groups' designations as Foreign Terrorist Organisations by the US Department of State. The NPA Web site contained the largest amount of materials relating to this issue including numerous articles alleging that the US blacklisting was a form of blackmail intended to force the former to cease their anti-government actions.[229] The following extract from an NPA statement made in 2005 is fairly representative:

---

[228] From the opening paragraph of the text entitled 'Unite the People Against the Fascist, Genocidal and Country-Selling Dictatorship by Further Developing the People's War.' Available online at http://www.csrp.org/pcp-uniteagainst.htm. It is worth pointing out here that such an interpretation of human rights discourse as bourgeois ideology has a long history in the radical Marxist tradition (see Geras 1985 & 1992; Lukes 1985).

[229] See, for example, 'CPP Challenges Arroyo to Denounce US Interference and Insistence on Terrorist Tag': http://web.archive.org/web/20050624074324/http://www.philippinerevolution.org/cgi-bin/statements/releases.pl?refer=kr;date=040224;language=eng; 'CPP Acknowledges Roco's Stand Against US Terror List': http://web.archive.org/web/20050624074109/http://www.philippinerevolution.org/cgi-bin/statements/releases.pl?refer=kr;date=040225;language=eng; 'On the Terrorism of US Imperialism and the Macapagal-Arroyo Regime': http://web.archive.org/web/20050624073832/http://www.philippinerevolution.org/cgi-bin/statements/statements.pl?author=kr;date=020912;language=eng.

> Who's the real terrorist? Countries that do not bombed [*sic*] and colonized other countries? Or the US who in just more than a year (1998-1999) bombed four countries, launched more or less a hundred aggressive wars and killed more than 12,000,000 people since 1900? Who's the real tyrant? Countries who readily submits [*sic*] the collective wisdom of the UN? Or the US who refuses to recognize the International Criminal Court, snubbed the Kyoto Protocol, went on with its unilateral decision to attack and colonize Iraq and passed the Patriot Act suppressing its own people? The US is becoming paranoid. It sees in every country having divergent views as possessing [*sic*] "weapons of mass destruction and a terrorist." Viewed from this angle, its war on terror will never end because contrary to its belief, in the eyes of many countries, the US is the number one terrorist. The influential scholar Samuel Huntington, in writing for the renown [*sic*] journal *Foreign Affairs* (which he edits), states that "in the eyes of much of the world (probably most of the world), the U.S. is becoming the rogue superpower and is considered the single greatest external threat to their societies" (see *Foreign Affairs*, May 1999).[230]

SL made similar comments in regard to their inclusion on the list summed up in the observation that "The emperor is allowed to burn down a thousand villages, but the people are forbidden to light even a candle."[231] The NPA were unique, however, in not only taking every opportunity to blast the US government for including them on the list of FTOs, but also denouncing the inclusion of the Moro Islamic Liberation Front (MILF) and Jemaah Islamiyah on the same list,[232] and castigating the Dutch government for bowing--as the NPA saw it--to US government pressure to designate Prof. Jose Maria Sison as a 'terrorist' also. Sison, a Philippine 'revolutionary,' is a political refugee resident in the Netherlands.

It is the Kahane organisation that sees itself as having the most reason for complaint, however: not just the group itself, but also the Kahane Web sites have been

---

[230] See 'US: The Number One Threat to World Peace': http://www.philippinerevolution.org/cgi-bin/statements/statements.pl?author=cr;date=050220;language=eng.

[231] See 'Dictating Terms: The US Anti-Terrorist List': http://www.csrp.org/rw/rw933.htm.

[232] See press release entitled 'CPP Says US Wants Arroyo to Scuttle Talks With MILF': http://www.philippinerevolution.org/cgi-bin/statements/releases.pl?date=050402;refer=kr;language=eng.

designated FTOs. The following is a flavour of what the site's creators had to say on the issue:

> The recent designation of Kahane.org and other Kahane sites as Foreign Terrorist organizations by the U.S. State Department is another one-sided, anti-Jewish, decree passed by the blatantly anti-Israel State Dept. This recent designation will definitely go down in history as one of the most irrational and obscene decisions ever carried out by the U.S. government. How does a website become a terrorist or a Foreign Terrorist Organization? Is it the fonts or html format that makes the anti-Semites in the State Department dizzy? Is it the Jewish star or the fist that symbolizes Jewish resistance to modern day Nazis that upsets our friends in the State Department?...Bombs and grenades are terrorism. Pencils, html and Torah-Bible are views and ideas!!! It seems that our words of truth scare them more than bombs and real terror. After all, Hamas, Hizbullah and Alkeada's [*sic*] websites are not on the State Department list of terrorist organizations. How sick and bizarre is that? Louis Farrakhan and hundreds of other white and black Nazi groups are not outlawed and their sites are not labelled terrorist, in spite of their terrorist words and actions. Yet Kahane.org a vehicle of Torah[233] ideas that never engaged in anything more than expressing views based on Torah is on the list.[234]

Aleph also responded to the US designation on their site with a letter to then Secretary of State Colin Powell pleading for the US government to reconsider their status[235] while the PKK site included an article describing the group's sharp response to their inclusion on the EU list, that went so far as to describe the latter as a "provocation to war."[236]

---

[233] 'Torah' is the name given to Mosaic or Jewish law as contained in the teaching or instruction, and judicial decisions, given by the ancient Hebrew priests as a revelation of the divine will and as assembled in the five books of the law, the Pentateuch.
[234] See 'Kahane.org Responds to State Department': http://www.kahane.org/response1.html.
[235] Available online at http://english.aleph.to/pr/13.html.
[236] See http://www.kongra-gel.com/index.php?option=content&task=view&id=50&Itemid=92.

THE IMPACT OF PHOTOGRAPHS AND OTHER VISUALS

The emphasis in this chapter upon the discursive structuring of terrorist Web sites does not necessitate the consideration of only the text-based components of the sites. Photographs and other images are constituent parts of the wider 'discourse' and serve a priming function. Even though photographs may not be solely responsible for cueing audiences to think about issues in a particular way, photographs still have the power to prime an audience to some degree. This is especially true of photographs with a dramatic and/or emotional content. "Photographs, because they mechanically reproduce what was in front of the camera, claim to denote reality" (Bignell 2001, 99). However, this denotative aspect of photographs is often a mythic foundation upon which connotations are then built. Just as language does not simply mediate 'objective reality' then, nor do still or moving images; instead they help to constitute political reality (Brysk 1995, 570).

This is not to deny that photographs may serve as confirmation and documentation of atrocities by acting as proof of the perpetration of crimes, but only that such 'proof' may have a metaphorical component also (Bissell 2002, 315). This is because many people assume that photographs simply record something that 'actually' happened. And while this is essentially 'true' in some instances, it is important to keep in mind, that photographs are, for the most part, not 'pure,' 'natural' images, but images that have been carefully selected and processed in order to generate particular connotations. A specific picture is used "because its connotations support particular mythic meanings."

Photographs also gain some of their meaningfulness from the particular contexts in which they appear. "This context is the channel through which their messages are transmitted, which shapes their significance for us" (Bignell 2002, 95-96). In terms of the Internet, entire Web sites act as a 'message' too or, more accurately, a collection of various messages that surround the photograph. Thus the particular Web site on which a photograph appears ought to give rise to certain expectations about the kinds of images the visitor/user should expect to see there and the knowledge that the meaning(s) that the accompanying text loads onto the photograph is itself 'naturalized': rendered innocent and apparently self-evident. In such settings photographs come to function as the 'proof' that the text's message is true. Some of the Web sites studied here were particularly 'glitzy,' making available

thousands of photographs and other images; thorough analysis of all of these cannot be undertaken here; however, a sub-section of these are referred to below.

Recruitment Images

Terrorist Web sites are increasingly sophisticated. In terms of recruitment practices, terrorist groups use their Web sites to extol the virtues of their particular group, along with descriptions of the positive aspects of group membership (Fritz, Harris *et al* 2004, 9). The seductive quality of these messages ought not to be underestimated. Web sites maintained by Islamic groups in particular, including those of Hamas and Hizbollah, contain

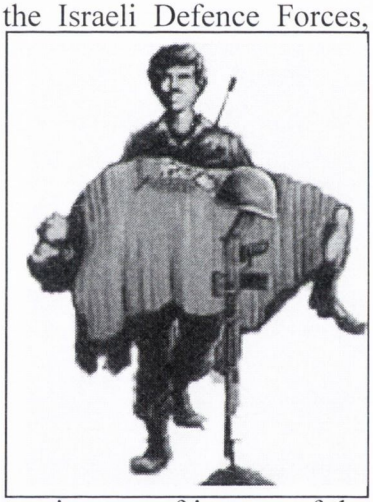
> Promises of martyrdom, heaven, fame, and remuneration to surviving family members [which] are interwoven with terrifying descriptions of slaughter both by and against the enemy... The rhetoric is inflammatory and explicit, and the visuals are meant to whip recruits into a frenzy of humiliation and anger against the West. Photos of dead and injured children can be great motivators (Fritz, Harris *et al* 2004, 9).

Whereas the Western-language version of a site may appear innocuous, composed largely of a rights-based discourse and written in neutral language that conveys a moral disengagement from the group's actions (e.g., "we bomb buildings, not people," as in the 9/11 attack), the indigenous language version may incite adherents to violence to a much greater extent. Even on English language sites however, photographs and digital video may be used to seek to rouse audiences to (violent) action.

In a 1979 newspaper article, Andre Glucksman contended "Dying power changes the world...[and] is what constitutes the strength of [many] social movements" (as quoted in Sreberny-Mohammadi & Mohammadi 1994, 124). A great deal has recently been made of the enduring power of martyrdom in Islamic thought, but much less is generally made of the symbolic power of death within contemporary secular political violence movements. A majority of the Web sites studied, of groups both religious and secular, elevated death to martyrdom and, therefore, a beginning rather than an end, empowering rather than disqualifying, and therefore something

glorious rather than terrifying. Many of the sites achieved this by identifying those who had died in pursuit of the groups' aims on their Web sites. Such strategies lend credence to Alison Brysk's assertion that "[t]he seemingly futile political preoccupation with absent actors who have passed beyond interests is actually a struggle by the living to wrest meaning from mortality, to situate the dead in history, to tell a story that can reshape hearts and minds" (Brysk 1995 585).

As mentioned in Chapter Five, Hizbollah's Moqawama site contained a gallery of photographs of dead 'martyrs' while the Hamas site made available extensive video footage of persons taken previous to their engaging in suicide bomb attacks. In addition, a large number of the screensavers contained in the extensive archive of these on the Hamas site were devoted to glorifying the activities of those who had died in pursuit of Hamas' goals. These included named and pictured suicide bombers and other operatives, along with victims of the Israeli Defence Forces, including the group's deceased leaders: Sheikh Yassin and Abdel-Aziz Rantissi. The LTTE site also contained tributes to the group's deceased members. Along with a prominent drawing (opposite) that appeared on the site's top page and that acted as a link to the 'National Heroes Day: Salute to Our Fallen Heroes' section of the site, the LTTE site also included a number of images of deceased female operatives[237] and photographs of the graves of dead 'warriors.'[238] The Kach site also made extensive use of images of the dead, particularly the deceased members of the Kahane family.



Of course, images of the dead were not the only images contained on the Web sites studied nor were these the only images that might have functioned as aids to recruitment. All propaganda is, in one way or another, a call to action, an invitation to throw in one's lot with the speaker. As Jacques Ellul has argued, when

> propaganda intervenes in public opinion, it transforms the public into an acting crowd or, more precisely, into a participating crowd...Propaganda can make the individual feel the urgency, the necessity of some action, its unique character. And at the same time propaganda shows him what to do. The

[237] See http://www.eelamweb.com/women/.
[238] See http://www.eelamweb.com/cgi-bin/image/imageFolio.cgi?direct=Warriors_Statues&img=16.

> individual who burns with the desire for action but does not know what to do is a common type in our society...If propaganda can show him this 'how' it has won the game; action will surely follow" (as quoted in Wright 1991, 74).

As regards incitement to violence, the US military recently handed terrorists one of the greatest recruiting tool of all: the debacle at Abu Ghraib. The release of photographs of the abuse of detainees at Iraq's Abu Ghraib prison was met with revulsion and fury in the Arab world. A selection of these photographs were posted to the Hamas site and as well as acting as a record of the abuse were probably also meant to act as an additional recruitment tool. As Dorothy Denning has pointed out, the US soldiers who took the photographs probably gave no thought to how the images would impact upon international relations: how their snaps would one day be disseminated worldwide thus inspiring some to more actively support terrorist groups and possibly eventually themselves carry out violent attacks (Denning 2005, 4). It's probably fair to say that such direct impacts are relatively few and far between, one consequence of which is that they will remain difficult to prove; nonetheless, the question of audience impact with regard to terrorist Web sites remains an important one.

AUDIENCE RESPONSES TO TERRORIST SITES

Moving beyond the description and interpretation of discursive structures, this section initiates consideration of the impact and influence of terrorist Web sites on those international audiences identified earlier. The analysis that follows is necessarily preliminary: terrorist groups do not release verifiable information as to who is accessing their Web sites. The small amount of information that may be gleaned from those same sites must therefore be treated with care. Having said this, an analysis of the latter in conjunction with evidence available to us from other sources, means a grainy picture of audience impact is beginning to emerge.

States as Audiences

Although the targeting of states within the international community was earlier dismissed as a useful mode of ICT-based internationalization by terrorist groups, this does not, of course, mean that various state-based actors and institutions do not compose part of the audience for terrorist Web sites. On the contrary, as pointed out in Chapter Three, the events of 9/11 and subsequent events in Iraq and elsewhere have meant that terrorist Web sites have come under heightened scrutiny from intelligence and law enforcement agencies worldwide. Hara and Estrada make this point well in their discussion of hate sites:

> For marginalized groups, the Internet can provide opportunities to legitimise their existence, and increase credibility, visibility, and marketability. This 'legitimation' resource can be seen in the ways that hate groups have engaged the Internet to establish an aura of legitimacy. The strategies for establishing legitimacy online are various and cheaper than through other mass media. Attempts at establishing credibility and legitimacy can be seen as successful to the extent that others (i.e., watchdog groups and law enforcement agencies) have perceived such Web sites as a threat and have initiated legal action to shut them down (Hara & Estrada 2003, 3).

Indeed, in their response to the designation by the US government of their Web site as an FTO, which is quoted from at length above, the Kahane organisation makes a similar point, claiming "our words of truth scare them more than bombs and real terror." In fact, the July 2005 London bombings provided the spur for the British government to act against terrorist Web sites. In the immediate aftermath of the attacks Charles Clarke, the British Home Secretary, indicated in a parliamentary speech that he would be seeking to extend the state's powers "to deal with those who foment terrorism, or seek to provoke others to commit terrorist acts." In his speech Clarke referred specifically to the inclusion within the ambit of these new powers "running websites or writing articles that are intended to foment or provoke

terrorism."[239] His plans have been endorsed by Britain's Association of Chief Police Officers who themselves have requested new legislation be drawn up giving law enforcement agencies "powers to attack identified websites."[240]

International Society as Audience

The term 'international society' is being employed here as an umbrella term to refer to the mass of Internet users at which terrorist groups' English-language Web sites are targeted, which will be taken to include individual Internet users, along with diaspora populations, NGOs, and the mass media. The reasons for supposing that it is such an audience at which the latter are primarily targeted have already been rehearsed, what is emphasised here is the response(s) of these audiences.

Individual Audience Members

The responses of a small number of individual audience members were relayed directly via the SL and Hizbollah Web sites. While a majority of the Web sites studied invited comments from their readers only the latter two published any of the correspondence they received. The top page of the Hamas site, for example, included the following message:

> Announcement: Regarding reply to e-mails, it is not possible for us at the moment to reply, we do read most of the friendly mails, but replying to e-mails is not possible at the moment.[241]

While not using e-mail to correspond, the SL site administrators requested letters from their online audience and posted excerpts from some of these online. Below are a number of examples:

---

[239] The full text of Clarke's remarks may be accessed online at http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm050720/debtext/50720-04.htm.
[240] The APCO proposals are outlined in a press release available online at http://www.acpo.police.uk/asp/news/PRDisplay.asp?PR_GUID={423FD3C2-2791-403A-B5D0-8FC6B5476B0B}.
[241] See http://web.archive.org/web/20041128015706/http://www.hamasonline.com/.

> Please send me CSRP stickers. My city is overpopulated with North American NATO soldiers; it is fun to spread Sendero souvenirs in this town!
> - *Teacher, Northern Italy*

> I've about had it with all those presidential wannabees and their bogus "issues." If asked where Peru is they would probably answer "Indiana." Send info…
> - *Ohio Guy*

> Thank you for all the stuff you sent me. I am at the moment "redecorating" my guitar and I was hoping for a "Viva la Guerra Popular en el Peru!" sticker please. Your web site is superb. Free Mumia![242]
> - *Musician in Ireland*[243]

In contrast to SL, the administrators of Hizbollah's Moqawama site explicitly requested e-mail correspondence from their audience. On the 'Readers Letters' section of the site were posted examples of three types of correspondence received (see Figure 6.1):

- Greetings and congratulations
- 'Letters' containing "feelers and creative ideas about Islamic public affairs (political, intellectual, religious….etc), our web site in form or in content, or any other significant issues that can take a shape of an article, research or point of view in certain subject."
- 'Letters' containing "nasty and vulgar phrases and ideas."

The site administrators go on to explain their reasons for posting examples of each of the above types of contacts:

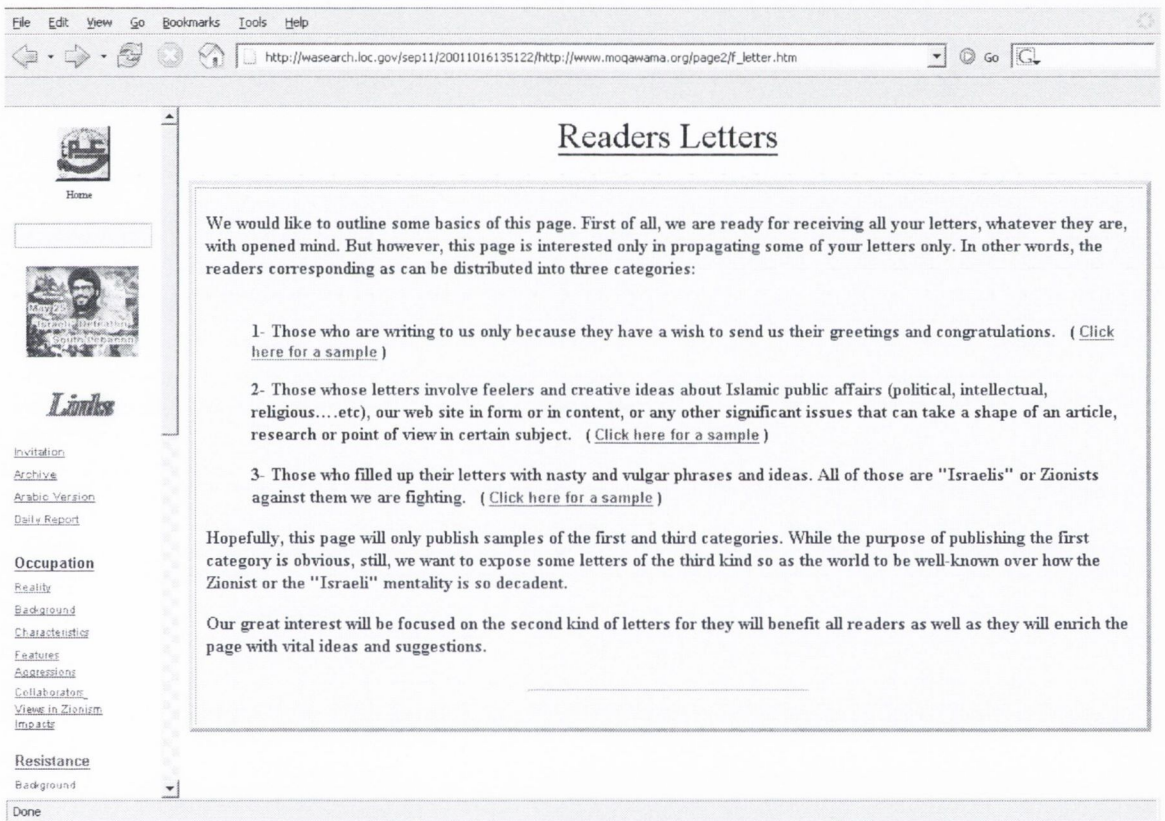
> Hopefully, this page will only publish samples of the first and third categories. While the purpose of publishing the first category is obvious, still, we want to expose some letters of the third kind so as the world to be well-known over

[242] Mumia Abu-Jamal is an African-American journalist and political activist who is on death row in the United States having been convicted of the murder of a police officer in Pennsylvania in 1982. Since that time many people and groups worldwide have worked to have his conviction, which they view as wrongful, overturned. For more information, see http://www.freemumia.org.
[243] For more, see 'Highlights of the CSRP Mailbag' at http://www.csrp.org/letters.htm.

how the Zionist or the 'Israeli' mentality is so decadent. Our great interest will be focused on the second kind of letters for they will benefit all readers as well as they will enrich the page with vital ideas and suggestions.[244]

There were seven congratulatory messages included in the relevant section of the site when last visited. At least three of the correspondents claimed to be from the United States. A selection of these congratulatory e-mails are reproduced below.

Figure 6. 1.
Top Page of 'Readers Letters' Section of Hizbollah's Moqawama Web Site



This is an excellent web site. Just to let you know I have added it to one of favorites [*sic*] on the Internet for quick and true Arabic points of views. I pray that the Zionist will be defeated very badly by Hizbullah or any other Arab resistance.

[244] See http://wasearch.loc.gov/sep11/20011016135122/http://www.moqawama.org/page2/f_letter.htm.

Subject: Great Page

I think your web site is very interesting because it shows a side of situation in Lebanon which I did not know about before. I believe ii [*sic*] human rights and I am upset that the Israelis have conducted such horrible atrocities against your people. But, I still do not completely understand how this situation could happen. Can you send me more information about it and what can be done to help the people of Lebanon? Thank you.

Subject: Israel [*sic*] wrongdoing

Greetings,

My name is Johnathan and I currently hold residence in Denver, Colorado, USA and am writing you to compliment you on a very fine job at making this web side happen. It is very informative and has helped me learn more about the Palestinian resistance and their rightful cause that they have for their attacks and Defenses [*sic*] against the Israeli forces.[245]

The section of the site devoted to those 'letters' of a "nasty and vulgar" sort contained just two entries, both of which are reproduced in full below.

Eliran Nager (Intl , 05:28 15/09/97, Your Doom Is Arriving...

Return-Path: <i-eliran@microsoft .com>

From: Eliran Nager (Intl Agency) <i-eliran@microsoft.com>

To: moqawama@cyberia.net.lb <moqawama@cyberia.net.lb>

Subject: Your Doom Is Arriving...

Date: Mon, 15 Sep 1997 05:28:47 -0700

You requested it. Now we have our own Resistance Movement that can and will destroy your organization with much suffer for your people (as much as 10 times of what you gave us and more). You can't just give us all "Live and let live" - So now were in business. We have full authorization to act by the Israeli government, and so -Prepare to die!!! Oh, by the way, you can't follow

[245] For the full text of the remainder of these 'letters', see http://wasearch.loc.gov/sep11/20011016122925/http://www.moqawama.org/r_letter/1.htm.

my location by using this mail as a lead. I'm using the name of a stupid ass who's not aware of it. We have been expecting for that kind of activity for all of our lives. Thank you for creating the right atmosphere for us to act.
Yours with great comforting for your death that will arrive soon....
USX.

eyal sela, 07:13 17/08/97, (no subject)
Return-Path: <eyal.sela@theclub.ipc.co.il>
Date: Sun, 17 Aug 1997 19:13:30 +0000
From: eyal sela <eyal.sela@theclub~ipc.co.il>
To: moqawama@cyberia.net. lb
Subject: (no subject)
I was a soldier in Lebanon and I saw many of your terrorists getting killed and I liked it every single time I saw it. I hope that all of you (f....) will die and burn in hell like the pigs that you are!!!!! (F.....) you. Sometimes i [*sic*] wish i [*sic*] was back in Lebanon to see some more bombings of MAGDAL-SLEM, SHAICRA, KABRIHA, FARCABBEE, BAR'ASHIT and of-course NABATIYE. I personally fired my tank on some of your friends and killed them. I was so happy! ! ! ! ! (F.....) off. You will be hearing from me and my friends soon as we will mailbomb [*sic*] your site!!! LONG LIVE "ISRAEL"! "' HALLELUYA! !![246]

The 'creative ideas' section of the site contained just three texts, a 'Quiz on the Middle East' highlighting Israeli transgressions of international law, an e-mail from 'An Arab in the USA' endorsing the use of force against Israel, and a request for information about an attack by a Hizbollah operative against IDF forces allegedly carried out using a hang glider.[247]

[246] From http://wasearch.loc.gov/sep11/20011016122925/http://www.moqawama.org/r_letter/3.htm.
[247] For complete texts, see http://wasearch.loc.gov/sep11/20011016122925/http://www.moqawama.org/r_letter/2.htm.

Diasporas as Audience(s)

Diasporas--immigrant communities established in other countries--frequently support terrorist groups operating in their homelands. "Despite being separated by thousands of miles, homeland struggles are often keenly felt among immigrant communities" (Byman *et al* 2001, 41). The proliferation of information technologies, including the Internet, in the last decade or so, has meant that diaspora populations can today have a greater knowledge of and influence upon the course of events in their homelands than ever before. Having said this, evidence supporting diaspora access of terrorist groups' English-language Web sites remains thin. It is to be supposed that many immigrants speak their native languages and therefore access groups' indigenous language sites. Those diaspora members further removed from their homeland--not just geographically, but also in time--and unfamiliar with their group's indigenous language might be expected to access English-language Web sites, however. For example, two pieces of correspondence reproduced on the Hizbollah site were signed "A Palestinian Lost in America"[248] and "An Arab in the USA"[249] respectively. That these individuals chose to correspond in English may suggest that they were unable either to speak or perhaps just write Arabic, or both.

NGOs as Audience(s)

NGOs are increasingly powerful organisations in our globalising world and many terrorist groups would surely like to have one or more influential NGOs on side. It is difficult to make this happen for groups employing violence, however. So while many NGOs may be unfavourably disposed towards a certain government because of their treatment of, say, political activists; the same NGOs would, in most instances, be careful to avoid endorsing the actions of those violently opposing the same government. This does not mean, of course, that NGOs and the individuals who compose them do not access the Web sites of terrorist organisations, but that should they do so, they have no reason to advertise same. Some reasons for NGOs to access such Web sites might include the collection of real-time information about the

[248] See http://wasearch.loc.gov/sep11/20011016122925/http://www.moqawama.org/r_letter/1.htm.
[249] See http://wasearch.loc.gov/sep11/20011016122925/http://www.moqawama.org/r_letter/2.htm.

situation in a given conflict zone, efforts to triangulate information received using information provided by as many parties to a conflict as possible, efforts to better understand the position of other parties to a conflict for bargaining purposes, etc. Evidence of such NGO use of terrorist Web sites is difficult to collect, however.

Mass-Media as Audience

If evidence of NGOs relying upon information obtained from the Web sites of terrorist organisations, indeed even accessing such sites, is virtually non-existent, the same cannot be said of the mass media. The Iraq conflict has put the spotlight on terrorist Web sites, which are increasingly viewed as newsworthy in themselves, but are also more and more used by journalists as legitimate sources of news and information.

That Western journalists and media outlets are a target of terrorist groups' English-language sites is clear from the structuring of those sites as described in Chapter Five. For example, the Hamas Web site acted as a repository for over 600 press releases while, as already mentioned, Hizbollah maintained a dedicated 'Central Press Office' site. The Hamas Web site was particularly successful in garnering media attention including both general articles about the existence of the site and literally hundreds of reports drawing on the site content to substantiate and/or repudiate events involving or related to the organisation and the Palestinian-Israeli conflict. Examples of the latter have appeared in *The Jerusalem Post*, *The Washington Post*, *The Houston Chronicle*, and *The Montreal Gazette* amongst a host of other newspapers. This is in keeping with the Hamas charter, which highlights the importance of having "information and media people" involved in awakening the masses and resistance. In fact, Fathi Hamad, the Hamas communications chief, has described the media as "the decisive weapon" (Levitt 2005).

