

2004

# The threat of cyberterrorism: Contemporary consequences and prescriptions

Galen Asher Thomas Stocking

Follow this and additional works at: <https://scholarworks.lib.csusb.edu/etd-project>

 Part of the [Defense and Security Studies Commons](#), and the [Information Security Commons](#)

---

## Recommended Citation

Stocking, Galen Asher Thomas, "The threat of cyberterrorism: Contemporary consequences and prescriptions" (2004). *Theses Digitization Project*. 2590.

<https://scholarworks.lib.csusb.edu/etd-project/2590>

This Thesis is brought to you for free and open access by the John M. Pfau Library at CSUSB ScholarWorks. It has been accepted for inclusion in Theses Digitization Project by an authorized administrator of CSUSB ScholarWorks. For more information, please contact [scholarworks@csusb.edu](mailto:scholarworks@csusb.edu).

THE THREAT OF CYBERTERRORISM: CONTEMPORARY CONSEQUENCES  
AND PRESCRIPTIONS FOR THE FUTURE

---

A Thesis  
Presented to the  
Faculty of  
California State University,  
San Bernardino

---

In Partial Fulfillment  
of the Requirements for the Degree  
Master of Arts  
in  
National Security Studies

---

by  
Galen Asher Thomas Stocking

June 2004

THE THREAT OF CYBERTERRORISM: CONTEMPORARY CONSEQUENCES  
AND PRESCRIPTIONS FOR THE FUTURE

---

A Thesis  
Presented to the  
Faculty of  
California State University,  
San Bernardino

---

by  
Galen Asher Thomas Stocking  
June 2004

Approved by:

  
\_\_\_\_\_  
Ralph Salmi, Chair, Political Science

  
\_\_\_\_\_  
William Green

  
\_\_\_\_\_  
Brian Levin

6/4/04  
Date

## ABSTRACT

This study researches the varying threats that emanate from terrorists who carry their activity into the online arena. It examines several elements of this threat. First, it explores elements of virtual to virtual attacks. Second, it looks at threats against critical infrastructures that can be traced to online sources. Third, this thesis reports on ways that terrorists are using information technology such as the Internet for propaganda and communication purposes. Finally, it highlights the most crucial ways in which the United States government has responded to the problem. It concludes with a few recommendations for best practices for future engagement with varying aspects of cyberterrorism.

## ACKNOWLEDGMENTS

This paper would not have been written without the constant urging and support of a number of people. Foremost among these, Dr. Ralph Salmi convinced me that my interest and talent in the field was sufficient to fill the gap in the scholarly literature. Dr. William Green and Dr. Brian Levin graciously agreed to serve on my advisory panel and have offered a number of incredibly useful insights. Ms. Debbie Fox has assisted me with paperwork that would have otherwise never gotten done.

Ms. Kelli Bissett did a wonderful job editing the varying drafts and urging me to continue when the end seemed out of reach. Likewise, Ms. Ann Marie Butler provided immeasurable help with editing and formatting. Ms. Christine McCowan helped with organization and put up with my mess. Mr. Michael Hillard and Mr. Dino Bozonelos consistently offered insight and listened to my complaints. Finally, my mother provided me the support without which this entire degree would have been out of reach.

## TABLE OF CONTENTS

ABSTRACT . . . . .	iii
ACKNOWLEDGMENTS . . . . .	iv
CHAPTER ONE: INTRODUCTION . . . . .	1
Definitions . . . . .	2
Literature Review . . . . .	7
Statement of the Problem . . . . .	11
Purpose of the Study . . . . .	14
Theoretical Basis and Organization . . . . .	14
Methodology . . . . .	18
Limitations of the Study . . . . .	22
CHAPTER TWO: VIRTUAL-TO-VIRTUAL ATTACKS . . . . .	23
Flooding and Denial of Service Attacks . . . . .	24
Worms and Viruses . . . . .	32
Web Site Defacement . . . . .	37
Conclusion . . . . .	42
CHAPTER THREE: THREATS TO CRITICAL INFRASTRUCTURE . . . . .	44
CHAPTER FOUR: THE INTERNET AS A COMMUNICATIONS DEVICE . . . . .	55
Online Terror Groups . . . . .	56
Steganography: A Case Study . . . . .	68
Conclusions . . . . .	84
CHAPTER FIVE: GOVERNMENT REACTIONS . . . . .	87

U.S. Reactions . . . . .	89
Conclusions . . . . .	99
CHAPTER SIX: CONCLUSIONS AND PRESCRIPTIONS . . . . .	101
APPENDIX A: GLOSSARY . . . . .	108
APPENDIX B: STUDY OF CYBERTERRORISM IN TERRORISM TEXTS . . . . .	113
APPENDIX C: RESULTS OF STEGANOGRAPHY TESTS . . . . .	117
ENDNOTES . . . . .	119
SELECTED BIBLIOGRAPHY . . . . .	139

CHAPTER ONE  
INTRODUCTION

The emergence of the post-modern era has brought with it incredibly bounty. Communication, facilitated by technologies like the Internet, has reached nearly instantaneous speeds - and this has positively impacted all sectors of the economy, from health care to banking. Arguably as a result of this technological mastery, post-industrial societies like that found in the United States have been able to elevate their political, social and economic position in the international community to unprecedented heights.

But just as communication technology brings promise of new hope for the present and future, it carries unforeseen dangers. Accessibility and convenience are easily exploited by those with nefarious intent. More menacing, the sacrifice of traditional values and the marginalization of social sectors that coincide with major societal shifts create a class of disaffected peoples for whom hope lies out of reach. Often, the brightest glimmers shine from extremist rhetoric, the devolution of which often leads to

fatalist action. Without other avenues of recourse, many lend a hand to support terrorism.

Terrorism, then, has increasingly become one of the gravest threats to the modern social order. It is not a monolithic entity, however. The broader term "terrorism" generally incorporates a variety of struggles, from nationalist efforts to millennial, religion-based ideologies. Furthermore, many terrorist actions are often confused with simple criminal acts, and distinguishing between them is often difficult. In order to proceed with a discussion of terrorism, then, a few definitions are required. From these, one can derive a working version of cyberterrorism, which will serve to facilitate the discussion at hand.

#### Definitions

Any discussion of terrorism cannot be effective without an initial definition of terms. Neither the international scholarly nor law enforcement communities have ever reached a consensus on a definition of "terrorism;" instead, agencies and scholarly journals use the definition that best suits their needs. The United

States Federal Bureau of Investigation (FBI), for example, defines terrorism as

“...the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”<sup>1</sup>

There are several key components to this definition.

First, it requires that terrorism incorporate force or violence. Second, both persons and property can be targeted. Third, the goal of the attack must be to coerce a government or society to adopt the perpetrator's political goal. This last component, in particular, is often the cause of overlap between terrorism and less threatening but equally potent political activism that turns violent.

There is no contiguity in definition even among branches of the U.S. government. In its 2003 *Patterns of Global Terrorism* report, the U.S. State Department employs the following definition, taken from Section 2656f(d) of Title 22 of United States Code:

The term terrorism means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.<sup>2</sup>

The primary difference between the State Department's definition and the FBI's rests in the classification of the actual attackers. Other agencies, like the U.S. Department of Defense, expand terrorism to include threats.<sup>3</sup> Academia suffers the same problem, with a wide range of definitions obscuring any resolution or compromise. In 2003, Ayla Schbley attempted to resolve this debate with a rather simple definition. Terrorism, in Schbley's view, is simply "any violent act upon symbolic civilians and their properties."<sup>4</sup>

Such a definition may in fact be too simple, since it avoids many of the specifics that delineate terrorism from regular crime - most notably the political motivations behind the actions. So instead of attempting to reach a clearly articulated definition, this paper merely incorporates the components above into a loose meaning. Terrorism, then, is motivated by political change, is often attributed to non-state actors, and involves violence against an individual, society, or property.

According to Mark Juergensmeyer, millennial terrorism, such as the world is facing from groups like al-Qaeda, seeks attacks that will result in the most destruction, thereby creating the most press for them and their cause.<sup>5</sup> A

"computer bomb" is not as photogenic as its dynamite based counterpart. Computer based attacks are often not readily noticeable; when they are, their complicated nature often does not allow for newspaper-selling headlines.

Since it does not generate media coverage, there is an implication that cyberterrorism is not a viable means of attack for terrorists. First, it often is hard to classify as violence. Even when targeted against critical infrastructure, it often does not cause death. As Chapter Three will show, only one cyber-based attack has caused widespread damage. Second, and more important, many other areas of cyberterrorism may remain in the area of activity that seems innocuous. For example, defacing a website is, in many ways, akin to little more than graffiti on a highway overpass. It is often expressive, but is usually cleaned up so quickly that it has little to no impact.

But perhaps this is ignoring a more important issue: the intent of known terrorists. Two tapes released by Al Qaeda in 2002 - one featuring leader Osama bin Laden, the other his right-hand man, Ayman Al-Zawahiri - called upon their troops to attack Western economic targets.<sup>6</sup> Although consistent with Al Qaeda's grand strategy,<sup>7</sup> this represents

a shift in tactics. Cyberspace provides a unique avenue for just such an attack, or the planning thereof.

One of the most prevalent definitions offered for cyberterrorism comes from Pollitt:

“...cyber terrorism is the premeditated, politically motivated attack against information, computer systems, and data which result in violence against noncombatant targets by sub national groups and clandestine agents.”<sup>8</sup>

This definition, like many others, only includes attacks. It therefore excludes those who may be preparing for an attack - a requirement for several techniques, including Denial of Service. Journalist Ann McFeatters addresses this issue in a limited manner, claiming that cyberterrorism is “...the intentional use of the computer to cause panic by destabilizing the U.S. economy or playing havoc with computer data systems.”<sup>9</sup> This definition, at least, allows for vagueness - an important factor in a situation that constantly evolves.

A loose definition seems appropriate here as well. In this text, cyberterrorism generally incorporates online activity that seeks to promote the political causes or ideology of conventional terrorism. Individuals or groups perpetrating these activities can be linked to terrorist groups, but they are often merely sympathizers.

Cyberterrorist activities as classified range from propaganda to devastating attacks on critical infrastructure; restricting the phenomenon to just a few tactics, however, neglects its ability to take on new forms. At the same time, however, a loose definition such as this allows the lines between terrorism and other, more legitimate forms of speech to blur more easily. This must be taken into account whenever an action is deemed terrorism.

A few other definitions are important. Hacktivism is hacking in the name of an activist cause.<sup>10</sup> Hacktivism can be found in the examples of the Zapatista movement in Mexico<sup>11</sup> and the online Hacktivismo community.<sup>12</sup> Netwar is an organizational structure in which the interconnectivity of modern technology allows for less hierarchy.<sup>13</sup> Denial of Service (DoS) attacks are the attempt to neutralize a network by flooding it with unnecessary information. Further definitions can be found in Appendix A.

#### Literature Review

Scholarly attention to the problems of cyberterrorism has been unnecessarily limited. Many of the books and articles produced have come from a few prominent computer

scientists, although a limited number of political scientists have addressed the issue as well. Usually, though, terrorist experts address cyberterrorism in passing, as an emerging threat that needs to be addressed. In many ways, this is a result of the youth of the threat itself; computers and the Internet have only become ubiquitous components in Western society in recent years. By neglecting this threat, however, terrorism scholars have allowed industry and media sources to set the tone. Consequently, any cyberterrorism study has to answer to the sensationalism raised by the media or security experts, each of which stands to profit from increased attention to the issue and could therefore be less than scrupulous in their comments and predictions. This study attempts to overcome this scholarly deficiency and fill that gap.

Before delving into the specifics of the texts that are available, though, a few statistics are required to illustrate just how little research is available. In late April 2004, a study conducted against prominent scholarly article databases found an incredibly low number of articles dealing with cyberterrorism; similar queries of media sources returned completely opposite results.

The first study was conducted on EbscoHost, a repository of over 3,500 peer-reviewed academic journals.<sup>14</sup> A search for "cyberterrorism" on this database reported 18 hits - but many of these are from the same journal issue. Five articles were printed in *American Behavioral Scientist's* February 2002 issue, which was dedicated solely to cyberterrorism. Likewise, several articles produced by this search came from the July 2002 issue of the *Information Management Journal*; however, these articles were all relatively short, (one to two pages), and so they were not of substantial length to provide a serious and in-depth study.<sup>15</sup> A similar search of academic database search engine WilsonWeb produced only fifteen hits, whereas a competitor, JStor, returned zero results.<sup>16</sup> Opposingly, news and media databases were rich with content. The same search on LexisNexis, a news database, only allows 125 results at a time; in this case, it maxed this allotment out.<sup>17</sup> Factiva, a similar system, has no such limitations on its searches. It found 1,236 articles on cyberterrorism in the two years from April 2002 to April 2004.<sup>18</sup>

This problem is not limited to journals, however; standard terrorism or national security books fared little better. A survey of 25 contemporary works on terrorist

found that only five books listed cyberterrorism in their index - and the most any of them dedicated to the topic was six pages.<sup>19</sup> Similarly, Jonathon White's beginner's guide to terrorism only spent seven paragraphs on the issue.<sup>20</sup>

Obviously, little has been done in the scholarly community to ensure that the issue of cyberterrorism has been properly addressed. That does not mean, however, that there are no articles. The few that do exist provide a foundation, however weak, upon which this study has been built.

These articles and books can generally be classified into just a few categories. Many, like James Ballard, et al's "Technological Facilitation of Terrorism,"<sup>21</sup> are aimed at providing a comprehensive survey of the topic. Some use this general survey approach as a means to address a specific facet of the problem. Michael Whine's "Cyberspace - A new Medium for Communication, Command and Control by Extremists"<sup>22</sup> uses this approach to describe the communications component of cyberterrorism. This works both ways: Gary Bunt uses cyberterrorism to explore Islam's presence online.<sup>23</sup>

Other issues are more specific. For Dorothy Denning and her peers, the free speech and civil rights abuses that

can result from cyberterrorist crackdowns on non-cyberterrorists has caused her to pen several articles on the difference between hacktivism, hackers, and cyberterrorism.<sup>24</sup> The broader umbrella of information warfare is also used to address cyberterrorist issues, although information warfare often is used in the context of state military use against a foe.<sup>25</sup> *Networks and Netwars* approaches cyberterrorism as symbolic of an emerging organizational structure.<sup>26</sup>

As a result of this relatively slim selection, articles on cyberterrorism and the media have become common. Many reviewed found the media to be misrepresentative of the problem.<sup>27</sup> Finally, Yonah Alexander and Michael Swetnam present an important edited work that incorporates essays on cyberterrorism from private industry, government officials, and legal and academic scholars.<sup>28</sup>

#### Statement of the Problem

A modern terrorism text, like Rohan Gunaratna's *Inside Al Qaeda*, addresses nearly every aspect of the threat. In his comprehensive research on the organization, Gunaratna explores issues of their organization, structure, ideology,

dispersion across the globe, strategy, mindset, and resulting threat and requisite response.<sup>29</sup> When addressing any of the dozens of terrorist groups that have emerged in the modern era, Walter Laqueur explores their motivations, history, and actions.<sup>30</sup> If this kind of attention is given to conventional terrorism, then the same should be afforded to its online counterpart.

Too often, the debate over the threat of cyberterrorism revolves around critical infrastructure. As shown in Chapter Three, the question often seems to come down to the effect of a cyberterrorist attack - if there is a potential for death or destruction, it can count as terrorism, if not, then the attack is something lesser.<sup>31</sup> Yet if Western society is to truly understand cyberterrorism, it must address all its forms, activities, purposes, motivations, history and actors. Neither the journalistic nor scholarly literature adequately does so.

