

Contents

| | |
|---|------|
| Foreword <i>by Bruce Hoffman</i> | ix |
| Acknowledgments | xiii |
| Introduction | 3 |
| 1. New Terrorism, New Media | 15 |
| 2. The War over Minds: The Psychology of Terrorism | 33 |
| 3. Communicative Uses of the Internet for Terrorism | 49 |
| 4. Instrumental Uses of the Internet for Terrorism | 111 |
| 5. Cyberterrorism: How Real Is the Threat? | 147 |
| 6. Fighting Back: Responses to Terrorism on the Internet, and Their Cost | 173 |
| 7. Balancing Security and Civil Liberties | 203 |

| | |
|---|-----|
| Appendix: Terrorist Organizations on the Internet | 243 |
| Notes | 249 |
| Index | 281 |
| About the Author | 309 |

Introduction

IN THE WAKE OF THE SEPTEMBER 11, 2001, TERRORIST ATTACKS, a single question seemed to arise from all quarters: how could U.S. authorities and intelligence agencies have failed so completely to detect the plot? Despite many unknowns, a common thread runs through most of the explanations, the FBI reports, and the numerous analyses: the Internet played a key role in the terrorists' attack—in collecting information, in communications between the various terrorist cells and individuals, and in coordinating and executing the attacks. The hard evidence is overwhelming:

FBI assistant director Ron Dick, head of the US National Infrastructure Protection Centre told reporters that the hijackers had used the Net, and “used it well.” In one instance, two of the hijackers equipped with laptops would not check into a Hollywood, Florida, hotel unless they had around-the-clock Internet access in their room. When the terrorists learned that such access was not available, they became angry and left. The terrorists also used the Internet to purchase “at least nine of their [airline] tickets for the four doomed September 11 flights.” The terrorists frequently used computers at public libraries to access the

Internet and used the Web to steal social security numbers and obtain fake drivers' licenses.¹

The events on 9/11 revealed to a shocked world that terrorism had entered a new era and a new arena. This book explores this new arena, examining the ways in which modern terrorist organizations exploit the unique attributes of the Internet and looking at various counterterrorism measures being applied to the Net. In turning the spotlight on cyberterrorists and exploring the efforts to stop them, we must also take into account the costs of this cyberwar in terms of civil rights. The following research questions have guided this study:

- Who are the terrorists of the Internet?
- How do terrorists use the Internet?
- What rhetorical devices do terrorist Web sites use?
- Who are the target audiences of terrorist sites?
- What counterterrorism measures are in place on the Internet, and how successful are they?
- What are the costs of such measures in terms of privacy and freedom of expression?

The material presented in this book is drawn from an ongoing study, during which the author has witnessed a growing and increasingly sophisticated terrorist presence on the World Wide Web. Terrorism on the Internet is a very dynamic phenomenon: Web sites suddenly emerge, frequently modify their formats, and then swiftly disappear—or, in many cases, *seem* to disappear but actually have only moved by changing their online address, while retaining much of the same content. In exploring this new arena, this study draws on several sources, databases, and methods. The databases used for this project are derived from eight years of monitoring and archiving terrorists' Web sites (1998–2005) and from public opinion surveys (U.S. national samples) conducted by the Pew Internet and American Life Project. The study of counterterrorism measures on the Net and their prices in terms of civil liberties and privacy relies on a survey of various organizations and agencies.²

Two earlier studies serve as pilot studies for the current project: Yariv Tsfati and the present author applied a systematic content analysis

to a sample of terrorist sites in 1998 and repeated this analysis after three years.³ These exploratory studies provided the methodological tools as well as the first evidence both of the diffusion of terrorism into the Internet and of the terrorists' growing sophistication. The method used to study Web sites was content analysis, which is defined as "any technique for reaching conclusions by systematic and objective identification of defined properties of messages."⁴ To locate the terrorists' sites, we conducted numerous systematic scans of the Internet, feeding an enormous variety of names and terms into search engines, entering chat rooms and forums of supporters and sympathizers, and surveying the links on other organizations' Web sites to create and update our own lists of sites. This is often a Herculean effort, especially since (in the case of al Qaeda's Web sites, for example) locations and contents change almost daily. For the purposes of this book, the Internet was scanned again, in 2003–05. The target population for the current study was defined as "the Internet sites of terrorist movements as they appeared in the period between January 1998 and May 2005." Using the U.S. State Department's list of terrorist organizations (see the appendix),⁵ we found more than 4,300 sites serving terrorists and their supporters.