Journalists are also known to have contacted the administrators of terrorist Web sites seeking specific information about groups and their sites. The 'Readers Letters' section of the Moqawama site included one such request, which is reproduced below.

To: moqawama@cyberia.net.lb

Subject: query

I am a reporter with *U.S. News and World Report*. I write about international affairs for the magazine, which is a news weekly based in Washington D.C. I came across your Web site and although it is still being built, I found it very useful to learn more about your organization.

Perhaps you can answer some of my questions by e-mail as soon as you have a chance.

Why did you set up a Web site? What gave you the idea? Where did you get the computer expertise? What do you hope to be able to accomplish with it?

Also, what do you feel about Israel's proposal to pull out of South Lebanon? Will that be a victory for your group? Would you continue your activities if they pulled out.

Thank you for your time.
Kevin Whitelaw
Diplomatic Correspondent
U.S. News and World Report
202-955-2234
kwhitelaw@usnews .co[250]

This solicitation by journalists of the opinions of terrorists and the increasing reliance of the former on terrorist Web sites for information about the course of various conflicts renders the mass media and its representatives the most important consumers of terrorist Web sites.

This is because terrorist Web sites that attract such a high-profile readership can rely on the information that they wish to disseminate being transmitted to much larger and more diverse audiences than those already familiar with their homepages. Reynolds makes this point well in his discussion of war blogs and, in particular, the high numbers of journalists amongst their readerships:

[250] See http://wasearch.loc.gov/sep11/20011016122925/http://www.moqawama.org/r_letter/1.htm.

> It is this sort of high-profile readership, I suspect, that has given weblogs the ability to punch above their weight in national discussion. Even the most popular weblogs have a readership approximating that of a medium-sized newspaper: nothing to sneeze at, but American medium-sized newspapers--of which there are hundreds--are not nationally influential. The readership of weblogs is heavily tilted toward journalists and politicians, however, which makes their influence more akin to that of 'insider' publications like trade newspapers or political newsletters. By the standard of those publications, weblogs have very large readerships (2004, 61).

At the same time, the publication in the mass-media of terrorist sites' URLs makes more people aware of their existence and thus increases the likelihood of their surfing to one of these destinations. In addition, when major media outlets such as the *New York Times* show 'trust' in a site, by using it as a source of information, others will too, thus gaining the site more attention, legitimacy, and ultimately users, and so on repeatedly.

CONCLUSION

A successful Web site must be created purposefully with a certain impact in mind. In all conflicts, the textual and visual display of atrocity is aimed at shaping public opinion: "The ultimate aim of the propagandist is to promote action" (Wright 1991, 74). This chapter sought to give a sense of how things look to the participants on the cyber front line. How do they characterise what they are doing? What kind of stories do they tell in order to make sense of their own actions and that of their enemies? Alyson Brysk argues that communication of this sort, both instrumental and normative, creates and sustains power.

According to Brysk, part of politics is convincing people of what they want, which implies that a power relationship can take at least three basic forms: coercion (force), bargaining (exchange), and persuasion (manipulation of meaning) (Brysk 1995, 564). This chapter has been primarily concerned with the discursive structuring of terrorist Web sites and the ensuing impacts on Internet audiences. The chapter was therefore centrally concerned with the manipulation of meaning. Although

unconcerned with either terrorism or the Internet, Brysk's description of what she terms "symbolic politics"[251] sums up the core thesis of this chapter rather well:

> The mechanism of symbolic politics produces collective action through the narrative structuring, interpretive resonance, and projection of affective information. We think about politics in stories, and our consciousness is changed when new stories persuade us to adopt a new paradigm. Collective action itself then involves a kind of storytelling or political theatre, performing the new paradigm to persuade others. Stories that work rewrite history because they contain the elements of successful communication--legitimate speakers, compelling messages, and satisfying plots--and can compensate for the lack of other resources. The successful exercise of symbolic politics then leads to social change through shifting priorities, building collective identities, shaping social agendas, or challenging state legitimacy (1995, 561-562).

In 2000, Susan Carruthers observed that "left to their own devices, terrorists are their own worst publicists" (p.169). For many such groups, however, this is no longer the case if, indeed, it ever was. With this in mind, the final chapter describes and analyses, in greater detail, the cyber strategy of one particular group, Hizbollah, which has been successfully telling its story via the Internet for some time.

[251] Brysk defines 'symbolic politics' as "clusters of messages intended to change attitudes, which may be enunciated by individuals, groups, states, societies, or international organisations" (1995, 562).

7

CYBERCORTICAL WARFARE: HIZBOLLAH'S INTERNET STRATEGY

INTRODUCTION

The increased acceleration of the historical tempo and the move from hierarchical to networked conceptions of power is disintegrating the mechanisms of control and political representation at the disposal of the state. The upshot of this is that "resistance confronts domination, empowerment reacts against powerlessness, and alternative projects challenge the logic embedded in the new global order." These reactions and mobilizations, often take "unusual formats and proceed through unexpected ways" (Castells 1997, 69). This chapter deals with one such alternative project.

In his introduction to the Vintage edition of *Covering Islam* (1997), Edward Said refers to the "information wars that have gone on since 1948 around the whole question of the Middle East" (Said 1997 [1981], xxi). He is particularly concerned with the way in which the Lebanese-based Shi'a group Hizbollah (Party of God) "who identify themselves and are perceived locally as resistance fighters" are "commonly referred to in the American media as terrorists" (Said 1997 [1981], xiii). Hizbollah[252] is one of a number of groups that have utilized the Internet "to produce and articulate a conscious and forceful self-image" (Said 1997 [1981], 66) of themselves not as terrorists but as resistance fighters and statesmen, as evidenced in Chapter Six. The major focus of this chapter is the way in which Hizbollah have

[252] The 'correct' English spelling of the group's Arabic name is Hizb'Allah or Hizbu'llah, however it is more usually spelled 'Hizbollah,' 'Hizballah,' or 'Hezbollah.' I have chosen 'Hizbollah' because that is the spelling employed in the URL designating the group's official homepage. However, where I have employed quotation I have retained the original spelling used by the author.

wielded the Internet as a weapon in their information war, essentially detailing the adoption by the group of a strategy of what I've termed 'cybercortical warfare,' a specific type of Internet-based soft power that is described below. In this respect, the chapter also acts as a more in-depth case study of the possibilities of the new technology for the conduct of information warfare (IW) at the sub-state level than laid out in previous chapters. As will be demonstrated, Hizbollah's collection of Web sites is targeted not just at Lebanese or Palestinian audiences, but at the Israeli population and global publics more generally. It is contended furthermore that whilst Hizbollah has instituted one of the most successful cyber strategies of the groups investigated in this text, it is increasingly also a victim of its own success.

SZAFRANSKI'S NEO-CORTICAL WARFARE

Neocortical warfare "attaches more importance to communicating with other minds than to targeting objects" (Szafranski 1997 [1994], 396). It points to the reframing of conflict as warfare against minds and envisions its weapons as any means used to change the enemy's will (Szafranski 1997 [1994], 404). It is founded on the belief that at base politics is the pursuit and eventual exercise of power, and that 'power' is "the ability to influence people who otherwise might not choose to be influenced" (Szafranski 1997 [1994], 397). The concept of neo-cortical warfare originated with Richard Szafranski in his article entitled 'Neocortical Warfare? The Acme of Skill,' which first appeared in the *Military Review*, a publication of the US Army Command and General Staff College, in 1994. Szafranski quotes Sun Tzu to the effect that "To subdue the enemy without fighting is the acme of skill" (1997 [1994], 399).

Neocortical warfare may be conceived of as a species of Perception Management, which is generally held to include the disciplines of Public Affairs, Public Diplomacy, Psychological Operations, Deception and Covert Action (Dearth 2002, 1). Perception Management may be defined as

> Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates,

ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives (Dearth 2002, 2).

This chapter is concerned more with the conveyance of information than its denial, and focuses on its effects upon foreign publics rather than intelligence systems and leaders. Its focus is therefore Public Diplomacy, rather than the other disciplines that compose Perception Management. The practice of Public Diplomacy has undergone significant change as a result of the information revolution.

The New Public Diplomacy

Diplomacy has traditionally been thought of as the development and implementation of foreign policy by diplomats. However, states and their representatives are no longer the only actors in diplomatic relations. There is an increasing emphasis on the role of non-state actors and publics in diplomacy, not only as recipients of diplomacy--the traditional understanding of 'public diplomacy' as a government's process of communicating with the public of another nation in order to influence its opinion--but also as diplomatic actors. Put simply, the public dimension of diplomacy has been increasing in importance. While there was a time when diplomats were the sole interlocutors between countries, now unmediated dialogue and information exchange between citizens from around the globe occurs twenty-four hours a day, seven days a week (Rothkopf 1998, 328; Wriston 1997). The theory and conduct of diplomacy is undergoing a radical rethink as a result. There have been repeated calls for diplomacy to be 'reinvented' to take account of the Information Revolution and a welter of analyses published suggesting how this might be accomplished (see Vickers 2001). This chapter is concerned with just such a reinvention, albeit a reinvention outside the purview of a majority of the research undertaken to date.

In the past, Public Diplomacy was often seen as irrelevant and unimportant. However, there is a growing movement to give Public Diplomacy a greater prominence in the conduct and study of international relations. This interest follows from an emergent view that the practice of world politics is changing; that things are being done in new ways, that new actors are important. Rather than a realist world composed purely of states acting militarily to maximize their power positions, this consensus points to a world in which international politics can be thought of in terms

of an 'informational pluralism.' On the one hand this is a world with a variety of agents at work, but where the operation of this pluralism is shaped by the impact of the information or communications revolution. These processes can be summarized in the idea that we are seeing the development of a 'new Public Diplomacy.' This idea has a double meaning. Firstly, that we are seeing diplomacy--understood in the broad sense as the practice of international relations--taking place in public and the public being involved. Secondly, that the central instrument of this new diplomacy is actually Public Diplomacy: that is communication and communications technologies (Brown 2001a; White 2001, 317-330).

The Increasing Importance of Soft Power

As Robin Brown has pointed out, "The new public diplomacy implies a change in the nature of power but it also helps us to understand how power is exercised in international politics" (Brown 2001a). One major consequence of this new environment is the importance of credibility as a source of power (Brown 2001b, 11). Although there have been many guerrilla groups fighting as oppressed national minorities, only five groups have had the credibility that allowed them to become significant diplomatic actors in the last two decades. In the mid-1970s, the Palestinian Liberation Organization (PLO) and South West African People's Organization (SWAPO) achieved membership of the Non-Aligned Movement and the Group of 77, along with observer status in the UN General Assembly and at all UN conferences. Three other groups the ANC, the Pan-African Congress, and the Patriotic Front of Zimbabwe obtained the right to attend UN conferences (Willetts 2001, 368). However, world politics today transcends simple inter-national relations and inter-governmental organization, and much of the change has taken place as a result of the spread of information infrastructures. Diplomacy is no longer the sole province of states and their representatives, instead the Internet offers the opportunity for non-state actors and marginalized groups to engage in what has been called 'virtual diplomacy' (Smith 2000) or 'cyber-diplomacy,' (Potter 2002) essentially the practice of Public Diplomacy via the Internet.

Cybercortical Warfare

"Neocortical warfare is warfare that strives to control or shape the behavior of enemy organisms, but without destroying the organisms" (Szafranski 1997[1994], 404), it "uses language, images and information to assault the mind, hurt morale and change the will" (Szafranski, 1997[1994], 407). In other words, neocortical warfare is the conduct of Public Diplomacy in an explicit conflict situation. 'Cybercortical warfare' is therefore an apposite term to describe the conduct of Public Diplomacy *via the Internet* in the same situation. In the broadest sense, cybercortical warfare is about offensively shaping the information environment, particularly the 'conflict space' (Dearth 2002, 8). To do this successfully, one must possess credible political and military power in order to command attention and convincingly project information power. In the realm of Public Diplomacy, for example, all Arab states have launched their own Web sites and many have several such sites. These sites are designed to get information about their countries out to the rest of the world, and to counter or balance information provided on the Web by Israel, Iran, and other states (Franda 2002, 81). States are not the only actors to establish a presence on the Internet, however. As previous chapters have shown, recent years have seen more and more groups that are engaged in militancy and political violence establish an online presence.

BACKGROUND INFORMATION ON HIZBOLLAH

Hizbollah[253] has been described as "One of the most significant terrorist organizations operating today" (Whittaker 2001, 41), yet it is also a legitimate political party with a wide base of support in Lebanon. The first Hizbollah representatives were elected to the Lebanese parliament in 1992. At the present time there are twelve Hizbollah deputies sitting in the Beirut parliament (see Hamzeh 1993 & 2000; Palmer Harik 2004, 95-110).[254]

---

[253] According to the US Department of State, the group is also known as Islamic Jihad, Revolutionary Justice Organization, Organization of the Oppressed on Earth, and Islamic Jihad for the Liberation of Palestine. They are also known to refer to themselves as the Islamic Resistance Movement.

[254] There are 128 seats in total in the Lebanese parliament.

Hizbollah was established in 1982 in response to the Israeli invasion of Lebanon.[255] It is composed of radical Shia's[256] and takes its ideological inspiration from the Iranian revolution and the teachings of the late Ayatollah Khomeini. The *Majlis al-Shura*, or Consultative Council, is the group's highest governing body and is presided over by Secretary General Hassan Nasrallah (see Ranstorp 1994 & 1998, 17-21). In principle, Hizbollah advocates the establishment of Islamic rule in Lebanon and the liberation of all occupied Arab lands, including Jerusalem. It has expressed as a goal the elimination of Israel and has rejected all international resolutions that have required recognition of the state of Israel (see Saad-Ghorayeb 2002, 134-167). These include the 1949 armistice between Lebanon and Israel, UN Resolutions 425 and 426, and the 1993 Oslo Accord. The group has also maintained its opposition to portions of the Ta'if Agreement, which terminated the Lebanese civil war.

Such stands in no way hindered the group from growing as a socio-religious movement nor taking its place in Lebanon's political institutions. Hizbollah is a significant provider of social welfare services in Lebanon where it has established and runs a network of some fifty hospitals and medical centres along with a commercial network that includes supermarkets, petrol stations, department stores, and construction firms (Hamzeh 2000, 743; Levitt forthcoming 2006). In 1998, Norton reported that its medical facilities were far better than those available in government hospitals, which the poor would otherwise have to rely upon (see also Ranstorp 1998, 20-21).

Although closely allied with and often directed by Iran, the group is thought to have conducted operations that were not approved by the Iranian leadership. While Hizbollah does not share the Syrian regime's secular orientation, the group was a strong tactical ally in helping Syria advance its political objectives in the region (see Palmer Harik 2004, 29-41). In addition to political, diplomatic and organizational aid, Hizbollah receives substantial amounts of money, training, weapons, and explosives from both Iran and Syria (US Department of State 2003). According to Ely Karmon (2002), Iran continues to support Hizbollah financially to the tune of $10 million per month while Matthew Levitt (forthcoming 2006) points out that some Western

[255] For a description of the events resulting in Israel's intervention in Lebanon from the Israeli perspective, see Schiff 1984.
[256] Shia's compose approximately 35-40% of the Lebanese population.

diplomats and analysts in Lebanon estimate that Iran funnels closer to $200 million per year to Hizbollah. There is some dispute about these figures, and while it is thought that Iran supplied the group with upwards of $500 million per year in the mid-1980s, some analysts now contend that has decreased to as low as $20 million per year at the present time (Whitaker 2000). It is certainly true that Hizbollah has sought to diversify its sources of income in the last decade and it is now an important stakeholder in Lebanon's economy as well as profiting from various criminal enterprises with which it is involved internationally (Levitt forthcoming 2006).

Hizbollah is thought to have a well-armed 25,000-man militia at its disposal, some 5,000 active fighters involved in its combat organization, and a few hundred terrorist operatives. These operate in the Bekaa Valley, the southern suburbs of Beirut, and southern Lebanon. According to US experts the group has also established cells in Europe, Africa (see Levitt 2004), South America (see Meehan 2004), North America (see Newman & Diaz 2005), and Asia. Hizbollah is suspected to have been involved in numerous anti-US terrorist attacks, including the suicide truck bombings of the US Embassy in Beirut in April 1983, the US Marine barracks in Beirut in October 1983, and the US Embassy annex in Beirut in September 1984. Three members of Hizbollah are on the FBI's list of 'Most Wanted Terrorists' for the hijacking in 1985 of TWA Flight 847 during which a US Navy diver was murdered.[257] Elements of the group were responsible for the kidnapping and detention of US and other Western hostages in Lebanon in the 1980s (see Jaber 1997, 97-144; Ranstorp 1997); Hizbollah also attacked the Israeli Embassy in Argentina in 1992 and is a suspect in the 1994 bombing of an Israeli cultural center in Buenos Aires (US Department of State 2003; see also Saad-Ghorayeb 2002, 88-111).

Israeli attacks on southern Lebanon that resulted in Hizbollah counterattacks on northern Israel are generally perceived to have brought about an end to popular Israeli support for the Israeli Defence Forces (IDFs) continued presence in Lebanon. The IDF withdrew from southern Lebanon on 25 May, 2000. Hizbollah "considered Israel's unconditional implementation of Resolution 425 outside of any auxiliary peace treaty or security arrangement a resounding success and realisation of its aims, and proof that it is a military and political force that can win" (Mouzahem 2001). The IDF withdrawal did not spell the end of Hizbollah's interactions with Israel, however.

[257] The three are Imad Fayez Mughniyeh, Hassan Izz-Al-Din, and Ali Atwa. See http://www.fbi.gov/mostwant/terrorists/fugitives.htm for more information.

There is ongoing conflict over the continued Israeli occupation of the area known as Sheba'a Farms, the continued detention of Lebanese citizens in Israel and, more generally, the status of the Occupied Territories and the Palestinian people as a whole.

The US Position

Prior to 9/11, Hizbollah was responsible for more American deaths than any other terrorist group; indeed Osama Bin Laden has cited Hizbollah's 1983 suicide bombing of the US marine barracks in Beirut as the first "American defeat" by Islamists (Karmon 2005; see also Kean, Hamilton *et al* 2004, 96). Given the Beirut blasts and the spate of other attacks against American interests enumerated above, it is unsurprising that "[n]o manifestation of the Islamist phenomenon evokes more antipathy from U.S. policy makers than Lebanon's Hizballah" (Norton 1998). While "[i]n the U.S. demonology of terrorism, Osama bin Laden and al Qaeda are relative newcomers. For most of the past two decades, Hezbollah has claimed pride of place as the top concern of U.S. counterterrorism officials" (Byman 2003, 56). On September 20, 2001, in a historic speech to a joint session of Congress, US President George W. Bush famously declared: "Our war on terror begins with al Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped, and defeated." According to Daniel Byman, "few terrorist organizations meet this standard, but Hezbollah is definitely one of them" (2003, 54).[258]

Many in the United States have argued that Hizbollah ought to be a prime 'War on Terror' target. Shortly after 9/11, a group of leading scholars, pundits, and former US government officials, including William Kristol[259] and Richard Perle,[260] declared in an open letter to President Bush that "any war on terrorism must target Hezbollah" (as quoted in Byman 2003, 54). Since that time the rhetoric employed by Bush administration officials has been ratcheting increasingly upward. Hizbollah was among the few groups that President Bush mentioned by name in his January 2002 State of the Union address:

---

[258] The *9/11 Commission Report* also describes Hizbollah as a "worldwide terrorist organization" (Kean, Hamilton *et al* 2004, 240).

[259] Kristol is editor of the influential Washington-based political magazine *The Weekly Standard.*

[260] Perle was at that time the Chairman of the Defence Policy Board, a federal advisory committee to the US Department of Defence.

> Our military has put the terror training camps of Afghanistan out of business, yet camps still exist in at least a dozen countries. A terrorist underworld--including groups like Hamas, Hezbollah, Islamic Jihad, Jaish-i-Mohammed--operates in remote jungles and deserts, and hides in the centers of large cities (Bush 2002a).

FBI officials testified in February 2002 that "FBI investigations to date continue to indicate that many Hezbollah subjects based in the United States have the capability to attempt terrorist attacks here should this be a desired objective of the group" (Byman 2003, 55). The US president went on to condemn the group as terrorists again in his June 2002 speech on the Middle East:

> I've said in the past that nations are either with us or against us in the war on terror. To be counted on the side of peace, nations must act. Every leader actually committed to peace will end incitement to violence in official media and publicly denounce homicide bombings. Every nation actually committed to peace will stop the flow of money, equipment and recruits to terrorist groups seeking the destruction of Israel, including Hamas, Islamic Jihad and Hezbollah (Bush 2002b).

Also in 2002, then Deputy Secretary of State Richard Armitage identified Hizbollah as "the A team of terrorism," and warned "their time will come, there's no question about it" (as quoted in Levitt forthcoming 2006; also Byman 2003, 55). In 2003, CIA director George Tenet followed up with his testimony that "Hezbollah, as an organization with capability and worldwide presence, is [al Qaeda's] equal, if not a far more capable organization. I actually think they're a notch above in many respects" (as quoted in Byman 2003, 57; see also Levitt forthcoming 2006). What then explains, President George W. Bush's recent statement that Hezbollah could prove that it is not a terrorist organization "by laying down arms and not threatening peace" (Byman 2005; Herzog 2005)? The suggestion advanced here is that one of the reasons for the US administration's softened stance is the success of Hizbollah's media

strategy,[261] including its cyberspace component, which portrays the group as a legitimate resistance organisation, not just within Lebanon, but also internationally.

Hizbollah's Cyber Capabilities

Regarding Hizbollah's cyber capabilities, as early as 1996 John Deutch, former director of the Central Intelligence Agency (CIA), testified before the Permanent Subcommittee on Investigations of the United States' Senate Governmental Affairs Committee that international terrorist groups had the capability to attack the critical information infrastructure (CII) of the United States. He said the schemes employed could range from such traditional terrorist methods as a vehicle-delivered bomb--directed against, say, a telephone switching center or other communications node--to electronic attacks relying on paid hackers. Deutch identified Hizbollah as one of a number of terrorist groups who used the Internet for their communications and might therefore have both the inclination and the ability to launch such an attack (Deutch 1996).

More recently, a CIA report to the US Senate Intelligence Committee identified a number of terrorist organizations, Hizbollah among them, that "have both the intentions and the desire to develop some of the cyberskills necessary to forge an effective cyberattack modus operandi" (McCullagh 2002a). There is ample evidence confirming that "Terrorists who fight modernity and its perceived evils in the name of defending traditional values and religious principles do not shy away from enlisting advanced technology for their holy wars or secular fights to enforce their agendas" (Nacos 2002, 108). The contradictions of anti-modern and, indeed, anti-imperialist groups such as Hizbollah making use of essentially Western technologies was first commented upon by Sreberny-Mohammadi and Mohammadi in relation to the 1979 Iranian revolution (1994, 27-28). The leadership of Hizbollah wear traditional dress and adhere to Islamic custom in the way they live their daily lives and in their preaching. But like other similar fundamentalist and anti-modern groups, they rely heavily on the predominantly younger members of their organization that are trained in and familiar with modern communication technologies. Members of Hizbollah are

261 In addition to its satellite television station and suite of Web sites, Hizbollah also own and control a radio station, al-Nour ('the Light'), magazines, and a newspaper.

known to be computer-literate. The group is responsible for the establishment and day-to-day running not just of a suite of Web sites, but also a satellite television station, and there is evidence that operatives on the ground compose training manuals on their laptop computers, distribute them on CD-ROM, and transmit their files via e-mail to trusted operatives (see Whine 1999, 236). This leads Saad-Ghorayeb to observe that, in many ways, Hizbollah "typifies the Islamic Party that espouses modernity" (2002, 111).

Chapter Three included a discussion about the impact of IT use on terrorists' organizational structures. It is worth pointing out that although Hizbollah has often been characterized as a loosely organized alliance, it instead adheres to "a highly sophisticated hierarchical organizational structure" (Ranstorp 1998, 4). It would be wrong therefore to characterize it as a networked grouping in the organizational sense. This chapter is concerned neither with the ability nor the desire of Hizbollah to carry out a cyberattack on the United States, which is a matter for further research, nor with detailing the group's organizational structure, however. Instead, this chapter seeks to describe and analyze the effect of the group's strategy of cybercortical warfare, carried out via its collection of Web sites, on the citizens of Israel and Western publics more generally.

HIZBOLLAH'S INTERNET STRATEGY

The Major Web Sites

Autonomous communication is a paramount objective for Hizbollah. They first went online in early 1996. The Central Press Office site, or Hizbollah.org, is the group's official homepage, and is available in both English and Arabic. Hizbollah maintains at least three other sites of an official character (all of which are available in both English and Arabic versions): http://www.moqawama.org known as the 'Islamic Resistance Support Association' and which describes the group's attacks on Israeli targets; http://www.manartv.com the news and information site that is essentially the homepage of Hizbollah's Al-Manar ('the Lighthouse') Television; and http://www.nasrollah.net the official homepage of the group's leader Sayyed Hassan

Nasrallah (and available in Arabic, English, and French). The sites are said to receive between one and three thousand hits per day.

A study published in November 1997, over a year after the establishment of the Hizbollah sites, found that the total number of Internet users in the Arab world, (excluding Israel) at that time (July 1997), was 215,500. Of a population of over 3.5 million people, there were just 35,520 Internet users in Lebanon (Nua 1997).[262] Hizbollah maintained their sites in both Arabic and English from the outset. This was despite the low number of Internet users in the whole of the Middle East and the fact that a 1998 study found that Arabic sites with Arabic text received many more visitors from within the Arab world than Arabic sites with English text (Nua 1998).[263] Further, Pippa Norris has shown that in societies where the online population is not large there is minimal incentive for groups to develop Web sites, and the (lack of) infrastructure hinders their development (Norris 2001). This indicates that Hizbollah were interested in targeting a non-Lebanese and non-Middle Eastern audience from the outset. Their targeted audiences were the citizens of Israel and English-speaking publics more generally.[264]

Discursive Structuring of Sites

The Value Structure of Hizbollah: Identity, Adversaries, and Goals

How do Hizbollah portray themselves online? According to a statement entitled 'Hezbollah: Identity and Goals' contained in the 'Introduction' of the CPO site, "Hezbollah is an Islamic struggle movement. Its emergence is based on an

---

[262] The study's findings were based on actual subscription numbers to ISPs. It has since been shown that the average number of users per Internet account in most Arab counties is three, see Nua 2001.

[263] In terms of the Internet's impact in the Middle East, there was a fairly early realisation that the technology would present something new for the region (Gabbard & Park 1995). Anthropologist Jon Anderson's work (1998) provides an overview of how Arab society "enculturates" the Internet by assessing the interaction between the Net and it's users and local culture, society, and religion. Jon Alterman's work has a more political focus; his *New Media, New Politics?* (1998)--though now, like Andersons work, somewhat dated--provides a good overview of the impact of new media in the Arab world. More recently, Marcus Franda has contributed *Launching Into Cyberspace* (2002), which includes a number of chapters on the Middle East region. Burkhart and Older's slim volume entitled *The Information Revolution in the Middle East and North Africa* (2003) is also instructive. On the intersection of Islam and the Internet, see Gary Bunt's *Virtually Islamic* (2000) and *Islam in the Digital Age* (2003).

[264] For an introduction to Israel's low-tech, but nonetheless transnational, "communications offensive" in the pre-Internet 1970s, see Alexander 1973, 61-68. The latter may usefully be compared with Marcus Franda's analysis in his *Launching Into Cyberspace* (2002, Ch.s 2 & 3).

ideological, social, political and economical mixture in a special Lebanese, Arab and Islamic context."[265] On the one hand then, they place themselves in historical continuity with almost one hundred years of struggle by the Palestinian people against colonization and oppression; on the other hand, they are also actors on the domestic Lebanese political scene.