Because of this, mass media and culture are allowed to set the tone of the social discussion on cyberterrorism. This often leads to sensationalistic documents like Winn Schwartau's *Pearl Harbor Dot Com*. In this novel, the U.S. is attacked by a wide, concerted electronic attack by unknown sources.<sup>32</sup> In 1991, Schwartau achieved limited

notoriety by using the phrase "Electronic Pearl Harbor" to describe the threat to cyberspace during testimony to the House Committee on Science, Space and Technology.<sup>33</sup>

Similarly, an otherwise informative book on cyberterrorism opened with an unlikely scenario in which cyberterrorists cooperated with conventional terrorists to shut down a large regional power grid, give the wrong medicine to patients in hospitals, and otherwise cause havoc on society.<sup>34</sup>

Such sensationalism is damaging to a debate on cyberterrorism for two reasons. First, it incites fear into those who are unable or unwilling to look into the situation more thoroughly. This can lead to unnecessarily abusive legislation passed in the name of protection and the general closure of social openness *vis-à-vis* the Internet. Second, this dialectic turns many who would otherwise be worthy contributors to the debate away from it. It then becomes dominated by whomever can make the most fear-inspiring claims. Academia has a responsibility to ensure this trend does not continue.

## Purpose of the Study

Given the statement of the problem, the purpose of this study is to provide a straightforward and comprehensive survey of the threat posed by this phenomenon. It recognizes that while a study of cyberterrorism must not ignore motivations like ideology, it is more critical to develop an analysis of the threats posed by cyberterrorism. This paper seeks to answer the deficiencies of previous research, especially in formulating a holistic theoretical approach to cyberterrorism, and provide the analysis to do so. By so doing, this thesis will advance the scholarly debate, which inevitably impacts the law enforcement community.

## Theoretical Basis and Organization

Since they are often designed to address a specific aspect of cyberterrorism, many of the past studies have been light on broad theory. They are often designed to address a specific aspect of cyberterrorism. François Debrix, for example, explores the interactions between cyberterrorism and the mass media.<sup>35</sup> David Ronfeldt and John Arquilla use cyberterrorism as an example of their netwar theory.<sup>36</sup>

Few works try to establish a model with which to analyze cyberterrorism. The closest appears in Bunt's *Islam in the Digital Age*. In this text, the author looks at Islamic-based cyberterrorism from four viewpoints: the theological support for online jihad, or "e-jihad;" varying examples of hacking, cracking and hacktivist activities on the Internet; extremist Islamic rhetoric on the Internet after 9/11; and the association of the Palestinian/Israeli conflict with online Islamic activity.<sup>37</sup>

His analytical model provides several important points. First, it looks at ideological justifications for the activity. Following this, the book provides examples that illustrate exactly what activity is being highlighted. Finally, it extends this illustration into the real world by providing the context of two major and polarizing battles: the 9/11 attacks and the Palestinian *Intifada*. In this manner, he has conceptualized the problem, described its various implementations and actors, and provided evidence of the correlation between the activity and the real-world events that motivate the attackers.

While Bunt's model is helpful, it does not necessarily apply to the expanse of threats contained in cyberterrorism. But this is because Bunt's text focuses on

Islam on the Internet, not cyberterrorism. A cyberterrorism paper would have to restructure Bunt's model in order to be effective.

This thesis does just that. First, it must remove the aspects of Bunt's models that are too specific to an examination of the Islamic Internet. Those, of course, are the in-depth explorations of ideology and real-world linkage. If cyberterrorism is a real and long-lasting threat, it will not be limited to a specific ideology set or sequence of events. Nonetheless, these facets of cyberterrorism, which essentially provide the individual or group's motivations, cannot be completely neglected. Instead, they must remain central to the analysis of a specific individual or group.

Stripping out the causes will also allow for a more careful analysis of the threat. To this end, this paper posits that there are four main threats or activities that could constitute or support cyberterrorism. Their classification tends to rely on the means of action.

First, and most evident, cyberterrorism can occur in the form of a virtual attack upon other virtual objects. This primarily includes flooding and denial of service attacks, but it can also incorporate web site defacements

and computer intrusions. Next in progression are virtual attacks on real world institutions, most notably critical infrastructures like electricity, water, and transportation systems.

The last form of attack, which lies more within the bounds of traditional terrorism, is the physical targeting - that is, a bomb - of infrastructures critical to the functioning of Internet systems. This paper does not address this topic, however. First, the physical nature of these attacks makes it difficult to distinguish them from conventional attacks against other critical infrastructure systems. As such, this threat has been recognized before in the literature on terrorism; some have even dubbed it "technoterrorism."<sup>38</sup> Second, the Internet was designed to be resilient against attacks; traffic is automatically re-routed when traffic congestion occurs as a result of a real-world emergency. Although this strategy was tested by the attacks on the World Trade Center and shown to be a threat, the attack, which destroyed a major Internet switching station, did not permanently knock out Internet service. For these reasons, this paper leaves this issue to future research.

The final and most important element of cyberterrorism is the use of the Internet for information gathering and communication. Obviously, this does not constitute a direct attack. Often, this aspect is limited to the spread of propaganda or as a collection site for individuals supporting terrorist or cyberterrorist causes. Nevertheless, these are important aspects to any terrorist campaign, whether conventional or virtual.

The following chapters address these issues through this model. Chapter Two explores the possibilities and challenges of virtual-to-virtual attacks; Chapter Three similarly addresses attacks on real world critical infrastructure. Chapter Four examines the ways in which the Internet can be used as an information-sharing and communication device. Chapter Five describes the U.S. government's reactions to the cyberterrorist threat. Finally, Chapter Six offers a summary of the arguments presented herein and prescriptions for the future.

### Methodology

Most research for this thesis was undertaken in a standard manner, and drawn from familiar academic resources. Unfortunately, the dearth of texts on

cyberterrorism (discussed in the Literature Review section of this chapter), along with the delay for new texts to be published, has forced the author to look to other avenues for research. News sources figure prominently into this, as does primary research from websites. These are generally not taken as fact, but instead as an example of rhetoric or activities taken.

Much of this research has been conducted over the previous two years. During this time, however, many websites used as primary sources were taken offline, moved, or were otherwise unreachable. This included, especially, extremist Islamic or terrorist-linked websites like Azzam.com. Since they were unreachable, verifying their existence and their contents for this study threatened to undermine it.

Fortunately, there are several services that archive webpages. Archive.org continuously scans the Internet for site changes. If the page encountered does not match the page they have previously saved, Archive.org saves a new copy of the website. All saved copies are then available for later review through their "Internet Archive Wayback Machine." The objective of this project is to ensure that

the Internet's contents to not fall off the web as sites change.<sup>39</sup>

Unfortunately, the Archive is not always reliable. The servers often respond slowly or not at all. In these instances, the researcher can turn to Google.com. In its efforts to quickly search the web, it saves the most recent copy of each website it visits. Unless the site's owners have asked Google to limit access to this copy, which Google calls the cached copy, users can view it.<sup>40</sup> This has become a useful way to view the contents of a website that has recently gone offline.

Several avenues were taken to find these websites. Azzam.com was found through a 2002 USA Today news story by Jack Kelley.<sup>41</sup> Many were found via the database housed at Internet Haganah.<sup>42</sup> Since this lists not just the website address, but its unique identifier and contact information as well, it provides ready information for finding these websites when they move. The primary tool for this is *whois*, which allows the user to search for detailed information for each website, including contact and technical information. Internet Haganah uses similar techniques. Finally, some sites were initially found by searching for the online presence of terrorist groups found

in the literature. Al-Mujahiroun's website was located in this manner.

Although the research for this project was primarily conducted over the past two years, much of the background knowledge required for its understanding is much older. In fact, the author has been active, often in a passive way, in online communities for at least the past fifteen years. Additionally, the author's conceptions of computer systems were cemented in 2002 when he received a Bachelor of Science in Computer Science. Consequently, many parts of this thesis, like the description of varying attack techniques, were written from his understanding of the situation and the technologies involved.

This paper was written, however, not for the computer scientist but for the political scientist or policymaker. Therefore, except where noted, much of the technical information was summarized and explained in simple, non-computer terms. When trying to explain these sections, the author attempted to find academic sources that either supported his definitions or expanded upon them. Most of these were acquired through the Association for Computer Machinery (ACM)'s Digital Library.<sup>43</sup> To assist those not

familiar with computer and terrorism jargon, the author included a definition of terms as Appendix A.

In essence, much of this paper was arrived at through standard research techniques - exhaustive reviews of the scholarly books and journals in university library holdings, online databases like EBSCOHost and Lexis-Nexis, and similar online sources. The only exceptions were listed above.

#### Limitations of the Study

Obviously, the absence of substantial previous research presents a challenge to this study. At the same time, though, it offers an opportunity for this study to explore issues that may otherwise be ignored. Instead, the largest limitation for this survey is its lack of primary research. This deficiency is especially poignant in its lack of research on the uniqueness of an individual or group of cyberterrorists. However, the author has no links to such individuals, and no way to establish them, so that research will have to be left to future studies. This is further stymied by the author's limited language skills, which exclude the possibility of primary research from non-English sources, particularly Arabic websites.

## CHAPTER TWO

### VIRTUAL-TO-VIRTUAL ATTACKS

Of the three forms of attack referred to above, virtual attacks on virtual targets are the most prevalent. Due to the technical nature of these attacks, however, they often do not garner the level of press coverage that more traditional attacks can - like the physical attacks on critical infrastructure mentioned in the Introduction. At the same time, though, they are often easier to conduct than more extensive attacks, like virtual attacks against the same critical infrastructures (Chapter Three). Virtual attacks, then, should be distinguished as attacks through the Internet (or a similar system) upon attacks that have no real-world salience.

This compendium of attacks is by no means intended to be all-inclusive. One of the great failings of counter cyberterrorism efforts is that there is no such compendium. But to try to make up for this deficiency in this volume would unnecessarily add to its length and detract from its message. The examples contained within this chapter, then, are included simply to show the wide range of the threat. In the following pages, the reader will find three main

forms of attack under discussion: flooding or denial of service attacks (which can be categorized together), worms and viruses, and web site defacements. These were chosen as the simplest and most common examples.

### Flooding and Denial of Service Attacks

The first recorded cyberterrorism attack was perpetrated by sympathizers of Sri Lanka's Tamil Tigers terrorist organization.<sup>44</sup> The Liberation Tigers of Tamil EElam (LTTE), colloquially known as the Tamil Tigers, are a nationalist terrorist organization that has been fighting for the independence of ethnic Tamils in Sri Lanka via various means - from guerilla warfare to suicide bombing - since 1970.<sup>45</sup> In this instance, a splinter group that called itself the Internet Black Tigers (the Black Tigers are the commando branch of the LTTE) attacked Sri Lankan embassies with a flood of e-mails. Sent at a rate of about 800 per day for two weeks, the e-mails read, "We are the Internet Black Tigers and we're doing this to disrupt your communications."<sup>46</sup> The continuous stream of e-mails choked the bandwidth to and from e-mail servers, essentially causing them to shut down. Until they crashed, though, worker's e-mail inboxes were filled with the unwanted

messages, thereby obscuring their ability to recognize more genuine communications.

This e-mail based attack did little damage. Its effects were relatively concentrated, applying only to Sri Lankan government officials and those trying to communicate with them. Although it did cause certain Sri Lankan government servers to shut down temporarily, the headache was limited mostly to those in the computer support services section of the Sri Lankan government.

That does not mean, however, that it had no effect. Governments all across the world noticed the unique nature of the activity, and assumed that it was a sign of an emerging trend. In the United States, for example, Central Intelligence Agency (CIA) Director George Tenet notified the Senate Committee on Governmental Affairs in June, 1998, that such attacks could be replicated by terrorist or conventional foes against the United States, specifically naming Iran, Iraq and Libya as potential attack sources.<sup>47</sup>

The threat becomes more obvious and more worrisome when one recognizes that these tactics are not limited simply to attacks on e-mail servers. Although usually not sparked by political motives, there is considerable precedent of this activity. One of the most attention

grabbing of these was a 2000 Distributed Denial of Service (DoS) against numerous high-profile websites, including internet web portal Yahoo.com.

On February 7, 2000, Yahoo's servers experienced an overwhelming number of requests emanating from sources across the Internet. From 10:30 am Pacific Standard Time (PST) to 1:00 pm PST, when activity was at its highest, Yahoo's website received more than 1 gigabit of information per second, an overwhelming number for their Internet Service Provider. The Yahoo website was quickly forced offline until the company was able to move to a backup location.<sup>48</sup> The next day, CNN.com, a major news source, experienced a similar attack; Dell.com, Amazon.com, eBay.com and several others were also shut down.<sup>49</sup>

Denial of Service attacks such as these, which essentially overwhelm the service provider such that they are unable to continue providing service, are relatively simple to orchestrate. In a typical attack scheme, the attacker first hacks into several computers across the Internet and installs "agent" software. The more computers that the hacker can break into at this stage, the better; they provide the soldiers in his or her digital army. Once satisfied, the hacker breaks into a few other computers and

installs "handler" software. These computers directly control the agents, allowing the hacker to remain a step removed from the process. Once the hacker gives the handler computers a few commands, generally little more than the target address, the handler directs the agent computers in the attack. Each agent then routinely sends a series of (usually invalid) requests to the target server, though not enough that they will squelch the bandwidth of the agent or seem unusual to a casual observer. The target computer, following protocol, responds with a simple message saying that the message was received, thereby doubling the amount of bandwidth used by the target machine. Such exchanges are fairly common, however, so it is only when several agents coordinate their requests that they have a noticeable impact on the target.<sup>50</sup>

As such, it is often difficult for the owner of an agent computer to detect an attack, especially in a large network. Furthermore, determining the individual or group behind the attack, which is obviously important for law enforcement purposes, provides even more challenges. Most detection methods involve various means of traffic monitoring, although alternative traceback methods are often used to determine the hacker's identity.<sup>51</sup> Other

detection methods include "sniffers," which detect suspicious activity on vulnerable computers, and processing and network analysis tools that pinpoint load anomalies.<sup>52</sup>

The February 2000 attacks against CNN, Yahoo and others were perpetrated by a Canadian teenage hacker known as "Mafiaboy."<sup>53</sup> Mafiaboy was not driven by any political motivation, so his attacks cannot be classified as cyberterrorism. But there are many other reasons for including them in this compendium. First, Mafiaboy's youth provides important demographic information. In a similar attack, for example, an autistic British teenager crashed the servers of the Port of Houston through a DoS attack, effectively halting shipping until the systems were restored.<sup>54</sup>

Second, Mafiaboy's attacks were relatively unsophisticated, facilitated by tools easily accessible on many hacking sites.<sup>55</sup> Third, the effects of the attacks, although minimal (Yahoo, for example, was online later the same day),<sup>56</sup> were limited by the technical resources of the companies attacked. Potential cyberterrorists can employ similar attack means and methods, but their targets are not always so prominent.