The Structure of This Book

Chapter 1 of this volume, "New Terrorism, New Media," starts with a brief history of the Internet. Ironically, this medium originated from the Cold War and U.S. security services' fears about the vulnerability of strategically vital communications networks to a nuclear attack. Decades later the Internet has become a handy tool of one of Western security's scariest foes: modern-day terrorists. As new communication technologies have emerged, terrorism has kept pace, constantly changing its character and modes of operation, so that today's postmodern terrorism has a new face. It is less centralized, less structured, and less organized, yet far more dangerous than the terrorism of the late twentieth century. In this chapter we will review the attributes of postmodern terrorism and how it depends on modern communication technologies to maintain its decentralized structure, launch global attacks, and control a loosely knit network of operatives and supporters.

We then examine the advantages of using the Net for political activism, and how some political groups and national minorities with Internet access have begun to challenge the state's domination of political discourse and political culture, both of which have traditionally been maintained through the state's control of the media and through its monopoly on the media and education systems. Thus, the Internet's attraction for modern terrorists should come as no surprise: the more severely the interests of a minority group have been ignored, the more attractive the Internet will be for that group. The study distinguishes between various abuses and abusers of the Internet—between, for example, the commonly confused potential and actual damage inflicted by cyberterrorists, and between the relatively benign activities of most hackers and the specter of true cyberterrorism.

Chapter 2, "The War over Minds: The Psychology of Terrorism," gives the theoretical and conceptual framework for this research. Terrorism is a form of psychological warfare, the word itself stemming from "terrorize," meaning "to frighten" or "to scare." Terrorism seeks to threaten a society by spreading fear, distrust, and a sense of helplessness among its citizens. We review the history of psychological warfare and demonstrate how modern terrorism has learned the lessons of state-operated terror campaigns, using the same weapon of psychological warfare with growing sophistication and impact. It is clear that such psychological impact relies on the mass media: the desired panic is produced via a constant broadcasting, by radio and television, videos, and the Internet, of vicious acts, threats, and declarations—all according to the familiar, tried-and-true methods of psychological warfare.

This leads us to an examination of the media's role in modern terrorism, applying the theory of "terrorism as theater." The theater metaphor is used to examine modern terrorism as an attempt to communicate messages through the use of orchestrated violence.⁶ As we suggest, the growing use and manipulation of the mass media by terrorist organizations led governments and several media organizations to consider certain steps in response. These included limiting terrorists' access to the conventional mass media, reducing and censoring news coverage of terrorist acts and their perpetrators, and minimizing the terrorists' capacity for manipulating the media. However, new media technologies, especially computer-mediated communication and the Internet, allow ter-

rorist organizations to transmit messages more easily and freely than through other means of communication. Finally, this chapter examines the advantages that the Internet provides to modern terrorism, ranging from easy access and rapid flow of information to multimedia applications. Web sites are only one of the Internet applications used for terrorism; many terrorists are adept at manipulating other services on the Net, including e-mail, chat rooms, e-groups, forums, online magazines, virtual message boards, and online manuals and guidebooks. It is especially this interactive aspect of the Internet that enables terrorists to activate their audiences in a manner and to a degree unachievable by other mass media.