The Israeli-Palestinian conflict is a dominant element of the group's web sites. Statements of solidarity with the Palestinian people are common. One such text, entitled 'A Hizbollah Statement on the Escalating Egressions [*sic*] Against the Palestinians,' reads as follows:

> As the days passé [*sic*], we witness mounting egressions [*sic*] on our Palestinian people, the Israeli army uses different methods to stop the Intifad [*sic*], which proves every day its readiness to continue the struggle till it achieves the full liberation of Palestine. We highly appreciate and salute our people in Palestine for their steadfastness and strong will. We also hail the sacrifices of Palestinian factions and martyrdom operations, which became an effective weapon and capable of inflicting a huge loss among Israeli occupation forces. We strongly warn of the suspected plots of the Israeli enemy and the American administration to stop the Intifada whenever the Palestinian resistance inflicts damage in the Israeli entity. The continuation of the Intifada as well as the national unity of the Palestinian people is the base that should be relied on to confront the Israeli and US projects and plots.

Such admonitions against alleged Israeli and US government machinations are commonplace on the Hizbollah sites.

Hizbollah is a recognised political party with wide electoral support within Lebanon. The group is involved in a vast array of domestic social, cultural, and educational activities and initiatives, evidence of which were available on the group's Web sites. For example, a July 2001 article in the *Daily Star* newspaper detailed how some 25 Muslim couples "tied the knot" at a wedding party organized by Hizbollah in Baalbek: "As a band played Islamic songs at Sunday's ceremony, a Muslim clergyman handed the newlyweds copies of the Quran a gift from Hizbullah

[265] Available online at http://web.archive.org/web/20030212120225/http://www.hizbollah.org/english/info.htm#1.

Secretary-General Sayyed Hassan Nasrallah." According to the report, which was posted on the CPO Web site,[266] about 10,000 people, including Hizbollah MPs and clergymen, attended the ceremony. Other newspaper reports contained on the site detailed Hizbollah's concern with the deleterious consequences of the Lebanese government's "arbitrary dismissal" of employees of Middle East Airlines and their concern that "financial cutbacks should not come at the worker's expense,"[267] and described Hizbollah taking the lead in criticising a government increase in oil prices, which the organisation claimed would negatively affect the poor.[268]

What are Hizbollah's stated goals? These are threefold: the liberation of Jerusalem and the Palestinian people; the complete withdrawal of Israeli forces from Lebanon, to include the area known as Sheba'a Farms; and the establishment of an Islamic state in Lebanon. As regards the latter, Amal Saad-Ghorayeb, the author of *Hizbu'llah: Politics and Religion*, asserts "the exemplary just state for Hizbullah is the Islamic republic" (2002, 22). This is clear from the group's logo, which is composed of the martyr Husayn's raised arm wielding an AK-47 assault rifle, a globe, and the group's name, topped with the Koranic verse from which the movement derives its name: "Verily the party of God shall be victorious" (Ranstorp 1998, 8). The logo was prominently displayed on the group's Web pages (see Figure 7.1).

The difficulties of establishing an Islamic republic within the borders of Lebanon are not foreign to Hizbollah, however. Saad-Ghorayeb points out that such an undertaking would not only be anathema to Lebanon's Christian, Sunni, and Druze populations, but would even by rejected by a significant portion of Shi'ites. According to a 1992 study, only 13% of Lebanese Shi'ites would lend their support to the creation of an Islamic republic in Lebanon (Harik 1996, 56 & 61; Saad-Ghorayeb 2002, 35). So, while the ideal of an Islamic state in Lebanon remains a central tenet of Hizbollah's political theory and goals, it is not currently part of its concrete political programme.

---

[266] Available online via the Internet Archive at http://web.archive.org/web/20021207153723/www.hizbollah.org/english/press/p2001/p20010724.htm.
[267] Available online via the Internet Archive at http://web.archive.org/web/20021124070304/www.hizbollah.org/english/press/p2001/p20010517.htm.
[268] Available online via the Internet Archive at http://web.archive.org/web/20021207132616/www.hizbollah.org/english/press/p2001/p20010917.htm.

Figure 7.1 Image from Top Page of Hizbollah.org



the borders of Lebanon only be brought about on the basis of the consent of the majority of Lebanon's citizens; and, second, a central tenet of the Islamic faith, which disallows the enforced adoption of Islam by those who adhere to other faiths. These and related issues were dealt with at some length in the group's online 'manifesto,' which is worth quoting from at length:

> Hezbollah today also commands respect politically after it proved its strength with its presence by respecting the values of others in the field. Hezbollah also sees itself committed in introducing the true picture of Islam, the Islam that is logical. Committed to introduce the civilized Islam to humanity. Hezbollah also sees itself committed in introducing the Islam that is confidant [*sic*] in achieving justice, as well as introducing the Islam that protects all human rights. Introducing the Islam that supports education, the Islam that offers medical support. Hezbollah also has its own cultural plan to attract and

> convince through civilized and humanitarian means as specified in the human rights laws, far from any use of violence or coercion. It should also be clear that the kind of Islam that Hezbollah seeks is a civilized one that refuses any kind of oppression, degradation, subjugation and colonization. Hezbollah also stretches its arm of friendship to all on the basis of mutual self-respect. The Islamic path that Hezbollah follows is one of a message that aims to establish peace and justice to all humanity whatever their race or religion. Hezbollah does not have a problem with anyone, but it feels responsible towards him or her to clarify the true Islam far away of [*sic*] any fanaticism. Hezbollah does not wish to implement Islam forcibly but in a peaceful and political manner, that gives the chance to the majority to either accept or refuse. If Islam becomes the choice of the majority only then will it be implemented. If not it will then continue to co-exist with others on the basis of mutual understanding using peaceful methods to reach peaceful solutions. And that is how the case should be to the non-Islamists as well.

Saad-Ghorayeb further underscores Hizbollah's commitment to those principles:

> Hizbu'llah's reference to the Qur'anic injunction, 'Let there be no compulsion in religion' (2:256), both in its Open Letter of 1985 and 14 years later as articulated by Shaykh Na'im Qasim, is indicative of the tenacity with which this conviction is held. Moreover, the party's constant reassurance that it has no intention of forcibly 'imposing' an Islamic state on the Lebanese people, from as far back as 1985 to the present, is further testimony to this point (Saad-Ghorayeb 2002, 36).

There are, of course, those who doubt the sincerity of such assertions (Herzog 2005, Karmon 2004; Webman 1998), but most analysts are agreed that the group has all but abandoned this aspect of its original programme (Byman 2003, 58; Norton 1998; Ranstorp 1998, 6).

The main aim of Hizbollah's eighteen-year struggle against the Israelis was to end the occupation of southern Lebanon, a goal that was finally achieved in May 2001. However, the organisation has an ongoing quarrel with the Israelis because their withdrawal did not include the tiny Sheba'a Farms area on the Lebanese-Syrian

border, which the Israelis insist belongs to Syria. Both Syria and Lebanon say it is Lebanese. In an article that appeared in the UK newspaper *The Guardian* in 2001 and which was reprinted on the CPO Web site, Mr Naboulsi was described as "not exactly breathing fire over that issue": "Whenever we find a target in the Sheba'a Farms, we attack if it's easy to hit without any casualties...But it's very hard to launch an operation there" (Whitaker 2001).[269] As pointed out earlier, Hizbollah gained enormous prestige from forcing the IDFs withdrawal from southern Lebanon. This surge in support was not restricted to its core Shi'ite followers, but extended throughout Lebanese society, and was alluded to in the group's 'manifesto' 'Hezbollah: Identity and Goals': "The resistance also established an internal national axis in a way that was never witnessed in Lebanon before. This matter is of vital interest when we notice how Lebanon is divided into various religions, sects, ideologies, societies, cultures, etc." Since that time, Hizbollah has devoted strenuous efforts to capitalising on that goodwill and thus becoming a major force in Lebanese politics.

Israel is clearly viewed as the enemy of Hizbollah and is not recognised by the latter. On Hizbollah's Web sites Israel was either referred to as "the Zionist entity" or "the Jewish state," or its name placed in inverted commas (i.e. "Israel"). In the same *Guardian* article referred to above, it was reported that Hizbollah would in fact "like [Israel] to disappear off the map," but it was also observed that "while Hizbullah is convinced that Israel will eventually be defeated, it seems in no particular hurry" (Whitaker 2001). The organisation's spokesperson, Hussein Naboulsi, was reported to have said: "The Crusaders stayed in Palestine for 200 years and have gone. Israelis have only been in Palestine since 1948" (Whitaker 2001). Since the IDF withdrawal from south Lebanon, however, Hizbollah has become increasingly involved in the Israeli-Palestinian conflict. In fact, according to Ely Karmon (2005), the group was behind some seventy per cent of all terrorist attacks carried out by Palestinian factions in 2004. This appears to contradict Daniel Byman's assertion that "[Hezbollah] is embedded in Lebanese politics and society and, unlike al Qaeda, is a stakeholder in the existing regional order, not a force bent on destroying it " (Byman 2003, 60).

This apparent contradiction may be transcended however if one views the export of the so-called 'Hizbollah model' (Byman 2003, 58-59) to the Israeli-

[269] See http://web.archive.org/web/20031012004339/www.hizbollah.org/english/press/p2001/p20010412.htm.

Palestinian conflict as a continuation of the group's hearts and minds campaign. The achievement of a successful IDF withdrawal from the south undoubtedly represented a great victory for Hizbollah and one in line with its stated ideological objectives; nonetheless it also threatened to seriously undermine the groups' underlying revolutionary character and identity as well as its forward momentum (Ranstorp 1998, 3). Prominent involvement in Israel-Palestine has forestalled any such eventuality, however. And while this position has doubtless made Hizbollah stronger, it has also forced it to become more "cautious, cunning, and subtle" (Byman 2003, 60).

9/11 and Its Aftermath

On 9/11, Hizbollah's spiritual guide (*al-murshid ar-ruhi*), Mohammed Hussein Fadlallah, cautiously declared "no religion justifies such action," and later claimed the suicide attackers did not die in a holy jihad.[270] However, he also posited that it was US government policies that were responsible for the attacks (Karmon 2002). A few days later, Hizbollah also expressed regret for "the loss of innocent lives," but in the same breath also attributed "this level of hate" against the US to "oppressive" American government policy and warned the United States against taking advantage of the attacks in order "to practice all sorts of aggression and terrorism."[271] Interestingly, a survey conducted amongst Lebanese Muslims (N=337) enquiring as to their feelings about the 9/11 attacks found that while only thirty percent of respondents said they supported the attacks, some eighty-eight percent nevertheless felt that Arab grievances against the US warranted the attacks (Haddad & Khashan 2002, 821-822). The identity of response may suggest that either Hizbollah took their cue from Lebanese Muslims or, perhaps more likely, many Lebanese Muslims took their cue from Hizbollah and its media apparatus.

Hizbollah met the US campaign in Afghanistan and subsequent events with a considerably more aggressive attitude and language than the events of 9/11. In

---

[270] Clearly neither Fadlallah nor Hizbollah are against the use of suicide bombing as a strategy *per se*; after all, Hizbollah are credited with being the originators of this tactic. See 'Fadlallah Defends Suicide Missions':
http://web.archive.org/web/20021207155923/www.hizbollah.org/english/press/p2001/p20010511a.htm

[271] Excerpted from a 'political declaration' on the CPO Web site entitled 'Hizbullah Regrets Lives Lost and Warns the US Not To Resort To Unjust Policies.' See
http://web.archive.org/web/20030407085523/www.hizbollah.org/english/frames/index_eg.htm.

February 2002, *The Times* of London reported that a senior Al-Qaeda operative had discussed the relocation of fugitives from the Afghan conflict with Hizbollah leaders (Evans 2002, 1). In the meantime, the Israeli Minister of Defence, Benyamin Ben Eliezer, alleged that fleeing militants had indeed entered Lebanon and joined Hizbollah. Subsequently, the *Washington Post*, quoting both US and European intelligence officials, reported that the newly established *ad hoc* tactical 'terror alliance' involved logistical and training cooperation between mid-level operatives of Al-Qaeda and Hizbollah (Priest & Farah 2002, A01). US intelligence officials have also expressed concern over possible links between Hizbollah and Abu Musab al-Zarqawi. In September 2003, when US authorities named Zarqawi and several of his associates as Specially Designated Global Terrorist entities, the US Treasury Department said that Zarqawi not only had ties to Hizbollah, but that plans were in place for his deputies to meet with both Hizbollah and Asbat al-Ansar,[272] "and any other group that would enable them to smuggle mujaheddin [*sic*] into Palestine" (as quoted in Levitt forthcoming 2006).

On their Web sites, Hizbollah hotly and repeatedly denied any link to Al-Qaeda. In a *Daily Star* article posted on the CPO Web site, and which referred to the *Times* article mentioned above, Nasrallah was quoted as saying "If Al-Qaeda members were really able to come out of Afghanistan and travel all the way to Lebanon and hide here, then this is major proof of the failure of American security, intelligence and weapons."[273] Numerous follow-up articles posted on the same site ridiculed the notion of ties between the two groups and presented allegations of the latter as an Israeli plot. In fact, not only was Nasrallah quoted as denying such links, but the Lebanese President Emile Lahoud,[274] the Lebanese Foreign Minister Mahmoud Hammoud,[275] the Iranian Foreign Minister Kamal Kharrazi,[276] and the Italian Ambassador Giuseppe Cassini[277] were all quoted scorning the accusations.

---

[272] Asbat al-Ansar is a Sunni Lebanese terrorist group.
[273] See 'Nasrallah Ridicules Notion of Al-Qaeda Presence in Lebanon': http://web.archive.org/web/20031006160951/www.hizbollah.org/english/press/p2002/p20020209a.htm
[274] See 'Lahoud Denies Al-Qaeda-Hizbullah Link': http://web.archive.org/web/20031015154217/www.hizbollah.org/english/press/p2002/p20021111.htm.
[275] See 'Nasrallah Ridicules Notion of Al-Qaeda Presence in Lebanon' above.
[276] See 'Kharrazi Denies Cooperation Between Hizbullah and Al-Qaeda': http://web.archive.org/web/20030831021146/www.hizbollah.org/english/press/p2002/p20021210.htm.
[277] See 'Cassini Cuckolds Claims of Bekaa Bases': http://web.archive.org/web/20031006160936/www.hizbollah.org/english/press/p2002/p20020209.htm.

The above notwithstanding, analysts associated with Israel's International Policy Institute for Counter-Terrorism (IPICT) insist that cooperation between the two groups is quite possible, particularly given that in the past Hizbollah has provided training in its camps in Lebanon--the existence of which Hizbollah also disputed on its Web sites[278]--to members of both Egyptian Jihad and Algeria's Armed Islamic Group, which organizations have provided some of Al-Qaeda's most prominent operatives. It has also been claimed that a top Hizbollah operative, Imad Mughniyeh--who is on the FBI's list of most-wanted terrorists--actually met with Bin Laden himself prior to the East African embassy bombings in 1998 and may now be in Iraq (Fighel & Shahar 2002; Karmon 2002; Marzuk 2003). IPICT analysts also point out that in March 2002, Fadlallah called

> upon the Muslim Religious Scholars to consolidate Muslim unity among the two major sects of Sunni and Shiite... [to] transform the political and jihad unifying positions into cultural and ideological meeting places... and concentrate on the common issues that have to do with Muslims fate, especially that the arrogant powers have put both Muslim sects of Sunni and Shiite in the same category as being part of 'the axis of evil' (as quoted in Karmon 2002; see also Karmon 2004).

This is pointed to as evidence of not only potential Al-Qaeda-Hizbollah cooperation, but also a desire on the part of the latter to become involved in the Iraqi theatre.

It is certainly true that Hizbollah has become embroiled in the controversy surrounding the American invasion of Iraq. This is relatively unsurprising given that a number of high-ranking members of Hizbollah studied at the same religious seminary in the Iraqi holy city of Najaf--where the late Ayatollah Khomeini and the Lebanese Mullah Fadlallah were also educated--and retain close ties with Iraqi Shi'ites (Byman 2003, 54; Hamzeh 1997; Palmer Harik 2004, 22; Ranstorp 1997, 25-30 & 180-182). Immediate upon its passage Hizbollah condemned UN Security Council Resolution 1441 on Iraq as "humiliating," arguing that its purpose was to "subjugate" Arabs.[279] Shortly thereafter a high-ranking 'politburo' member alleged that America's hidden

---

[278] See 'US Senator Mocked for Parroting Israeli Line on Hizbullah 'Terror'': http://web.archive.org/web/20031006164512/www.hizbollah.org/english/press/p2002/p20020711.htm.
[279] See 'Hizbullah Denounces UN's Iraq Resolution': http://web.archive.org/web/20031015154243/www.hizbollah.org/english/press/p2002/p20021112.htm.

agenda was to "lay its hands on the oil wells in Central Asia and countries that might form an axis against it in the future."[280] Apart from these pronouncements, however, there was very little else included on the Hizbollah sites regarding the Iraqi insurgency or the US abuse of prisoners at Abu Ghraib, for example. While this is certainly surprising given the political capital to be made on such issues, it may be that the structural and design overhaul that the Hizbollah Web sites have been subject to recently and the pressures the CPO site in particular has come under from hacktivists in the past year or so negatively impacted the group's ability to fully implement their cyber strategy during that time.

It is important to point out that the group has not been silent on the Iraq issue, but has simply not devoted the amount of attention one might have expected to it on their English-language sites. Elsewhere, for example, Hizbollah was reported as having condemned the beheading of Nicolas Berg in Iraq in May 2004 as "an ugly crime that flouted the tenets of Islam." "Hizbollah condemns this horrible act that has done very great harm to Islam and Muslims by this group that claims affiliation to the religion of mercy, compassion and humane principles," the group said in a statement. They further asserted that Berg's killing had diverted the world's gaze from an escalating furore over the abuse of Iraqis by US soldiers: "The timing of this act that overshadowed the scandal over the abuse of Iraqi prisoners in occupation forces prisons is suspect timing that aims to serve the American administration and occupation forces in Iraq and present excuses and pretexts for their inhumane practices against Iraqi detainees." In a tactic familiar from their Web sites, they alleged that the killers' behaviour-- the video disseminated over the Internet showed masked men sawing Berg's head off with a large knife and holding it in the air--was closer to "the Pentagon school--the school of killing, occupation, crimes, torture and immoral practices that were exposed by the great scandal in occupation prisons" (Agencies 2004).

With regard to the Iraq issue, IPICT analysts claim that Hizbollah has established a significant presence of its own inside the country and while conceding that the group's operatives have not yet been involved in attacks on coalition forces, point out that they could eventually assume an active role (Karmon 2004). Others agree that Hizbollah links with Iraqi Shia's could be potentially explosive, with

[280] See 'Hizbullah Official Accuses US of Plot to Control Oil': http://web.archive.org/web/20031015154836/www.hizbollah.org/english/press/p2002/p20021115.htm.

Daniel Byman at one time describing Iraq as "a critical test case in the fight against Hezbollah" because the "organization's potential for wreaking havoc there is immense" (2003, 66). In a recent follow-up analysis, however, Byman doesn't even mention Iraq and focuses instead on Hizbollah's relationship with Syria (Byman 2005). Indeed, no other reliable sources have evidenced a prominent Hizbollah presence in Iraq in the fashion that IPICT claims.[281]

With regard to the US, not only did Hizbollah on its Web sites chide the 9/11 attackers and disavow any links with Al-Qaeda, but a high-ranking member was reported in 2002 as telling a group of Danish journalists that Hizbollah played no part in the 1983 Beirut bomb attack that killed 241 US soldiers serving as part of multinational peacekeeping forces.[282] If the group hoped that such denials would see their removal from the US State Department's list of designated FTOs, they were to be disappointed however. Hizbollah's continued appearance on said list drew a predictably stinging response from the group: "Distorting the hizbollah [*sic*] pure image and trying to pin the name terrorism on it, clearly shows the American and Israeli fear of the great example that the resistance provided specifically in terms of fighting the occupation."[283] The alleged iniquity of the US position was underlined by an article on the CPO site which quoted the Italian Ambassador to Lebanon to the effect that the US had failed to provide sufficient evidence to prove that Hizbollah was a terrorist group and the assertion that the party was an "annoyance" to Israel rather than a real threat.[284] In keeping with the rhetoric employed on many of the sites analysed in Chapter Six, the Hizbollah sites are littered with articles and text painting the US and Israel as the 'true' terrorists. The following is indicative:

> [The US] supports the terrorist Zionist state with all the strength it possesses…[The US] has practiced terrorism in the most horrible ways (such as) when it used nuclear bombs on Hiroshima and Nagasaki.

---

[281] The assertion by IPICT analyst Moshe Marzuk (2003) that Lebanese Hizbollah have a formal Iraqi offshoot, which he terms 'Iraqi Hizballah,' remains unsubstantiated. There is a small Shi'ite militia operating in southern Iraq who term themselves 'Hizballah-Iraq,' but they are not thought to have any connection with Lebanese Hizbollah (Katzman 2005, 10).

[282] See 'Hizbullah Denies Role in 1983 Bombing of US Marines': http://web.archive.org/web/20031227074725/www.hizbollah.org/english/press/p2002/p20021002.htm.

[283] See 'Hizbollah Statement in Response to the Annual Report of the U.S State Department': http://web.archive.org/web/20031227091950/www.hizbollah.org/english/statm/sm2001/sm20010501.htm.

[284] See 'Italian Ambassador Scoffs at US Claims Against Hizbullah': http://web.archive.org/web/20031227074206/www.hizbollah.org/english/press/p2002/p20020907.htm.

It will therefore take advantage of the war against terror to exercise the worst of its terrorist acts again.[285]

AN INTEGRATED MEDIA STRATEGY

Hizbollah's suite of Web sites are not the only tools at the group's disposal in the information war; the group has a satellite television station that attracts 10-15 million viewers worldwide daily and has recently developed a computer game to aid it in inculcating the young with its values. Both the television station and the video game have accompanying English-language Web sites, and it is this synergism that has ensured that Hizbollah's cyber strategy has met with a high level of success.

Al-Manar Television

"Symbolism and the projection of messages to internal and external audiences have occupied a central place for Hizballah throughout its evolution" (Ranstorp 1998, 7). In his *Inside Terrorism*, Bruce Hoffman recounts how, during the crisis precipitated by the hijacking of TWA flight 847 in 1985, Hizbollah deftly manipulated the US television networks: "There were graduates of media studies from American colleges at meetings at Nabih Berri's house in West Beirut while ['spin doctoring'] tactics were being worked out" (1998, 134). Later, during the 1990s, Hizbollah utilized its media apparatus to wage successful campaigns against both the IDF and South Lebanese Army (SLA). In terms of Hizbollah's offensive against the SLA, a campaign of psychological warfare was waged in conjunction with improved armed operations against SLA units. Infiltration within SLA ranks was subject to particular exploitation by the group who capitalized on deteriorating SLA morale by regularly publicizing and distributing the names of SLA officers with promises of punishment. Hizbollah also enticed defections with promises of financial inducements coupled with pardons and even established a special information unit which highlighted SLA soldiers returning to their families (Ranstorp 1998, 9). Hizbollah also waged an effective psychological warfare campaign against IDF soldiers serving in South

[285] See 'US Unfit to Lead War on Terrorism': http://web.archive.org/web/20031226102525/www.hizbollah.org/english/press/p2001/p20011003.htm.

Lebanon previous to the withdrawal. It utilized its own camera-crews to record the efficiency of its attacks against IDF posts, which it then broadcast on Al-Manar and, on a number of occasions, distributed to foreign media. In addition, the video-taping and dissemination of daring resistance operations served not only to boost the morale of Hizbollah's own fighters and supporters, but also undermined the morale of the 'enemy,' who were in some instances seen fleeing from advancing Hizbollah fighters. The group also regularly publicized on its television station and its Web sites the acquisition of new and upgraded weaponry in an effort to instill a degree of uncertainty into IDF units without actually having to employ the actual hardware.

In March 1997, an article in Beirut's *Al-Safir* newspaper drew attention to the "psychological warfare" being employed by Hizbollah. The article described Hizbollah's Al-Manar television station's Web site, which was depicted as Hizbollah's corrective to the Israeli's mis-education of Western publics:

> Psychological warfare can be used as a weapon of war to be added to the military materiel, not only to repulse the aggression, but also to confront the enemy's deceptive policy toward the world public. Although this war has many faces, it has one head only, namely the media... Hizballah's step is primarily aimed at refuting the fallacies Israel has been spreading abroad concerning the occupation of south Lebanon. (FBIS 1997).[286]

The report went on to say that the site managers regularly received e-mail from Internet surfers "some of which salute the resistance and others request information on the Lebanese-Israeli conflict" (FBIS 1997). In addition, it was reported that some of the subscribers to the site's e-mail list--"who began to show sympathy with the resistance when the Qana massacre[287] occurred" (FBIS 1997)--transmitted the information they received across other networks and lists thus spreading these messages further than would otherwise be the case. Finally, the article also explained

---

[286] For an alternative position on Al-Manar TV, see Jorisch 2004.

[287] The Qana Massacre took place on April 18, 1996 in the headquarters of the Fijian battalion of UNIFIL, located in the small town of Qana, in southern Lebanon. The compound came under heavy artillery shelling by nearby Israeli Defence Forces in response to two rocket and mortar attacks launched toward the unit earlier that day from close to the compound. As a result of the shelling, 102 civilians died and more were wounded. Most of the casualties were women and children from nearby villages, who had sought refuge in the UN compound from the fierce fighting going on between the IDF and Hizbollah. Four UN troops were also wounded in the incident.

that Al-Manar employees viewed Internet access as a useful educational resource due to the availability of reports and analyses produced by the Israeli Foreign Ministry and other agencies, which allowed Hizbollah members to become familiar with the methods by which governments demonize terrorist organizations and thus educated the former as to how to carry out a counter-campaign. A number of employees were also said to be taking training courses via the Net (FBIS 1997).

In a September 2001 interview, Hassan Ezzieddine, the head of Hizbollah's Department of Media Relations, confirmed:

> We feel that the media can be effective in creating a special climate in public opinion on the main issues of interest...We are heading toward a new sensitive security situation (in the region) which means we need to follow events very closely so that we can informatively help shape international and Arab public opinion...We believe that the media has an important role in the conflict, as important as the military wing (Blanford 2001).

To underscore the importance of the media's role in the conflict, Hizbollah's leadership decided in 2001 to place Al-Manar TV under the direct supervision of a committee composed of senior figures in the organization and chaired by the group's secretary-general, Sayyed Hassan Nasrallah. The Central Information Office, the role of which was liaison with the press and which also had responsibility for the publication of Hizbollah's weekly newspaper *Al-Ahed*, was abolished and replaced by the new Department of Media Relations of which Mr. Ezzieddine, a member of Hizbollah's political council, was put in charge. Ezzieddine and his staff reportedly examine newspaper articles dealing with Hizbollah and follow television and radio broadcasts. The new department is also responsible for maintaining the group's official Web sites, which are currently in the process of a major overhaul.

'Special Force'

The availability of online gaming on the Kahane Web site was referred to briefly in Chapter Five. In February 2003, Hizbollah also launched its own computer game, which allows players to simulate its fighters during military operations against IDF soldiers prior to the latter's withdrawal from South Lebanon. *Special Force*, which is

said to have taken over two years of development by the Hizbullah Central Internet Bureau, was clearly designed to introduce the 'resistance' to young people. The following message appears on the game's packaging: "The designers of Special Force are very proud to provide you with this special product, which embodies objectively the defeat of the Israeli enemy and the heroic actions taken by heroes of the Islamic Resistance in Lebanon...Be a partner in the victory. Fight, resist and destroy your enemy in the game of force and victory." A Hizbollah official, Mahmoud Rayya, told Beirut's Daily *Star* newspaper that the game was "designed to compete against foreign computer games that show Arabs as enemies and Americans as the heroes that defeat them." He went on to say that the "game is resisting the Israeli occupation through the media...In a way, Special Force offers a mental and personal training for those who play it, allowing them to feel that they are in the shoes of the resistance fighters" (Chayban 2003). The game is not available to play online, but has a dedicated Web site,[288] which describes the purpose of the game, provides screenshots, and allows one to download *Special Force* screensavers. In 2003, hard copies of the game were available for purchase in Lebanon, Syria, Iran, Bahrain, and the United Arab Emirates.[289]

ELECTRONIC INTERFADA

It's not all plain sailing for these 'netizens,' however; over time Hizbollah's Internet presence has come under increasing pressure as has its satellite broadcast capabilities.