One such example is the dual October 2003 DoS attacks against the independent Internet Haganah organization. Internet Haganah attempts "to make the Internet an unfriendly environment for jihadists [sic]," according to its owner, Aaron Weisburd.<sup>57</sup> Mr. Weisburd targets websites that he deems are connected to Islamic-based terrorist organizations. After gathering information on the owner of the website and the company providing them with hosting space (known as their hosting company), Weisburd publicly pressures the hosting company to remove the questionable content.<sup>58</sup> Weisburd claims that he has shut down 420 websites in this manner.<sup>59</sup>

These efforts eventually resulted in blowback, however. On October 16, 2003, and then again on October 20, 2003, Internet Haganah was the subject of a DoS attack that succeeded in knocking the website offline. In so doing, the attackers effectively shut down Internet Haganah's hosting company, Hosting Matters. The first attack left Hosting Matters offline for nearly a full day,<sup>60</sup> taking a number of prominent politically oriented websites, message boards, and weblogs offline at the same time. Commentators at some of the websites affected found message

board discussions in Arabic and English alluding to further DoS attacks on the organization.<sup>61</sup>

This was not an isolated incident. In March, 2004, the website for the Al-Aqsa Martyr Brigades, a secular Palestinian nationalist group, reportedly called for a DoS attack on the El Al Airlines website. The message offered training for anyone wishing to participate in the assault.<sup>62</sup> Similar energy has been directed toward Internet attacks by pro-Pakistani, pro-Palestinian, and many other groups. These attacks have accelerated since the outbreak of the Second *Intifada* in 2000, and, at least in the case of the Israel-Palestine conflict, have been led by hackers from both sides.<sup>63</sup> Each side has used several means of attack during that time:

"The most common weapons used were variations on denial-of-service and 'ping-flood' type tools with nefarious names like 'EvilPing,' and 'QuickFire.' EvilPing...can completely crash most machines...Once one side distributes an attack tool, that same tool is then reconfigured and used against the [attacker]."<sup>64</sup>

The prevalence of such attacks is facilitated by a variety of easy to use tools, EvilPing and QuickFire just being two examples. Evilping is an older tool that lacks sophistication. Some of the newest software, like 'Phatbot,' offers the user an almost completely automated

DoS experience through the exploitation of advanced peer to peer networking technology.<sup>65</sup> Furthermore, these tools are readily available, both on sites dedicated to hacking and those dedicated to security. They often come complete with instruction sets on use. Hackerworld, for example, promises to teach the reader, "step by step, keystroke by keystroke...exactly how us Hackers work our magic."<sup>66</sup> Internet website 7hg reportedly combined hacking information with extremist rhetoric, although its contents could not be confirmed.<sup>67</sup>

Symptoms similar to those produced by such DoS activity are often not directly connected to any particular hacker or terrorist attacks. Instead, they are often little more than a by-product of events in the real world. During the morning of September 11, 2001, for example, news websites such as CNN.com and the Baltimore Sun were so overwhelmed with legitimate traffic that they were unable to serve all requests. Even more innocent, interest in National Security Agency (NSA) computer security guides posted online crashed the NSA computers hosting them.<sup>68</sup> This phenomenon has been dubbed "slashdotting" or the "Slashdot effect" after a popular internet news site whose users unwittingly cause server meltdowns.<sup>69</sup>

Both instances are side effects of legitimate use. Consequently, they point to flaws in the implementation of current infrastructure schemes that can be easily exploited - namely, that the phenomenon of increased public interest in an event serves only to stifle the ability to disseminate information about the news story. Left in the dark, users tend to try to find information via any means possible, thereby unwittingly widening the malaise. It would be unsurprising if would-be terrorists coordinated any real-world terrorist attacks to coincide with similar cyberterrorist efforts. When aimed at news sources or government agencies, these efforts could become a force multiplier of the original attack.

### Worms and Viruses

On November 2, 1988, the fledgling Internet slowed to a crawl. Three to ten percent of the computers online at the time found their Internet connections disconnected as the Internet's first major worm spread throughout the network. Though the number of infected computers was low (about 2,000-6,000), the incident remains, proportionally, the largest and most effective attack on the global network since its inception.<sup>70</sup> Nonetheless, the worm was written to

be totally innocuous: the author, an MIT graduate student named Robert Morris, merely desired to show the flaws in sendmail, a popular mail program.<sup>71</sup> Both the systems the worm exploited and the resulting chaos and damage that ensued foreshadowed later attacks.

While Morris's early worm was the most widespread, the mantle of most damaging politically oriented malicious software (malware) goes to the CodeRed series of worms. Released on July 19, 2001,<sup>72</sup> the worm first propagated throughout the Internet by connecting to a randomly generated set of computers and attempting to exploit a flaw in the Windows operating system. This behavior continued from the 1<sup>st</sup> of the month until midnight on the 19<sup>th</sup> day of the month, after which the worm launched a concerted DoS attack on the U.S. White House website. The worm was programmed to renew this cycle at the beginning of each month.<sup>73</sup> In the process of shutting down the White House website, the worm replaced the website of every 100<sup>th</sup> Microsoft Windows NT server with a simple message that stated that the machine had been "Hacked by Chinese."<sup>74</sup> By the time the worm was contained, it had caused USD\$2.62 billion in damage.<sup>75</sup>

Worms and viruses are a relatively similar phenomenon. Both are designed to seize control of some aspect of a computer's functionality. Most, although not all, viruses and worms have a malicious motivation, and often delete files, corrupt the machine's operating system into an unworking state, install a 'backdoor' to allow future access, or otherwise wreak havoc on the system.<sup>76</sup> Viruses and worms differ from each other in that worms are designed to be more automated, relying less on human input than viruses. They therefore tend to spread rapidly throughout a network.<sup>77</sup> Viruses, on the other hand, usually are attached to a host program, and can only infect a computer when the host program is run.<sup>78</sup> Additionally, many worms, like the most recent Netsky variant,<sup>79</sup> initiate DoS attacks after infection. In many ways, therefore, worms represent the greater threat.

Some of the most common worms of recent years have spread through e-mail programs, wherein an effected machine sends copies of the worm as e-mail attachments to everyone in the user's address book. Others, like Code Red or the more recent Slammer worm, which attacked both computers and ATM machines and had infected the majority of vulnerable machines in just ten minutes, take advantage of software

bugs.<sup>80</sup> Many worms and viruses, including Code Red, exploit vulnerabilities reported in computer security media.<sup>81</sup> Makers of the effected software often release a patch to update the software before a malicious program can take advantage of the vulnerability; in these instances, worms spread by infecting machines whose owners have not updated their software accordingly.

Both worms and viruses are often replicated, reconfigured, and re-released. The first instance of CodeRed, for example, had a bug that limited the damage it could cause. Subsequent versions changed the intent of the program, targeting different sites for DoS attacks or doing something else entirely. CodeRed II, itself a variant, has been re-released in six different versions.<sup>82</sup> The worm spreading through the Internet at time of writing, Netsky, had 26 variants.<sup>83</sup>

Often, the new variant of the virus is not authored by the original programmer. Instead, others download the source code or otherwise copy the innovation to create their own variation of the malware. This applies to hackers connected to terrorist organizations just as equally as it does to less politically motivated hackers.

In fact, this phenomenon has popped up with relative frequency in cyberterrorist circles. The Muslim Hackers Club, which espouses pro-Palestinian and Pakistani rhetoric, offers tutorials for would-be hackers on writing new viruses or adapting old ones.<sup>84</sup> Additionally, a variant of the Toal virus that appeared in October 2001 (at the beginning of the Afghanistan conflict) sends the infected computer a randomly selected message. Users with an infected computer who open the e-mail that carries the virus are greeted with messages as varied as "Usa against geneva convention [sic]," "Is osama bin laden bad-loved ? [sic]," and "Anthrax mail is true(not a joke) [sic]."<sup>85</sup> The attachment, when run, distorts the screen image and pops a similar anti-American message onto the screen.<sup>86</sup> Similarly, the Nedal virus, though relatively harmless, was so named by the virus author because it is "Laden" spelled backwards. Nedal.a, a more effective variant, overwrites popular file formats, including music and video files and documents, and deletes all files on the computer on 11 September each year.<sup>87</sup>

In the run-up to the 2003 war in Iraq, the reputed author of the Nedal virus, a Malaysian hacker known as Melhacker, threatened to "attack or launch [a] worm if

America attacks Iraq.”<sup>88</sup> The worm he claimed to be ready to release - early versions of which had reportedly already appeared on the Internet - was a combination of several earlier viruses and worms, including some attributed to the same hacker.<sup>89</sup>

Although no subsequent worm was attributed to this threat, it raised concerns over the phenomenon of viruses as a cyberterrorism tool. Through an accomplice, Melhacker reportedly had ties to A.Q.T.E. Al Qaeda network,<sup>90</sup> although that group’s actual ties to Osama Bin Laden and Al Qaeda are unknown, and presumed to be non-existent.<sup>91</sup> Moreover, several other viruses and worms emerged as a result of the Iraq War. The Ganda, Lisa and Wanor worms, which all appeared near the beginning of the war, urged the infected against the conflict.<sup>92</sup> Accordingly, concerns over rising pro-terrorist viral activity continue.

### Web Site Defacement

Web site defacements are the most common, closest to traditional hacking in method and means, and, in many ways, the least threatening of the potentially cyberterrorist activities addressed in this chapter. Many consider them to be nothing more than an annoyance that leaves little

long-lasting effect. Regardless, they can be used by cyberterrorists to limit the availability or content of important information sources.

Defacements are usually relatively straightforward. The potential hacker tunnels his or her way into a website through any of a number of exploits and methods. Some use security holes in software or their configuration; others use social engineering - the process of convincing a target to unknowingly give up sensitive information about their website<sup>93</sup> - to gain access. Once inside, the malicious explorer replaces the website's content with their own.

In most cases, the new content holds little information - usually just the hacker's name, group affiliation, and 'shout-outs' to friends and colleagues. Most individuals or groups that engage in these activities target local sites. Accordingly, Ion, a prominent Brazilian group, targets mostly Brazilian sites;<sup>94</sup> the Italian group IR4Dex leaves their signature primarily on Italian sites.<sup>95</sup> Both these groups rank in the Top 10 attackers tracked by defacement monitoring website Zone-H.org.<sup>96</sup>

Many are less innocent, however. Unix Security Guards (USG), a pro-Muslim hacking group that has performed 5069

defacements, has emerged as a leader in the anti-American web site defacement trend.<sup>97</sup> The night after the start of the war in Iraq, the group left hundreds of websites marred with their own text.<sup>98</sup> The text of a typical USG defacement condemned the target, the United States, Israel, or any group or individual deemed an enemy of Islam. The following is the text of the defacement of copts.org on 8 April 2004. Copts.org is a website designed to promote awareness of abuses perpetrated by the Egyptian government against its Coptic minority:

"well.. that was for the shit u post in your sites/forums/chatting rooms .. ur whole machine is mine now... u punch of morons. u fucked now..ha !?.

copts of usa/canada are punsh of real losers, all what u say about the persecutions in egypt is bullshit , the same thing about the alleged kidnapping of your girls , insulting islam all over your websites doesn't help your case , its just help us to learn how lame you are ,and how gay is your demands... get the backup disks readfy,coz u gonna have a long night lamers .. i bit u will spend long days staring at your stupid machine wondering how could i get in , and u wont figure it out , so get the other -leet- asses copts and u guyz figure it out together.

be happy , u have a clean HDs now.. plenty of free space !, ayy khedma :0)

p/s stop your mean way of insulting islam/muslims in your sites ... most of you grow up in muslim neighborhoods , i don't think they were as assholes to you as your are now , so have some

respect to yourselves and to the others ... its just a thought.

cheeeeers to baasseem<sup>99</sup>

The text is revealing in a number of ways. Besides the obvious misspellings, swearing, and juvenile insults, it reveals a narrow-minded commitment to the defense of a cause - in this case, the defense of Muslims. Furthermore, although the attack and its rhetoric showed a focus on its target, the resulting text indicates the lack of sophistication such an attack requires.

USG was preceded by a number of like-minded groups, all leaving their own trail of virtual graffiti. Muslim Hacker's Club (MHC), mentioned above in the viral section, performed 28 defacements during November and December 2001 against mostly Indian targets.<sup>100</sup> These attacks came at a time when the Indian-Pakistani dispute over Kashmir was devolving into violence; twelve died in December when the Indian parliament was attacked by a group of terrorists.<sup>101</sup>

Another group, the World's Fantabulous Defacers (WFD), has led more high profile attacks. For example, the WFD led an attack on Ariel Sharon's election website a week before the 2001 Israeli election that elevated Sharon to Prime Minister. The initial reaction from the press attributed the attack to HAMAS, indicating the potential

link to terrorist groups.<sup>102</sup> In its place, the group left graphic photos and text that accused Sharon of being a war criminal. At the same time, it left a message expressing the attackers' solidarity with Hezbollah and other fighters in Palestine, Kashmir, Chechnya, and Bosnia.<sup>103</sup>

In a number of texts, Dr. Denning has asserted that this kind of behavior is "hacktivism," or hacking for an activist cause, and not cyberterrorism. Her justification is that the attacks do not result in violence, "severe economic hardship or sustained loss of power or water."<sup>104</sup> This paper disagrees with her assessment. Instead, it posits that while such activity is, indeed hacktivism, it bleeds into the terrorism category when the actions are in support of terrorism or terrorist causes, as is the case with MHC and WFD.

The potential effects of these attacks, especially when coupled with more sophistication, could be devastating. Instead of completely defacing the website, a potential cyberterrorist could replace the contents more subtly. For example, one of the many attacks on the Recording Industry of America's (RIAA) website left the site a parody of its former self. Angered by the RIAA's crackdown on music piracy, the hacker replaced several of

its headlines with titles such as "Piracy can be beneficial to the music industry" and "Are there subscription music services up and running?"<sup>105</sup> Similar attacks, especially if timed to reflect real-world events like the WFD-Sharon defacement, could spark the political change the attackers seek. On the other hand, if conducted in conjunction with DoS, real-world or other attacks, such defacements could set the tone of the information reported in a time of crisis.

#### Conclusion

The three means of attack explored above - flooding, viral, and defacement - are by no means representative of all the virtual attacks available to the would-be cyberterrorist. Prominently missing are classical hacking alternatives and goals, like intrusions into classified systems. As a December 2001 attack on servers of the U.S. General Accounting Office by members of the "Al-Qaeda Muslim Alliance" shows, such attacks do occur, and can be traced to terrorist-sympathizing hacker groups.<sup>106</sup> Such methods only augment the attacks discussed here.

These methods, and their supporting precedents, point to a growing trend toward increased activity on the part of

hackers supporting terrorist groups. Moreover, the tools that facilitate most of these attacks are both easy to use and readily available. As a result, the prevalence of this illegal behavior will undoubtedly continue to rise.

Furthermore, world events, including major conflicts like the one between Israel and Palestine, will probably continue to cause spikes in activity. When coupled with anger over world events, the availability and ease of the tools required for these attacks often serve to enfranchise a class of people whose voices often get lost in the shuffle of life.

Moreover, actively participating in the ideology in this manner can reinforce its tenets. Since many of these hackers presumably - no studies on cyberterrorist demographics currently exist - are not on the front lines of the cause with a bomb and a gun, stories of the activities of their ideological brethren can acquire a heroic tenor. This provides a fruitful recruiting ground for terrorist organizations looking to diversify their activity.

## CHAPTER THREE

### THREATS TO CRITICAL INFRASTRUCTURE

When Dorothy Denning,<sup>107</sup> Scott Berinato,<sup>108</sup> Bruce Schneier,<sup>109</sup> and other scholars, journalists, and security experts claim that there is little to no risk from cyberterrorism, they draw their conclusions from the lack of a risk they see emanating from critical infrastructure. Their skepticism, though, is countered by the results of numerous hearings, presidential directives, and at least one breach of security.

The skeptics have a variety of points. Schneier does not believe that the general hacker ethic is not compatible with terrorist ideology; he also claims that it will be difficult for cyberterrorists to know which attack strategies will have the greatest impact.<sup>110</sup> Through interviews with security representatives from the critical infrastructure industry, Berinato attempts to show that the threat of cyberterrorism has been neutralized through effective security measures.<sup>111</sup> Denning articulates that although the threat from cyberterrorism is emerging, it is currently not viable.<sup>112</sup> These arguments have been augmented by others who claim that the cyberterrorism

threat has been overstated and overhyped by a mass media eager for a sound bite and security experts trying to increase their business.<sup>113</sup> No one, they assert, has ever been killed by a cyberterrorist attack.<sup>114</sup>

Indeed, many of these arguments carry salience. The youth of cyberterrorism scholarly research and the general neglect of the trend by traditional terrorist experts have allowed the debate on the topic to be dominated by the media and security experts. As Mark Pollitt wrote in a paper for FBI Laboratory, cyberterrorism incorporates two areas that people traditionally do not understand: terrorism and information technology.<sup>115</sup> As such, it is easy for the media and security establishments to take advantage of the situation. In fact, a study on mass media's coverage of cyberterrorism found that it was often based on reports from earlier articles "with already obscure sources;" employ a "sensationalist tone," including the "spectacularly dominat[ing]" "use of negative words and references to the magnitude of possible adverse actions;" and legitimize their assertions through "official sources" or security experts.<sup>116</sup> On the other hand, a significant number of the experts testifying at a 2002 House of Representatives hearing on cyberterrorism were private

security specialists.<sup>117</sup> Such access to official debate allows private industry to set the tone of a debate from which they could profit.

Hyper-exaggeration does not negate the threat, however. Neglecting the threat of cyberterrorism on critical infrastructure could become the catalyst that enables an attack to succeed. Although predicting the course or success of an attack is a difficult endeavor, this activity can be an important factor in protecting critical infrastructure. Several recent incidents have shown that modern infrastructures may not be as prepared against cyber-attacks as the optimists would like to think.