In chapter 3, "Communicative Uses of the Internet for Terrorism," we see how terrorist organizations are increasingly using the Internet for communication purposes from propaganda and dissemination of messages to psychological warfare. Numerous organizations have entered cyberspace and created Internet sites. The search for Internet-based organizations reveals much about the identities and characteristics of those groups and movements that use this new communication channel. In this chapter we present the scope and content of terrorist Web sites, their messages and rhetoric, target audiences, and persuasive appeals. Who do the terrorist Web sites target? Are they appealing to potential supporters, to their enemies (namely, the public who is part of the opposing sociopolitical community in the conflict), or to international public opinion? Judging from the content of many of the sites, we infer that journalists constitute another target audience. Our findings reveal a proliferation of radical Islamic Web sites. This is not a methodological bias but rather a significant trend highlighted in our study. This study explores how the freedom offered by the Internet is vulnerable to abuse from groups that, paradoxically, are themselves hostile to uncensored thought and expression, and how extreme anti-Western and antimodernity forces are using the most sophisticated tools of modern Western culture.

Applying the theory of selective moral disengagement to terrorist Web sites, we reveal their use of all the various disengagement practices, including displacement of responsibility, diffusion of responsibility, dehumanization of targets, euphemistic language, advantageous comparisons, distortion of sequence of events, and attribution of blame. The most popular theme is the displacement of responsibility: violence is presented as a necessity foisted upon the weak as the only means for dealing with

an oppressive enemy. The blame is thus attributed to others. Another rhetorical structure used to legitimize violence is the demonizing and delegitimizing of the enemy by shifting the responsibility to the enemy and displaying his brutality, inhumanity, and immorality: "Terrorist rhetoric on the Internet tries to present a mix of images and arguments in which the terrorists appear as victims forced to turn to violence to achieve their just goals in the face of a brutal, merciless enemy devoid of all moral restraint. Demonizing the enemy, playing down the issue of terror victims, shifting blame for the use of violence, and proclaiming peace-loving messages are all strategies used on most terror sites."⁷

As illustrative examples, this chapter presents a more detailed analysis of several groups' presence on the Net. We chose them because they represent a variety of motives, locations, types of action, and aggression levels and because each has an impressive presence on the Net. The use of the Internet for conveying terrorist propaganda is well illustrated by the Web site of the Japanese Aum Shinrikyo (meaning "Supreme Truth"). Another section focuses on the "phoenix of the Internet": al Qaeda and its numerous Web sites. We see how this widespread network of Web sites is used by al Qaeda's leaders to spread information, incitement, and instructions to supporters and sympathizers around the world. Al Qaeda publishes several online magazines, including *Sawt al-Jihad*, or *The Voice of Jihad*, highlighted in this chapter because it serves as al Qaeda's tool of ideological indoctrination. All the attempts to prevent al Qaeda from using the Internet are futile. If one Web site is hacked or removed from the Net, many others will surface, using other service providers, new URLs, and new formats. Our study describes how al Qaeda changes its Web site names and URLs every few days to avoid being hacked, and how it directs followers and supporters to these new sites. Other case studies of Internet-based campaigns of propaganda and indoctrination include FARC (Revolutionary Armed Forces of Colombia), Hamas, Hezbollah, the IRA splinter groups, and the insurgents in Iraq. Finally, this chapter discusses the impact of these campaigns, suggesting several indirect measures to assess the real effectiveness and impact of terrorist uses of the Internet, including testimonies of terrorists and affected individuals.

Along with communicative uses, terrorists also use the Internet for practical purposes: chapter 4, "Instrumental Uses of the Internet for

Terrorism,” presents seven different, though sometimes overlapping, means by which contemporary terrorists take advantage of the Internet for such purposes. Some of these parallel the uses to which everyone puts the Internet—information gathering, for instance. Some resemble the uses made of the medium by traditional political organizations—for example, raising funds and coordinating actions. Others, however, are much more unusual and distinctive—for instance, hiding instructions, manuals, and directions in coded messages or encrypted files. The Internet may be viewed as a vast digital library. It offers more than a billion pages of information, much of it free and much of it of interest to terrorist organizations. Terrorists, for instance, can learn from the Internet about the schedules and locations of targets such as transportation facilities, nuclear power plants, public buildings, and air- and seaports, and can even reveal and preempt or avoid counterterrorism measures. This chapter presents evidence of the data mining done by Internet-savvy terrorists and looks at the numerous tools that are available to facilitate such data collection, including search engines, e-mail distribution lists, chat rooms, and discussion groups. While some of this information may also be available in the traditional media, online searching capabilities allow terrorists to capture it anonymously and with very little effort or expense.