In Autumn 2000, political tensions in the Middle East spilled over onto the Internet, resulting in an increased level of hostile online activity that has continued sporadically for the past five years. The Mideast 'cyberwar' began in November 2000--about three weeks after Hizbollah seized three Israeli soldiers on patrol in the Sheba'a Farms area and held them for ransom--when pro-Israeli hackers created a

---

[288] http://www.specialforce.net. For more on gaming and conflict, see Thomas 2005.

[289] In February 2000, an individual in the US was arrested for piracy and suspected fundraising for Hizbollah. The individual sold pirated music CDs, Sega, Sony and Nintendo game discs to fund a Hizbollah-related organization. Among the discs in this man's possession on his arrest were discs containing images and short films of terrorist attacks and interviews with suicide bombers, which were allegedly used as propaganda to generate funds for Hizbollah. This man is currently a fugitive (Noble 2003).

website to host FloodNet attacks. Within days, Hizbollah's site was flooded by millions of 'pings'--the cyber-equivalent of knocks on the door--and crashed. Hizbollah then tried reviving the site under slightly different spellings, but they too came under sustained attack. In all, six different Hizbollah sites, the Hamas site, and other Palestinian informational sites were victims of the FloodNet device (Gentile 2000a & 2000b; Hockstader 2000, A01). Hizbollah's Central Press Office (CPO) site came under attack once again when the group posted video clips of Israeli ground attacks on Palestinians in Gaza. Hizbollah then increased their server capacity in order to ward off further attacks (Gentile 2000a). These efforts notwithstanding, pro-Israeli hackers successfully hacked into the Hizbollah site on December 26 2000. They posted pictures of the three Israeli soldiers who were abducted in early October and the slogan "Free Our Soldiers Now" on a screen full of blue and white Star of David flags (Hosein 2001). In addition, a group called Hackers of Israel Unite allegedly crashed the Al-Manar TV site using one computer with a 56K modem, an ADSL line, and a popular tool called WinSmurf that enables one to conduct a mass pinging (Hosein 2000b).

The Hizbollah site had already come under 'attack' in October 2000; at that time a number of media outlets in the US and Europe were contacted by a group claiming that hackers had defaced a Hizbollah site. When journalists accessed the site they were greeted by the Israeli flag, Hebrew text and a tinny piano recording of Hatikva, the Israeli national anthem (see Geers & Feaver 2004, 23). This prompted several news organisations to report that Hizbollah's CPO site had been defaced by pro-Israeli hackers (Hockstader 2000, A01; Piller 2001). Only later did it become apparent that the site at hizbolla.org (which is no longer operational) was a fraud that had been established by an unidentified individual or group using an address in Lebanon.

In terms of the 'cyberwar,' one of the most prolific Israeli hacking groups went by the name of 'm0sad.' This group was the first pro-Israeli hacking group to expand the cyber-campaign against the Palestinian Intifada beyond pro-Palestinian Web sites by targeting sites throughout the Arab world. Amongst its many defacements of pro-Palestinian Web sites, m0sad was responsible for the attack on the home page of the service provider Destination, the Internet component of Beirut's ITX. This defacement was apparently carried out in retaliation for the company's provision of service to Hizbollah's Al-Manar Television site. The attack disrupted

service on ITX's Destination Web site for over six hours: on accessing the site, instead of the normal home page, visitors were treated to a black screen that stated in large white type "site closed by m0sad," and followed up with: "How come that the [P]alestinians that claims that they want to be like Europians [*sic*] are executing people in public without a fair justice like in Pakistan, Iran, Iraq[?]" ITX's general manager later told news sources that m0sad had accessed the company's Web site through NetVision, an Israeli ISP. He went on to say "It was clear that the hackers wanted us to know they were Israelis, because usually hackers clean up their traces after they vandalize a site. They did not." Despite the incursion, ITX said it had no plans to stop providing services to Al-Manar's Web site (Weisman 2001; see also Geers & Feaver 2004, 22).

Two companies that immediately discontinued their 'relationship' with Hizbollah when alerted to same were Microsoft and Amazon.com. It was reported in early 2001 that Microsoft Corporation and Amazon.com were supporting Hizbollah due to the appearance on the Al-Manar Web site of prominent banner advertisements from these two companies. A Microsoft banner appeared on each page of the English-language section of the site, while Amazon's banner appeared atop the Arabic-language pages. The advertisements were apparently unauthorised. "It looks like someone used our banner ad without our permission," a Microsoft spokesperson was reported to have said. "We're contacting the site and asking them to remove that immediately. This is not something we did. We don't support political activities." The advertisements were pulled from the sites shortly thereafter (Kiggen 2001).[290]

As regards the cyberwar, according to Hizbollah's then-Webmaster, Ali Ayoub, "Our counterattack is just to remain on the Net" (Hosein 2001). The Palestinians and their supporters were not long in striking back, however. In a coordinated counterattack, the web sites of the Israeli army, Foreign Ministry, prime minister and parliament, among others were hit (Hockstader 2000, A01). On a single day, December 29, 2000 eighty Israel-related sites were hacked and defaced by pro-

[290] More recently, a Google search in Arabic employing terms such as 'Hamas,' 'Gaza,' and 'Palestine' linked to text advertising Hamas' military wing. In addition to the search results returned, an AdWord message linking directly to the website of the Izzedine al-Qassam Battalions, Hamas' terrorist-operative wing also appeared. Above the link were the words "Al-Qassam Battalions, the resistance website and the legend of jihad." The link was sponsored, showing that Hamas had paid for the use of Google's services. According to a Google spokesperson: "As soon as the matter was brought to our attention we removed the advertisement." See http://www.intelligence.org.il/eng/sib/3_05/google.htm for screenshot.

Palestinian hackers. It is estimated that, in all, more than 246 Israeli-related sites were attacked between October 2000 and 1 January 2001 as compared with approximately thirty-four Palestinian-related sites that were hit in the same period (Hosein 2001). The success of the Palestinian counterattack--variously dubbed the 'e-jihad,' 'cyber-jihad,' or 'inter-fada'--may be explained by the way in which the pro-Palestinian hackers systematically worked their way through sites with dot-il domain names. Palestinian-related sites are generally harder to find because, although in March 2000 dot-ps was delegated the country code Top Level Domain (ccTLD) for the Occupied Palestinian Territories, only one such domain is currently operational (gov.ps) (see Cisneros 2001) and not many groups have such an easily identifiable URL as Hizbollah. In addition, at the outbreak of the 'cyberwar,' there were approximately two million Internet hook-ups in Israel, which was considerably more than any other Middle Eastern country (see Table 1). The upshot of this is that the Israeli's have a far greater online presence than the Palestinians and their supporters in the Arab world and are therefore more easily targeted (Geers & Feaver 2004, 28-30; Weisman 2001).[291]

Table 7.1 Numbers of Internet Users in the Middle East, 2001

Country	Number of Subscribers	% of Population
Bahrain	140,200	21.36
Iran	420,000	0.63
Iraq	12,500	0.05
Israel	1,940,000	17.12
Jordan	212,000	3.99
Kuwait	200,000	9.47
Lebanon	300,000	8.38
Oman	120,000	4.42
Palestine	60,000	N/A
Qatar	75,000	9.75
Saudi Arabia	570,000	2.5
Syria	60,000	0.35
UAE	900,000	36.79
Yemen	17,000	0.09

Source: Nua Internet Surveys (www.nua.ie)

[291] For a brief, but concise, rundown of the 1999-2002 Israeli-Palestinian cyberwar, see Allen & Demchak 2003; for an exhaustive account of the 'cyberwar's' major players and their exploits, see iDefense 2001.

As discussed in Chapter Three, the events of 9/11 have resulted in increased pressure on the operators and facilitators of terrorist Web sites. Due to their notoriety, Hizbollah's Web sites have been subject to particularly sustained campaigns for their removal from the Internet. This increasingly takes the form of pressure brought to bear on their ISPs from groups such as Internet Haganah. As a result, the sites are increasingly difficult to access. In a further twist, the Coalition Against Terrorist Media (CATM) was established in Autumn 2004 to specifically target Al-Manar Television, which it says is "the most dangerous terrorist-sponsored broadcaster operating today."[292] CATM claims that pressure it brought to bear resulted in the dropping of Al-Manar broadcasts by seven satellite providers globally. At present, Al-Manar is still broadcast to the Middle East, North Africa, and Europe by ARABSAT, whose largest stockholder is the government of Saudi Arabia, and Nilesat, owned by the government of Egypt.

CYBERCORTICAL WARFARE: THE EFFECTS

Tsfati and Weimann (2002) have pointed out that almost all terrorist groups that maintain an online presence avoid presenting and detailing their violent activities: "Although the organizations behind these sites have a record of bloodshed, they hardly ever record these activities on their sites" (p.321). The exceptions, they point out, are Hizbollah and Hamas. Hizbollah's site contains a section ('Daily Operations') that provides updated statistical reports of its actions that "display in minute detail all of the organization's operational successes" (p.321). A separate page enumerates the number of dead 'martyrs,' along with the number of 'Israeli enemies' and 'collaborators' killed. This is part of Hizbollah's campaign of cybercortical warfare.

> Hizbollah differs somewhat from other organizations in that it highlights its military achievements, gloating over enemy victims (showing pictures of funerals of murdered Israelis), and publishing detailed statistics about its military successes. The motive for this unique approach has been Hizbollah's attempt to influence the public debate in Israel about withdrawal from

[292] See CATM's Web site at http://www.stopterroristmedia.org/ for more information about the group's founders, partners, goals, etc.

> Lebanon. The organization has stated explicitly that its aim has been to exert pressure in Israel in favor of withdrawal. The organization knows that many Israelis visit the site, whose address is published in Israeli media. Hizbollah publishes its records of murdered Israelis, maintains electronic connections with Israelis, and appeals to Israeli parents whose sons serve in the Israeli army, all with the aim of causing demoralization (Tsfati & Weimann 2002, 325).

Hizbollah succeeded in entering the homes of Israelis via the Internet, thus creating an important psychological breakthrough (see Tsfati & Weimann 1999, 317). The group accomplished this goal in 1999 when it provided details about the return of the bodies of Israeli marine commandoes who had fallen in Lebanon on its Internet site. Hizbollah stated that the single coffin returned contained not just a single body, but the body parts of a number of the fallen marines. The statement caused uproar among the families of the deceased and resulted in a bitter confrontation between the latter and the Israeli Defense Force (IDF) authorities. Hizbollah also published appeals to the parents of Israeli soldiers stationed in Lebanon on their sites. A prominent example was the publication of an interview, originally aired in Israel, with four mothers of IDF soldiers entitled 'I Don't Want My Son to Die in Lebanon.' Many Israelis, particularly parents of soldiers serving in Lebanon, admitted visiting the Hizbollah sites to get news updates. "I regard these sites as a legitimate source of information," one Israeli father is reported to have said. According to Tsfati and Weimann (1999, 327), "the Hizbollah site even offers to answer anyone who sends questions by e-mail, and does indeed reply to Israeli questioners, sending information and news to their e-mail addresses."

In terms of the Israeli-Palestinian conflict, Hizbollah's media strategising is said to be having an impact in this sphere also. According to Matthew Levitt, Hamas is said to be losing the battle of the 'media Jihad' to the smaller, less popular Islamic Jihad. Fathi Hamad, the Hamas communications chief, has lamented Islamic Jihad's ability to project itself as an equal to Hamas despite being smaller, lacking a developed social welfare wing, and commanding less support on the street. What explanation is provided for Islamic Jihad's success? Apparently taking a leaf out of Hizbollah's playbook, they have instituted a savvy media strategy, with an Internet component about which Hamad had this to say:

> We outnumber them, we have many more mosques, and much more commitment, but they are ahead of us in the satellite TV stations, and their websites are much bigger than the group itself...They are stealing attacks from Hamas, exaggerate the number of the killed [*sic*], and inflate the numbers of their street demonstrations as if they are a domestic group, even though they are supported by Hizbullah. The media has turned them into the equals of the Muslim Brotherhood [Hamas] (Levitt 2005).

Such observations also point to the possible influence of the Hizbollah media model upon, for example, various of the Iraqi insurgent groups.

There is no doubt that Hizbollah's leadership would like to gain access to Western, particularly American, audiences via the Internet. Evidence of dramatic effects, similar to those referred to above, upon Western audiences is lacking, however. Having said this, the pressures recently brought to bear on Hizbollah's Web sites and the group's satellite broadcast capabilities may point to the effectiveness of Hizbollah's information operations (IO) strategy in the Western context. There has been a huge upsurge in Western publics' interest in the issue of terrorist use of the Net arising out of the increased use of the Web sites of insurgent groups operating in Iraq as sources of news and information by major Western media outlets. In comparison with these Web sites, which are generally not available in English, many of which are maintained by relatively unknown groups, are difficult to locate online, and which are notoriously ephemeral in terms of their locations and the lengths of time they remain accessible, the official nature of Hizbollah's sites, the group's longtime notoriety in the West, the massive amounts of English-language content provided, and the (until recently) stable and easily identifiable location of the Hizbollah sites, meant that these sites were--and, in many respects, remain--attractive destinations for those wishing to peruse 'real' terrorist sites. Further, judging by the efforts of Internet Haganah, CATM, and others, there are those who are fearful of the impact of Hizbollah's IO strategy on Western audiences and are thus engaged in concerted efforts to disrupt it.

CONCLUSION

Thanks to the availability of independent media sources and fairly unobstructed access to the Internet, facilitated by the widespread knowledge and use of English and French, the Lebanese are probably the most politically informed and outspoken of Arab publics (Haddad & Khashan 2002, 815). Indeed nowhere else in the Middle East do Islamist groups "have the freedoms they enjoy in Lebanon, giving them a wide cultural influence" (Hamzeh 1997). Much of Hizbollah's influence, in particular, arose out of the group's development of an integrated media strategy, which employed the use of wall murals, posters, leaflets, magazines, newspapers, radio, television, the Internet, and a computer game to project an image of the group as a defender of the Lebanese people and the only effective spearhead against renewed Israeli military occupation. This strategy has met with high levels of success both within Lebanon and the Middle East region more widely. Hizbollah officials have often expressed their desire to improve the image of the 'party' in the United States and globally, however. This led Norton (1998) to observe that that would be "a public-relations job that would challenge the best that Madison Avenue has to offer." Undeterred, Hizbollah has sought to implement just such a campaign both via its satellite television station and its suite of Web sites.

Josef Goebbels, Hitler's Minister of Propaganda, once said: 'We do not talk to say something, but to obtain a certain effect' (Schmid & De Graaf 1982, 14). Terrorism entails the use of violence for effect, 'speaking with action' rather than words. The meaning of terrorist acts is not always clear, however. An integral part of most terrorist activity, therefore, is the explanation later provided in written and oral forms (Cordes 1998, 164). There is an added dimension to cybercortical warfare, however. The object of the strategy adopted by Hizbollah was to understand the adversary well enough to condition or determine the choices they made: "Using the adversary's lexicon, syntax and representational systems allows the neocortical warrior to lead the adversary through the cycle of observation, orientation, decision and action. Mastery is the result" (Szafranski 1997[1994], 408).

In a similar fashion and with a view to rebranding itself as a legitimate political, social, and cultural organization amongst Western governments and people, Hizbollah has sought to cultivate a gentler image towards the West. Thence repeated assurances that Hizbollah's problems are not with the American people, but with its

leaders and administration, stringent disavowals of any links with al-Qaeda, and denials of responsibility for attacks carried out against US interests in Lebanon in the early 1980s. In terms of its global Internet audience, Hizbollah provided broader justification for its political violence activity by detailing alleged Israeli transgressions of international law and human rights in minute detail (as discussed in Ch.5) in order to illustrate the organization's legitimacy.

Clearly, the leadership of Hizbollah realized early in the Internet revolution that establishing a meaningful virtual power-base was reliant on a functioning and effective Web presence. The fact that they have become a favoured target of hacktivists of all stripes seems to indicate that they have met with some success in this regard. The fact that the group is presently invested in overhauling its suite of Web sites with a view to providing audiences with more professional looking pages containing more up-to-date information is also an indicator that Hizbollah's cyber strategy is having some tangible effect and that, far from being a passing fad, terrorist use of the Net is here to stay.

CONCLUSION

"For the conduct of war...in the youth of a state, arms do flourish; in the middle age of a state, learning; and then both of them together"

- Francis Bacon[293]

"[I]nformation generally thought to be immaterial, is increasingly seen to be an essential part of all matter. In contrast, power, long thought to be based mainly on material resources, is increasingly seen to be fundamentally immaterial, even metaphysical in nature. As information becomes more material and power more immaterial, the two concepts become more deeply intertwined than ever."

- John Arquilla & David Ronfeldt (1996b)

INTRODUCTION

"In 'Internet time', as in 'dog years', eons have passed since the first messages were sent between computers. The Internet now has its own history, though most of the events took place just years ago and portentous changes are taking place today" (Guice 1998, 201). Along with a summing up then, in this final chapter I also want to suggest that the way we understand the 'current history' of the Internet is crucial to our understanding of future social and political choices regarding the Net. Looking behind us intelligently and looking around us perceptively will allow us to see the paths ahead more clearly.

Much discussion, both public and scholarly, of the role of the Internet in international affairs remains dominated by cheerleaders and hyperbole, with little critical appraisal of how the Internet is actually used and how the logic of the medium means that it can be a force for both good and ill. Kluver provides the example of Nicholas Negroponte--founder and director of MIT's Media Lab--who declared that, thanks to the Internet, children in the future "are not going to know what nationalism is." Another cheerleader pointed to by Kluver is Michael Dertouzos--onetime director of MIT's Laboratory for Computer Science (1974 - 2001)--who argued that digital

[293] As quoted in Arquilla & Ronfeldt 1996b, 132.

communication would bring "computer-aided peace," which "may help stave off future flare-ups of ethnic hatred and national break-ups." Dertouzos' reasoning is that "any new channel of communication among the people and organizations of this world is likely to contribute to increase understanding hence greater peace" (as quoted in Kluver 2002, 508) In other words, the logic of the conversation enabled by the Internet and other new media formats will prevail over the narrative logic, which distinguishes between 'us' and 'them'. In certain circumstances, of course, the presumption that improved communications technologies will reduce misunderstandings and avert political conflict has proved correct, and the Internet and other new media are increasingly employed as a force for good in the world. But they are also increasingly employed as a force for ill. It is this aspect of new media technologies and their effects that has been largely ignored within the discipline of International Relations with a preference shown instead for exploring the use of ICTs by civil society actors and others engaged in what might broadly be termed 'good works.'

In their seminal contribution to the study of terrorism and the media, *Violence as Communication* (1982), Alex Schmid and Janny De Graaf point out that

> Before technology made possible the amplification and multiplication of speech, the maximum number of people that could be reached simultaneously was determined by the range of the human voice and was around 20,000 people. In the nineteenth century, within one lifetime, the size of an audience was expanded twenty-five to fifty times. In 1839 the *New York Sun* published a record 39,000 copies; in 1896, on the occasion of President McKinley's election, two US papers, belonging to Pulitzer and Hearst, for the first time printed a million copies. William McKinley paid dearly for this publicity. In 1901 he was killed by an anarchist, Leon Czolgosz, who explained his deed with the words: 'For a man should not claim so much attention, while others receive none' (p.10).

Historically, access to the communication structure was intimately related to power (Crelinsten 1987, 443). With the growth of the press, and later television, a situation arose that gave unequal chances of expression to different people. This connection between power and free expression was summed-up by A.J. Liebling who observed

that "Freedom of the press is limited to those who own one" (Schmid & De Graaf 1982, 177).

The major difference the Internet has brought to international relations at the beginning of the twenty-first century is a vast reduction in the cost of communicating and sending data across great distances. At first glance this may appear to be a relatively insignificant breakthrough; in practice, however, this reduction in the cost of international communications transactions has amounted to a paradigm shift (Franda 2002, 7). This is because it has radically swelled the ranks of the 'powerful.' The overarching goal of this text has been to gain some sense of the complex interaction taking place between Internet development and the changing nature of international relations with respect to terrorism and its practice in the last decade. More specifically, this text has been concerned with the delineation of the differences between cyberterrorism and terrorist use of the Net, which has been undertaken in conjunction with an analysis of the increased relevance of soft power within the domain of international relations and, ultimately, the assertion that the instrumental power of the Internet lies not in its capacity to be used as a tool of cyberterrorism, but as an instrument for the multiplication of information-based or soft power resources. Within this text, in other words, information-level threats were distinguished from more technical threats (i.e. cyberterrorism); because the primary lever of an information-level attack is the content of a message or claim, rather than its form, information-level threats are less about security in a technical or computational sense than notions of propaganda, opinion formation, and perception management.

DESECURITIZING THE CYBERTERRORIST THREAT

In the Western world, in particular, the Internet has been extensively integrated into the economy, the military, and society as a whole. As a result, and in conjunction with media speculation as to the effects of the aforementioned integration, many people now believe that it is possible for people to die as a direct result of a cyberterrorist attack and that such an attack is imminent. What the present text has sought to illustrate, on the contrary, is that at the present time, the principal appeal of the Internet to terrorists is the powerful assistance it provides for getting their message out and not as either a tool or target of cyberterrorism.

On Wednesday morning, 12 September 2001, you could still visit a Web site that integrated three of the wonders of modern technology: the Internet, digital video, and the World Trade Center. The site allowed Internet users worldwide to appreciate what millions of tourists have delighted in since Minoru Yamasaki's architectural wonder was completed in 1973: the glorious 45-mile view from the top of the WTC towers. According to journalists, the caption on the site still read 'Real-Time Hudson River View from World Trade Center' (O'Toole 2001). In the square above was deep black nothingness. The terrorists hadn't taken down the Net, they had taken down the towers. "Whereas hacktivism is real and widespread, cyberterrorism exists only in theory. Terrorist groups are using the Internet, but they still prefer bombs to bytes as a means of inciting terror," wrote Dorothy Denning (2001b) just weeks before the September attacks. Terrorist 'use' of the Internet has been largely ignored, however, in favour of the more headline-grabbing 'cyberterrorism.'

The bulk of the evidence to date shows that terrorist groups are making widespread use of the Internet, but so far they have not resorted to cyberterrorism, or shown the inclination to move heavily in this direction. In keeping with this reality, Richard Clarke, former White House special adviser for Cyberspace Security, has said that he prefers not to use the term 'cyberterrorism,' instead, he favours the term 'information security' or 'cyberspace security,' since at this stage terrorists have only used the Internet for propaganda, communications, and fundraising (Wynne, 2002). In a similar vein, Michael Vatis, former head of the US National Infrastructure Protection Center (NIPC), has stated that "Terrorists are already using technology for sophisticated communications and fund-raising activities. As yet we haven't seen computers being used by these groups as weapons to any significant degree, but this will probably happen in the future" (Veltman 2001, 12E). The problem certainly can't shrink much, hovering as it does at zero cyberterrorism incidents per year. That's not to say that cyberterrorism cannot happen or will not happen, but that, contrary to popular perception, it has not happened yet.

FOCUSING ON TERRORIST 'USE' OF THE NET

What is the future of the Internet? It is generally agreed that it is difficult to predict outcomes for the Internet because of the complicated relationships between secrecy

and openness, security and insecurity, freedom and oppression, the public and the private, the individual and the community, etc. It is generally agreed also that the potential for a 'digital 9-11' in the near future is not great. This does not mean that IR scholars may continue to ignore the transformative powers of the Internet. On the contrary, as of 9-11 the Internet has come of age. Both terrorism and the Internet are significant global phenomena, reflecting and shaping various aspects of world politics (sometimes separately but oftentimes in unison).

The political dynamic that exists between these two might even be described as a 'transversal' phenomenon.[294] Roland Bleiker, in his text *Popular Dissent, Human Agency and Global Politics* (2000), describes the latter as "a political practice that not only transgresses national boundaries, but also questions the spatial logic through which these boundaries have come to constitute and frame the conduct of international relations" (p.2). Bleiker points to the way in which the concept of transversalism draws attention to various political (and, one might add, technological) transformations that are currently taking place and the ensuing need to rethink the manner in which the domain of IR has traditionally been theorised. In a similar vein, David Campbell has argued that globalized life is best understood as "a series of transversal struggles rather than as a complex of inter-national, multi-national or transnational relations" (Campbell 1996, 24). He points to the way in which the latter are modes of representation that are strongly invested with the maintenance of those borders that are currently being problematized. To conceptualise global politics as a site of transversal struggle, in contrast, is to recognise the complex cross-border flows of people, goods, ideas, capital, etc. and underline the plural and multi-layered interactions that compose contemporary life.

The Internet is a critical instrument for generating political support, fundraising, networking, recruitment, and information gathering for many, perhaps most, contemporary terrorist groups, both within their theaters of operation and among broader international audiences, as illustrated in Chapter Three. The establishment of an effective Web site can be a particular boon to terrorist organizations as Part III further illustrates. The maintenance of an accessible and dynamic Web presence allows terrorist groups to engage in unmediated online identity performance, which in turn gives them the opportunity to tell the story of the

[294] The term transversal was used briefly by Michel Foucault to describe struggles against authority that were not limited to one country (see Bleiker 2000, 2).

conflicts in which they are involved from purely their own perspectives. And stories can be powerful: they do not just describe; they can also motivate and explain collective action. In fact, a good story can contribute to political change via a two-step process: first, the projection or performance of narratives can open hearts and changes minds, and then changes in consciousness can produce changes in political behaviour (Brysk 1995, 574).

When US Defense Secretary Donald Rumsfeld was asked about soft power in 2003, he replied "I don't know what it means" (as quoted in Nye 2006). In February 2006, in a speech at the Council on Foreign Relations in New York, however, Rumsfeld was forced to concede:

> Our enemies have skillfully adapted to fighting wars in today's media age, but for the most part we, our country, our government, has not adapted. Consider that the violent extremists have established media relations committees—these are terrorists and they have media relations committees that meet and talk about strategy, not with bullets but with words. They've proven to be highly successful at manipulating the opinion elites of the world. They plan and design their headline-grabbing attacks using every means of communication to intimidate and break the collective will of free people...They know that communications transcend borders and that a single news story handled skillfully can be as damaging to our cause and helpful to theirs as any other method of military attack. And they're doing it. They're able to act quickly. They have relatively few people. They have modest resources compared to the vast and expensive bureaucracies of Western governments. Our federal government is really only beginning to adapt our operations to the 21st century. For the most part, the U.S. government still functions as a five and dime store in an eBay world (Council on Foreign Relations 2006).

"In the global 'war' against terrorism, the ability to take command and control of the global info-sphere is every bit as important as any other weapon on the military, intelligence, financial or any other fronts" (Taylor 2004, 108).

On this analysis, an increasingly important dimension of power is the ability to have one's account become the perceived reality of others on the basis of attraction rather than coercion. A large body of research has shown this to be true in the case of the mass-media and was further illustrated here with the analysis in Chapters Two and Four of the high levels of soft power at the disposal of the latter in terms of the framing of the debates on cyberterrorism and terrorist use of steganography respectively. In 1990, Alvin Toffler wrote that

> High-tech governments face a future in which multiple, conflicting, custom-tailored commercial, cultural, and political messages will bombard their people, rather than a single message repeated in unison by a few giant media outlets. The old 'politics of mass mobilization' and the 'engineering of consent' both become far more difficult in the new media environment (p.344).

Philip Seib made a similar observation in 2004:

> ...the Internet dilutes the potency of governments' 'official news,' which is most effective when it faces minimal competition. The voices of the Web are obstacles to the flow of propaganda because they provide so many information options. As Owen Gibson of the *Guardian* puts it, 'when you have a worldwide depository of millions of points of view, the propaganda war becomes a lot harder to win (p.95).

The present research illustrates that Toffler was partially correct in his assessment: the information provision component of terrorist Internet use has been shown to be one of the most important facets of the terrorism-Internet relationship. It is important to bear in mind, however, that the traditional mass-media remain the world's soft power behemoths. And that it is recognition and coverage by the latter that is the goal of many terrorist Web masters. This is because when you have, as the *Guardian* journalist points out, a surfeit of information at your disposal it is perhaps easiest to fall back on the 'old reliables' in the form of trusted sources such as the *BBC*, *CNN*, *The New York Times*, and the host of other global, regional, national, and local media outlets with which each of us, as news and information consumers, is most familiar.