The first came in 1997. Conducted over four days in June 1997, *Eligible Receiver* was an exercise mandated by the Joint Chief of Staff to target government websites using readily available products. Unclassified computers from the National Military Command Center, the Pentagon, U.S. Pacific Command, and many others were compromised, and the attackers were able to deny services, change information, and manage computer account information.<sup>118</sup> Some reports have claimed that participants in the exercise were able to gain access to the nation's power grid and simulated shutting down major portions of it.<sup>119</sup> The

Department of Defense confirmed that the nation's power systems had indeed been compromised by *Eligible Receiver*, but refused to detail the extent of the potential damage it could have caused.<sup>120</sup> The head of the Pentagon's Joint Task Force on Computer Network Defense said that the operation "clearly demonstrated [the] lack of preparation for a coordinated cyber and physical attack on [the nation's] critical military and civilian infrastructure."<sup>121</sup>

Subsequent attacks or exercises on U.S. infrastructure or military systems have attempted to take advantage of this vulnerability. In 1998, for example, as the United States was preparing for possible military operations against Iraq, several Department of Defense computers were compromised (through a known and resolvable vulnerability in the Solaris operating system) in a coordinated attack known as "Solar Sunrise."<sup>122</sup> Once the computers were compromised, the attackers explored the system, left tracking software to gather information, and returned later to retrieve their results.<sup>123</sup> The sources of the attacks, which appeared to emanate from the United Arab Emirates, raised further concern. In the end, though, no political motivations were found - the systems were compromised by an Israeli hacker and two California teenagers.<sup>124</sup>

Nonetheless, the attacks proved the limitations of the U.S. government's cybersecurity, which could be just as easily compromised by a group or individual with political motivations.

Similarly, the 2002 Blue Cascades exercise, which incorporated several Canadian and Pacific Northwest power and other infrastructure companies as well as federal and state agencies, explored the results of a potential cyberterrorist attack or physical disaster.<sup>125</sup> It found that the involved parties generally had "at best a surface-level understanding" of the threat, including "little recognition of the overwhelming dependency upon IT-related resources" for business operation and disaster recovery.<sup>126</sup> Furthermore, there were little to no inter-agency or inter-governmental reporting system, public information channels, or evidence preservation strategies. The result was a system ripe for exploitation by a cyberterrorist attack. By neglecting the "human factor" of public information, the infrastructure outages of the disaster could spur mass panic and lead the public to believe the worst rumors.<sup>127</sup>

The 14 August 2003 power outage in the Northeastern United States provides another interesting illustration. Although the blackout was rooted in irresponsible overloads

in the system,<sup>128</sup> not terrorism, the initial reaction forced U.S. President Bush to quickly release a statement assuring the public that it "was not the work of terrorists."<sup>129</sup> It proved several vulnerabilities that terrorists can exploit, however: the potential disaster when businesses in charge of public utilities do not adhere to government regulations,<sup>130</sup> the interconnected nature of regional infrastructures can lead to wide-ranging cuts in service,<sup>131</sup> and the intrinsic role information technology plays in critical infrastructure.<sup>132</sup>

Despite all these exercises and attacks, only one successful incident of hacking a nation's infrastructure has been proven. Nevertheless, the case shows some important vulnerabilities.

In March, 2001, an Australian hacker was convicted of an earlier attack against his former employer, an Australian sewer company. After being passed over for a promotion, the hacker broke into the computer systems that controlled the sewage storage tanks and instructed them to release their contents into the public waterways.<sup>133</sup> Albeit not a terrorist incident, it shows the potential threat employees pose. Since terrorists are not limited in their location or employment, they can instigate cyberterrorist

attacks on critical infrastructure through the inside knowledge of an employee sympathetic to their cause.

Al-Muhajiroun provides an illustration of this. The London based Islamic group "swear[s] allegiance to Osama bin Laden and his goal of toppling Western democracies to establish an Islamic superstate under Shariah [sic] law."<sup>134</sup> In a May 5, 2004 Press Release on the organization's website, the group highlighted a demonstration they organized that rejected democracy in favor of a Shari'ah state and called for U.S. President Bush and U.K. Prime Minister Blair to be tried under a Shari'ah court.<sup>135</sup> The last bullet in their Vision Statement is the "establish[ment] of Al-Khilafah in order that Islam dominates the World (Izhaar ud-Deen) and becomes the World order[sic]."<sup>136</sup>

Reliable sources confirmed in 2002 that individuals living in the United Kingdom and employed in the British government's telecommunications sector have expressed their support for extremist fighters such as those in Chechnya and Afghanistan. At least one of these sympathizers held a degree in computer science from a British university.<sup>137</sup> Although there is no confirmation that any of these individuals are interested in disrupting Britain's

telecommunications systems or providing others with the expertise to do so, their proximity to crucial information systems provides them the opportunity.

Likewise, it is not a huge stretch to subsume that similar individuals hold similar positions in the utility corporations of America's infrastructure. Essentially, if individuals connected to terrorists can allegedly enter America's prison system as chaplains,<sup>138</sup> what would stop them from finding key positions in private infrastructure providers? This is certainly not without precedent. Japan's Aum Shinrikyo excelled at bribing public officials to gain access to public buildings, even after their deadly attack on Tokyo's subways.<sup>139</sup> Similarly, the Church of Scientology's (which is obviously not a terrorist organization) successful infiltration of the U.S. legal system while under investigation shows that such actions are not necessarily fruitless.<sup>140</sup> Consequently, it is not unreasonable to expect that Al Qaeda may attempt the same.

Al-Qaeda itself has shown an interest in critical infrastructure. In 2001, city officials in Mountain View, California - located in the heart of Silicon Valley, the nation's technology hub - noticed increased website traffic from Middle Eastern countries. Particularly, the webmaster

noticed that several revealing documents pertaining to the city's standards *vis-à-vis* its police, fire, and utility sectors had been downloaded.<sup>141</sup> More menacing, a January 2002 National Infrastructure Protection Center Information Bulletin reported that:

A computer that belonged to an individual with indirect links to Osama bin Ladin contained structural architecture computer programs that suggested the individual was interested in structural engineering as it related to dams and other water-retaining structures. ... In addition, U.S. law enforcement and intelligence agencies have received indications that Al-Qa'ida members have sought information on Supervisory Control and Data Acquisition (SCADA) systems available on multiple SCADA-related web sites.<sup>142</sup>

This computer, among others, was discovered in a house in Pakistan that was reportedly "devoted solely" to cyberterrorism training.<sup>143</sup>

SCADA offers a unique opportunity for the cyber-terrorist interested in critical infrastructure. SCADA networks provide remote access for control and data acquisition of a variety of infrastructure control equipment, from water pumps to traffic signals.<sup>144</sup> These are the networks that, according to Berinato, can be controlled remotely in only limited ways.<sup>145</sup> Nonetheless, limited access can still be exploited.

In general, the nation's critical infrastructure poses a number of opportunities to the potential cyberterrorist. Erbschloe identifies 51 key areas that cyberterrorists may find to be attractive targets. Prominent among these are electric, gas and water systems; aircraft operations; telecommunications infrastructure, including radio and television networks and distribution systems; transportation systems; and a number of others.<sup>146</sup> Moreover, a recent analysis of wireless communication networks, which have been used to control such systems as railroad crossings, found a glaring security flaw. Requiring equipment found in any computer hardware store for less than 100 dollars, exploitation of the security gap can lead to a complete jamming of the frequencies used by the wireless network.<sup>147</sup> Once discovered, the news of such flaws often propagates quickly; the necessary patches to negate their effects often cannot be implemented at the same dispersion rate.

A compromise in infrastructure control systems such as these, especially when controlled by remote access systems like SCADA, can enable the shutdown of water, power, and other utility systems. Their interconnected nature allows this to effect a broad segment of society, and spreads the

effect through the entire region. Moreover, this form of cyberterrorism can increase the hysteria that can accompany a traditional terrorist attack. Therefore, whether conducted via internal sources or solely from external break-ins, the cyberterrorist threat to critical infrastructure remains overwhelming; nonetheless, it is probably not as apocalyptic as the sensationalist descriptions prevalent in the media assert.

## CHAPTER FOUR

### THE INTERNET AS A COMMUNICATIONS DEVICE

The Internet has sparked a new communications era. Family members can use its faculties to communicate, virtually free of charge, across the world over chat networks. Multinational corporations can remain in constant contact with their farthest flung offices through e-mail. The disaffected can raise awareness of their plight via a simple webpage.

These uses of new technology are valid, and are employed with a positive intent. That does not mean, however, that every human being with access to modern technology will approach its use without any sense of nefariousness. Indeed, terrorists can use the communications resources of the Information Age to promote their cause and activities. Chat rooms and websites are especially viable means to promote awareness of terrorist causes; in the hands of a marketing mind, they can attract otherwise unreachable new recruits. At the same time, the anonymity of chat rooms and e-mail, especially when coupled with obscuring methods like encryption and steganography, can facilitate the planning of a terrorist attack.

This chapter addresses this issue through the exploration of these technologies. First, it will provide examples of who is online, and what has been done to limit the effect of Internet-based terrorism. Although the depth of the Internet does not allow for truly authoritative statistics, a few examples can indicate the dangers this phenomenon presents. The paper will then present a case study of steganography, a method used to obscure data that many fear Internet-based terrorists could exploit.

The growing ubiquity of the Internet provides a fertile recruiting ground and communications channel for the politically motivated of any vein. Scholarly research can not only recognize the threat this poses, it can and should offer solutions to contain it.

### Online Terror Groups

Almost all ideologies, from extremist Islamic groups to far right hate groups, have established themselves online. They have accomplished this via both concerted and individual methods. Creating a website, for example, to represent a particular terrorist organization would be a concerted undertaking, whereas an individual website that echoed the same rhetoric would have been established by

individual efforts. Either way, the effect is often the same: the political message of the terrorist group is spread.

The effectiveness of these tactics is facilitated by the organizational structure of the organization. Terror groups that operate under a loosely knit organizational scheme (as opposed to a strict, hierarchical one) are often more able to take advantage of these technologies. Arquilla and Ronfeldt described this phenomenon as netwar. Essentially, netwar is the "use of networked forms of organization, doctrine, strategy and technology attuned to the Information Age."<sup>148</sup> It is the adaptation of advanced computer networking structures wherein no single leader or communication path dictates the campaign or specifics of individual actions. Often, those involved are "dispersed organizations, small groups, and individuals" who can be separated geographically, culturally, or otherwise.<sup>149</sup>

In essence, the Internet and other telecommunications technology bring people with a similar mindset yet diverse locations to the same discussion and then empower them to take an active role in furthering the cause. Correspondingly, at least one study on persuasion has shown that the typical message on many far right-wing message

boards and websites is extraordinarily effective in reinforcing a pre-existing ideology.<sup>150</sup> It is even more powerful if the end-user is able to directly interact with his peers. The result is that an "inverse relationship" develops between a public's access to modern technology and its government's ability to exert control.<sup>151</sup>

Consequently, Louis Beam, a leader of the American far right, calls this phenomenon "leaderless resistance."<sup>152</sup> The hate groups of the far right, both in the United States and abroad, have been especially adept at adapting to new technology. In 1984, Beam created one of the first hate-centered online Bulletin Board System (BBS). In it, like-minded individuals could gather to discuss issues pertinent to the BBS' "'pro-American, pro-white, anti-Communist" theme.<sup>153</sup> The advent of the Internet merely enabled hate groups to spread their message; when it was confined to BBS', the message base was limited by the technical capacity of the BBS' equipment, specifically by the amount of dial-up lines on which users can connect to the system.

The Internet's decentralized framework has no such limitations. As a result, the number of Internet outlets for hate groups has exploded. The newest edition of a compendium of hate groups, for example, lists 113 pages of

websites, chat groups, newsgroups, mailing lists and other outlets that have emerged online.<sup>154</sup>

Of course, the harboring of hatred against another group does not make someone a terrorist. In fact, a public debate still rages as to the necessity of differentiating between hate crimes and more traditional incidents.<sup>155</sup> Discussion of hate groups is included, however, because the "us versus them" mentality that develops among their denizens is reflected in the rhetoric of millennial terrorist groups like Al-Qaeda. Osama bin Laden's rhetoric, for example, has often illustrated this trend. Bin Laden routinely elevates the role of American power until America becomes a "mythic monster" that "only divine power can subdue."<sup>156</sup> This effectively marginalizes any role of compromise and polarizes supporters. Moreover, the rhetoric can have a powerful effect on an impressionable viewer - like a curious website visitor.

Authors of extremist Islamic websites have adopted much of this language. In fact, many have been particularly adept in using the rhetoric as a marketing tool. In a telling case, a Saudi born graduate student residing in Idaho is, at the time of writing, currently under trial for creating a website that allegedly promoted

Islamic extremism.<sup>157</sup> Similarly, the example of Azzam.com provides a particularly telling illustration of this trend.

At the time of the September 11, 2001 attacks, Azzam.com had already served as a mouthpiece for extremist Islamic groups for several years. Run by London-based Azzam Publications, the website claimed to be little more than a "media organization providing authentic news and information about *Jihad* and the Foreign *Mujahideen* everywhere."<sup>158</sup> The website sold a variety of books, CD-ROMS, and audio and video tapes on the subject. Many, such as the "Stories of Foreign *Mujahideen* killed in Bosnia" series, glorified the tales of *mujahideen* (loosely translated to be freedom fighters) fighting in various conflicts involving Muslims, from Chechnya to Kashmir.<sup>159</sup>

As part of their reporting on these conflicts, Azzam.com also promoted tales of the *mujahideen* on their website. These narratives, often replete with obvious hyperbole, glorified the efforts of the fighters highlighted. From a text eulogizing Saudi-born Abu Thabit Ad-Daheishi:

I still remember the day you approached me, venting your anger about the withdrawal of the Mujahideen ahead of a Serb flanking manoeuvre in Kosovo; you were angry and stressed that Jihad demands steadfastness and sacrifice. I told

myself, such words would only come from a man of courage who would never withdraw from the face of danger.

You made your way through<sup>6</sup> the fields of sacrifice, from Afghanistan to Bangladesh, to Albania to Chechnya. You sought the glory of martyrdom, and we ask Allah to grant martyrdom to your noble spirit. Those who knew of Abu Thabit would ask if he was still alive, for in him they all had seen the signs of a martyr, and all knew of his eagerness to fight and die for Allah..

Two weeks before you met your Creator, Sheikh Abu Umar had a vision of you; in his dream he saw you digging your grave with your own hands; Sheikh Abu Umar interpreted this as the inevitability of your martyrdom, so did another of your brothers who had the same vision. ... During the preparations for the assault, Abu Thabit raised his hands in supplication to Allah. As he prayed to his Lord, a missile exploded between Abu Thabit and a brother Mujahid, Abdus-Samad of Tajikistan, killing both of them.<sup>160</sup>

This language mirrors bin Laden's. By promoting the warrior role of the fighters, it glosses over details in the ideology or the fighter's actions - like fighting in the first place - that a reader might find questionable. Furthermore, it conveys to the reader that they could gain a sense of empowerment by volunteering for the cause. This helps overcome the sense of frustration and disenfranchisement that characterizes many terrorists and their recruits.<sup>161</sup> Terrorists themselves are often either "alienated from society" and/or "have a grievance or regard themselves as victims of injustice."<sup>162</sup> Often, they are

most loyal to each other;<sup>163</sup> websites that cater to them consequently help these individuals find others like themselves. The contact often serves to reinforce the sense of injustice.

Azzam.com's story is particularly interesting. In July, 2002, USA Today journalist Jack Kelley reported that the website was being used as a communications device by Al Qaeda members planning their next move. Messages between terrorists, he claimed, were hidden in Azzam.com's images through a process known as steganography (steganography will be examined in the next section). Although the reliability of the story was later thrown into doubt when Kelley was proven to be a chronic fabricator and plagiarist,<sup>164</sup> the story resounded in several circles. Politechbot.com, an online privacy website, challenged its readers to try to determine the veracity of the story.<sup>165</sup> They found several images that could contain hidden messages, although the messages themselves were not discerned.<sup>166</sup>

Azzam.com drew attention from other sources, however. In particular, Jonathon Galt, a private citizen from the United Kingdom, pressured the company hosting Azzam.com to remove the questionable content. In order to elicit a

response, Mr. Galt sent the hosting company an e-mail detailing the technical justification for his suspicions and simultaneously threatened to take his claims to the media and the U.S. government. He then posted his correspondence on his website.<sup>167</sup> From that point, Azzam.com moved servers several times, including to entirely different domains like waaqiah.com.<sup>168</sup> Eventually, its owners gave up and closed the site down in a letter that reiterated and highlighted the polarized mentality of their rhetoric.<sup>169</sup>

Azzam's closure and Mr. Galt's efforts did not take place in a vacuum; other websites and vigilantes replaced them. Whereas the number of extremist Islamic websites (most of whose content remains in Arabic) has increased, a majority of the pressure exerted upon extremist Islamic or terrorist websites emanated from one group: Internet Haganah (IH, originally introduced in Chapter Two).