Other instrumental uses of the Internet for modern terrorists include the sharing and distribution of information, instructions, manuals, and guidebooks. The World Wide Web is home to dozens of sites that provide information on how to build explosive and chemical weapons, providing maps, photographs, directions, codes, and technical details of how to use explosives. The Internet can serve as a virtual training camp, as illustrated by al Qaeda’s *Al Battar Training Camp*. This bimonthly online magazine contains detailed articles on cell organization and management, weapons training, physical fitness, and even wilderness survival training. Some issues focus on how to conduct kidnapping operations, negotiate release of hostages, and collect information on targets. The Internet, as this chapter demonstrates, was used for networking terrorists, coordinating attacks, and planning actions including the attacks of September 11, 2001, as well as those of March 11, 2004, in Madrid and of July 2005 in London. The Internet is used to recruit and mobilize supporters to play a more active role in supporting terrorist activities or

causes. In addition to seeking converts by using the full panoply of Web site technologies (audio, digital video, and so on) to enhance the presentation of their message, terrorist organizations capture information about the users who browse their Web sites (culled, for instance, from personal information entered on online questionnaires and order forms). Users who seem most interested in an organization's cause or who are well suited to carrying out its work are then contacted. Here we also explore the sophisticated methods used by terrorists to refine or customize recruiting techniques on the Net.

Like many other political organizations, terrorist groups use the Internet to raise funds. We reveal how the Internet allows terrorists to identify users sympathetic to a particular cause or issue. These individuals are then asked to make donations, typically through e-mails sent by a front group (an organization broadly supportive of the terrorists' aims but operating publicly and legally, and usually having no direct ties to the terrorist organization). Finally, the Internet serves as a battlefield between and within terrorist organizations, which use the Net to conduct ideological debates or even personal disputes and internal power struggles, some of which are discussed in this chapter.

Chapter 5, "Cyberterrorism: How Real Is the Threat?," is devoted to the scariest scenario: using the Internet as a weapon of terrorism. The growing reliance of modern society on information technology has created a new form of vulnerability, giving terrorists the chance to approach targets that would otherwise be utterly unassailable, such as national defense systems, nuclear plants, and transportation control systems. The threat posed by cyberterrorism has grabbed headlines and the attention of politicians, security experts, and the public. But just how real is the threat? Could terrorists cripple critical military, financial, and service computer systems? This chapter charts the rise of cyberangst and examines the evidence cited by those who predict imminent catastrophe. Many of these fears, the chapter contends, are exaggerated: not a single case of cyberterrorism has yet been recorded, hackers are regularly mistaken for terrorists, and cyberdefenses are more robust than is commonly supposed. Even so, the potential threat is undeniable and seems likely to increase, making it all the more important to address the danger without inflating or manipulating it.

This chapter examines the reality of the cyberterrorism threat, present and future. It begins by outlining why cyberterrorism angst has gripped so many people, defines what qualifies as “cyberterrorism” and what does not, and charts cyberterrorism’s appeal for terrorists. The text then looks at the evidence both for and against Western society’s vulnerability to cyberattacks, drawing on a variety of recent studies and publications to illustrate the kinds of fears that have been expressed and to assess whether we need to be so concerned. The conclusion looks to the future and argues that we must remain alert to real dangers while not becoming victims of overblown fears.