Having sounded this note of caution, it is doubtless also the case that due to its global reach and rich multilingual context, the Internet has the potential to influence in manifold ways many different types of political and social relations. Unlike the traditional mass media, the Internet's open architecture has restricted efforts by governments to regulate Net activities which, in turn, has provided Netizens with immense freedom and space to shape the Internet in their own likeness: a patchwork of peoples, ideas, hierarchies, ideologies, images, etc. In large part, Internet users learn by doing. Once users figure out what the Net is good for--donating to charity, disseminating information, communicating securely, etc.--on their own terms, they quickly begin to develop new uses, and the volume and sophistication of traffic on the Net is increased. This, in turn, contributes to users' unprecedented independence as information gatherers and producers.

Before the Internet, most of the information produced by governments, interest groups, and others had to be disseminated via the news media. Few ordinary individuals had the requisite time, knowledge, or inclination to track down primary materials, such as politician's speeches, government reports, and the like, or indeed to produce their own commentaries. It was easier to let journalists assemble the 'pertinent' information and deliver it in digestible form. In the Internet age, however, anyone with access can use the Web to easily track down primary information, whether from the White House, 10 Downing St., the Palestinian Authority or, indeed, Hamas. The Web sites of many terrorist groups and their supporters are freely available as are those of the law enforcement agencies seeking to contain them. The sites of news organisations throughout the world are accessible twenty-four hours a day. During crises, the Internet allows the individual user to operate on at least two levels: near and far. The Internet allows one to connect with those in one's immediate vicinity--whether geographically, socially, culturally, politically, etc.--but also enables users to break free from parochialism and view events from many different perspectives. This break with the past is already having profound effects on the way the world works.

In terms of conclusions then, on the micro level this text shows that the cyberterrorist threat has been over hyped and that we ought to be more concerned instead with the way in which terrorists are currently using the Internet, particularly for the purposes of information dissemination. On the macro level, the text illustrates the way in which the Internet is contributing to the reshaping of international

relations, particularly in terms of the way in which power is conceived therein, while at the same time advocating for the retention of a balanced view of the relationship between 'big' and 'small' media. Summing up, if the Internet is a sling and content the stone with which terrorists in the guise of David are seeking to overcome the Goliath that remains traditional mass media, then David's opening shot is on target, but there's still a way to go before he overpowers the giant.

FUTURE RESEARCH

The relationship between modern international relations and the Internet is a broad and multifaceted topic; the relationship between international relations and contemporary terrorism equally so. Both areas of research would benefit from more attention from IR scholars. Due to space restraints, however, the recommendations for future research recorded here will be limited to the area of terrorism and the Internet.

Terrorists are not limiting themselves to the traditional means of communication; they increasingly employ the new media to pursue their goals. The terrorists of today, like those of yesteryear, are keen to exploit the traditional mass media while also recognizing the value of more direct communication channels. As has been pointed out, "if what matters is openness in the marketplace of ideas...then the Web delivers an equal opportunity soapbox" (Norris 2001, 172). As far back as 1982, Alex Schmid and Janny De Graaf acceded that

> If terrorists want to send a message, they should be offered the opportunity to do so without them having to bomb and kill. Words are cheaper than lives. The public will not be instilled with terror if they see a terrorist speak; they are afraid if they see his victims and not himself...If the terrorists believe that they have a case, they will be eager to present it to the public. Democratic societies should not be afraid of this (Schmid & De Graaf 1982, 170).

A problem has nevertheless arisen that was not foreseen by Schmid and De Graaf: some terrorist groups have taken their killing directly to the 'airwaves' by posting footage of hostages being beheaded online. The Web sites on which such footage originally appeared, and will doubtless do so again in the future, were alluded

to here only briefly. This was mainly due to the emphasis within this text on terrorists' English-language sites. This was necessitated by the author's inability to read Arabic and the fact that none of those Web sites associated with al-Qaeda, nor those relating to the Iraqi conflict, are available in English. There is a pressing need therefore for those with the requisite language skills to systematically investigate and report upon the appearance, discursive structuring, functioning, and effectiveness of these sites.

In terms of the sites investigated here, engaging in a similar study, but including a larger number of cases/sites would doubtless prove fruitful as would a comparative research program. The latter could involve both a systematic comparison of the contents of terrorist groups' English-language sites with their indigenous-language sites and, more broadly, a comparison of terrorist sites with those of hate groups. In fact, the latter might be broadened further to eventually include a comparison of terrorist sites not just with hate sites, but also political party and NGO Web sites, for example. This might be undertaken with a view to eliciting whether terrorist sites have more in common with hate sites as is commonly held or, in fact, are closer in their contents and appearance to, say, political party sites.

Three further avenues for research would likely also prove productive. First, the Kahane site was the only one investigated here to include a chat forum, but there are many so-called 'Jihadi forums' now accessible online. A description and analysis of the topics prominent on these would be a worthwhile contribution in this area. Second, having the opportunity to actually question those responsible for maintaining terrorist Web sites and eliciting from them the purposes of their sites, the resources invested in their maintenance, their overall cyber-strategy, and future plans would be exceedingly beneficial. Third, researching the cyber-strategies of all of the major parties to a conflict in a given region and seeking to measure the impact of these could also throw up some interesting findings.

Clearly, research in this area has only just begun. There are many facets of terrorism and the Internet that have never yet been explored. Many of those avenues that have been opened to exploration have as yet been only cursorily examined while many new avenues of exploration are sure to open in this area in the future. The research presented here, as elsewhere, is necessarily incomplete as the terrorism-Internet relationship is one in which innovation and change is taking place all the time. This can be challenging for the researcher, but also means that one is occupying a front-row seat for a show that's sure to run and run.

APPENDICES

Appendix A.
What is the Internet and How Does it Differ From the Web?*

The Internet is a computer network made up of thousands of networks worldwide; it is therefore, a network of networks. All computers on the Internet communicate with one another using the Transmission Control Protocol/Internet Protocol suite, abbreviated to TCP/IP. Computers on the Internet use a client/server architecture. This means that the remote server machine provides files and services to the user's local client machine. Software can be installed on a client computer to take advantage of the latest access technology.

The World Wide Web (abbreviated as the Web or WWW) and the Internet are not the same thing. The Web lives on top of the Internet. The Internet's network is at the core of the Web, although the Web itself is something different. The World Wide Web consists of files, called pages or sites, containing links to documents and resources throughout the Internet.

The World Wide Web is a system of Internet servers that supports hypertext to access several Internet protocols on a single interface. Almost every protocol type available on the Internet is accessible on the Web. This includes e-mail, FTP, Telnet, and Usenet News. In addition to these, the World Wide Web has its own protocol: HyperText Transfer Protocol, or HTTP. The World Wide Web provides a single interface for accessing all these protocols. This creates a convenient and user-friendly environment. It is no longer necessary to be conversant in these protocols within separate, command-level environments. The Web gathers together these protocols

into a single system. Because of this feature, and because of the Web's ability to work with multimedia and advanced programming languages, the Web is the fastest-growing component of the Internet.

The operation of the Web relies primarily on hypertext as its means of information retrieval. HyperText is a document containing words that connect to other documents. These words are called links and are selectable by the user. A single hypertext document can contain links to many documents. In the context of the Web, words or graphics may serve as links to other documents, images, video, and sound. Links may or may not follow a logical path, as the creator of the source document programs each connection. Overall, the Web contains a complex virtual web of connections among a vast number of documents, graphics, videos, and sounds.

Producing hypertext for the Web is accomplished by creating documents with a language called HyperText Markup Language, or HTML. With HTML, tags are placed within the text to accomplish document formatting, visual features such as font size, italics and bold, and the creation of hypertext links. Graphics and multimedia may also be incorporated into an HTML document. HTML is an evolving language, with new tags being added as each upgrade of the language is developed and released.

---

* Based on *A Basic Guide to the Internet* (University Libraries: State University of New York), which is available online at http://library.albany.edu/internet/internet.html.

Appendix B.
Definitions of Cyberterrorism, 1997-2003

Definition	Year	Publication	Author(s)
Cyberterrorism is the execution of a surprise attack by a subnational foreign terrorist group or individuals with a domestic political agenda using computer technology and the Internet to cripple or disable a nation's electronic and physical infrastructures	2003	*Black Ice: The Invisible Threat of Cyberterrorism*, p.xx	Dan Verton
Cyberterrorism....typically [refers] only to the use of networked media for the execution of destructive acts coordinated by terrorists and terrorist groups	2003	*Bombs and Bandwidth*, p.89	Rachel Yould
We define CT as the usage of computer or information technology resources to coerce someone to do or believe something, primarily for political, social or religious objectives , but also financial objectives, if they support terrorist activities	2003	*The Journal of Information Warfare* 2(2): 15-16	Michael W. David & Kouichi Sakurai
The words cyberterrorism should refer to an act or acts of terrorism carried out through the use of a computer	2002	*American Behavioral Scientist* 45(6): 1035	Ayn Embar-Seddon
Cyberterrorism [is] the use of cyber tools to attack computers as the principal target	2001	In Yonah Alexander & Michael Swetnam (ed.s), *Cyber Terrorism and Information Warfare: Threats and Responses*, p.6	Michael Vatis
Cyberterrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda	2001	*National Infrastructure Protection Center: Highlights* 6(01): 3	National Infrastructure Protection Center, Analysis and Information Sharing Unit
Cyberterrorism can be described as the....general destruction of critical computer systems that are	2001	*Computer Fraud and Security* No. 11: 12	Berni Dwan

vital to the smooth running of a country. These critical systems include information and communications, electric power generation, transmission and distribution, oil and gas production and distribution, banking and finance, transportation, water supply, and emergency government services....Its goal can be mass destruction or personal downfall, propagation of hate, lies or downright dangerous information to everyone, or to select groups who will use it cleverly			
Cyberterrorism is the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological	1999	*Cyberterror: Prospects and Implications*, p.9	Bill Nelson, Rodney Choi, Michael Iacobucci, Mark Mitchell, & Greg Gagnon
Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks 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, 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	1999	*Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* (for the Nautilus Institute)	Dorothy Denning
Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents	1998	*Computer Fraud and Security* February: 9	Mark Pollitt
Information Terrorism = the intentional abuse of a digital information system, network or component toward an end that supports or facilitates a terrorist campaign or action	1997	*Terrorism and Political Violence* 9(1): 75	Matthew Devost, Paul Houghton & Neal Pollard
Cyberterrorism is terrorism that operates exclusively in cyberspace	1995	*Information Age Terrorism: Toward Cyberterror*	Matthew J. Littleton

Appendix C.
Five Major Categories of Terrorist Internet Use*

Use	Author(s)
Information Provision	
Propaganda & Publicity	Furnell & Warren; Weimann
Information Dissemination	Furnell & Warren
Political Action	Cohen
Propaganda	Thomas; Weimann
Generating "Cyberfear"	Thomas
Misinformation	Thomas
Psychological Warfare	Weimann
Financing	
Fundraising	Furnell & Warren; Weimann
Finance	Cohen; Thomas
Profiling**	Thomas
Networking	
Secure Communications	Furnell & Warren
Planning	Cohen
Coordination & Operations	Cohen
Anonymous/Covert Communication	Thomas
Command & Control	Thomas
Mitigation of Risk	Thomas
Networking	Weimann
Planning & Coordination	Weimann
Recruitment	
Mobilisation & Recruitment	Thomas; Weimann
Information Gathering	
Profiling**	Thomas
Information Gathering	Thomas
Data Mining	Weimann
Sharing Information	Weimann

* Takes each of the uses identified in Table 3.2 and places each in one of the five major categories identified as core terrorist uses of the Net.

** Appears in two categories because it is used by the author to describe two separate issues (see Thomas 2003, 155).

NB: Two items that appear in Table 3.2 are not included here. These are theft/manipulation of data and disruption (Thomas 2003, 119-120), which fall under the rubric of offensive use.

BIBLIOGRAPHY

Adams, James. 2001. 'Virtual Defense.' *Foreign Affairs* 80(3).

Adams, Jonathan & Fred Guterl. 2003. 'Bringing Down the Internet.' *Newsweek* 3 November. http://msnbc.msn.com/id/3339638/

Adams, Paul C. 1996. 'Protest and the Scale Politics of Telecommunications.' *Political Geography* 15(5).

Agencies. 2004. 'Hezbollah Condemns "Un-Islamic" Berg's Beheading.' *Palestine Chronicle* 13 May. http://new.palestinechronicle.com/story.php?sid=20040513103141151

Aglionby, John. 2003. 'Jakarta Bomber in Terror Network.' *The Guardian* 9 August. http://www.politics.guardian.co.uk/indonesia/Story/0,2763,1015293,00.html

Ahlers, Mike M. 2004. 'Blueprints for Terrorists?' *CNN.com* 19 November. http://www.cnn.com/2004/US/10/19/terror.nrc/

Alali, A. Odasuo & Gary W. Byrd. 1994. *Terrorism and the News Media: A Selected, Annotated Bibliography*. Jefferson, NC: McFarland.

Alexander, Yonah. 1973. *The Role of Communications in the Middle East Conflict*. New York: Praeger.

Alexander, Yonah & Michael S. Swetnam (Ed.s). 2001. *Cyber Terrorism and Information Warfare: Threats and Responses*. New York: Transnational Publishers.

Allen, Patrick D. & Chris Demchak. 2003. 'The Palestinian-Israeli Cyberwar.' *Military Review* March-April. http://www.leavenworth.army.mil/milrev/download/English/MarApr03/allen.pdf

Alterman, Jon. 1998. *New Media, New Politics? : From Satellite Television to the Internet in the Arab World*. Washington DC: Washington Institute for Near East Policy.

Alvey, Ruth. 'Russian Hackers for Hire: The Rise of the E-Mercenary.' *Jane's*

Intelligence Review 13(7).

Anderson, Benedict. 1983. *Imagined Communities*. London: Verso.

Anderson, Jon. 1998. *Arabizing the Internet*. Abu Dhabi: Emirates Centre for Strategic Studies and Research.

Anderson, Ross. 2001. 'Reply to the Times Article: Secrets Concealed by Software.' http://lists.jammed.com/crime/2001/10/0027.html

Anderson, Ross & Fabien A.P. Petitcolas. 1998. 'On the Limits of Steganography.' *IEEE Journal of Selected Areas in Communication* 16(4). http://www.cl.cam.ac.uk/~fapp2/publications/jsac98-limsteg.pdf

Anderson, Ross. 1996. 'Stretching the Limits of Steganography.' *Lecture Notes in Computer Science* No. 1174.

Andrew, Christopher. 2001. 'Counsel of War.' *The Times* (*T2* Supplement) 4 October.

Anonymous. 2001. 'Hackers Divert Indonesian Hits.' *The Age* 10 May.

Anti-Defamation League (ADL). 1998. 'Terrorist Activities on the Internet.' *Terrorism Update* Winter.http://www.adl.org/Terror/focus/16_focus_a.asp

Aoki, Kumiko. 1994. 'Virtual Communities in Japan.' Paper presented at the Pacific Telecommunications Council Conference. http://www.ibiblio.org/pub/academic/communications/papers/Virtual-Communities-in-Japan

Appadurai, Arjun. 1996. *Modernity At Large: Cultural Dimensions in Globalization*. Minneapolis & London: University of Minnesota Press.

Arquilla, John. 1998. 'The Great Cyberwar of 2002.' *Wired* 6(2). http://www.wired.com/wired/archive/6.02/cyberwar.html

Arquilla, John & David Ronfeldt. 2001a. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. California: Rand. http://www.rand.org/publications/MR/MR1382/

Arquilla, John & David Ronfeldt. 2001b. 'Emergence and Influence of the Zapatista Social Netwar.' In John Arquilla & David Ronfeldt (Eds.), *Networks and Netwars*. California: Rand. http://www.rand.org/publications/MR/MR1382/MR1382.ch6.pdf

Arquilla, John & David Ronfeldt. 2001c. 'Networks, Netwars and the Fight for the Future.' *First Monday* 6(10). http://www.firstmonday.org/issues/issue6_10/ronfeldt/index.html

Arquilla, John & David Ronfeldt. 2001d. 'What Next for Networks and Netwars?' In John Arquilla and David Ronfledt (Ed.s), *Networks and Netwars*. California: Rand. http://www.rand.org/publications/MR/MR1382/MR1382.ch10.pdf

Arquilla, John & David Ronfeldt. 1999. *The Emergence of Noopolitik: Toward an American Information Strategy*. California: Rand. http://www.rand.org/publications/MR/MR1033/

Arquilla, John, David Ronfeldt & Michele Zanini. 1999. 'Networks, Netwar and Information-Age Terrorism.' In Ian O. Lesser, Bruce Hoffman, John Arquilla, David F. Ronfeldt, Michele Zanini & Brian Michael Jenkins, *Countering the New Terrorism*. California: Rand. http://www.rand.org/publications/MR/MR989/MR989.chap3.pdf

Arquilla, John & David Ronfeldt (Eds.). 1997. *In Athena's Camp: Preparing for Conflict in the Information Age*. California: Rand. http://www.rand.org/publications/MR/MR880/

Arquilla, John & David Ronfeldt. 1996a. *The Advent of Netwar*. California: Rand. http://www.rand.org/publications/MR/MR789/

Arquilla, John & David Ronfeldt. 1996b. 'Information, Power, and Grand Strategy: In Athena's Camp.' In Stuart J. Schwartzenstein (Ed.), *The Information Revolution and National Security*. Washington DC: Center for Strategic and International Studies.

Arquilla, John & David Ronfeldt. 1993. 'Cyberwar is Coming.' *Comparative Strategy* Vol. 12.

Associated Press. 2005. 'Leader of US Embassy Bomb Plot Gets 10 Years.' *International Herald Tribune* 15 March. http://www.iht.com/articles/2005/03/15/europe/web.0315france2.html

Associated Press. 2004. 'US Spies on Chat Rooms.' *Wired News* 11 October. http://www.wired.com/news/privacy/0,1848,65305,00.html

Associated Press. 2002. 'Man Hijacks Al-Qaeda Site for FBI Use.' *USA Today* 30 July. http://www.usatoday.com/tech/news/2002-07-30-al-qaeda-online_x.htm

Associated Press. 2001a. 'Bin Laden's Cybertrail Proves Elusive.' *USA Today* 20 September. http://www.usatoday.com/tech/news/2001/09/20/attacks-cybertrail.htm.

Associated Press. 2001b. 'CIA Can't Compare with Hackers.' 21 June. http://www.cbsnews.com/stories/2001/06/21/tech/main297811.shtml

Australian Broadcasting Corporation (ABC). 2004. 'NSW Considers Limits on Government Website.' *ABC Online* 28 April.

Badey, Thomas J. 1998. 'Defining International Terrorism: A Pragmatic Approach.' *Terrorism & Political Violence* 10(1). http://www.dushkin.com/text-data/articles/30791/body.pdf

Baker, John C., Beth E. Lachman, Dave Frelinger, Kevin O'Connell, Alex Hou, Michael S. Tseng, David T. Orletsky & Charles Yost. 2004a. *Mapping the Risks:*

Assessing the Homeland Security Implications of Publicly Available Geospatial Information. California: Rand. http://www.rand.org/publications/MG/MG142/

Baker, John C., Beth E. Lachman, Dave Frelinger, Kevin M. O'Connell, Alex Hou, Michael S. Tseng, David T. Orletsky, Charles Yost. 2004b. 'America's Publicly Available Geospatial Information: Does It Pose a Homeland Security Risk?' *Rand Research Brief* RB-9045-NGA. http://www.rand.org/publications/RB/RB9045/
Baldwin, David A. 1979. 'Power Analysis and World Politics: New Trends Versus Old Tendencies.' *World Politics* 31(2).

Ballard, James D., Joseph G. Hornik, & Douglas McKenzie. 2002. 'Technological Facilitation of Terrorism: Definitional, Legal and Policy Issues.' *American Behavioral Scientist* 45(6): 989-1016.

Barstow, David & Robin Stein. 2005. 'Under Bush, A New Age of Prepackaged TV News.' *New York Times* 13 March.

Bass, Gary D. & Sean Moulton. 2002. 'The Bush Administration's Secrecy Policy: A Call to Action to Protect Democratic Values' [Working Paper]. Washington DC: OMB Watch. http://www.ombwatch.org/rtk/secrecy.pdf

Bassiouni, Cherif. 1983. 'Problems of Media Coverage of Nonstate-Sponsored Terror-Violence Incidents.' In Lawrence Z. Freedman & Yonah Alexander (Eds.), *Perspectives on Terrorism*. Wilmington, DE: Scholarly Resources.

Baudrillard, Jean. 1983. *Simulations*. New York: Semiotexte.

Bendrath, Ralf. 2003. 'The American Cyber-Angst and the Real World: Any Link?' In Robert Latham (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*. New York: New Press.

Benhold, Katrin. 2005. 'Trial Begins in US Embassy Plot.' *International Herald Tribune* 4 January.

Bennett, W. Lance. 2003a. 'New Media Power: The Internet and Global Activism.' In Nick Couldry & James Curran (Ed.s), *Contesting Media Power*. Rowman & Littlefield. http://depts.washington.edu/gcp/pdf/bennettnmpower.pdf

Bennett, W. Lance. 2003b. 'Communicating Global Activism: Strengths and Vulnerabilities of Networked Politics.' *Information, Communication, and Society* 6(2).

Bennett, W. Lance & Robert M. Entman (Eds.). 2001. *Mediated Politics: Communication in the Future of Democracy*. Cambridge: Cambridge University Press.

Berkowitz, Ben. 2004. 'Look Closely: The Picture May Tell a Story.' *USA Today* 30 August. http://www.usatoday.com/tech/news/2004-06-30-steganography_x.htm

Berkowitz, Bruce D. 1996. 'Information Age Intelligence.' *Foreign Policy* No. 103.

Bhattia, Michael. 2005. 'Fighting Words: Naming Terrorists, Bandits, Rebels and Other Violent Actors.' *Third World Quarterly* 26(1).

Blanford, Nicholas. 2001. 'Hizbullah Steps up Psychological Warfare: Party believes that the Media Plays Critical Role in Palestinian Uprising.' *Daily Star* (Beirut) 8 September. http://www.hizbollah.org/english/press/p2001/p20010908a.htm.
Bleiker, Roland. 2000. *Popular Dissent, Human Agency and Global Politics*. Cambridge: Cambridge University Press.

Bob, Clifford. 2001. 'Marketing Rebellion: Insurgent Groups, International Media, and NGO Support.' *International Politics* 38(3).

Bollier, David. 2003. *The Rise of Netpolitik: How the Internet is Changing International Politics and Diplomacy*. Washington DC: The Aspen Institute. http://www.aspeninstitute.org/AspenInstitute/files/CCLIBRARYFILES/FILENAME/0000000077/netpolitik.pdf

Borger, Julian. 2002. 'US Fears al-Qaida Will Hit Vital Computer Networks.' *The Guardian* (UK) 28 June.

Borland, John. 1998. 'Analyzing the Threat of Cyberterrorism.' *TechWeb: The Business Technology Network* 25 September. http://www.techweb.com/wire/story/TWB19980923S0016

Bowyer Bell, J. 1978. 'Terrorist Scripts and Live-Action Spectaculars.' *Columbia Journalism Review* 17(1).

Bradley, John R. 2004. 'Website Postings Give Away Terror Activities.' *The Straits Times* 5 May. http://www.asiamedia.ucla.edu/article.asp?parentid=10916

Bridis, Ted. 2001. 'Bush Backs Changes in Hacking Disclosure.' *Washington Post* 19 October. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A18052-2001Oct18&notFound=true

Brock, Jack L. 1991. *Computer Security: Hackers Penetrate DOD Computer Systems*. Washington DC: General Accounting Office. http://www.globalsecurity.org/security/library/report/gao/145327.pdf

Brown, Robin. 2002. 'The Contagiousness of Conflict: E.E. Schattschneider as a Theorist of the Information Society.' *Information, Communication & Society* 5(2).

Brown, Robin. 2001a. 'The New Public Diplomacy: Power in the Age of Mixed Media.' Paper presented at 4th Pan-European International Relations Conference, Canterbury, UK.

Brown, Robin. 2001b. 'Power and the New Public Diplomacy.' Paper presented at the British International Studies Association (BISA) Annual Conference, University of Edinburgh, Scotland.

Brysk, Alison. 1995. 'Hearts and Minds: Bringing Symbolic Politics Back In.' *Polity* 27(4).

Bunt, Gary. 2003. *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments*. London: Pluto Press.

Bunt, Gary. 2000. *Virtually Islamic: Computer-Mediated Communication and Cyber Islamic Environments*. Cardiff: University of Wales Press.

Burke, Jason. 2004. 'Think Again: Al Qaeda.' *Foreign Policy* Iss.142 (May/June).

Burkhart, Grey E. & Susan Older. 2003. *The Information Revolution in the Middle East and North Africa*. Santa Monica, CA: Rand. http://www.rand.org/publications/MR/MR1653/MR1653.pdf

Burnett, Jonny & Whyte, Dave. 2005. 'Embedded Expertise and the New Terrorism.' *Jc2m: Journal for Crime, Conflict, and the Media* 1(4). www.jc2m.co.uk/Issue4/Burnett&Whyte.pdf

Bush, George W. 2002a. *State of the Union Address*. Washington DC: White House. Available online at: http://www.law.ou.edu/hist/state2002.shtml.

Bush, George W. 2002b. 'Text of President Bush's Address on the Middle East.' *Washington Post* 25 June.

Buzan, Barry, Ole Wæver, & Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder & London: Lynne Rienner.

Buzan, Barry. 1995. 'Security, the State, the 'New World Order,' and Beyond.' In Ronnie Lipschultz (Ed.), *On Security*. New York: Columbia University Press.

Buzan, Barry. 1991. *People States and Fear: An Agenda for International Security Studies on the Post-Cold War Era* (Second Ed.). New York: Harvester Wheatsheaf.

Byman, Daniel. 2005. 'Hezbollah's Dilemma.' *ForeignAffairs.org* 13 April. http://www.foreignaffairs.org/20050413faupdate84277/daniel-byman/hezbollah-s-dilemma.html

Byman, Daniel. 2003. 'Should Hezbollah Be Next?' *Foreign Affairs* 82(6). http://www.foreignaffairs.org/20031101faessay82606/daniel-byman/should-hezbollah-be-next.html

Byman, Daniel, Peter Chalk, Bruce Hoffman, William Rosenau, & David Brannan. 2001. *Trends in Outside Support for Insurgent Movements*. California: Rand. http://www.rand.org/publications/MR/MR1405/

Byte, Mr. 1997/8. *Privacy Guide*. http://www.all-nettools.com/privacy/

David Campbell. 1996. 'Violent Performances: Identity, Sovereignty, Responsibility.' In Yosef Lapid & Friedrich Kratochwil (Ed.s), *The Return of Culture and Identity in IR Theory*. Colorado: Lynne Reinner.

CBS. 2004. 'Tracking Terror in Tangled Web.' *CBS Evening News* 17 August. http://www.cbsnews.com/stories/2004/08/17/eveningnews/main636626.shtml

Carr, E.H. 1964. *The Twenty Years Crisis, 1919-1939: An Introduction to the Study of International Relations*. New York: Harper & Row.

Carruthers, Susan L. 2000. *The Media at War*. Hampshire: Palgrave.

Castells, Manuel. 2000. *The Rise of the Network Society* (*The Information Age: Economy, Society, and Culture* Vol. 1) (Second Ed.). Oxford: Blackwell.

Castells, Manuel. 1997. *The Power of Identity* (*The Information Age: Economy, Society, and Culture* Vol. III). Oxford: Blackwell.

Caterinicchia, Dan. 2003. 'Kellogg Describes Cyber Battlefield.' *Federal Computer Week* 5 March. http://www.fcw.com/fcw/articles/2003/0303/web-kellogg-03-05-03.asp

Center for Strategic and International Studies (CSIS). 1998. *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo*. Washington DC: CSIS Press.

Cha, Ariana Eunjung. 2001. 'To Attacks' Toll Add a Programmer's Grief.' *Washington Post* 21 September.