The website, owned by American Aaron Weisburd, routinely searches for websites that are either linked to extremist Islamic groups or promote Islamic extremism. Weisburd then posts a digital snapshot of the site, along with the technical information for the site and the contact information for the hosting company, on the IH site. A 2

May 2004 snapshot of the Internet Haganah website points to several sites Weisburd claim are connected to HAMAS or Palestinian Islamic Jihad or espouse extremist Islamic rhetoric.<sup>170</sup> Most of the websites to which Weisburd links are written in Arabic, so their content cannot be verified by this author, but Weisburd professes that he only targets websites that espouse extremist rhetoric or are directly linked to a terrorist organization. When asked how he makes the distinction, Weisburd responded:

"An 'Islamic' website that provides, for example, support, encouragement or justifications for political violence would be an extremist site. An Islamic website that does not promote such violence is not extremist. In practice, this is easy. Osama Bin Laden [OBL] is not exactly the Prince of Peace. When someone presents OBL as a Great Man, they have gone over a line that should not be gone over."<sup>171</sup>

By posting all the relevant information for each site online, Weisburd is effectively calling upon his readers to assist him in contacting the hosting companies, even though he works closely with only a small group of individuals.<sup>172</sup> By distributing the effort thusly, the effectiveness of each individual website struggle is raised. In effect, Weisburd uses many of the same practices of online terrorists and Islamic extremists to target them: he uses

his website to promote his cause and simultaneously empowers his readers to take matters into their own hands.

This is not the only similarity. The intensity of the rhetoric Weisburd - and, much more magnified, many of the sites he approvingly links to - uses about Islamic extremism is itself often extreme, or at the very least, misrepresentative. As an illustration, IH provides several links to [danielpipes.org](http://danielpipes.org), the website of a prominent, but controversial<sup>173</sup> commentator on Middle Eastern affairs. The website prominently and directly links to Daniel Pipes' essay entitled "What is *Jihad*?" and several of its translations, as if endorsing the essay as a guide for understanding jihad-based movements.

Pipes' essay runs into theological problems because it ignores the mainstream Islamic perspective of the question, focusing instead on extremist justifications. Translated literally, the term "*jihad*" means "struggle." In mainstream Islamic discourse, the term has two forms, the greater and lesser *jihad*. The greater *jihad* describes each Muslim's inner struggle to find God; the lesser *jihad* is the defense of Islam against its enemies.<sup>174</sup> Pipes' essay ascribes the greater *jihad* simply to mysticism so as to focus on the lesser *jihad*. He then exploits the definition

of the lesser *jihad*, twisting it from a defensive to an offensive term and justifying its translation to "holy war."<sup>175</sup>

Another site to which Weisburd links often exhibits schoolyard characteristics. A typical day's lead news stories cried "antisemitic [sic]"<sup>176</sup> over some of Saudi Crown Prince Abdullah's statements, called a convicted terrorist a "murderbot,"<sup>177</sup> and implied that Islam was a "religion of RPGs."<sup>178</sup> Commentators on the website's discussion board claimed Muslim protestors were part of a "backward, Arab nazi movement [sic]"<sup>179</sup> and hoped that one, presumably an "Islamozoid"<sup>180</sup> would "have an AK pointed in that gaping sewer-hole of his in the near future."<sup>181</sup>

These issues are brought up not to discredit Weisburd's work, or attribute the prejudices of others to him. Weisburd systematically points out each new iteration of websites linked to HAMAS and other terrorist organizations; in fact, he believes that their organization and funding allow them to reappear more often than others. In so doing, he provides an invaluable service to the law enforcement community. Additionally, Weisburd has said that he takes pains to refrain from labeling the proprietors of any individual as 'terrorist,' instead

presenting the reader with information on the website and its contents. In this manner, he leaves judgment to the reader.<sup>182</sup>

Instead, this issue has been raised to highlight the prevalence of the polarization that can thrive in such emotive, politically oriented online communities, where one can 'speak' in an anonymous arena without immediate retribution and have prejudicial speech reinforced and cheered instead of castigated and discredited. The tone of such speech can quickly characterize the normal mode of communication. Doubtless, similar comments and situations are as proliferate on many of the websites to which Weisburd links, although language barriers, as mentioned before, pose a limitation to this study.

No matter what 'side,' though, the standardization of this type of rhetoric and misinformation - in the case of the *jihad* essay - serves only to demonize the other in such a manner that it becomes a monolithic enemy. Even if not directly linked to violence, it perpetuates the hostile emotions of those involved. Furthermore, since the public nature of these sites, terrorist or otherwise, turns them into propaganda outlets, it disseminates that hostility into the rest of the Internet, and into society itself.

## Steganography: A Case Study<sup>183</sup>

Encryption is the process of changing the visible appearance of a message in such a way that an observer cannot understand it. Encryption is obvious. It puts a lock on the data that the encryptor expects that only the recipient of the message will be able to unlock. It is easy to discern an encrypted message from an unencrypted one, because, as a rule, an encrypted message appears as nothing more than random garble. Once the lock is put on, a key is required to view the unencrypted message. Of course, that lock can be picked, and breaking encryption has become a cottage industry of its own.

In an encrypted message, however, the existence of the message itself is known to the intercepting party. Steganography is essentially an attempt to halt this by concealing the message in some other medium. The idea is not new. Ancient Greeks used wax covered tablets to conceal messages: once the message was written, the tablet would be sealed in wax and then transported to its destination with the appearance of a clean slate.<sup>184</sup> Other innovative approaches appeared over time. The Nazis developed an approach in World War II called micro-dots - dots of ink

the size of a period that contained a shrunken message. Invisible inks were also prevalent during the period.<sup>185</sup>

Steganography does not have to be so complex. A previously determined steganographic method could, for example, hide a message in the first letter of each word; a phrase could mean something else entirely; or the appearance of the cover message itself (for example, the shape of the loop of a hand-written letter 'l') could contain hidden meaning. The problem with all of these approaches, however, is that they can only be deemed secure until their use is discovered. In the interest of complete security, then, a new steganographic method has to be devised for each subsequent message.

With the rise of computing technology, this is no longer as necessary. Although Jackson contends that there is a constant "technological treadmill"<sup>186</sup> being run by those who want to hide data and those who want to find it; in practicality, the cycle is not as rigid as the one time system described above. It is not that technology cannot keep up: in reality, it can. However, the sheer enormity of the medium available (the entire Internet itself), along with the margin of error in message discovery tools, can

seem to give anyone trying to hide a message a tactical edge.

Steganography in the computer age, then, has become the art of hiding messages inside media files, especially image and audio files. The message being hidden is called an embedded message. The medium hiding the message is called a cover carrier or cover medium. (In this study, the two terms are used interchangeably.) The resulting message is a stego-message. There are several pieces of software available to assist in this. One website lists 41 different programs for Windows alone, 31 of which are completely free.<sup>187</sup> Three of these were chosen for research for this study based on availability, features, reputation and the nature of the program's steganographic and cryptographic algorithms. The only common factor was price: due to budget constraints, only software as freeware was used. Due to their vast availability, though, this would do little to limit the variety of the survey. In addition, it must be stressed that this is only a survey. This section does not endeavor to complete a comprehensive view of steganography; rather, it is an attempt to determine what a security response to the threat posed by steganography should be. As such, the demonstrations

contained in the next few pages are simply that:  
demonstrations.

Regardless of the nature of the discussion, only programs that divulged the nature of the algorithms used were selected. Fortunately, this does not limit as many programs as it would seem: approaches to hiding information in the most popular formats are generally well documented (discussions of the formats used for this paper can be found below), so it actually becomes more difficult to find software that does not fit into any of these simple paradigms.

A program's reputation was determined by entering the name into the Google<sup>188</sup> search engine. Google reports the number of matching web sites, or hits. This paradigm was chosen because of the ranking system Google uses determines a site's credibility by examining the number and quality of sites linked to it. Proceeding on the assumption that "links are the currency of the web,"<sup>189</sup> the most popular and most credible search criteria will then return the highest number of results, or hits. Programs of various hit counts were considered and included in this survey.

The features category was quite broad. Under consideration were the file types used as the cover

carrier, the type of message allowed, the ease of use, and the quality of encryption. Cover carriers included various image file formats, specifically JPG, GIF and BMP; and the audio format MP3. Software was also found that placed the message at the end of any file. The types of messages allowed followed similar lines; they included all the image types listed above, simple text messages, and the ability to include the contents of any file. Ease of use was determined by screenshots and other material (directions, feature lists, help files) found on the source websites. Most programs listed their encryption method on the source website as well. The decision making process was influenced by the same variable as the other categories; variety being the key point of contention.

The final consideration before undertaking this research was the carrier cover on which the embedded message would be transmitted. A decision was made early on to only use images files; since the results would be presented in a paper format, it was determined that audio files would be too complicated or technical to present in an understandable fashion. The image was chosen from stock photos available on the Internet.<sup>190</sup> It was downloaded in the Jpeg format, which was converted to bmp and gif.

Before the conversion was attempted, though, steganalysis was performed on the image (using the technique discussed below) in order to protect against the ironic instance of an image that is already a stego-image. As a further safeguard, the image was resized from 1152 x 830 pixels to 864 x 623 with MS Paint (included in MS Windows).

The first software tested was Hide & Seek. DOS-only, it is a relic from another age. The intended cover carrier must be a gif file; embedded messages must be plaintext. It allows for encryption, but the version downloaded for this paper did not come with the encryption package. A Google search for Hide & Seek was technically implausible because of the common name: over 14,000 hits were returned, and judging by the first page, few had anything to do with steganography.

Use of the program was simple. It asks for the cover medium, the embedded message, and the stegokey. A button allows one to "hide" the text file; another allows one to "seek" it. The results were unimpressive. The gif file was already grainy from its conversion, but the resulting image had an even more grainy appearance. On top of this, the image was resized to 1024 x 768 pixels. However, the image was not stretched to match the new size; instead, a

black matte was placed on the bottom and right sides. It would appear that most of the message was placed in this section of the image since the area is filled with tiny red specks. The file size increase was rather small, from 312 kilobytes (KB) to 351 KB, but it was greater than the text file size (12 KB). The beginning and resulting images can be found in Appendix B.

Jsteg Shell, a Windows program, was chosen because of the relatively high hit count returned by Google. At 576, it was the highest of any non-commercial program checked against the search engine. This program was fairly impressive. Selection of the cover medium and embedded message were done through a "wizard:" a step-by-step, user-friendly system. It tells the user the amount of space available for the embedded message, and will warn the user if the selected file is too large. It can hide files of any type, so the embedded message could just as easily be an executable file as a plaintext message. Once hidden, the resulting image appeared to be a reflection of the starting image even though it hid an 11 KB document at the expense of only a single kilobyte. Both images can be found in Appendix B.

The final program selected for this survey was Camouflage. Camouflage integrates into Windows, showing up when a user right clicks on a file. A wizard gently guides the user through the process of hiding the embedded message. Camouflage is unique because it allows any file to be hidden in any other file. Unfortunately, that adaptability comes at a cost. Its steganographic technique does not obscure the message in the cover carrier; rather, it places the message at the end of the cover. All files have an end of file character that tells the computer when to stop reading. Camouflage merely places the message after this character. Detection, therefore, is fairly straightforward; a search for files with this anomalous pattern - and this search is quite common in virus-detection tools - is all that is really necessary.

Actually, detection (more legitimately referred to as steganalysis) of any of these programs is rather unremarkable. There are several common, well-documented approaches to steganography, and traditional steganalysis simply looks for the tell-tale patterns of each. Both Hide & Seek and Jsteg are grandfathers of the genre; the 'readme' file of Hide & Seek traces versions back to 1996; Jsteg, 1998. The patterns of each, therefore, are widely

disseminated. Jsteg even includes a concise description of the steganographic algorithm used.<sup>191</sup> This paper will examine the method used by Hide & Seek.

Hide & Seek uses gif files, and only gif files, as the cover medium. In the least technical terms possible, the first part of any gif file is a 256-color palette, to which each section (or pixel) of the image refers in order to determine its color. The values of this color palette are represented as integers; on a common scale, a value of 0 means black and a value of 255 means white. (This palette starts with 0 and ends with 255.) However, this scale can slide: it could represent 256 shades of blue, for example. It would be inaccurate to say that only one palette is used per file; however, for the purpose of clarity, this representation will suffice.<sup>192</sup> Hide & Seek simply adjusts the integers in these palettes so that they are each divisible by 4, rounding any other values as appropriate.<sup>193</sup> This results in a slight color shift. The white represented by 255, for example, becomes 252: a shift of just over 1%. One byte of the embedded message is then assigned to this new value. Since it is uncommon to find a 'naturally occurring' palette (naturally occurring in this instance means an untampered image) with these characteristics,

detection of this manipulation becomes a simple examination of the palette.

Since it is the easiest to implement, the method used by Hide & Seek is one of the most common. Unfortunately for anyone trying to hide a message, that also makes it the easiest to detect with steganalysis. Manipulation of an integer, or any other computer-represented value, is nothing more than a shift of the binary representation of the integer (or other value). For example, the integer 255 is 11111111 in binary.

Before continuing, it is appropriate to explain a few technical computer terms and methodologies. Each of the 1's above is called a bit, and its value can be either 1 or 0. Eight bits is called a byte. Characters like 'a' or 'b' are generally represented by a single byte - so, essentially, they are transformed into integers. There are common scales to determine the integer representation of a character. Modern personal computers use the American Standard Code for Information Interchange (ASCII) chart.<sup>194</sup> It is important, then, to note that to a computer, 'a' is only one integer away from 'b' - and the value of two colors on a palette are only a few integers away from each other. Even more important is the representation of these

integers. If 11111111 represents 256, then 11111110 represents 255. 252 is 11111100 in binary.

The differences between these numbers are found in the least significant bits (LSBs): the last bit in the byte. The steganographic method used by Hide & Seek capitalizes on this idea, and so do the steganalytic tools that are designed to detect use of this type of algorithm. Whenever non-random information is saved in a file, an analysis of the file will discover patterns in the distribution of bits, or bit patterns. Since most pictures contain information themselves - whether of a family portrait or a nuclear silo - bit patterns will emerge naturally. It is easy to compare the patterns of a clean image and a steganographic image if both are readily available. Unfortunately, in the real world, most are not, so looking for a known steganographic signature becomes the safest attack. StegDetect, a piece of public domain steganalytical software written by Neil Provos, a doctoral candidate in Computer Science at the University of Michigan, is an example of this tactic. It searches images for the steganographic patterns of four steganographic programs: Jsteg, the author's own Outguess, Jphide, and the commercial program Invisible Secrets.<sup>195</sup>

While this is appropriate for experimental software, it is not conclusive enough to certify an image as message free. A better method is to second-guess the nature of the embedding software by basing detection methods on the statistical search for anomalies. For example, it is easy to estimate the distribution of colors in an image simply by developing a histogram from the MSBs of each pixel in the file.<sup>196</sup> Another histogram, this time developed by analyzing the full color depth of each pixel, is then compared to the first computation. Any sufficiently large differences between the two would point to the possibility of an embedded message.<sup>197</sup> Unfortunately, testing for these anomalies can lead to an unnecessarily large number of false positives. Even Provos, in a study of Internet images with StegDetect -which, as noted above, does not use this method - found what he concluded to be false positives.<sup>198</sup> Any steganalysis has to be cognizant of the potential for these anomalies.