In chapter 6, “Fighting Back: Responses to Terrorism on the Internet, and Their Cost,” we examine the war on terrorism as it is being waged on the Net. Up to now, most of the counterterrorism effort has been devoted to tracking down the terrorist networks, the perpetrators of terrorist attacks, and the transfer of money and funds. This chapter describes the post-9/11 counterterrorism measures on the Net, including the USA PATRIOT Act and the Domestic Security Enhancement Act of 2003, or “PATRIOT II,” as it has been labeled informally, which expand surveillance power, increase government access to private data, and broaden the definition of “terrorist activities.” We describe the United States’ Internet-wide monitoring center, which “detects and responds to attacks on vital information systems and key e-commerce sites.”⁸ According to the *Washington Post’s* Brian Krebs, this center “is a key piece of the White House’s national cybersecurity strategy and represents a major leap in the federal government’s effort to achieve real-time tracking of the Internet.”⁹

As we study Internet security and the legal measures to protect it, Asian countries may provide a useful and perhaps alarming example. Governments in Asia have become increasingly interested in cybersurveillance, both to monitor and to intimidate Internet users. The Singapore government’s system of Internet control has been a model for authoritarian states in Asia, and so we discuss the Singaporean model in particular. Then we explore the routine U.S. monitoring of e-mail traffic, presenting and explaining various monitoring procedures and techniques such as “sniffers,” Carnivore (DCS1000), Magic Lantern, Echelon, and others. We also discuss the criticism of these measures as abusing privacy or civil liberties. Another counterterrorism measure applied to

the Net is the removal of specific Web sites (entirely or partially) from the Internet. Is this removal of information from Web sites an efficient step in combating terrorism? As this chapter reveals, not really. Finally we examine cyberattacks against terrorist Web sites, and the banning of them, as relatively futile attempts to restrict terrorists' access and exposure.

The most important challenge presented to modern democracies by terrorism is addressed in chapter 7, "Balancing Security and Civil Liberties." Since September 11, 2001, many governments have sought ways to limit or minimize terrorists' use of the Internet. These measures have inspired fears among civil libertarian activists. It has been said that the first casualty of war is truth. In the digital war on terrorism, however, the first victim may be our civil liberties. In this chapter we review the counterweight of counterterrorism: while some argue that we must surrender some freedoms in order to enjoy the ones we cherish most, others emphasize the price in freedom that we pay for this war. Many in the Western world and especially in the United States worry about the abuse of civil liberties in the name of fighting terrorism. We review some of these voices of concern and their calls for some important modifications to the surveillance system of the Net.

We also discuss the missed opportunities: demonizing the Internet as a terrorist tool diverts our attention from its potential for nonviolent management of conflicts and for virtual diplomacy. The Internet furnishes advocacy groups and individuals with a free, easy-to-access mass medium where they can publish information to further policy objectives and present political grievances in nonviolent forms. The Zapatistas in Mexico represent one of the most successful examples of the positive use of computer communications by grassroots social movements. When activists turn to the Internet and use it efficiently to disseminate information, attract support and sympathy, and transform their conduct of the conflict, a traditional guerrilla insurgency is changed into a nonviolent political campaign.

Another missed opportunity presented in this chapter is virtual diplomacy. Computer-mediated communication can serve as an ideal channel for supporting good governance or managing international conflicts and crises effectively and expediently. A good example, though sadly one of very few, is the United States Institute of Peace's initiative on peace in Liberia; another virtual approach to training for peace is the use of com-

puter simulation to create peace support operations. The potential for virtual diplomacy, however, has yet to be fully employed.

The book concludes with policy recommendations. We should recognize that terrorism has been around for thousands of years and is not likely to go away soon. Modern societies, it appears, will have to learn to live with some terrorism, which leads to the issue of trade-offs between securing our safety and securing our liberties. Thus, a more realistic way to protect the Internet, prevent its abuse by terrorism, and at the same time protect civil liberties is to look for the “golden path,” or best compromise. This means that we will have to accept both some vulnerabilities of the Internet to terrorism and some constraints on civil liberties; the underlying guidelines, determined by examining the trade-offs between securing our safety and securing our liberties, should minimize the threats to both. Among the recommendations presented here for following that golden path to a balanced “middle ground” are modifying the USA PATRIOT Act, encouraging self-policing of the Internet, applying the social responsibility model, developing international collaboration, building a proactive presence on the Internet, and promoting peaceful uses of the Internet.