Chaliand, Gerard. 1985. *Terrorism: From Popular Struggle to Media Spectacle*. New Jersey: Saqi Books.

Chalk, Peter. 1999. 'The Evolving Dynamic of Terrorism in the 1990s.' *Australian Journal of International Affairs* 53(2).

Chandler, Amanda. 1996. 'The Changing Definition and Image of Hackers in Popular Discourse.' *International Journal of the Sociology of Law* 24(2): 229-251.

Charity Commission. 2004. 'Palestinians Relief and Development Fund.' London: UK Charity Commission. http://www.charity-commission.gov.uk/investigations/inquiryreports/interpal.asp

Chayban, Badih. 2003. 'Hizbullah Rolls Out New Computer Game.' *Daily Star* (Beirut) 3 March. http://www.specialforce.net/english/news/dailystar.htm

Chomsky, Noam. 1991. *Pirates and Emperors: International Terrorism in the Real World*. Montreal: Black Rose.

Christen, Hank T., James P. Denney & Paul M. Maniscalco. 2002. 'Weapons of Mass

Effect: Cyber-Terrorism.' In Paul M. Maniscalco & Hank T. Christen (Ed.s), *Understanding Terrorism and Managing the Consequences*. New Jersey: Prentice Hall.

Cisneros, Oscar S. 2001. 'Dot-PS: Domain Without a Country.' *Wired* 12 January. http://www.wired.com/news/politics/0,1283,41135,00.html

Clarke, David (Ed.). 2004. *Technology and Terrorism*. New Jersey: Transaction Publishers.

Cleaver, Harry M. 1998. 'The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric.' *Journal of International Affairs* Vol. 51, No. 2.

Cobain, Ian. 2001. 'FBI Closes Website Linked to Real IRA.' *The Times* 8 October.

Cobb, Roger, Jennie Keith Ross, & Marc Howard Ross. 1976. 'Agenda Building as Comparative Political Process.' *American Political Science Review* 70(1).

Cochran, Jordon T. 2000. *Steganographic Computer Warfare*. Wright-Patterson Air Force Base, Ohio: Air Force Institute of Technology. http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2000/afit-gcs-eng-00m-03.pdf

Cohen, Adam. 2001. 'When Terror Hides Online.' *Time* 12 November.

Cohen, Eliot A. 1996. 'A Revolution in Warfare.' *Foreign Affairs* 75(2).

Cohen, Fred. 2002. 'Terrorism and Cyberspace.' *Network Security* Vol. 5.

Cohen, Fred. 2003. 'Cyber-Risks and Critical Infrastructures.' *Strategic Security* 2003-02-27.

Cohn, Carol. 1987. 'Sex and Death in the Rational World of Defense Intellectuals.' *Signs: Journal of Women in Culture and Society* 12(4).

Collier, George Allen. 1999. *Basta! Land and the Zapatista Rebellion in Chiapas*. Chicago: Food First.

Collin, Barry C. 1996. 'The Future of Cyberterrorism.' Paper presented at the 11th Annual International Symposium on Criminal Justice Issues, University of Illinois at Chicago. http://afgen.com/terrorism1.html

Cook, Timothy E. 2001. 'The Future of the Institutional Media.' In W. Lance Bennett and Robert M. Entman (Ed.s), *Mediated Politics*. New York: Cambridge University Press.

Cordes, Bonnie. 1988. 'When Terrorists Do the Talking: Reflections on Terrorist Literature.' In David C. Rapoport (Ed.), *Inside Terrorist Organizations*. London: Frank Cass.

Corera, Gordon. 2004. 'A Web Wise Terror Network.' *BBC News* (World Edition) 6 October. http://news.bbc.co.uk/2/hi/in_depth/3716908.stm

Cornfield, Michael 2005. *The Internet and Campaign 2004: A Look Back at the Campaigners*. Washington DC: Pew Internet and American Life Project. http://www.pewinternet.org/pdfs/Cornfield_commentary.pdf

Couldry, Nick and James Curran (Ed.s). 2003. *Contesting Media Power*. New York: Rowman.

Council on Foreign Relations. 2006. 'New Realities in the Media Age: A Conversation with Donald Rumsfeld.' Transcript of remarks made by Rumsfeld at the Council on Foreign Relations, New York, 17 February. http://www.cfr.org/publication/9900/

Crelinsten, Ronald D. 1987. 'Power and Meaning: Terrorism as a Struggle Over Access to the Communication Structure.' In Paul Wilkinson & Alexander M. Stewart (Eds.), *Contemporary Research on Terrorism*. Aberdeen: Aberdeen University Press.

Crilley, Kathy. 2001. 'Information Warfare: New Battlefields. Terrorists, Propaganda, and the Internet.' *ASLIB Proceedings* 53(7).

Dahan, Michael & Gabriel Sheffer. 2001. 'Ethnic Groups and Distance Shrinking Communication Technologies.' *Nationalism and Ethnic Politics* 7(1).

Dalglish, Lucy A., Gregg P. Leslie, & Phillip Taylor. 2002. *Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know*. Arlington, VA: Reporters Committee for Freedom of the Press. http://www.rcfp.org/news/documents/Homefront_Confidential.pdf

Damphousse, Kelly R. and Brent L. Smith. 1998. 'The Internet: A Terrorist Medium for the 21st Century.' In Harvey W. Kushner (Ed.), *The Future of Terrorism: Violence in the New Millennium.* London: Sage.

Dartnell, Michael. 1999. 'Insurgency Online: Elements for a Theory of Anti-Government Internet Communications.' *Small Wars and Insurgencies* 10(3).

Davern, Paul & Michael Scott. 1996. 'Fractal Based Image Steganography.' *Lecture Notes in Computer Science* No. 1174.

David, M.W & K. Sakurai. 2003. 'Combating Cyber Terrorism: Improving Analysis and Accountability.' *Journal of Information Warfare* 2(2): 15-26.

De Armond, Paul. 2001. 'Netwar in the Emerald City: WTO Protest Strategy and Tactics.' In John Arquilla & David Ronfeldt (Eds.), *Networks and Netwars*. California: Rand. http://www.rand.org/publications/MR/MR1382/MR1382.ch7.pdf

Dearth, Douglas H. 2002. 'Shaping the "Information Space."' *Journal of Information Warfare* 1(3).

Debrix, François. 2001. 'Cyberterror and Media-Induced Fears: The Production of Emergency Culture.' *Strategies* 14(1).

Dedeoglu, Beryl. 2003. 'Bermuda Triangle: Comparing Official Definitions of Terrorist Activity.' *Terrorism & Political Violence* 15(3).

Deibert, Ronald J. 1997. *Parchment, Printing, and Hypermedia: Communication in World Order Transformation*. New York: Columbia University Press.

Deibert, Ronald J. 2002. 'Circuits of Power: Security in the Internet Environment.' In James N. Rosenau & J.P. Singh (Ed.s), *Information Technology and Global Politics*. Albany: SUNY Press.

Deibert, Ronald. 2003. *Black Code: Censorship, Surveillance, and the Militarization of Cyberspace*. New York: Social Science Research Council. http://www.ssrc.org/programs/itic/publications/ITST_materials/blackcode.pdf

Delio, Michelle. 2004. 'Hacktivism and How it Got Here.' *Wired* 14 July. http://www.wired.com/news/infostructure/0,1377,64193,00.html?tw=wn_story_related

Dembart, Lee. 2001. 'Hide Your Secrets: Old Art of Concealed Messages Rediscovered on the Internet.' *International Herald Tribune* 7 May.

Denning, Dorothy. 1999. 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.' In John Arquilla and David Ronfeldt (Ed.s), *Networks and Netwars*. California: Rand. http://www.rand.org/publications/MR/MR1382/MR1382.ch8.pdf

Denning, Dorothy. 2000a. *Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*, May 23. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Denning, Dorothy. 2000b. 'Cyberterrorism.' *Global Dialogue* Autumn. http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc

Denning, Dorothy. 2001a. 'Is Cyber Terror Next?' In Craig Calhoun, Paul Price, and Ashley Timmer (Ed.s), *Understanding September 11*. New York: New Press. http://www.ssrc.org/sept11/essays/denning.htm

Denning, Dorothy. 2001b. 'Cyberwarriors: Activists and Terrorists Turn to Cyberspace.' *Harvard International Review* 23(2). http://www.hir.harvard.edu/articles/index.html?id=905

Denning, Dorothy. 2004. 'Information Operations and Terrorism.' [Unpublished Draft].

Denning, Dorothy. 2005. 'Power Over the Information Front.' Paper presented at the conference on *The Global Flow of Information*, Yale University, April 1-3. http://islandia.law.yale.edu/isp/GlobalFlow/paper/Denning.pdf

Denning, Dorothy & William E. Baugh. 2001. 'Hiding Crimes in Cyberspace.' In Peter Ludlow (ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge MA: MIT Press.

Denoeux, Guilain. 1993. *Urban Unrest in the Middle East: A Comparative Study of Informal Networks in Egypt, Iran, and Lebanon.* Albany: State University of New York Press.

Der Derian, James. 1995. 'The Value of Security: Hobbes, Marx, Nietzsche, and Baudrillard.' In Ronnie Lipschultz (Ed.), *On Security*. New York: Columbia University Press.

De Rosa, Mary. 2004. *Data Mining and Data Analysis for Counterterrorism.* Washington DC: Center for Strategic and International Studies. http://www.csis.org/tech/2004_counterterrorism.pdf

Deutch, John. 1996. *Statement Before the US Senate Governmental Affairs Committee (Permanent Subcommittee on Investigations)*, 25 June. http://www.nswc.navy.mil/ISSEC/Docs/Ref/InTheNews/fullciatext.html

DPP News Agency. 2002. 'German Intelligence Says Al Qaeda's Preparing to Attack Western Computer Systems.' 11 September. http://www.zone-h.org/en/news/read/id=834/

Deuze, Mark. 2003. 'The Web and Its Journalisms: Considering the Consequences of Different Types of Newsmedia Online.' *New Media & Society* 5(2).

Devost, Matthew G., Brian K. Houghton, & Neal Allen Pollard. 1997. 'Information Terrorism: Political Violence in the Information Age.' *Terrorism and Political Violence* 9(1): 72-83.

Devost, Matthew, Houghton, & Neal Alan Pollard. 1996. 'Information Terrorism: Can You Trust Your Toaster?' In Robert E. Neilson (Ed.), *Sun Tzu's Art of War in Information Warfare*. Institute for National Strategic Studies: National Defence University, Washington DC. http://www.ndu.edu/inss/siws/ch3.html

Dobkin, Bethami A. 1992. *Tales of Terror: Television News and The Construction of the Terrorist Threat*. Westport, CT: Praeger.

Donohue, Laura K. 2003. 'Mediating Terror.' *International Studies Review* 5(2): 232-237.

Dorman, William& Mansour Farhang. 1987. *The US Press and Iran: Foreign Policy and The Journalism of Deference*. Berkeley: University of California Press.

Doyle, Neil. 2004. *Terror Tracker: An Odyssey into Pure Fear*. Edinburgh: Mainstream Publishing.

Dror, Yuval. 2004. 'BGU Web Scanner Can Detect Terror Content.' *Haaretz.com* 16 August.

Duff, Liz & Simon Gardiner. 1996. 'Computer Crime in the Global Village: Strategies for Control and Regulation – In Defence of the Hacker.' *International Journal of the Sociology of Law* 24(2): 211-228.

Dunn, Myriam A. 2002. *Information Age Conflicts: A Study of the Information Revolution and a Changing Operating Environment*. Zurich: ISN. http://www.isn.ethz.ch/crn/_docs/zb_64_wholedoc.pdf

Dunn, Myriam A. 2004. 'Cyber-Terror: Looming Threat or Phantom Menace?' Paper presented at the Fifth International CISS Millennium Conference, Salzburg, Austria, July 7-8.

Dunnigan, James F. 2003. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press.

Duyvesteyn, Isabelle. 2004. 'How New is the New Terrorism?' *Studies in Conflict and Terrorism* 27(5).

Dwan, Berni. 2001. 'Cyberterrorism: Virtual for Who?' *Computer Fraud & Security* No.11: 12-14.

Eedle, Paul. 2004. 'Al Qaeda's Super-Weapon: The Internet.' Paper presented at *Al-Qaeda 2.0*, New America Foundation, Washington DC, 1-2 December. http://www.outtherenews.com/modules.php?op=modload&name=News&file=article&sid=89&topic=7

Ehrenfeld, Rachel. 2003. *Funding Evil: How Terrorism is Financed*. New York: Basic Books.

Ehrenfeld, Rachel. 2004. 'How Terrorist Propaganda Kills.' *FrontPage Magazine* 10 December. http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=16275

Elovici, Yuval, Abraham Kandel, Mark Last, Bracha Shapira, & Omer Zaafrany. 2004. 'Using Data Mining Techniques for Detecting Terror-Related Activities on the Web.' *Journal of Information Warfare* 3(1).

Embar-Seddon, Ayn. 2002. 'Cyberterrorism: Are We Under Siege?' *American Behavioral Scientist* 45(6).

Emerson, Steven. 2002. 'Fund-Raising Methods and procedures for International Terrorist Organizations.' Testimony before the House Committee on Financial Services, 12 February. http://financialservices.house.gov/media/pdf/021202se.pdf

Emery, Norman E., Robert S. Earl, & Raymond Buettner. 2004. 'Terrorist Use of Information Operations.' *Journal of Information Warfare* 3(2).

Entman, Robert M. 2000. 'Declarations of Independence: The Growth of Media Power After the Cold War.' In Brigitte L. Nacos, Robert Y. Shapiro, & Pierangelo Isernia (Ed.s), *Decisionmaking in a Glass House*. New York: Rowman & Littlefield.

Entman, Robert. 1991. 'Framing US Coverage of International News: Contrasts in Narratives of the KAL and Iran Air Incident.' *Journal of Communication* 41.

Entman, Robert M. 1993. 'Framing: Toward Clarification of a Fractured Paradigm.' *Journal of Communication* 43(4).

Eriksson, Johan & Giampiero Giacomello. 2004. 'International Relations Theory and Security in the Digital Age.' Paper presented at the International Studies Association (ISA) annual conference Montreal, Canada, 17-20 March. http://www.threat-politics.net/docs/eriksson_isa.pdf

Eriksson, Johan. 2001. 'Cyberplagues, IT, and Security: Threat Politics in the Information Age.' *Journal of Contingencies and Crisis Management* 9(4).

Eriksson, Johan & Erik Noreen. 2002. 'Setting the Agenda of Threats: An Explanatory Model.' *Uppsala Peace Research Papers* No. 6. http://www.pcr.uu.se/publications/UPRP_pdf/uprp_no_6.pdf

Erlanger, Steven & Chris Hedges. 2001. 'Terror Cells Slip Through Europe's Grasp.' *New York Times* 28 December. http://www.pulitzer.org/year/2002/explanatory-reporting/works/122801.html

Ettinger, J. Mark. 1998. 'Steganalysis and Game Equilibria.' *Lecture Notes in Computer Science* No. 1525.

Evans, Michael. 2002. 'Al-Qaeda in Secret Talks with Lebanon Terror Group.' *The Times* (UK) 1 February.

Fallis, D.S. & Arianna E. Cha. 2001. 'Agents Following Suspects' Lengthy Electronic Trail.' *The Washington Post* 4 October.

Fandy, Mamoun. 1999. 'CyberResistance: Saudi Opposition Between Globalization and Localization.' *Comparative Studies in Society and History* 41(1).

Fielding, Nick. 2002. 'Leaders of Sept 11 Boast of US Attack.' *The Sunday Times* 8 September.

Fighel, Yoni & Yael Shahar. 2002. 'The Al-Qaida-Hizbollah Connection.' Herzliya, Israel: International Policy Institute for Counter-Terrorism. http://www.ict.org.il/articles/articledet.cfm?articleid=425

Foreign Broadcast Information Service (FBIS). 1997. 'Hizballah's al-Manar TV on Internet.' FBIS-NES-97-043, 3 March.

Foreign Broadcast Information Service (FBIS). 2002a. 'Government Sets Up Anti-Cyberterrorism Homepage.' *Sankei Shimbun* FBIS-EAS-2002-0410, 10 April.

Foreign Broadcast Information Service. 2002b. 'Right-Wing Internet Site Urges Players to Kill Oslo 'Criminals,' Arafat.' *FBIS-NES-2002-0214* February 14.

Foreign Broadcast Information Service (FBIS). 2002c. 'Russia Cracks Down on 'Cyberterrorism.'' *ITAR-TASS* FBIS-SOV-2002-0208, 8 February.

Fouda, Yosri. 2002. 'The Masterminds.' *The Sunday Times* 8 September.

Franda, Marcus. 2002. *Launching Into Cyberspace: Internet Development and Politics in Five World Regions*. London: Lynne Rienner.

Friedman, Thomas L. 2002. 'Webbed, Wired and Worried.' *The New York Times* 26 May. http://www.nytimes.com/2002/05/26/opinion/26FRIE.html

Fritz, Kathryn, Lindsay Harris, Daniel Kolb, Paula Larich, & Kathleen Stocker. 2004. 'Terrorist Use of the Internet and National Response.' [Unpublished Paper]. College Park: University of Maryland. http://www.wam.umd.edu/~larich/735/index.html

Furnell, Steve & Matthew Warren. 1999. 'Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium.' *Computers and Security* 18(1).

Gabbard, C.Bryan & George S. Park. 1995. *The Information Revolution in the Arab World: Commercial, Cultural, and Political Dimensions*. Santa Monica, CA: Rand.

Gallie, W.E.B. 1962. 'Essentially Contested Concepts.' In Max Black (Ed.), *The Importance of Language*. Englewood, NJ: Prentice Hall.

Gallo, Jason. 2003. 'Online Oppositional Communities as Discursive Counterpublics.' Paper presented at the Association of Internet Researchers (AoIR) Annual Conference, Toronto, Canada, 16-19 October.

Garrido, Maria & Alexander Halavais. 2003. 'Mapping Networks of Support for the Zapatista Movement: Applying Social Networks Analysis to Study Contemporary Social Movements.' In Martha McCaughey & Michael D. Ayers (Eds.), *Cyberactivism: Online Activism in Theory and Practice*. London: Routledge.

Garrison, Linda & Martin Grand. 2001a. 'Localization Facilitates Foreigners' Access to Hacker Tools.' *National Infrastructure Protection Center: Highlights* 1(01). http://www.iwar.org.uk/infocon/nipc-highlights/2001/highlight-01-01.pdf

Garrison, Linda & Martin Grand. 2001b. 'Cyberterrorism: An Evolving Concept.' *National Infrastructure Protection Center: Highlights* 6(01). http://www.iwar.org.uk/infocon/nipc-highlights/2001/highlight-01-06.pdf

Gearty, Conor. 1998. *Terror*. London: Faber & Faber.

Geers, Kenneth & Peter Feaver. 2004. 'Cyber Jihad and the Globalization of Warfare: Computer Networks as a Battleground in the Middle East and Beyond.' Presentation

at the Black Hat Briefings, Las Vegas, USA, 28-29 July.
http://blackhat.com/presentations/bh-usa-04/bh-us-04-geers.pdf

Gellman, Barton. 2002a. 'Cyber-Attacks by Al Qaeda Feared.' *Washington Post*, 27 June. http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26

Gellman, Barton. 2002b. 'Qaeda Cyberterror Called Real Peril.' *International Herald Tribune*, 28 June.
General Accounting Office. 2003. *Terrorist Financing*. Washington DC: general Accounting Office. http://www.gao.gov/new.items/d04163.pdf

Gentile, Carmen J. 2000a. 'Hacker War Rages in Holy Land.' *Wired*, 8 November. http://www.wired.com/news/politics/0,1283,40030,00.html

Gentile, Carmen J. 2000b. 'Palestinian Crackers Share Bugs.' *Wired*, 2 December. http://www.wired.com/news/politics/0%2C1283%2C40449%2C00.html

George, Alexander (Ed.). 1991. *Western State Terrorism*. Cambridge: Polity Press.

Geras, Norman. 1985. 'The Controversy About Marx and Justice.' *New Left Review* Iss. 150 (March-April).

Geras, Norman. 1992. 'Bringing Marx to Justice: An Addendum and Rejoinder.' *New Left Review* Iss.195 (September-October).

Gerbner, George. 1992. 'Violence and Terrorism in and By the Media.' In Mark Raboy & Bernard Dagenais (Eds.), *Media, Crisis and Democracy: Mass Communication and the Disruption of Social Order*. London: Sage.

Gerges, Fawaz A. 2005. *The Far Enemy: Why Jihad Went Global*. Cambridge: Cambridge University Press.

Giacomello, Giampiero. 2003. 'Measuring "Digital Wars": Learning from the Experience of Peace Research and Arms Control.' *Infocon Magazine* No. 1. http://www.iwar.org.uk/infocon/measuring-io.htm

Giacomello, Giampiero. 2004. 'Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism.' *Studies in Conflict and Terrorism* 27(5).

Gibson, Rachel and Stephen Ward. 2000. 'A Proposed Methodology for Studying the Function and Effectiveness of Party and Candidate Web Sites.' *Social Science Computer Review* Vol. 18(3).

Goldman, Emily O. (Ed.). 2004. *National Security in the Information Age*. London: Frank Cass.

Gordon, Avishag. 2001. 'Terrorism and the Scholarly Communication System.' *Terrorism and Political Violence* Vol. 13, No. 4.

Gordon, Sarah & Richard Ford. 2002. 'Cyberterrorism?' *Computers and Security*

21(7).

Graham, Stephen. 2004. 'War in the "Weirdly Pervious World": Infrastructure, Demodernisation, and Geopolitics.' Paper presented at the conference on Urban Vulnerability and Network Failure, University of Salford, UK, 29-30 April. http://www.surf.salford.ac.uk/documents/UrbanVulnerability/Graham.pdf

Gray, Chris Hables. 2001. *Cyborg Citizen: Politics in the Posthuman Age*. London: Routledge.

Greene, Thomas C. 2004. 'Cyber-Terror Drama Skates on Thin *Black Ice*.' *The Register* 25 February. http://www.theregister.co.uk/2004/02/25/cyberterror_drama_skates_on_thin/

Greene, Thomas C. 2002. 'Soon Al-Qaeda Will Kill You on the Internet.' *The Register* 28 June. http://www.theregister.co.uk/2002/06/28/soon_alqaeda_will_kill_you/

Greene, Thomas C. 2003. 'Al-Qaeda Said to be Using Stegged Porn.' *The Register* (UK) 12 May. http://www.theregister.co.uk/content/55/30654.html

Gronke, Paul & Timothy Cook. 2002. 'Disdaining the Media in the Post 9/11 World.' Paper presented at the annual meeting of the American Political Science Association (APSA), Boston MA, August. http://web.reed.edu/academic/studentgrants/corbandgold/apsa2002.pdf

Gruner, Stephanie & Gautam Naik. 2001. 'Extremist Sites Under Heightened Scrutiny.' *The Wall Street Journal Online* 8 October. http://zdnet.com.com/2100-1106-530855.html?legacy=zdnn.

Guelke, Adrian. 1998. *The Age of Terrorism and the International Political System*. London & New York: IB Tauris Publishers.

Gugliotta, Guy. 2001. 'Agencies Scrub Web Sites of Sensitive Chemical Data.' *Washington Post* 4 October. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A2738-2001Oct3

Guice, Jon. 1998. 'Looking Backward and Forward at the Internet.' *The Information Society* 14(3).

Gupta, Suman. 2002. *The Replication of Violence: Thoughts on International Terrorism After September 11th 2001*. London: Pluto Press.

Haddad, Simon & Hilal Khashan. 2002. 'Islam and Terrorism: Lebanese Muslim Views on September 11.' *Journal of Conflict Resolution* 46(6).

Hajnal, Peter I. (Ed.). 2002. *Civil Society in the Information Age*. Aldershot: Ashgate.

Hammes, Thomas X. 2004. The *Sling and the Stone: On War in the 21st Century*. Minnesota: Zenith Press.

Hamzeh, A. Nizar. 1993. 'Lebanon's Hizbullah: From Islamic Revolution to Parliamentary Accommodation.' *Third World Quarterly* 14(2).

Hamzeh, A. Nizar. 1997. 'Islamism in Lebanon: A Guide.' *Middle East Review of International Affairs* 1(3). http://www.biu.ac.il/SOC/besa/meria/journal/1997/issue3/jv1n3a2.html

Hamzeh, A. Nizar. 2000. 'Lebanon's Islamists and Local Politics: A New Reality.' *Third World Quarterly* 21(5).

Hara, Noriko & Zilia Estrada. 2003. 'Hate and Peace in a Connected World: Comparing MoveOn and Stormfront.' *First Monday* 8(12). http://www.firstmonday.org/issues/issue8_12/hara/

Harik, Judith. 1996. 'Between Islam and the System: Sources and Implications of Popular Support for Lebanon's Hizballah.' *Journal of Conflict Resolution* 40(1).

Harmon, Amy. 1998. '"Hacktivists" of All Persuasions Take Their Struggle to the Web.' *The New York Times* 31 October. http://www.cs.du.edu/~lavita/hacktivists.pdf

Harris, Aaron Keith. 2004. 'Israeli Spy Agency Recruits Staff on Web.' *USA Today* 5 May. http://www.usatoday.com/tech/world/2004-05-25-isreal-spy-recruiting_x.htm

Harris, Larry Wayne. 1995. *Bacteriological Warfare: A Major Threat to North America*. Indianapolis, IN: Virtue International Publishing.

Hauss, Charles & Alexandra Samuel. 2002. 'What's the Internet Got to Do With It? Online Responses to 9/11.' Paper presented at the American Political Science Association Annual (APSA) Annual Convention, Boston, 29 September-1 August.

Hayden, Tom. 2002. *The Zapatista Reader*. New York: Thunder's Mouth Press.

Henderson, Mark. 2001. 'Secrets Concealed by Software.' *The Times* (London) 6 October.

Henych, Mark, Stephen Holmes & Charles Mesloh. 2003. 'Cyber Terrorism: An Examination of the Critical Issues.' *Journal of Information Warfare* 2(2).

Herman, Edward S. & Noam Chomsky. 1988. *Manufacturing Consent: the Political Economy of the Mass Media*. London: Vintage.

Herman, Edward S. 1982. *The Real Terror Network*. Boston: South End Press.

Hershman, Tanya. 2000. 'Cyberterrorism is Real Threat, Say Experts at Conference.' *Israel.internet.com*, 11 December.

Herzfeld, Mindy. 2003. 'Restricting the Flow of Funds from US Charities to International Terrorist Organizations.' *Tax Lawyer* 56(4).

Herzog, Michael. 2005. 'The Hizbollah Conundrum.' *Policy Watch* No. 981. http://www.washingtoninstitute.org/templateC05.php?CID=2286

Hill, Kevin A. & John E. Hughes. 1998. *Cyberpolitics: Citizen Activism in the Age of the Internet*. Lanham: Rowman & Littlefield.

Hine, Christine. 2001. 'Web Pages, Authors and Audiences: The Meaning of a Mouse Click.' *Information, Communication and Society* 4(2).
Hinnen, Todd M. 2004. 'The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet.' *Columbia Science and Technology Law Review* Vol. 5. http://www.stlr.org/html/volume5/hinnenintro.html

Hockstader, Lee. 2000. 'Pings and E-Arrows Fly in Mideast Cyber-War.' *Washington Post*, 27 October. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A21154-2000Oct26&notFound=true

Hoffman, Bruce. 1998. *Inside Terrorism*. London: Indigo.

Hoffman, Bruce. 1999. 'Terrorism Trends and Prospects.' In Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, & Michele Zanini, *Countering the New Terrorism*. California: Rand.
http://www.rand.org/publications/MR/MR989/MR989.chap2.pdf

Holloway, John, Elofna Pelaez, & Eloina Pelaez. 1998. *Zapatista! Reinventing Revolution in Mexico*. London: Pluto Press.

Holmgren, Jonas & Jan Softa. 2003. 'The Functional Security Agenda in the Nordic States.' *Threat Politics Project*. Sweden: University of Uppsala. http://www.threat-politics.net/docs/softa-functional.pdf

Holms, John Pynchon. 1994. *Terrorism*. New York: Windsor Publishing Corps.