The security of steganography as a means of communication has not yet been decided by the academic community. Many researchers have contended that the science of steganography has not yet matured to the security allowed by its cousin encryption,<sup>199</sup> although a

level of security is added by encrypting the embedded message before it is placed in the cover carrier. However, the point of steganography is to communicate without the knowledge of a third party. N.J. Hopper contends in a September 2002 paper that he has discovered a series of steganographic techniques that are provably secure.<sup>200</sup> The science of encryption has labored under this methodology of theorize, disprove and theorize again since its inception; the most recent example being distributed.net's crack of RSA's RC5-64 encryption.<sup>201</sup>

The theories and practices of steganography are not going away. Methodologies and techniques are widely available on the Internet, in scholarly journals and books, and the minds of scholars worldwide. Even if this were not the case, the art of hiding information is not a completely nefarious occupation. It can be vital to corporate and private interests for the same reasons that encryption is; namely, that people deserve the right to keep secrets protected from unwanted eyes. In addition, steganography can be used in the practical application of watermarking. Copyright holders can use watermarks to protect their legal holdings and prevent the illegal distribution or tampering of these works. The 'broadcast flag' that the Federal

Communications Commission (FCC) is currently considering for digital television broadcasts<sup>202</sup> is just such an example.

So any concerted defense against steganography should not be so strong that it results in false positives or intervenes in legitimate uses of the technology. There has been discussion of taking an active approach to steganalysis: instead of merely listening to the data river of the Internet, random noise can be inserted into pictures to obscure or destroy any steganographic content.<sup>203</sup> It has also been suggested that steganalysis should become "a part of every virus-detection software."<sup>204</sup> While both can be valid bulwarks of our cyber-defense, it is the first suggestion, which is commonly referred to as an 'active warden,' that contains the most potential in stopping the spread of steganographic methods on the Internet.

Unfortunately, this also raises civil libertarian issues - an unseen government with unfettered access to all Internet communication - that may make an unmetered implementation of this defense hard for the public at large to accept.

The experiences of Azzam.com bring to light several concerns - especially when they are considered in an environment where an active warden is present. Fisk

suggests that these wardens should be used in a firewall-like configuration to block and reconfigure any steganographic messages.<sup>205</sup> Firewalls block malicious hackers from gaining access to a network, and can often be used to block certain websites and other content. Fisk's active warden would not block any traffic, but instead add noise to potentially steganographic traffic. This noise would have to remain in a precarious balance: it must not degrade image quality so much that the end user can notice the loss of quality, but it must add enough noise that any embedded message is destroyed. In order for this to be effective on a national level, a series of these firewalls must be placed on or near all of the major Internet thoroughfares (the 'backbone' in computer terms). This centralizes the burden of detection and elimination of steganographic threats. Otherwise, the publisher of each website would be responsible for keeping the contents steg-free. This is the current system. It is the shortcomings of taking this approach that raise these concerns in the first place.

In the case of Azzam.com, if the webmaster knew the contents were secret al-Qaeda communications (and it was proved that they were), and never did anything about it,

that webmaster could be held liable under current legal trends.<sup>206</sup> What about eBay.com then? eBay is a commercial site with no proven links to any terrorist organizations. There are thousands of active auctions on the site at any given time, each of which could contain a number of images. Would it then be eBay's responsibility to ensure there are no malicious pictures? Finally, what about the website in the middle? This could be, for example, one with a forum that allows users to post images in their messages. These are often run on shoestring budgets as a hobby of the webmaster. Would it still be the webmaster's responsibility to remove any of these images? If so, how would he or she obtain the resources to do so? Are we, as a society, willing to allow the tradeoff of the loss of a few 'hobby' websites for a supposed measure of increased security?

These questions lead to a more centralized approach to the problem of an active warden. So, then, what content would be analyzed? It would be implausible for these computers to filter every piece of a potential stego-medium. Instead, it is fair to assume that a 'blacklist' of destination sources and destinations would be identified and constantly updated so that the traffic coming in and

out of each would get a clean bill of health. Certainly, a statistical approach designed to trace this information would have to be taken because a known signature attack would not necessarily return enough results. But who is to decide what websites are on the blacklist? The reporting of newspapers and websites is not sufficient evidence to warrant the systematic tampering of a website's contents and traffic. Finally, an argument could be made that tampering would be an infringement on the image producer's right to free speech. These are issues the nation will have to deal with, especially as it adapts its laws to reflect emerging technologies.

### Conclusions

The Internet presents a new set of challenges for the counter-terrorist officer simply because it allows for greater communication capabilities. Essentially, the transnational nature of the Internet and similar technologies facilitates the global spread of organizations such as al-Qaeda. Cell leaders (small, non-connected groups of would-be terrorists that have reportedly been established in most Western countries) can remain in constant communication with their connections in al-Qaeda

and other terrorist groups. At the same time, the Internet remains one of the easiest and most efficient direct recruiting and communication channels of the disaffected and disenfranchised.

Countering these developments is often futile. Steganalysis, for example, is akin to a search for a needle in a haystack - only in this case, the needle has been disguised to look and feel like any other piece of straw. Even when the rhetoric and communications are left in the open, they are often difficult to counter. Websites can be established quickly and fleetingly, located in disinterested countries or hosted by sympathetic companies, and contain extremist rhetoric, commands, or communications.

Moreover, many mediums, including chat rooms, are unstable sources for the law enforcement official; the information in chat rooms exists only for the moment at which the conversation exists. The software that runs chat rooms, websites, et cetera, is readily available and relatively easy to install for anyone with the relevant background knowledge. In these cases, terrorists can simultaneously connect to a private, unadvertised server for a short time, engage in their communication, and then

never visit the server again. Obviously, the temporary nature of these practices enables terrorist activity to remain under the radar, throwing up a significant roadblock against counter-terrorist efforts.

Even websites that are more permanent, like Azzam.com or its successors, tend to regenerate. Since they are intended more for propaganda purposes than communication, the impetus to keep these websites alive is strong. Whether through IH's efforts or otherwise, HAMAS's reputed website, Palestine-Info, has been closed several times, but that has not stopped its owners from simply moving to a different server.

The dynamicism displayed by the tenacity of terrorists to keep their online presence viable is symbolic of their real-world tactics. The long-term futility and endless nature of counter-terrorism strategy, then, calls for a different approach. Ideology drives terrorists, keeping the fervor to continue strong. An effective counter-terrorism strategy, even one limited to cyberspace, cannot focus simply on these back-and-forth tactics and ignore the role of ideology. Chapter six offers a few such suggestions.

CHAPTER FIVE  
GOVERNMENT REACTIONS

Western governments have not neglected the cyberterrorism threat. Indeed, since 1998, when U.S. President Clinton signed Presidential Decision Directive 63 (PDD-63) has, at varying levels, focused on the intricacies of the threat. A particular theme since this time has been the integration of the public and private sectors in addressing vulnerabilities. This exploration of means to counteract the threat were reinforced and addressed at more length in the 2002 *National Strategy to Secure Cyberspace*, the official U.S. policy paper on the matter.

The U.S. has not been alone in formulating policy and legislation to protect cyberspace. The European Union, in particular, created the Convention on Cybercrime in 2001 to deal with the problems of protecting cyberspace. Although it did not specifically deal with the threat from cyberterrorism, it nevertheless established an inter-governmental framework for a criminal justice question that transcends borders. This, of course, can be problematic, as the intergovernmental cooperation clauses could require one state's definition of a terrorist to trump another's.<sup>207</sup>

Nonetheless, it moves the debate into the realm of international law. President Bush has urged the Senate to ratify the treaty.<sup>208</sup>

Several other nations have established legislation or executive action to deal with cyberterrorism. Their numbers have mostly been limited, though, to states that perceive it as a threat – a problem when dealing with a security threat that can emanate from any state. In 2000, for example, the “I Love You,” or “Love Bug” virus infected more than 1.27 million computers, forced the U.S. State Department to temporarily disconnect from the Internet, and spawned several variants.<sup>209</sup> Despite all this damage, the suspected author, a Filipino man living in Manila, was never convicted because the Philippines did not have any laws against such actions.<sup>210</sup>

This illustration serves to underscore the importance of international contiguity of legal codes dealing with this issue. The E.U.’s Convention, which was signed in 2001 by 30 countries including the United States, can help serve this purpose, since it attempts to build an international consensus in the approach to countering cyberterrorism.<sup>211</sup> The remainder of this chapter, however, will be limited to exploring the U.S. government’s reaction

to the cyberthreat, focusing particularly on the *National Strategy to Secure Cyberspace* and its criticisms.

### U.S. Reactions

The U.S. government's first notable recognition of the threat from cyberterrorism emerged from the 1997 report of the President's Commission on Critical Infrastructure Protection. The Commission determined that cyberthreats took several forms: an attack on specific databases or other information repositories; one geared simply toward gaining network access; simple espionage; shutting a particular service or sets of services down (particularly via Denial of Service techniques); and the "introduction of harmful instructions" - everything from viruses to deliberate corruptions of data.<sup>212</sup>

The report sparked the 1998 Presidential Decision Directive 63 (PDD-63). The document recognized seven categories that made up critical infrastructure: "telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."<sup>213</sup> Equally important, PDD-63 sought a public-private partnership to determine the best way to protect critical infrastructure, much of which was

controlled by private institutions. It conveyed the belief that market forces should sufficiently pressure private institutions into compliance with accepted best practices; in so doing, the directive asserted that those charged with protecting the nation's critical infrastructure should "seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector."<sup>214</sup> This idea continued as a trend in future policy documents.

PDD-63 called for several other changes as well. Most prominent among these, the Directive called for the establishment of a National Infrastructure Protection Center (NIPC) and an Information Sharing and Analysis Center (ISAC).<sup>215</sup> Three ISACs were eventually created, serving the Financial Services, Telecommunications and Information Technology sectors.<sup>216</sup>

The Information Technology ISAC (IT-ISAC) is the ISAC most relevant to the discussion at hand. Serving as a trade association, its membership is restricted to U.S. based "firm[s] or corporation[s]."<sup>217</sup> Despite this limitation, its 24 members include several top security and software companies like Microsoft, Symantec, and Oracle.<sup>218</sup> Nonetheless, significant information technology sectors,

particularly open source representatives, are notably absent. As such, the alerts the Center releases are limited to problems with software from the companies represented.<sup>219</sup>

Part of the cause for this lies in the membership restrictions. Most open source software is not controlled by a specific company; instead, volunteers develop the product. Accordingly, the software is usually free to install, often leading to widespread use. For example, Netcraft, a company specializing in web site statistics, found in a May 2004 survey that 66.99% of websites (33,329,879 total sites) currently use the open source Apache web server.<sup>220</sup> IT-ISAC's exclusion of this product therefore limits its ability to provide an effective alert system to the public. Furthermore, since its membership is based in the private sector, the entire alert system is completely voluntary. There is little impetus for firms to not only release vulnerability alerts to the public, but also share that information with competitors.

The NIPC, established under the FBI but now under the Department of Homeland Security, provides weekly warnings and emergency bulletins regarding cyberthreats. Although it still exists in a limited form, it was merged in 2003

with several other agencies to create the United States Computer Emergency Readiness Team (US-CERT). US-CERT provides Alerts, Information Bulletins, and Tips to assist the public in their efforts to protect their computer systems. The most recent weekly bulletin at the time of writing, dated April 28, 2004, lists new vulnerabilities, exploits and viruses in software systems discovered between April 6 and April 26, 2004. The document is 70 pages in length.<sup>221</sup> Obviously, this is an incredible amount of information for the end user to wade through. At the same time, though, it shows the continued proliferation of threats in cyberspace.

Released in February 2003, *The National Strategy to Secure Cyberspace* updated the policies outlined in PDD-63. Most importantly, it recognized that the effective defense of cyberspace requires the cooperation and "coordinated and focused effort" from "the federal government, state and local governments, the private sector, and the American people."<sup>222</sup> Furthermore, it recognized that the challenge is threefold: prevention of critical infrastructure from cyber-based attacks, reduction in vulnerability, and the absolute minimization of both the damage caused and the

time required to recover.<sup>223</sup> Finally, it recognized five priority areas:

- "I.A National Cyberspace Security Response System;
- II. A National Cyberspace Security Threat and Vulnerability Reduction Program;
- III. A National Cyberspace Security Awareness and Training Program;
- IV. Securing Government's Cyberspace; and
- V. National Security and International Cyberspace Security Cooperation."<sup>224</sup>

These three aspects - society wide involvement, focal points and priority areas - provide a useful structure for establishing a system wide cybersecurity strategy. It extends the public-private partnership paradigm to include all sectors, recognizes the threats, and provides the impetus for a centralized, system-wide information sharing center that all Americans are aware of and use.

Unfortunately, some of the fundamental ideas built into the structure, particularly in information dissemination and standards compliance, limit its effectiveness.

Priority I, the Cyberspace Response System, looks to establish a system that provides analysis and vulnerability assessments, a warning and information network that simultaneously provides a "synoptic view of the health of cyberspace," and an incident management and recovery system.<sup>225</sup> Priority II recommends threat deterrence and

reduction campaigns, including new law enforcement techniques; the concerted recognition and neutralization of existing threats; and the greater incorporation of security concerns into new products. Particularly, it looks to improve both Supervisory Control And Data Acquisition Systems (SCADA), which control critical infrastructure, and the underlying technologies and physical components that allow the Internet to function. It also recognizes that the threats and vulnerabilities to cyberspace constantly evolve.<sup>226</sup> The third priority seeks to establish an extensive awareness campaign in the country, particularly in large enterprises and home user sectors. Its only proposed method of addressing home users, however, is through education at the primary, secondary, and higher education levels; it ignores those not involved in the nation's education system.<sup>227</sup>

The *Strategy's* efforts to secure the federal government's information system, found in the fourth priority, are among the most thorough recommendations offered. It addresses several components to this process, including continued vulnerability and threat assessment, especially on an agency specific basis; tight user management; and special attention to ensuring that private

contractors the government outsources projects to adopt responsibly security strategies. State and local governments, on the other hand, are simply directed to work with DHS to find solutions that fit their needs.<sup>228</sup> Finally, the last priority seeks to strengthen law enforcement coordination on cyberspace matters between U.S. agencies and their counterparts worldwide, assisting countries whose capabilities in this regard are deficient.<sup>229</sup>

The release of the *Strategy* was greeted with criticism from several corners of the computer security sector. Most of their complaints stemmed from the fact that the document did not actually require anything of anyone - it only made recommendations; particularly to the private sector, whose cooperation was completely voluntary. News.com said it "lacked muscle."<sup>230</sup> On the other hand, The Center for Democracy and Technology, a think tank dedicated to privacy and security issues, was concerned that the draft version of the document did not do enough to protect online privacy.<sup>231</sup> Bruce Schneier of Counterpane Industries, a prominent security firm, had a much more long-winded, but still important, set of criticisms:

"This National Strategy document isn't law, and it doesn't contain any mandates to government agencies. It has lots of recommendations. It has all sorts of processes. It has yet another list of suggested best practices. ... But plans, no matter how detailed and how accurate they are, don't secure anything; action does.

And consensus doesn't secure anything. Preliminary drafts of the plan included strong words about wireless insecurity, which were removed because the wireless industry didn't want to look bad for not doing anything about it. Preliminary drafts included a suggestion that ISPs provide all their users with personal firewalls; that was taken out because ISPs didn't want to look bad for not already doing something like that.

And so on. This is what you get with a PR document. You get lots of varying input from all sorts of special interests, and you end up with a document that offends no one because it demands nothing.

...Security is a commons. Like air and water and radio spectrum, any individual's use of it affects us all. The way to prevent people from abusing a commons is to regulate it. Companies didn't stop dumping toxic wastes into rivers because the government asked them nicely. Companies stopped because the government made it illegal to do so."<sup>232</sup>

Certainly, many of these, and other criticisms,<sup>233</sup> are valid. Their concerns may not have been addressed, however, because of the difficulty of enforcement. At the user level, public understanding and awareness of computer related issues remains low. Much like an automobile or any other technological tool, many end users simply expect

their computer to function. The inner workings of the system do not enter into their daily life, so forcing them to incorporate security concerns, even with the threat of punishment, could stifle growth and/or lead to an unnecessary overload in computer crime enforcement cases.

Mandates at the corporate level face similar roadblocks. Should a software firm, such as Microsoft, face a punitive response if a heretofore unforeseen security vulnerability is discovered in their products? Likewise, mandates could open the door for litigation, both against software creators and a compromised organization, which could be sued by business partners concerned by their security policies or by customers negatively affected by the downtime.

Finally, there is an inherent problem in trying to enforce legislation on an issue that constantly evolves.<sup>234</sup> Bureaucratic and congressional inertia often delays law-making and enforcement activities. Due to their dynamic nature, attention to cybersecurity issues must remain fluid to be effective.

Nonetheless, it is difficult to find evidence of the effectiveness of the current voluntary strategy. Although the software of several firms was listed as compromised in

the April 27, 2004 US-CERT Information Bulletin,<sup>235</sup> as of May, 2004, IT-ISAC's alert archive had not been updated since January, 2004.<sup>236</sup> Obviously, corporations are not voluntarily divulging information that could negatively impact their bottom line. A compromise, then, would have to find a path between absolute mandates and mere encouragement.

Congress has provided a few alternatives that may be helpful. One of the most promising of these is the *Cyber Security Research and Development Act* (H.R. 3395), which was passed by Congress in 2002. The law provides funding for fellowships and research programs on cyber security research.<sup>237</sup> The *Cyber Security Enhancement Act* of 2002, which comprised Section 225 of the *Homeland Security Act* of the same year, addressed cyberterrorism from a law enforcement viewpoint. It directs sentencing authorities to account for the intentions of the attack, especially whether or not human or public health was threatened, when determining a guilty cyberterrorist's punishment.<sup>238</sup> Congressional committees have also conducted several hearings on cyberterrorism and the protection of critical infrastructure systems.

## Conclusions

U.S. policy *vis-a-vis* cyberterrorism is still in its infancy. It has not had the time required to develop into a full-fledged policy set, especially in the prevention area. It has, however, taken the first few steps toward that goal, particularly in *The National Strategy to Secure Cyberspace's* efforts to achieve ubiquitous online security throughout all sectors.

The *Strategy* holds two key themes. First, an effective counter-cyberterrorism strategy must encompass all of society. Schneier is correct in his assertion that online security represents a commons; this threat can be best understood in the context of compromised agent machines involved in a Denial of Service attack. Similarly, the nation's Internet infrastructure is held in private hands. Protection of that infrastructure therefore rests primarily on those entities.

Second, the *Strategy* recognizes that information sharing and dissemination will remain key to any effective policy. This includes information collected before, during, and after an attack, and requires the cooperation of the public and private sector with an information clearinghouse such as US-CERT. Information dissemination

is ineffective, however, without a public conscientious of both the threat and vulnerabilities they face and an information source for solutions.

The implementation of these policies does have problems, however. Most of these revolve around the weight of the *Strategy's* recommendations, which require nothing but voluntary cooperation of the involved sectors. Mandating policy in such a dynamic environment is problematic, of course, so an alternative approach needs to be taken. As time passes, however, workarounds to this contradiction are likely to occur. Like cyberterrorism itself, cybersecurity is constantly evolving. Given proper attention, public policy will undoubtedly advance with it.

## CHAPTER SIX

### CONCLUSIONS AND PRESCRIPTIONS

"Not long ago, we marked the 20th anniversary of a terrorist attack in Beirut, Lebanon, when the suicide bomb truck attacked the Marine barracks. And that blast killed more than 240 Americans. Soon after that attack, President Reagan and Secretary of State Shultz asked me to serve as the Middle East envoy for a period. That experience taught me lessons about the nature of terrorism that are relevant today as we prosecute the global war on terror. After the attack, one seemingly logical response was to put a cement barricade around the buildings to prevent more truck bombings -- a very logical thing to do. And it had the effect of preventing more truck bombings. But the terrorists very quickly figured out how to get around those barricades, and they began lobbing rocket-propelled grenades over the cement barricades. And the reaction then was to hunker down even more, and they started seeing buildings along the Cornish that runs along the sea in Beirut draped with metal wire mesh coming down from several stories high so that when rocket-propelled grenades hit the mesh, they would bounce off, doing little damage. It worked, again, but only briefly. And the terrorists again adapted. They watched the comings and goings of embassy personnel and began hitting soft targets. They killed people on their way to and from work. So for every defense, first barricades then wire mesh, the terrorists moved to another avenue of attack. One has to note that the terrorists had learned important lessons: that terrorism is a great equalizer, it's a force multiplier, it's cheap, it's deniable, it yields substantial results, it's low risk and it's often without penalty. They had learned that a single attack by influencing public opinion and morale can alter the behavior of great nations..."<sup>239</sup>

Unique among the mediums by which terrorists can attack, cyberspace is characterized by a mindset that must constantly evolve to survive. This has been an intricate part of cybersecurity since the first worm, the first virus, the first hacking attempt. When combined with the ideological fervor that drives many terrorist organizations, this sense of perpetual adaptability grows stronger.

This thesis has shown, albeit in abbreviated form, several of the current and potential approaches to cyberterrorism. This is nothing more than a snapshot of past and present threats. A new, heretofore unforeseen approach or attack could emerge at the blink of an eye and spread like wildfire throughout the hacking, cracking, hacktivist, and cyberterrorist communities. This phenomenon becomes evident each time a new, quickly spreading worm emerges. Upon detection, cybersecurity experts examine the intrusive software, determine a fix, and then, once the fires have died down a bit, attempt to find similar vulnerabilities that could be exploited. They do not expect their work to ever be fully completed, so neither should a counter-cyberterrorist agent.

Three areas of cyberterrorism have been addressed: (1) virtual attacks upon other virtual entities; (2) virtual attacks focused on physical critical infrastructure systems; and (3) the use of the Internet as a communications device. The latter is not only the most prevalent example of cyberterrorism, but the most dangerous as well. Even attacks on critical infrastructure, as devastating as they could be, still are confined in scope. Information on the Internet, on the other hand, is global. It can be used as propaganda or to recruit new members. Moreover, it can be employed as a communications medium between disparate terrorist cells and their leadership. This facilitates the global nature of modern terrorist organizations, providing them with a greater means for attack. Accordingly, cybersecurity experts in counterterrorist units must be allowed to address each of these areas in order to fulfill their duties.

There are several ways to facilitate their work. Like the *National Strategy to Secure Cyberspace*, most of these recommendations revolve around information sharing, both on the database and awareness fronts. An effective implementation of these prescriptions would see them realized, where appropriate, at all levels of an

interconnected, global society - local, national, and inter-governmental.

US-CERT's Information Bulletins have the potential to efficiently distribute important information to protect the public's online entities. They could nonetheless use some improvement in their ability to distribute the information they contain, however.

In addition to the Bulletins and other alerts, US-CERT should create a searchable database of vulnerabilities and exploits. This database should enable the end user to list vulnerabilities by date recognized for a specific software product. By doing so, the database will enable the user to ensure their software is completely up to date. In fact, a useful add-on to this database would be a piece of software that scans a user's computer and, after connecting to the database, presents the user with software patches and updates that will protect their machine. In addition, software vendors should include a link to this database and update software in their installation program. Instead of forcing the user to go to each software vendor for updates, then, this centralizes and streamlines the process for the end user and makes him or her more likely to take the steps necessary to protect the machine.

This idea is not without flaws, of course. Privacy issues spring foremost to the list of criticisms, as any government-sponsored investigation of a user's hard drive could be misused or viewed as suspicious. Another problem may arise from the software industry. Understandably, companies will not want to admit that their software could be vulnerable to security issues, as that is tantamount to admitting an inability to create secure software. The lack of timely alerts on IT-ISAC's websites indicates the resistance of software companies to sharing this knowledge. Furthermore, software vendors will probably express concern over giving up control over their products to a third party. Nonetheless, these issues can be expressed through a careful and concerted campaign.

The public will also stand to benefit from a more effective awareness campaign than the one outlined in *The National Strategy to Secure Cyberspace*. The *Strategy's* campaign is limited to business and educational institutions. Awareness programs should also target home users, especially since the increasing prevalence of broadband connections increases the pool of machines available to serve as agents in a denial of service attack. Advertising campaigns may work for this; more effective,

though, representatives of US-CERT should make themselves available to the media whenever an attack occurs or a major new virus or worm hits the Internet. If the media looks to US-CERT for guidance at such times, the public will probably follow.

Cyberterrorism experts should also seek to create a database that tracks cyberterrorist activity. The RAND-MIPT Terrorism Incident database provides a useful model for this. It allows a user to search for information on terror attacks by group, target, weapon used, region, country, and city.<sup>240</sup> Updated regularly, the database should track all cyberspace attacks in which law enforcement officials believe cyberterrorism was involved. Moreover, it should consider a number of variables, including the type of attack, source, tools used (and whether they seemed to be publicly available or homegrown), probability of repetition, and rationale for classifying it as terrorism. Even if law enforcement officials later rescind this categorization (which should be in the database as well), an entry for the attack should remain so as to facilitate a better understanding of law enforcement's relationship to the threat. Further analysis can determine flaws in the law enforcement system or

legislation that can be corrected to help assist later inquiries.

Finally, every counter-cyberterrorism effort should be undertaken with an eye toward two facets: cooperation with other states and inter-governmental agencies, and the motivations behind the attacks. This comprehensive understanding and approach will facilitate a quicker response to the threat, and an ability to predict the sources, methods and motivations of future attacks or activities:

Cyberterrorism is a global problem; it requires a global solution. Its low entry cost makes it the most equalizing attack method or force multiplier available to many actors. As a result, cyberterrorist threats will only continue to grow. To protect themselves, states, along with the scholars that research the topic, must not only heighten their awareness of the threats, but take steps to counter them as well. Serious problems from cyberterrorism may not arise immediately, but they will eventually. Without proper attention and precautionary steps taken now, those problems will become catastrophes.

APPENDIX A

GLOSSARY

## Terms

**Bit** - The smallest piece of information a computer can store. A bit can either have the value '0' or '1.'

**Byte** - A string of eight bits. One byte usually stores one character, such as a number or letter.

**Critical Infrastructure** - The infrastructure systems that allow modern society to function. These include electricity, water, transportation, and telecommunications equipment and stations.

**Cyberterrorism** - A loose definition is used in this text. Generally, it refers to online activity used to promote the political causes of terrorists.

**Cyberterrorist** - An individual or group that engages in cyberterrorism.

**Denial of Service (DoS) Attack** - An attempt to neutralize a network by flooding it with unnecessary information.

**Hacktivist** - Hacker who uses his or her skills to further an activist cause.

**Jihad** - Literally, jihad means "struggle" in Arabic. In the context of mainstream Islamic discourse, there are

two forms of jihad. The Greater Jihad refers to the internal struggle between a person and God; the Lesser Jihad is the defense of Islam.

**Load anomaly** - Occurs when an unusual amount of resources are used without an apparent cause. Applies to networks and processors.

**Mujahideen** - Warriors fighting to defend Islam.

**Netwar** - An organizational structure, especially attuned to the Information Age and asymmetrical warfare, in which the interconnectivity of modern technology allows for less hierarchy and more adaptability.

**Steganalysis** - The process of analyzing a file to determine if it holds a steganographic message.

**Steganographic Message** - A message hidden using steganography.

**Steganography** - Hidden messages in Greek, steganography is the act of hiding a message inside an innocuous container. In the computer world, this often refers to attempts to hide information within image files.

**Terrorism** - An ill-defined term, in this text, terrorism is motivated by political change, is often attributed to non-state actors, and involves violence against an individual, society, or property.

**Virus** - A software program designed to gain ungranted access to a computer. Viruses often produce malicious results, including deleted or corrupt files. They require some form of user interaction to attack.

**Worms** - A worm is basically a self-replicating virus. When connected to a network, many worms can spread across the Internet in a matter of minutes.

Agencies

D.H.S. - Department of Homeland Security.

F.B.I. - Federal Bureau of Investigation.

IT-ISAC - Information Technology Information Sharing and  
Analysis Center.

N.I.P.C. - National Infrastructure Protection Center.

US-CERT - United States Computer Emergency Response Team.

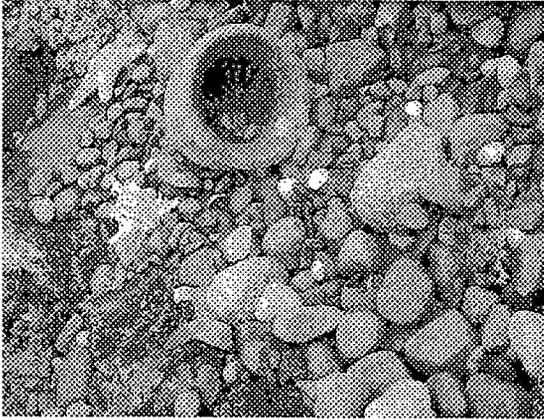
APPENDIX B  
STUDY OF CYBERTERRORISM IN  
TERRORISM TEXTS

- Alexander, Yonah, GK Hall and Company and Alan O'Day.  
*Middle East Terrorism: Current Threats and Future Prospects (The International Library of Terrorism, Vol 5)*. Boston: GK Hall, 1994.
- Badey, Thomas J. *Annual Editions: Violence and Terrorism 03/04*. New York: McGraw Hill/Dushkin, 2002.
- Bergen, Peter L. *Holy War, Inc.: Inside The Secret World of Osama Bin Laden*. New York: The Free Press, 2001.
- Bushart, Howard L., John R. Craig and Myra Edwards Barnes.  
*Soldiers of God: White Supremacists and Their Holy War for America*. New York: Kensington Publishing Corporation, 2000.
- Combs, Cindy C. *Terrorism in the 21st Century (3rd Edition)*. Englewood Cliffs: Prentice Hall, 2002.
- Cooley, John K. *Unholy Wars: Afghanistan, America and International Terrorism*. Sterling: Stylus Publishing, 2000.
- Emerson, Steven. *American Jihad: The Terrorists Living Among Us*. New York: The Free Press, 2002.
- Esposito, John L. *Unholy War: Terror in the Name of Islam*. New York: Oxford University Press, 2002.
- Hoffman, Bruce. *Inside Terrorism*. New York: Columbia University Press, 1998.
- Juergensmeyer, Mark. *Terror in the Mind of God: The Global Rise of Religious Violence*. Los Angeles: University of California Press, 2001.
- Lake, David A. and Donald Rothchild. *The International Spread of Ethnic Conflict*. Princeton: Princeton University Press, 1998.
- Laqueur, Walter. *A History of Terrorism*. New Brunswick: Transaction Publications, 2001.
- Laqueur, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. New York: Oxford University Press, 1999.

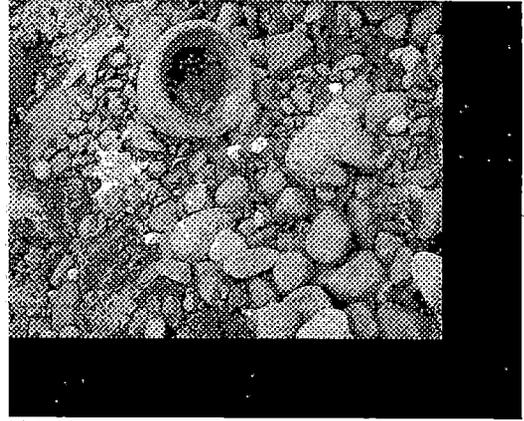
- Martin, Gus. *Understanding Terrorism: Challenges, Perspectives and Issues*. Thousand Oaks: Sage Publications, 2003.
- Michael, Lou and Dan Herbeck. *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing*. New York: Regan Books, 2001.
- Pillar, Paul R. and Michael H. Armacost. *Terrorism and U.S. Foreign Policy*. Washington, D.C.: The Brookings Institution, 2001.
- Rashid, Ahmed. *Taliban: Militant Islam, Oil and Fundamentalism in Central Asia*. New Haven: Yale University Press, 2001.
- Reich, Walter and Walter Laqueur. *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*. Washington, D.C.: Woodrow Wilson Center Press, 1998.
- Seale, Patrick. *Abu Nidal: A Gun for Hire: The Secret Life of the World's Most Notorious Arab Terrorist*. New York: Random House, 1992.
- Stern, Jessica. *Terror in the Name of God: Why Religious Militants Kill*. New York: Ecco Press, 2003.
- Tourish, Dennis and Tim Wohlforth. *On the Edge: Political Cults Right and Left*. Armonk: M.E. Sharpe, 2000.
- Weimann, Gabriel and Conrad Winn. *The Theater of Terror: Mass Media and International Terrorism*. Boston: Addison-Wesley Publishing, 2000.
- Whitaker, David J. *The Terrorism Reader*. New York: Routledge, 2003.
- Wiktorowicz, Quintan. *The Management of Islamic Activism: Salafis, the Muslim Brotherhood, and State Power in Jordan*. New York: State University of New York Press, 2001.
- Worcester, Kenton, Sally Avery Bermanzohn and Mark Ungar. *Violence and Politics: Globalization's Paradox (New Political Science Reader)*. New York: Routledge, 2002.