Homer-Dixon, Thomas. 2002. 'The Rise of Complex Terrorism.' *Foreign Policy* January/February. http://www.foreignpolicy.com/story/cms.php?story_id=170

Hosein, Hanson. 2001. 'Bytes Without the Blood in Mideast.' *MSNBC*, 4 January.

Hosenball, Mark. 2002. 'Islamic Cyberterror: Not a Matter of If, But of When.' *Newsweek* 20 May. http://archive.infopeace.de/msg01346.html

Hosmer, Chet & Christopher Hyde. 2003. 'Discovering Covert Digital Evidence.' Paper presented at the Digital Forensic Research Workshop, 6-8 August. http://www.dfrws.org/dfrws2003/presentations/Paper-Hosmer-digitalevidence.pdf

iDefense Intelligence Services. *Israeli-Palestinian Cyber Conflict*. Reston, VA: iDefense Inc. http://www.securitymanagement.com/library/Israeli_pales0401.pdf

Institute for Security Technology Studies (ISTS). 2001. *Cyber Attacks During the War on Terrorism: A Predictive Analysis*. Dartmouth College: Institute for Security

Technology Studies.
http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm.

Ingles-le Noble, John. 1999. 'Cyberterrorism Hype.' *Jane's Intelligence Review*.
http://www.iwar.org.uk/cyberterror/resources/janes/jir0525.htm

Intelligence and Terrorism Information Centre (ITIC). 2004. 'Educating Children For Hatred and Terrorism.' Israel: Center for Special Studies.
http://www.intelligence.org.il/eng/sib/11_04/edu.htm
Jaber, Halah. 1997. *Hezbollah: Born With a Vengeance*. New York: Columbia University Press.

Jacobs, David. 2005. 'Internet Activism and the Democratic Emergency in the US.' *Ephemera: Theory and Politics in Organization* 5(1).
http://www.ephemeraweb.org/journal/5-1/5-1jacobs.pdf

Jehl, Douglas & David Johnston. 2004. 'Reports That Led to Terror Alert Were Years Old, Officials Say.' *New York Times* 3 August.

Jenkins, Brian M. 1975. 'International Terrorism: A New Mode of Conflict.' In David Carlton & Carlo Schaerf (Eds.), *International Terrorism and World Security*. London: Croom Helm.

Jenkins, Brian M. 1978. 'International Terrorism: Trends and Potentialities.' *Journal of International Affairs* 1(1).

Jenkins, Brian M. 1980. *The Study of Terrorism: Definitional Problems*. California: Rand.

Jenkins, Brian M. 1981. 'The Study of Terrorism: Definitional Problems.' In Yonah Alexander & John M. Gleason (Eds.), *Behavioral and Quantitative Perspectives on Terrorism*. New York: Pergamon Press.

Johnson, Neil F. 1995. *Steganography*. Virginia: George Mason University.
http://www.jjtc.com/stegdoc/steg1995.html

Johnson, Neil F. 2000. 'Steganalysis.' In Stefan Katzenbeisser & Fabien A. Petitcolas (ed.s), *Information Hiding: Techniques for Steganography and Digital Watermarking*. Boston & London: Artech House.

Johnson, Neil F. & Sushil Jajodia. 1998. 'Steganalysis of Images Using Current Steganography Software.' *Lecture Notes in Computer Science* No. 1525.

Johnson-Cartee, Karen S. and Gary A. Copeland. 2004. Strategic Political Communication: Rethinking Social Influence, Persuasion, and Propaganda. Maryland: Rowman & Littlefield.

Johnston, David. 2003. 'Bin Laden Tape May Hint at Attack, CIA Says.' *The New York Times* 13 February.

Joint Economic Committee. 2001. *Wired World: Cyber Security and the US Economy.* Washington DC: US Government Printing Office. http://www.house.gov/jec/hearings/6-21-01.pdf

Jolish, Barak. 2002. 'The Encrypted Jihad.' *Salon.com* 4 February. http://www.salon.com/tech/feature/2002/02/04/terror_encryption/

Jordan, Tim. 2001. 'Mapping Hacktivism: Mass Virtual Direct Action (MVDA), Individual Virtual Direct Action (IVDA) and Cyberwars.' *Computer Fraud & Security* Iss. 4.

Jorisch, Avi. 2004. *Beacon of Hatred: Inside Hizballah's Al-Manar Television.* Washington DC: The Washington Institute for Near East Policy.

Juergensmeyer, Mark. 2000. *Terror in the Mind of God.* Berkeley: University of California Press.

Kahney, Leander. 2003. 'Internet Stokes Anti-War Movement.' *Wired News* January 21. http://www.wired.com/news/culture/0,1284,57310,00.html?tw=wn_story_related

Kaihla, Paul. 2002. 'The Technology Secrets of Cocaine Inc.' *Business 2.0* July. http://seclists.org/lists/isn/2002/Jul/0015.html

Kalathil, Shanthi. 2002. 'Community and Communalism in the Information Age.' *Brown Journal of World Affairs* 9(1). http://www.watsoninstitute.org/bjwa/archive/9.1/Essays/Kalathil.pdf

Karmon, Ely. 2002. 'Hizbollah and the War on Terror.' Herzliya, Israel: International Policy Institute for Counter-Terrorism. http://www.ict.org.il/articles/articledet.cfm?articleid=444

Karmon, Ely. 2004. 'Fight on all Fronts: Hizballah, the War on Terror, and the War in Iraq.' Herzliya, Israel: International Policy Institute for Counter-Terrorism. http://www.ict.org.il/articles/articledet.cfm?articleid=510

Karmon, Ely. 2005. 'The Double Game of Hizbollah.' Herzliya, Israel: International Policy Institute for Counter-Terrorism. http://www.ict.org.il/articles/articledet.cfm?articleid=531

Karp, Jack. 2002. 'A Novice Tries Steganography.' *Tech TV* 12 February. http://www.techtv.com/cybercrime/privacy/story/0,23008,3359041,00.html

Katzenbeisser, Stefan C. 2000. 'Principles of Steganography.' In Stefan Katzenbeisser & Fabien A. Petitcolas (ed.s), *Information Hiding: Techniques for Steganography and Digital Watermarking.* Boston & London: Artech House.

Katzman, Kenneth. 2005. *Iraq: U.S. Regime Change Efforts and Post-Saddam Governance.* Washington DC: Congressional Reporting Service. http://www.usembassy.it/pdf/other/RL31339.pdf

Kean, Thomas H., Hamilton, Lee H., *et al.* 2004. *The 9/11 Commission Report* (Authorized Edition). New York: WW Norton. http://www.9-11commission.gov/report/911Report.pdf

Kelley, Jack. 2001a. 'Terrorist Instructions Hidden Online.' *USA Today* 5 February. http://www.usatoday.com/tech/news/2001-02-05-binladen-side.htm

Kelley, Jack. 2001b. 'Terror Groups Hide Behind Web Encryption.' *USA Today* 6 February. http://www.usatoday.com/tech/news/2001-02-05-binladen.htm

Kelley, Jack. 2001c. 'Militants Wire Web with Links to Jihad.' *USA Today* 10 July. http://www.usatoday.com/news/world/2002/07/10/web-terror-cover.htm

Keohane, Robert & Joseph S. Nye. 1989 [1977]. *Power and Interdependence*. Boston: Longman.

Keohane, Robert O. and Joseph S. Nye. 1998. 'Power and Interdependence in the Information Age.' *Foreign Affairs* 77(5). http://www.ksg.harvard.edu/prg/nye/power.pdf

Kern, Montague, Marion Just, & Pippa Norris. 2003. 'The Lessons of Framing Terrorism.' In Pippa Norris, Montague Kern, & Marion Just (Ed.s), *Framing Terrorism: The News Media, the Government, and the Public*. New York & London: Routledge.

Kessler, Gary C. 2004. 'An Overview of Steganography for the Computer Forensics Examiner.' *Forensic Science Communication* 6(3). http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm

Khalilzad, Zalmay M. & John P. White (Ed.s). 1999. *Strategic Appraisal: The Changing Role of Information in Warfare*. California: Rand.

Kiggen, Elizabeth. 2001. 'Microsoft, Amazon Appear to Sponsor Terrorist Web Site.' *NewsFactor* 16 January. http://www.newsfactor.com/story.xhtml?story_id=6731

King, Brad. 2002. 'Fear and Lockdown in America.' *Wired* 25 July. http://www.wired.com/news/digiwood/0,1412,54099,00.html

Kluver, Alan R. 2002. 'The Logic of New Media in International Affairs.' *New Media and Society* 4(4).

Knudsen, Olav F. 2001. 'Post-Copenhagen Security Studies: Desecuritizing Securitization.' *Security Dialogue* 32(3): 355-368.

Kolata, Gina. 2001. 'Veiled Messages of Terrorists May Lurk in Cyberspace.' *New York Times* 30 October. http://www.merit.edu/mail.archives/netsec/2001-10/msg00045.html

Kornblum, J. 2001. 'Radical Radio Shows Forced from the Net.' *USA Today* 25 October.

Krebs, Brian. 2002. 'Homeland Security Bill Heralds IT Changes.' *The Washington Post* 25 November.
http://foi.missouri.edu/homelandsecurity/homelandsecuritybill.html

Laqueur, Walter. 1999. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford: Oxford University Press.
Lasker, John. 2005. 'Watchdogs Sniff Out Terror Sites.' *Wired News* 25 February.
http://www.wired.com/news/privacy/0,1848,66708,00.html

Lasswell, Harold & Daniel Lerner (Eds.). 1965. *World Revolutionary Elites: Studies in Coercive Ideological Movements*. Cambridge, MA: MIT Press.

Lasswell, Harold. 1971 [1927]. *Propaganda Technique in World War I*. Cambridge, MA: MIT Press.

Lasswell, Harold, Daniel Lerner, & Hans Speier (Eds.). 1980. *Propaganda and Communication in World History*. Honolulu: University of Hawaii Press.

Lathem, Niles. 2003. '9/11 Plot Hidden in E-Porn.' *New York Post* 9 May.
http://www.nypost.com/news/worldnews/57502.htm

Leizerov, Sagi. 2000. 'Privacy Advocacy Groups Versus Intel: A Case Study of How Social Movements are Tactically Using the Internet to Fight Corporations.' *Social Science Computer Review* 18(4).

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, & Michele Zanini. 1999. *Countering the New Terrorism*. California: Rand.
http://www.rand.org/publications/MR/MR989/

Lettice, John. 2004. 'Al Qaeda Boss Confused Phone SIM With Cloaking Device.' *The Register* 5 March.
http://www.theregister.co.uk/2004/03/05/al_qaeda_boss_confused_phone/

Levin, Brian. 2002. 'Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America.' *American Behavioral Scientist* 45(6).

Levitt, Matthew. 2004. 'Hizbollah's African Activities Remain Undisrupted.' *RUSI/Jane's Homeland Security and Resilience Monitor* 1 March.
http://www.washingtoninstitute.org/templateC06.php?CID=463

Levitt, Matthew. 2005. 'Hamas and Islamic Jihad Clash over 'Media Jihad'.' *RUSI/Jane's Homeland Security & Resilience Monitor* February.
http://www.washingtoninstitute.org/templateC06.php?CID=768

Levitt, Matthew (Forthcoming 2006). 'Hezbollah Finances: Funding the Party of God.' In Jeanne Giraldo & Harold Trinkunas (Ed.s), *Terrorism Financing and State Responses in Comparative Perspective*.
http://www.washingtoninstitute.org/templateC06.php?CID=772

Leyden, John. 2001. 'Militants Plan Terror in Chat Rooms Shocker.' *The Register* (UK) 6 February. http://www.theregister.co.uk/content/archive/16684.html

Libbenga, Jan. 2004a. 'Dutch Internet Blackmailer Gets 10 Years.' *The Register* 24 March. http://www.theregister.co.uk/2004/03/24/dutch_internet_blackmailer_gets/

Libbenga, Jan. 2004b. 'Terrorists Grow Fat on E-Mail Scams.' *The Register* 28 September. http://www.theregister.co.uk/2004/09/28/terrorist_email_scams/

Lin, Wan-Ying and William H. Dutton. 2003. 'The "Net" Effect in Politics: The "Stop the Overlay" Campaign in Los Angeles.' *Party Politics* Vol. 9, No. 1.

Lipschutz, Ronnie D. 1995. *On Security*. New York: Columbia University Press.

Littleton, Matthew J. 1995. *Information Age Terrorism: Toward Cyberterror* [Unpublished MA Thesis]. Monterey, California: US Naval Postgraduate School. http://fas.org/irp/threat/cyber/docs/npgs/notes.htm#notes

Liu, M. 2001. 'Holy War on the Web.' *Newsweek* (International) 15 October.

Livingston, Steven. 1994. *The Terrorism Spectacle*. Boulder: Westview Press.

Long, David. 1990. *The Anatomy of Terrorism*. NewYork: Maxwell Macmillian International.

Lonsdale, David J. 2004. *The Nature of War in the Information Age: Clausewitzian Future*. London: Frank Cass.

Luke, Timothy W. 2001. 'Cyberspace as Meta-Nation: The Net Effects of Online E-Publicanism.' *Alternatives* 26(2).

Lukes, Steven. 1974. *Power: A Radical View*. London: Macmillan.

Lukes, Steven. 1985. *Marxism and Morality*. Oxford: Clarendon Press.

Lyman, Jay. 2001. 'How Terrorists Use the Internet.' *NewsFactor Network* 12 September. http://www.newsfactor.com/perl/story/7731.html

Macdonald, Andrew. 1996. *The Turner Diaries*. New Jersey: Barricade Books.

Manach, Jean-Marc. 2001. 'Terrorisme: Les Dessous de la Filière Porno.' *Transfert.net* 27 September. http://www.transfert.net/a7413

Manjoo, Farhad. 2001. 'Hidden Messages: Any There?' *Wired* 8 November. http://www.wired.com/news/technology/0,1282,48235,00.html

Margulies, Peter. 2004. 'The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment.' *UCLA Journal of Law and Technology* 8(2). http://www.lawtechjournal.com/articles/2004/04_041207_margulies.pdf

Marighella, Carlos. 1971. 'Mini-Manual of the Urban Guerrilla.' In Jay Mallin (Ed.), *Terror and Urban Guerrillas: A Study of Tactics and Documents*. Florida: University of Miami Press.

Marsh, Pearl-Alice. 1995. 'Grassroots Statecraft and Citizens' Challenges to US National Security Policy.' In Ronnie Lipschutz (Ed.), *On Security*. New York: Columbia University Press.

Martin, Gus. 2003. *Understanding Terrorism: Challenges, Perspectives, and Issues*. Thousand Oaks, CA: Sage.

Marvel, Lisa M., Charles G. Boncelet, & Charles T. Retter. 1998. 'Reliable Blind Information Hiding for Images.' *Lecture Notes in Computer Science* No. 1525.

Marzuk, Moshe. 2003. 'The Iraqi Hizballah: Dangerous Implications for Allied Forces in Iraq.' Herzliya, Israel: International Policy Institute for Counter-Terrorism. http://www.ict.org.il/articles/articledet.cfm?articleid=496

Mates, Michael. 2001. *Technology and Terrorism*. Brussels: NATO. http://www.tbmm.gov.tr/natopa/raporlar/bilim%20ve%20teknoloji/AU%20121%20STC%20Terrorism.htm

Matthews, William. 2002. 'Al Qaeda Cyber Alarm Sounded.' *Federal Computer Week* 25 July. http://www.fcw.com/fcw/articles/2002/0722/web-attack-07-25-02.asp

Mayk, Lauren. 2004. 'Restoring Power Likely to Take Weeks, Not Days.' *Southwest Florida Herald Tribune* 16 August. http://www.newscoast.com/apps/pbcs.dll/frontpage

McAlearney, Shawna. 2001. 'Cyberspace Braces for Escalation and War.' *Information Security* 3(89). http://infosecuritymag.techtarget.com/2001/nov/digest19.shtml

McCullagh, Declan. 2001a. 'Bin Laden: Steganography Master?' *Wired* 7 February. http://www.wired.com/news/politics/0,1283,41658,00.html

McCullagh, Declan. 2001b. 'Secret Messages come in .Wavs.' *Wired* 20 February. http://www.wired.com/news/politics/0,1283,41861,00.html

McCullagh, Declan. 2002a. 'CIA Warns of Net Terror Threat.' *C|Net* 29 October. http://news.com.com/2100-1023-963771.html?tag=cd_mh.

McCullagh, Declan. 2002b. 'Bush Signs Homeland Security Bill.' *CNET News* 25 November. http://news.com.com/2102-1023-975305.html

McCullagh, Declan. 2003. 'Military Worried About Web Leaks.' *C|Net News* 16 January. http://news.com.com/2100-1023-981057.html

McCullagh, Declan. 2004. 'CIA Funds Chatroom Surveillance.' *C|Net News* 25 November.
http://news.zdnet.co.uk/communications/networks/0,39020345,39175016,00.htm

McGray, Douglas. 2003. 'The Minister of Net Defense.' *Wired* 11(05).
http://www.wired.com/wired/archive/11.05/schmidt.html
McGrory, Daniel. 2001. 'Al-Qaeda Hid Coded Messages on Porn Websites.' *The Times* (London) 6 October.

McKay, Niall. 1998a. 'The Golden Age of Hacktivism.' *Wired* 22 September.
http://www.wired.com/news/print/0,1294,15129,00.html

McKay, Niall. 1998b. 'Do Terrorists Troll the Net?' *Wired* 4 November.
http://www.wired.com/news/politics/0,1283,15812,00.html

McLaughlin, W. Sean. 2003. 'The Use of the Internet for Political Action by Non-State Dissident Actors in the Middle East.' *First Monday* 8(11).
http://www.firstmonday.org/issues/issue8_11/mclaughlin/index.html

Meehan, Howard Vincent. 2004. *Terrorism, Diasporas, and Permissive Threat Environments: A Study of Hizballah's Fundraising Operations in Paraguay and Ecuador*. Monterey, CA: Naval Postgraduate School.
www.fas.org/irp/world/para/hizb-fund.pdf

Mendoza, Martha. 2003. 'Virus Sender Helped FBI Bust Hackers, Court Records Say.' *USA Today* 18 September.
http://www.usatoday.com/tech/news/computersecurity/2003-09-18-reformed-hacker_x.htm

Middleton, James. 2002. 'US Hackers Could Face Life Sentences.' *Vnunet.com* 28 February. http://vnunet.com/News/1129590.

Morgenthau, Hans. 1967. *Politics Among Nations: The Struggle for Power and Peace*. New York: Alfred Knopf.

Mouzahem, Haytham. 2001. 'Hizb'Allah's Future in the Wake of the Events of September 11.' Paper presented at the British International Studies Association (BISA) Annual Conference, Edinburgh, UK.

Mowlana, Hamid. 1993. 'Toward a NWICO for the Twenty-First Century.' *Journal of International Affairs* 47(1).

Mueller, John. 2005. 'Simplicity and Spook: Terrorism and the Dynamics of Threat Exaggeration.' *International Studies Perspectives* 6(2).

Mulloy, D.J. 1999. *Homegrown Revolutionaries: An American Militia Reader*. Norwich U.K.: Arthur Miller.

Nacos, Brigitte L. 2002. *Mass-Mediated Terrorism: The Central Role of the Media in Terrorism and Counterterrorism*. New York: Rowman & Littlefield.

Nacos, Brigitte L. 1994. *Terrorism and the Media: From the Iran Hostage Crisis to the Oklahoma City Bombing*. New York: Columbia Press.

Napoleoni, Loretta. 2003. *Modern Jihad: Tracing the Dollars Behind the Terror Networks*. London: Pluto Press.
Napoleoni, Loretta. 2004. 'Money and Terrorism.' *Strategic Insights* 3(4). http://www.ciaonet.org/olj/si/si_3_4/si_3_4_nal01.pdf

Napoleoni, Loretta. 2005. 'Profile of a Killer.' *Foreign Policy* Iss. 151 (Nov./Dec.).

National Communications System. 2000. *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications: An Awareness Document*. Arlington, VA: Office of the Manager, National Communications Systems.
http://www.ncs.gov/library/reports/electronic_intrusion_threat2000_final2.pdf

National Infrastructure Protection Center. 2001. *Cyber Protests Related to the War on Terrorism: The Current Threat*. Washington DC: National Infrastructure Protection Center. http://www.iwar.org.uk/cip/resources/nipc/cyberprotestupdate.htm

National Infrastructure Protection Center. 2001a. *NIPC Daily Report*. 11 December.

National Infrastructure Protection Center (NIPC). 2001b. *NIPC Daily Report* 3 December. http://lists.jammed.com/crime/2001/12/0005.html

National Infrastructure Protection Center. 2001c. *NIPC Daily Report*. 18 October.

National Research Council. 1991. *Computers at Risk: Safe Computing in the Information Age*. Washington DC: National Academy Press.
http://www.nap.edu/books/0309043883/html/index.html

Nelson, Bill, Rodney Choi, Michael Iacobucci, Mark Mitchell, Greg Gagnon. 1999. *Cyberterror: Prospects and Implications*. Monterey, CA: Center for the Study of Terrorism and Irregular Warfare.
http://www.nps.navy.mil/ctiw/files/Cyberterror%20Prospects%20and%20Implications.pdf.

Nesser, Petter. 2004. *Jihad in Europe: A Survey of the Motivations for Sunni Islamist Terrorism in Post-Millennium Europe*. Oslo: Norwegian Defence Research Establishment. http://rapporter.ffi.no/rapporter/2004/01146.pdf

New, William. 2004. 'Former Cybersecurity Chief Opposes New Regulations.' *GovExec.com* 24 May. http://www.govexec.com/dailyfed/0504/052404tdpm2.htm

Newman, Barbara & Thomas Diaz. 2005. *Lightning Out of Lebanon: Hezbollah Terrorists on American Soil*. New York: Random House.

Nissenbaum, Helen. 2004. 'Hackers and the Contested Ontology of Cyberspace.' *New Media and Society* Vol. 6, No. 2.

Noble, Ronald K. 2003. *The Links Between Intellectual Crime and Terrorist Financing*. Testimony before the United States House Committee on International Relations, 16 July. http://www.interpol.int/Public/ICPO/speeches/SG20030716.asp

Norris, Pippa. 2001. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge: Cambridge University Press.

Norton, Augustus Richard. 1998. 'Hizballah: From Radicalism to Pragmatism.' *Middle East Policy* 5(4). http://www.mepc.org/public_asp/journal_vol5/9801_norton.asp

Norton-Taylor, Richard. 2001. 'MI5 Posts Terror Appeal on Arab Websites.' *The Guardian* 26 October.

Nua Internet Surveys. 1997. 'Middle East Internet Usage.' http://www.nua.com/surveys/index.cgi?f=VS&art_id=878906966&rel=true

Nua Internet Surveys. 1998. 'Internet Usage in the Arab World.' http://www.nua.com/surveys/index.cgi?f=VS&art_id=888945819&rel=true.

NUA Internet Surveys. 2001. 'Arab Net Population Passes 3.5 Million.' http://www.nua.com/surveys/index.cgi?f=VS&art_id=905356603&rel=true.

Nye, Joseph S. 1990. *Bound to Lead: the Changing Nature of American Power*. New York: Basic Books.

Nye, Joseph S. and William A. Owens. 1996. 'America's Information Edge.' *Foreign Affairs* 75(2).

Nye, Joseph S. 2002. *The Paradox of American Power*. Oxford: Oxford University Press.

Nye, Joseph S. 2004. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.

Nye, Jospeh. 2006. 'Think Again: Soft Power.' *Foreign Policy* 26 February. http://www.foreignpolicy.com/story/cms.php?story_id=3393

O'Brien, Kevin A. 2001. 'Carnivore Feeds on PATRIOT.' *Jane's Intelligence Review* 13(12).

O'Brien, Kevin & Izhar Lev. 2002. 'Information Operations and Counterterrorism.' *Jane's Intelligence Review* 14(9).

O'Brien, Kevin & Joseph Nusbaum. 2000a. Intelligence Gathering on Asymmetric Threats: Part 1.' *Jane's Intelligence Review* 15(10): 50-55.

O,Brien, Kevin & Joseph Nusbaum. 2000b. Intelligence Gathering on Asymmetric Threats: Part 2.' *Jane's Intelligence Review* 15(11): 50-55.

O'Day, Alan. 2004. *Cyberterrorism*. Aldershot: Ashgate.

O'Toole, Fintan. 2001. 'Terrorists Hold Levers of Control of New Kind of War.' *Irish Times* 16 September.
Paletz, David L. & Alex P. Schmid. 1992. *Terrorism and The Media: How Researchers, Terrorists, Governments, Press, Public, Victims View and Use the Media*. Newbury Park, CA: Sage.

Palmer Harik, Judith. 2004. *Hezbollah: The Changing Face of Terrorism*. London: I.B. Tauris.

Parker, Donn. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley & Sons.

Pew Internet & American Life Project. 2003. *Survey with Federal Computer Week Magazine About Emergencies and the Internet*.
http://www.pewinternet.org/pdfs/PIP_Preparedness_Net_Memo.pdf

Pew Internet and American Life Project. 2002. *One Year Later: September 11 and the Internet*. Washington DC: Pew Internet and American Life Project.
http://www.pewinternet.org/pdfs/PIP_9-11_Report.pdf

Pfitzmann, Birgit. 1996. 'Information Hiding Terminology.' *Lecture Notes in Computer Science* No. 1174.

Picard, Elizabeth. 1997. 'The Lebanese Shi'a and Political Violence in Lebanon.' In David E. Apter (Ed.), *The Legitimization of Violence*. London: Macmillan.

Piller, Charles. 2001. 'Terrorists Taking Up Cyberspace.' *Los Angeles Times* 8 February. http://seclists.org/lists/politech/2001/Feb/0024.html

Pollard Neal A. 2004. 'Indications and Warning of Infrastructure Attack.' In Lars Nicander & Magnus Ranstorp (Ed.s), *Terrorism in the Information Age: New Frontiers?* Stockholm: National Defence College.

Pollitt, Mark M. 1998. 'Cyberterrorism: Fact or Fancy?' *Computer Fraud and Security* February.

Porteus, Liza. 2001. 'Feds Still Need to Define Role in Tackling Cyberterror, Panelists Say.' *GovExec.com* 15 May.
http://www.govexec.com/dailyfed/0501/051501td.htm

Post, Jerrold M., Erich Shaw, and Keven Ruby. 2000. 'From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism.' *Terrorism and Political Violence* Vol. 12, No. 2.

Potter, Evan H. (Ed.). 2002. *Cyber-Diplomacy*. Canada: McGill-Queens University Press.

Poulsen, Kevin. 1999. 'Info War or Electronic Sabre Rattling?' *ZDNet* 8 September. http://zdnet.com.com/2100-11-515631.html?legacy=zdnn

Poulsen, Kevin. 2001. 'Cyber Terror in the Air.' *SecurityFocus.com* 30 June. http://www.securityfocus.com/columnists/6

Poulsen, Kevin. 2002. 'Lawyers Fear Misuse of Cyber Murder Law.' *SecurityFocus Online*, 21 November. http://www.theregister.co.uk/2002/11/25/lawyers_fear_misuse_of_cyber/

Poulsen, Kevin. 2003. 'Official: Cyberterror Fears Missed Real Threat.' *SecurityFocus.com* 31 July. http://www.securityfocus.com/news/6589

Powell, William. 2003 [1971]. *The Anarchist Cookbook*. Ozark PR LLC.

Presidential Commission on Critical Infrastructure Protection (PCCIP). 1997. *Critical Foundations: Protecting America's Infrastructures*. Washington DC: Critical Infrastructure Assurance Office (CIAO). http://www.ciao.gov/resource/pccip/report_index.htm

Priest, Danah & Douglas Farah. 2002. 'Terror Alliance Has U.S. Worried: Hezbollah, Al Qaeda Seen Joining Forces.' *Washington Post* 30 June. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A2324-2002Jun29&notFound=true

Provos, Neils & Peter Honeyman. 2001. *CITI Technical Report 01-11: Detecting Steganographic Content on the Internet*. University of Michigan: Center for Information Technology Integration. http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

Raghavan, Tara Mythri. 2003. 'In Fear of Cyberterrorism: An Analysis of the Congressional Response.' *University of Illinois Journal of Law, Technology, and Policy* 3(1). http://www.jltp.uiuc.edu/recdev/Spring%202003/raghavan.pdf

Rainie, Lee, Michael Cornfield & John Horrigan. 2005. *The Internet and Campaign 2004*. Washington DC: Pew Internet and American Life Project. http://www.pewinternet.org/pdfs/PIP_2004_Campaign.pdf

Ranstorp, Magnus. 1994. 'Hizbollah's Command Leadership: Its Structure, Decision-making and Relationship with Iranian Clergy and Institutions.' *Terrorism and Political Violence* 6(3). http://www.st-andrews.ac.uk/intrel/research/cstpv/pdffiles/Hizbollah.pdf [preprint]

Ranstorp, Magnus. 1997. *Hizb'Allah in Lebanon: The Politics of the Western Hostage Crisis*. London: Macmillan.

Ranstorp, Magnus. 1998. 'The Strategy and Tactics of Hizballah's Current "Lebanonization Process".' *Terrorism and Political Violence* 3(1). http://www.st-andrews.ac.uk/academic/intrel/research/cstpv/pdffiles/The%20Strategy%20and%20Tactic.pdf [preprint]

Ranstorp, Magnus. 2004. 'Al-Qaida in Cyberspace: Future Challenges of Terrorism in an Information Age.' In Lars Nicander & Magnus Ranstorp (Ed.s), *Terrorism in the Information Age: New Frontiers?* Stockholm: Swedish National Defence College.

Rash, Wayne. 1997. *Politics on the Nets: Wiring the Political Process*. New York: W.H. Freeman.

Rathmell, Andrew. 1997. 'Cyber-Terrorism: The Shape of Future Conflict?' *RUSI Journal* October: 40-46. http://www.kcl.ac.uk/orgs/icsa/Old/rusi.html.

Rathmell, Andrew, Richard Overill, Lorenzo Valeri, John Gearson. 1997. 'The IW Threat from Sub-State Groups: An Interdisciplinary Approach.' Paper presented at the Third International Symposium on Command and Control Research and Technology, Institute for National Strategic Studies, National Defense University, Washington DC, 17-20 June. http://www.kcl.ac.uk/orgs/icsa/Old/terrori.html

Rattray, Gregory J. 2001. 'The Cyberterrorism Threat.' In James M. Smith & William C. Thomas (Ed.s), *The Terrorism Threat and US Government Response: Operational and Organizational Factors*. Colorado: US Air Force Institute for National Security Studies. http://www.usafa.af.mil/inss/terrchp5.doc

Regular, Arnon. 2004. 'Leading Hamas Preacher Warns of Clash with Islamic Jihad.' *Haaretz* 15 December.
http://www.haaretz.com/hasen/objects/pages/PrintArticleEn.jhtml?itemNo=514500

Resnick, David. 1999. 'Politics on the Internet: The Normalization of Cyberspace.' In Chris Toulouse & Timothy W. Luke (Ed.s), *The Politics of Cyberspace*. New York & London: Routledge.

Reuters. 2004. 'Malaysia PM Says Web Terror Sites Unacceptable.' May 14.
http://www.reuters.co.uk/newsArticle.jhtml?type=internetNews&storyID=5145293&section=news

Reuters. 2001. 'Researchers: No Secret bin Laden Messages on Sites.' *USA Today* 17 October. http://www.usatoday.com/tech/news/2001/10/17/bin-laden-site.htm

Reuters. 1997. 'Peruvian Rebels Wage Propaganda War on Internet.' 3 January.
http://www.spunk.org/library/copyrite/news/sp001719.html

Reynolds, Glenn H. 2004. 'The Blogs of War: How the Internet is Reshaping Foreign Policy.' *The National Interest* Vol. 75 (Spring).
http://www.findarticles.com/p/articles/mi_m2751/is_75/ai_n6077652/print

Rheingold, Howard. 1998. 'Why Education is Needed So Much on the Internet.' *Irish Times* (Internet Supplement) 17 November.

Ribeiro, John. 2005. 'Terrorists Targeted India's Outsourcing Industry.'
NetworkWorldFusion 7 March.
http://www.nwfusion.com/news/2005/0307terrotarge.html

Richardson, Francis. 2001. 'Cyberterrorist Must Serve Year in Jail.' *Boston Herald* 6 June.

Rogers, Richard. 2002. 'Operating Issue Networks on the Web.' *Science as Culture* 11(2).

Ronfeldt, David, John Arquilla, Graham E. Fuller, & Melissa Fuller. 1998. *The Zapatista Social Netwar in Mexico*. California: Rand. http://www.rand.org/publications/MR/MR994/

Rosenau, James. 1990. *Turbulence in World Politics: A Theory of Change and Continuity*. Princeton, NJ: Princeton University Press.

Rosencrance, Richard. 1999. *The Rise of the Virtual State: Wealth and Power in the Coming Century*. New York: Basic Books.

Rosenheim, Shawn. 1997. *The Cryptographic Imagination: Secret Writing From Edgar Poe to the Internet*. Baltimore & London: Johns Hopkins University Press.

Ross, Andrew. 2000. 'Hacking Away at the Counter-Culture.' In David Bell & Barbara M. Kennedy (Eds.), *The Cybercultures Reader*. London & New York: Routledge.

Ross, Brian. 2001. 'A Secret Language: Hijackers May Have Used Secret Internet Messaging Technique.' *ABC News* 4 October. http://abcnews.go.com/sections/primetime/DailyNews/PRIMETIME_011004_steganography.html

Rothkopf, David J. 1998. ' Cyberpolitik: The Changing Nature of Power in the Information Age.' *Journal of International Affairs* 51(2).

Ruffin, Oxblood. 2004. 'Hacktivism, From Here to There.' Paper presented at the Cybercrime and Digital Law Enforcement Conference, Yale Law School, 28 March. http://www.cultdeadcow.com/cDc_files/cDc-0384.html

Rutherford, Kenneth R. 2002. 'Essential Partners: Landmines-Related NGOs and Information Technologies.' In Peter I. Hajnal (Ed.), *Civil Society in the Information Age*. Aldershot: Ashgate.

Ryan, Patrick S. 2004. 'War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics.' *Virginia Journal of Law & Technology* 9(7). http://ssrn.com/abstract=585867

Saad-Ghorayeb, Amal. 2002. *Hizbu'llah: Politics and Religion*. London: Pluto Press.

Said, Edward. 1997 [1981]. *Covering Islam*. London: Vintage.

Samuel, Alexandra. 2001. 'Digital Disobedience: Hacktivism in Political Context.'

Paper presented at the American Political Science Association (APSA) Annual Conference, San Francisco, California, USA, 29 September-2 August. http://www.alexandrasamuel.com/digitaldisobedience.pdf

Schattschneider, E.E. 1960. *The Semi-Sovereign People: A Realist's View of Democracy in America.* New York: Holt, Rinehart & Winston.

Scheeres, Julia. 2001a. 'Suppression Stifles Some Sites.' *Wired News* 25 October. http://www.wired.com/news/business/0,1367,47835,00.html.

Scheeres, Julia. 2001b. 'Blacklisted Groups Visible on Web.' *Wired News* 19 October.

Scheeres, Julia. 2002. 'Colombia's Cyber (Un)Civil War.' *Wired News* 4 March. http://wired-vig.wired.com/news/politics/0,1283,50748,00.html?tw=wn_story_related

Schiff, Ze'ev. 1984. 'Lebanon: Motivations and Interests in Israel's Policy.' *Middle East Journal* 38(2).

Schmid, Alex P. & Janny De Graaf. 1982. *Violence as Communication: Insurgent Terrorism and the Western News Media.* London: Sage.

Schmid, Alex P., and Albert J. Jongman. 1998. *Political Terrorism: A New Guide to Actors, Authors, Concepts, Databases, Theories and Literature.* Amsterdam: North-Holland Publishing Company.

Schmid. Alex P. 2004. 'Frameworks for Conceptualizing Terrorism.' *Terrorism & Political Violence* 16(2).

Schneier, Bruce. 2001. 'Terrorists and Steganography.' *CRYPTO-GRAM* (Special Issue) 30 September. http://www.schneier.com/crypto-gram-0109a.html

Schwartau, Winn. 1994. *Information Warfare: Cyberterrorism- Protecting Your Personal Security in the Electronic Age* (2nd Ed.). New York: Thunder's Mouth Press.

Schwartz, John. 2000. 'When Point and Shoot Becomes Point and Click.' *New York Times* 12 November. http://www.nytimes.com/2000/11/12/weekinreview/12SCHW.html?ex=1107406800&en=a9f1afabd947142e&ei=5070

Schwartz, John. 2001. 'Securing the Lines of a Wired Nation.' *New York Times* 4 October.

Schwartz, John. 2002. 'Case-Sensitive Crusader; Who Owns the Internet? You and i Do.' *New York Times* 29 December.

Schwartzstein, Stuart (Ed.). 1996. *The Information Revolution and National Security.* Washington DC: Center for Strategic & International Studies.

Segaller, Stephen. 1987. *Invisible Armies: Terrorism Into the 1990s*. Orlando, FL: Harcourt Brace Jovanovich.

Seib, Philip. 1997. *Headline Diplomacy: How News Coverage Affects Foreign Policy*. New York: Praeger.
Seib, Philip. 2004. *Beyond the Front Lines: How the News Media Cover a World Shaped by War*. Hampshire: Palgrave.

Sellars, Duncan. 1999. *An Introduction to Steganography*. South Africa: University of Cape Town.
http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html

Sher, H. 2000. 'Cyberterror Should be International Crime- Israeli Minister.' *Newsbytes* 10 November.

Shin, Natori. 2000. 'One-Time Hash Steganography.' *Lecture Notes in Computer Science* No. 1768.

Shirriff, Ken. 2001. 'The Anarchist Cookbook FAQ.'
http://www.righto.com/anarchist-cookbook-faq.html

Sieber, Ulrich. 2005. 'The Threat of Cybercrime.' In Council of Europe (Ed.), *Octopus: Organised Crime in Europe- The Threat of Cybercrime*. Strasbourg: The Council of Europe.

Singh, J.P. 2002. 'Information Technologies and the Changing Scope of Global Power and Governance.' In James N. Rosenau & J.P. Singh (Eds.), *Information Technologies and Global Politics*. Albany, NY: SUNY Press.

Singh, Simon. 2001. *The Cracking Codebook*. London: Harper Collins.

Sipress, Alan. 2004. 'An Indonesian's Prison Memoir Takes Holy War into Cyberspace.' *Washington Post* 14 December. http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html

Skibell, Reid. 2002. 'The Myth of the Computer Hacker.' *Information, Communication & Society* 5(3).

Smith, George. 2004a. 'The Recipe for Ricin: Examining the Legend.' *National Security Notes* 20 February. http://www.globalsecurity.org/org/nsn/nsn-040220.htm

Smith, George. 2004b. 'The Recipe for Ricin, Part II: The Legend Flourishes.' *National Security Notes* 4 March. http://www.globalsecurity.org/org/nsn/nsn-040304.htm

Smith, Gordon S. 2000. 'Reinventing Diplomacy: A Virtual Necessity.' *United States Institute of Peace: Virtual Diplomacy Report* (VDS6), February.
http://www.usip.org/vdi/vdr/gsmithISA99.html

Smolla, Rodney A. 2002. 'From Hit Man to Encyclopedia of Jihad: How to Distinguish Freedom of Speech from Terrorist Training.' *Loyola Entertainment Law Review* 22(2). http://elr.lls.edu/issues/v22-issue2/smolla.pdf

Soloway, Colin, Rod Nordland, & Barbie Nadeau. 2002. 'Hiding (and Seeking) Messages on the Web.' *Newsweek* 17 June. http://cert.uni-stuttgart.de/archive/isn/2002/06/msg00040.html

Soo Hoo, Kevin, Seymour Goodman, & Lawrence Greenberg. 1997. 'Information Technology and the Terrorist Threat.' *Survival* 39(3).

Spafford, Eugene. 2003. *Testimony before the US House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities* 24 July. http://commdocs.house.gov/committees/security/has205260.000/has205260_0f.htm

Specter, Michael. 2001. 'The Doomsday Click: How Easily Could a Hacker Bring the World to a Standstill?' *The New Yorker* 28 May.

Spencer, Alexander. 2006. 'Questioning the Concept of 'New' Terrorism.' *Peace, Conflict, & Development* Iss. 8. http://www.peacestudiesjournal.org.uk/docs/Feb%2006%20SPENCER%20version%202.pdf

Sreberny-Mohammadi, Annabelle & Ali Mohammadi. 1994. *Small Media, Big Revolution: Communication, Culture and the Iranian Revolution.* Minneapolis & London: University of Minnesota Press.

Staff Statement No. 9. 2004. *Law Enforcement, Counterterrorism, and Intelligence Collection in the United States prior to 9/11.* Washington DC: 9/11 Commission. http://www.9-11commission.gov/staff_statements/staff_statement_9.pdf

Staff Statement No. 11. 2004. *The Performance of the Intelligence Community.* Washington DC: 9/11 Commission. http://www.9-11commission.gov/staff_statements/staff_statement_11.pdf

Staff Statement No. 12. 2004. *Reforming Law Enforcement, Counterterrorism, and Intelligence in the United States.* Washington Dc: 9/11 Commission. http://www.9-11commission.gov/staff_statements/staff_statement_12.pdf

Stallings, William. 1998. *Cryptography and Network Security: Principles and Practice*. New Jersey: Prentice Hall.

Steinberg, Jacques. 2004. 'Ascent of USA Today Reporter Stumbled on Colleagues' Doubts.' *New York Times* 19 January.

Stern, Jessica. 1999. *The Ultimate Terrorists*. Cambridge, MA: Harvard University Press.

Still, Kathy. 2001. 'Wise County Circuit Court's Webcam 'Cracked' by Cyberterrorists.' *Bristol Herald Courier* 20 December.

Stohl, Michael. 1990. 'Demystifying the Mystery of International Terrorism.' In Charles Kegley (Ed.), *International Terrorism: Characteristics, Causes, Controls*. New York: St. Martins.

Stohl, Michael & George Lopez (Eds.). 1986a. *The State as Terrorist: The Dynamics of Governmental Violence and Repression*. Connecticut: Greenwood Press.

Stohl, Michael & George Lopez (Eds.). 1986b.*Government Violence and Repression: An Agenda for Research*. Connecticut: Greenwood Press.

Stoll, Clifford. 1991. *The Cuckoo's Egg*. London: Pan Books.

Stone, Andrea. 2001. 'Cyberspace: The Next Battlefield.' *USA Today* 16 June. http://www.usatoday.com/tech/news/2001-06-19-cyberwar-full.htm

Sullivan, John P. 2001. 'Gangs, Hooligans and, Anarchists: The Vanguard of Netwar in the Streets.' In John Arquilla & David Ronfeldt (Eds.), *Networks and Netwars*. California: Rand. http://www.rand.org/publications/MR/MR1382/MR1382.ch4.pdf

Swartz, Jon. 2001. 'Experts: Cyberspace Could Be Next Target', *USA Today*, October 16. http://www.usatoday.com/tech/news/2001/10/9/cyberwar-usat.htm

Swett, Charles. 1995. *Strategic Assessment: The Internet*. Washington DC: Department of Defense. http://www.fas.org/cp/swett.html

Swett, Charles. 1996. 'Revisiting *A Strategic Assessment of the Internet*.' *First Monday* 1(4). http://www.firstmonday.org/issues/issue4/swett/index.html

Szafranski, Richard. 1997 [1994]. 'Neocortical Warfare: The Acme of Skill?' In J. Arquilla & D. Ronfeldt (Eds.), *In Athena's Camp: Preparing for Conflict in the Information Age*. California: Rand. http://www.rand.org/publications/MR/MR880

Szumski, Bonnie (Ed.). 1986. *Terrorism: Opposing Viewpoints*. St. Paul, MN: Greenhaven Press.

Taylor, Paul A. 1999. *Hackers: Crime in the Digital Sublime*. London: Routledge.

Taylor, Philip M. 1992. *War and the Media: Propaganda and Persuasion in the Gulf War*. Manchester & New York: Manchester University Press.

Taylor, Philip M. 1995. *Munitions of the Mind: A History of Propaganda From the Ancient World to the Present Era*. Manchester & New York: Manchester University Press.

Taylor, Philip M. 1997. *Global Communications, International Affairs and the Media Since 1945*. London & New York: Routledge.

Taylor, Philip M. 1999. *British Propaganda in the Twentieth Century: Selling Democracy*. Edinburgh: Edinburgh University Press.

Taylor, Philip. 2004. 'Desert Storm Blowback: Psychological Operations in Operation Iraqi Freedom, 2003.' In Lars Nicander & Magnus Ranstorp (Ed.s), *Terrorism in the Information Age: New Frontiers?* Stockholm: National Defence College.
Technical Analysis Group. 2003. *Examining the Cyber Capabilities of Islamic Terrorist Groups*. Dartmouth College, New Hampshire: Institute for Security Technology. https://www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf.

Thomas, Amelia. 2005. 'When Games Become Propaganda.' *Middle East Times* 10 February. http://metimes.com/print.php?StoryID=20050210-051749-6506r

Thomas, Douglas. 2000. 'Finding a New Term: From "Hacking" to "Cybercrime."' *Online Journalism Review* 22 February.
http://www.ojr.org/ojr/ethics/p1017965933.php

Thomas, Timothy L. 2003. 'Al Qaeda and the Internet: The Danger of "Cyberplanning."' *Parameters* Spring. http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.htm

Thompson, Caroline. 2005. 'Software Would Scan Arabic Documents for Information.' *USA Today* 20 January.
http://www.usatoday.com/tech/products/software/2005-01-20-arabic-scans_x.htm

Tibbetts, Patrick S. 2002. 'Terrorist Use of the Internet and Related Information Technologies.' [Unpublished Paper]. Fort Leavenworth, Kansas: United States Army Command and General Staff College. http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=0&keyfieldvalue=ADA403802&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA403802.pdf

Toffler, Alvin. 1980. *The Third Wave.* London: Pan Books.

Toffler, Alvin. 1990. *Powershift*. New York: Bantam Books.

Townshend, Charles. 2002. *Terrorism: A Very Short Introduction.* Oxford: Oxford University Press.

Tsfati, Yariv & Gabriel Weimann. 2002. 'WWW.Terrorism.Com: Terror on the Internet.' *Studies in Conflict and Terrorism* Vol. 25: 317-332.

Tucker, David. 2001. 'What's New About the New Terrorism and How Dangerous Is It?' *Terrorism and Political Violence* 13(3).

Tucker, David. 2000. *The Future of Armed Resistance: Cyberterror? Mass Destruction?* (Conference Report). Monterey, CA: The Center on Terrorism and Irregular Warfare. http://www.nps.navy.mil/ctiw/files/substate_conflict_dynamics.pdf

Tuman, Joseph S. 2003. *Communicating Terror: The Rhetorical Dimensions of Terrorism*. Thousand Oaks: Sage.

Two Crows Corporation. 1999. *Introduction to Data Mining and Knowledge Discovery* (Third Ed.). Maryland: Two Crows Corporation. http://www.twocrows.com/intro-dm.pdf

US Department of Justice. 1997. *Report On The Availability of Bombmaking Information, the Extent to Which Its Dissemination Is Controlled by Federal Law, and the Extent to Which Such Dissemination May Be Subject to Regulation Consistent With the First Amendment to the United States Constitution.* Washington DC: US Department of Justice. http://cryptome.org/abi.htm.

US Department of State. 2003. *Patterns of Global Terrorism 2001.* Washington DC: Department of State. http://www.state.gov/s/ct/rls/pgtrpt/2003/

US Department of State. 2004. *Patterns of Global Terrorism 2003.* Washington DC: Department of State. http://www.state.gov/s/ct/rls/pgtrpt/2003/

Valeri, Lorenzo & Michael Knights. 2000. 'Affecting Trust: Terrorism, Internet and Offensive information Warfare.' *Terrorism and Political Violence* 12(1): 15-36.

Van De Donk, Wim, Brian Loader, Paul Dixon, and Dieter Rucht (Ed.s). 2003. *Cyberprotest: New Media, Citizens, and Social Movements*. London: Routledge.

Van Natta, Don & Desmond Butler. 2004. 'How Tiny Swiss Cellphone Chips Helped Track Global Terror Web.' *New York Times* 4 March. http://www.nytimes.com/2004/03/04/international/europe/04PHON.html?ex=1112932800&en=50df806d66af8ffb&ei=5070&hp=&pagewanted=all&position

Vatis, Michael. 2001. 'What is Cyber-Terrorism?' In Yonah Alexander & Michael S. Swetnam (Ed.s), *Cyber Terrorism and Information Warfare: Threats and Responses*. New York: Transnational Publishers.

Vegh, Sandor. 2002. 'Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking.' *First Monday* 7(10). http://firstmonday.org/issues/issue7_10/vegh

Vegh, Sandor. 2003. 'Classifying Forms of Online Activism: The Case of Cyberprotests Against the World Bank.' In Martha McCaughey & Michael D. Ayers (Eds.), *Cyberactivism: Online Activism in Theory and Practice*. London: Routledge.

Veltman, Chloe. 2001. 'Beating Cyber Crime.' *Daily Telegraph* 1 March. http://www.chloeveltman.com/features/technology/michael_vatis.html

Verton, Dan. 2003. *Black Ice: The Invisible Threat of Cyberterrorism*. New York: McGraw Hill.

Verton, Dan & Lucas Mearian. 2004. 'Online Data a Gold Mine for Terrorists.' *ComputerWorld* 6 August. http://www.computerworld.com/securitytopics/security/story/0,10801,95098,00.html

Vickers, Rhiannon. 2001. 'The New Public Diplomacy in Britain and Canada.' Paper presented at the British International Studies Association (BISA) Annual Conference, Edinburgh, UK.

Wæver, Ole. 1995. 'Securitization and Descuritization.' In Ronnie Lipschultz (Ed.), *On Security*. New York: Columbia University Press.
Wald, Matthew L. 2004. 'Toppled Power Lines are Posing a Herculean Task in Florida.' *New York Times* 19 August.

Wall, Melissa A. 2002. 'The Battle in Seattle: How Nongovernmental Organizations Used Websites in Their Challenge to the WTO.' In Eytan Gilboa (Ed.), *Media and Conflict: Framing Issues, Making Policy, Shaping Opinions*. New York: Transnational Publishers.

Wallace, Chris. 2002. 'Internet as Weapon: Experts Fear Terrorists May Attack Through Cyberspace.' *ABC News.com* 16 September. http://abcnews.go.com/sections/wnt/DailyNews/cyberterror020913.html

Waltz, Kenneth. 1979. *Theory of International Politics*. Reading, MA: Addison-Wesley.

Wardlaw, Grant. 1982. *Political Terrorism: Theory, Tactics, and Countermeasures*. Cambridge: Cambridge University Press.

Warner, Bernhard. 2003. 'Experts Comb Web for Terror Clues.' *The Washington Post* 12 November. http://cryptome.org/web-panic.htm

Wayland, Sarah. 2004. 'Ethnonationalist Networks and Transnational Opportunities: The Sri Lankan Tamil Diaspora.' *Review of International Studies* 30(3).

Wayner, Peter. 1996. *Disappearing Cryptography: Setting Up Networks with Hidden Communications*. Boston: AP Professional.

Webman, Esther. 1998. 'Anti-Semitic Motifs in the Ideology of Hizballah and Hamas.' Tel-Aviv University: Project for the Study of Anti-Semitism. http://www.ict.org.il/articles/articledet.cfm?articleid=51

Weimann, Gabriel. 1983. 'The Theatre of Terror: Effects of Press Coverage.' *Journal of Communication* 33(1).

Weimann, Gabriel & Conrad Winn. 1993. *The Theatre of Terrorism: Mass Media and International Terrorism*. Boston: Addison-Wesley.

Weimann, Gabriel. 2004a. *WWW.terror.net: How Modern Terrorism Uses the Internet*. Washington DC: United States Institute of Peace. http://www.usip.org/pubs/specialreports/sr116.pdf

Weimann, Gabriel. 2004b. 'Terror on the Internet: The New Arena, the New Challenges.' Paper presented at the annual meeting of the International Studies

Association (ISA), Montreal, Canada, 17 March. http://archive.allacademic.com/publication/prol_index.php

Weimann, Gabriel. 2004c. *Cyberterrorism: How Real is the Threat?* Washington DC: United States Institute of Peace. http://www.usip.org/pubs/specialreports/sr119.pdf

Weimann, Gabriel. 2006. *Terror on the Internet: The New Arena, the New Challenges*. Washington DC: United States Institute of Peace.

Weinberg, Leonard, Ami Pedahzur, & Sivan Hirsch-Hoefler. 2004. 'The Challenges of Conceptualizing Terrorism.' *Terrorism & Political Violence* 16(4).

Weisenberger, Kirsten. 2001. 'Hacktivists of the World, Divide.' *SecurityWatch.com* 23 April. http://www.thehacktivist.com/archive/news/2001/Hacktivists-SecurityWatch-2001.pdf

Weisman, Robin. 2001. 'Teen Hackers Crash Hizbollah ISP.' *NewsFactor* 22 January. http://www.newsfactor.com/perl/story/6880.html

West, Darrell M. 2001. *The Rise and Fall of the Media Establishment*. New York: Bedford/St. Martins.

Whine, Michael. 1999. 'Cyberspace: A New Medium for Communication, Command, and Control by Extremists.' *Studies in Conflict and Terrorism* Vol. 22, No. 3.

Whittaker, David J. (Ed.). 2001. *The Terrorism Reader*. London & New York: Routledge.

Whitaker, Brian. 2000. 'Hizbullah Seeks Friends.' *The Guardian* (UK) 1 June. http://www.al-bab.com/arab/countries/lebanon/hizbullah.htm

Whitaker, Brian. 2001. 'Hizbollah: Israel is an Illegitimate Entity.' *The Guardian* (UK) 12 March.

White, Brian. 2001. 'Diplomacy.' In John Baylis and Steve Smith (Eds.), *The Globalisation of World Politics* (2nd Ed.). Oxford: Oxford University Press.

Whittaker, David J. 2001. 'Lebanon.' In David J. Whittaker (Ed.), *The Terrorism Reader*. London: Routw

Whittaker, Jason. 2004. *The Cyberspace Handbook*. London & New York: Routledge.

Willan, Philip. 'Red Brigades' PDAs Highlight Encryption Controversy.' *ComputerWorld* 23 May. http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,81486,00.html

Willetts, Peter. 2001. 'Transnational Actors and International Organizations in Global Politics.' In John Baylis and Steve Smith (Eds.), *The Globalization of World Politics* (2nd Ed.). Oxford: Oxford University Press.

Williams, Grant. 2003. 'Advocacy Group's Online Savvy Nets More than Donations.' *The Chronicle of Philanthropy* 17 April. http://www.moveon.org/press/articles/chronicleofphilanthropy.pdf

Wray, Stefan. 1998. 'Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics.' Paper presented at The World Wide Web and Contemporary Cultural Theory Conference, Drake University, November.

Wright, Joanne. 1991. *Terrorist Propaganda: The Red Army Faction and the Provisional IRA, 1968-1986*. London: Macmillan.

Wriston, Walter. 1997. 'Bits, Bytes, and Diplomacy.' *Foreign Affairs* 76(5).

Wriston, Walter. 1988. 'Technology and Sovereignty.' *Foreign Affairs* 67(2).

Wynne, Jeff. 2002. 'White House Advisor Richard Clarke Briefs Senate Panel on Cybersecurity.' *Washington File* 14 February. http://www.iwar.org.uk/news-archive/2002/cip/02-14-02.htm

Yould, Rachel. 2003. 'Beyond the American Fortress: Understanding Homeland Security in the Information Age.' In Robert Latham (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*. New York: New Press.

Zanini, Michele. 1999. 'Middle Eastern Terrorism and Netwar.' *Studies in Conflict and Terrorism* 22(3).

Zeller, Tom. 2004. 'On the Open Internet, a Web of Dark Alleys.' *New York Times* 20 December. http://lists.jammed.com/ISN/2004/12/0066.html

Zimmermann, Doron. 2003. *The Transformation of Terrorism*. Zurich: ISN. http://www.isn.ethz.ch/crn/_docs/ACF88.pdf