Zinn, Howard and Anthony Arno. *Terrorism and War*. Canada:  
Seven Stories Press, 2002.

APPENDIX C  
RESULTS OF STEGANOGRAPHY  
TESTS



*Original file : wetrocks.jpg.*



*After hide & Seek.*



*After Jsteg.*

## ENDNOTES

<sup>1</sup> U.S. FBI Definition of Terrorism, cited in Jonathon White, *Terrorism* (Stamford: Wadsworth Thomas Learning, 2002), 12.

<sup>2</sup> United States Department of State, *Patterns of Global Terrorism*, April 2004.

<sup>3</sup> White 12.

<sup>4</sup> Ayla Schbley, "Defining Religious Terrorism: A Causal and Anthological Profile," *Studies in Conflict & Terrorism* 26 (2003), 105-134.

<sup>5</sup> Mark Juergensmeyer, *Terror in the Mind of God*, (Berkeley: University of California Press, 2001), 61.

<sup>6</sup> "Official: Voice on tape is bin Laden's," *CNN*, 13 November 2002; [home page on-line]; available from: <http://www.cnn.com/2002/WORLD/meast/11/12/binladen.statemen t/>; Internet; accessed 5 May 2004.

<sup>7</sup> U.S. Department of Transportation, "Marad Advisory 02-07 (102300Z)" 02 October 2002; [home page on-line]; available from: [http://www.marad.dot.gov/Headlines/advisories/2002\\_07.html](http://www.marad.dot.gov/Headlines/advisories/2002_07.html); Internet; accessed 5 May 2004.

<sup>8</sup> "Mark Pollitt, "Cyberterrorism - Fact or Fancy?" FBI Laboratory, 1997; [home page on-line]; available from: <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>; Internet; accessed 4 May 2004.

<sup>9</sup> Ann McFeatters, "Cyber-enemy: America's newest threat is lurking behind computer screens," *Pittsburgh Post-Gazette* 21 March 2001; [e-journal]; available at: <http://www.post-gazette.com/forum/20010325edann5.asp>; accessed 5 May 2004.

<sup>10</sup> Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *Networks and Netwars: The Future of Terror, Crime and Militancy*, ed. Arquilla and Ronfeldt (Santa Monica: Rand Corporation, 2001), 239-288.

<sup>11</sup> Annaliza Savage, "Hacktivism Changes the Rules," 15 September 2000; [home page on-line]; available from: <http://www.techtv.com/news/securityalert/story/0,24195,11867,00.html>; accessed 5 May 2004.

<sup>12</sup> Hacktivism, available from: <http://www.hacktivism.com/>; accessed 5 May 2004.

<sup>13</sup> David Ronfeldt and John Arquilla, "What next for Networks and Netwars?," *Networks and Netwars: The Future of*

*Terror, Crime, and Militancy*, ed. J. Arquilla and D. Ronfeldt (Santa Monica: Rand Corporation, 2001), 311-361.

<sup>14</sup> Statistic taken from EbscoHost's Library Holdings page. As this page is only available after logging in, no retrievable link can be given.

<sup>15</sup> Search conducted several times, most recently on 24 April 2004.

<sup>16</sup> Search conducted several times, most recently on 24 April 2004.

<sup>17</sup> Search conducted on 24 April 2004.

<sup>18</sup> Search conducted on 24 April 2004.

<sup>19</sup> Survey conducted on 5 May 2004.

<sup>20</sup> White 254.

<sup>21</sup> James Ballard, Joseph Hornik, and Douglas McKenzie, "Technological Facilitation of Terrorism," *American Behavioral Scientist* 45 6 (2002), 989-1016.

<sup>22</sup> Michael Whine, "Cyberspace - A new Medium for Communication, Command and Control by Extremists," *Studies in Conflict and Terrorism* 22 3 (1999), 231-246.

<sup>23</sup> Bunt.

<sup>24</sup> See Denning, above, and Dorothy Denning, *Information Warfare and Security*, (Reading: Addison Wesley, 1999).

<sup>25</sup> Erbschloe 242-249.

<sup>26</sup> David Ronfeldt and John Arquilla, "What next for Networks and Netwars?," *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. J. Arquilla and D. Ronfeldt (Santa Monica: Rand Corporation, 2001), 311-361.

<sup>27</sup> To name a few: François Debrix, "Cyberterrorism and Media-Induced Fears: The Production of a Media Culture," *Strategies* 14 1 (2001).

Alison Anderson, "Risk, Terrorism, and the Internet," *Knowledge, Technology and Policy* 16 2 (2003), 24-34.

Shlomo Shpiro, "Conflict Media Strategies and the Politics of Counter-terrorism," *Politics* 22 2 (2002), 76-86.

<sup>28</sup> Yonah Alexander and Michael Swetnam, *Cyber Terrorism and Information Warfare: Threats and Responses*, (Ardsley: Transnational Publishers, 2001).

<sup>29</sup> Rohan Gunaratna, *Inside Al Qaeda* (Berkley Books: New York 2002).

<sup>30</sup> Walter Laqueur, *A History of Terrorism* (Transaction: New Brunswick, 2002).

<sup>31</sup> James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *Center for Strategic and International Studies*, December 2002.

<sup>32</sup> Winn Schwartau, *Pearl Harbor Dot Com*, (New York: Interpact Press, 2002).

<sup>33</sup> Winn Schwartau, "Infrastructures R Us," *Crossnodes* 8 July 1999; [home page on-line]; available from: <http://networking.earthweb.com/netsysm/article.php/613551>; Internet; accessed 5 May 2004.

<sup>34</sup> Verton, 1-16.

<sup>35</sup> François Debrix, "Cyberterrorism and Media-Induced Fears: The Production of a Media Culture," *Strategies* 14 1 (2001).

<sup>36</sup> David Ronfeldt and John Arquilla, "What next for Networks and Netwars?," *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. J. Arquilla and D. Ronfeldt (Santa Monica: Rand Corporation, 2001), 311-361.

<sup>37</sup> Gary Bunt, *Islam in the Digital Age*, (London: Pluto Press, 2003).

<sup>38</sup> Matthew Littleton, "Information Age Terrorism: Toward Cyberterror," Naval Post-Graduate School, December 1995; [home page on-line]; available from: <http://www.fas.org/irp/threat/cyber/docs/npgs/terror.htm>; Internet; accessed 6 May 2004.

<sup>39</sup> "Internet Archive," *Archive.org*, No Date; [home page on-line]; available from: <http://www.archive.org/>; accessed 6 May 2004.

<sup>40</sup> "Google Web Search Features," *Google.com*, No Date. [home page on-line] available from: <http://www.google.com/help/features.html#cached>; Internet; accessed 6 May 2004.

<sup>41</sup> Jack Kelley. "Militants wire web with links to Jihad," *USA Today*, 10 July 2002.

<sup>42</sup> Internet Haganah; [home page on-line]; available from: <http://www.haganah.us/haganah>; Internet; accessed 6 May 2004.

<sup>43</sup> "ACM Digital Library," Association for Computer Machinery (ACM), No Date; [home page on-line]; available from: <http://portal.acm.org/dl.cfm>; Internet; accessed 6 May 2004.

<sup>44</sup> Jim Wolf, "First 'Terrorist' Cyber-attack Reported by U.S.," *Reuters*, May 5 1998. Retrieved via *Factiva*, 1 May 2004.

<sup>45</sup> "Liberation Tigers of Tamil Eelam," *International Policy Institute for Counter Terrorism*, No Date; [home page on-line]; available from:  
[http://www.ict.org.il/inter\\_ter/orgdet.cfm?orgid=22](http://www.ict.org.il/inter_ter/orgdet.cfm?orgid=22);  
Internet; accessed 1 May 2004.

<sup>46</sup> Dorothy Denning, "Cyberwarriors: Activists and Terrorists Turn to Cyberspace," *Harvard International Review* 23, 2 (2001); [e-journal]; available from:  
<http://www.hir.harvard.edu/articles/index.html?id=905>;  
Internet; accessed 1 May 2004.

<sup>47</sup> Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw Hill/Osborne, 2003), 96.

<sup>48</sup> Corey Grice, "How a basic attack crippled Yahoo," *Cnet News.com*, February 7 2000; [e-journal]; available from: <http://news.com.com/2100-1023-236621.html?legacy=cnet>; Internet; accessed 23 April 2004.

<sup>49</sup> Linda Rosencrance, "'Mafiaboy' to plead guilty to hacking major Web sites," *Computerworld*, November 7, 2000; [e-journal]; available from:  
<http://www.computerworld.com/securitytopics/security/story/0,10801,53492,00.html>; Internet; accessed 23 April 2004.

<sup>50</sup> Sven Dietrich, Neil Long, and David Dittrich, "Analyzing Distributed Denial of Service Tools: The Shaft Case," *Proceedings of the Second ACM SIGCOMM Workshop on Internet Measurement*, 2002, 329-339.

<sup>51</sup> David Moore, Geoffrey Voelker and Stefan Savage, "Inferring Internet Denial-of-Service Activity," *Usenix Security Symposium*, 2001.

<sup>52</sup> Ahsan Habib, Mohamed Hefeeda and Bharat Bhargava, "Detecting Service Violations and DoS Attacks," *Network and Distributed System Security Symposium Conference Proceedings*, 2003.

<sup>53</sup> "Major Investigations: Mafiaboy," *United States National Infrastructure Protection Center*; [home page on-line]; available from:  
<http://www.nipc.gov/investigations/mafiaboy.htm>; Internet; accessed 23 April 2004.

<sup>54</sup> Rebecca Allison, "Hacker attack left port in chaos," *Guardian Unlimited*, 7 October 2003; [e-journal]; available from:  
<http://www.guardian.co.uk/online/news/0,12597,1057454,00.html>; Internet; accessed 23 April 2004.

<sup>55</sup> Alefiya Hussain, John Heidemann, and Christos Papadopoulos, "A Framework for Classifying Denial of

Service Attacks," *ACM SIGCOMM Conference Proceedings*, 2003; [home page on-line]; available from: <http://www.acm.org/sigcomm/sigcomm2003/papers/p99-hussain.pdf>; Internet; accessed 12 April 2004.

<sup>56</sup> Lynn Burke, "Hot on the Trail of 'Mafiaboy,'" *Wired News*, 15 February 2000; [home page on-line]; available from: [http://www.wired.com/news/politics/0,1283,34354,00.html?tw=wn\\_story\\_related](http://www.wired.com/news/politics/0,1283,34354,00.html?tw=wn_story_related); Internet; accessed 12 April 2004.

<sup>57</sup> Aaron Weisburd, cited in Cam McGrath, "Politics: Activists Crusade Against e-Jihad," *Inter Press Service*, 12 April 2004.

<sup>58</sup> The Internet Haganah website can be found at <http://haganah.us/haganah>. For a more thorough discussion of the role Internet Haganah plays, please see Chapter 3.

<sup>59</sup> McGarth 1.

<sup>60</sup> Service Announcement, "DOS attack Oct 20 2003," *Hosting Matters.com*, 20 October 2003; [home page on-line]; available from: <http://forums.hostmatters.com/showthread.php?t=10156>; Internet; accessed 18 April 2004.

<sup>61</sup> Again, for a more detailed discussion of this phenomenon, please see Chapter 3.

<sup>62</sup> "Al-Aq'sa Brigades site: 'Attack El Al Website, We'll show you how,'" *The Media Line*, 21 March 2004; [e-journal]; available from: [http://www.themedialine.org/news/news\\_detail.asp?NewsID=5263](http://www.themedialine.org/news/news_detail.asp?NewsID=5263); Internet; accessed 18 April 2004.

<sup>63</sup> Gary R. Bunt, *Islam in the Digital Age*, (London: Pluto Press, 2003), 46.

<sup>64</sup> Brian Krebs, "Hackers Worldwide Fan Flames in Middle East Conflict," *ComputerUser.com*, 25 November 2000; [home page on-line]; available from: <http://www.computeruser.com/news/00/11/25/news1.html>; Internet; accessed 18 April 2004.

<sup>65</sup> Brian Krebs, "Hackers Embrace P2P Concept," *Washington Post*, 17 March 2004; [home page on-line]; available from: <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A444-2004Mar17&notFound=true>; Internet; accessed 18 April 2004.

<sup>66</sup> "Your Portal to Hacker Greatness," *Hackerworld*, No Date; [home page on-line]; available from: <http://escape.to/Hackerworld> Internet; accessed 18 April 2004.

<sup>67</sup> Timothy L. Thomas, "Al-Qaeda and the Internet: The Dangers of 'Cyberplanning,'" *Parameters* (2003), 112-23.

<sup>68</sup> Adam Gaffin, "Slashdot crashes the NSA," *Network World Fusion*, 15 June 2001; [home page on-line]; available from:

<http://www.nwfusion.com/columnists/2001/0611compendium.html> Internet; accessed 18 April 2004.

<sup>69</sup> Stan Schwarz, "Web Servers, Earthquakes, and the Slashdot Effect," [home page on-line]; available from: <http://pasadena.wr.usgs.gov/office/stans/slashdot.html>; Internet; accessed 5 May 2004.

<sup>70</sup> Denning 280.

<sup>71</sup> Edward Wilding, *Virus Bulletin*, February 1990; [home page on-line]; available from: <http://www.virusbtn.com/magazine/archives/pdf/1990/199002.pdf>; Internet; accessed 5 May 2004.

<sup>72</sup> The author's birthday. Since the author worked in computer security at the time, it did not make for a very enjoyable day. Bitterness still exudes at the mention of the worm.

<sup>73</sup> David Moore, Colleen Shannon and Jeffery Brown, "Code-Red: a case study on the spread and victims of an Internet worm," unpublished paper presented at the ACM SIGCOMM/USENIX Internet Measurement Workshop, 2002; [home page on-line]; available from: <http://www.caida.org/outreach/papers/2002/codered/codered.pdf>; Internet; accessed 23 March 2004.

<sup>74</sup> "CERT Advisory CA-2001-19 'Code Red' Worm Exploiting Buffer Overflow in IIS Indexing Service DLL," Carnegie Mellon Software Engineering Institute, CERT Coordination Center, 2001; [home page on-line]; available from: <http://www.cert.org/advisories/CA-2001-19.html>; Internet; accessed 23 April 2004.

<sup>75</sup> Executive White Paper, "The Enterprise Strikes Back: Defending Against Blended Threats," *Network Associates* (2002), [e-journal] [http://www.mcafee2b.com/common/media/mcafee2b/us/products/pdf/wp\\_us\\_blended\\_threats.pdf](http://www.mcafee2b.com/common/media/mcafee2b/us/products/pdf/wp_us_blended_threats.pdf) (accessed 23 April 2004).

<sup>76</sup> Valery Vasenin and Aleksei Galtenko, "Computer Terrorism and Internet Security Issues," *High Impact Terrorism: Proceedings of a Russian-American Workshop*, trans. R. Kit (Washington DC: National Academy Press, 2002): 183-197.

<sup>77</sup> Symantec Anti-Virus Research Center, "Learn more about Viruses and Worms," *Symantec.com*; [home page on-line]; available from:  
<http://www.symantec.com/avcenter/reference/worm.vs.virus.pdf>; Internet; accessed 23 April 2004.

<sup>78</sup> Denning 269.

<sup>79</sup> "Netsky.x Wild on the Net," *TechWeb News*, 20 April 2004; [home page on-line]; available from:  
<http://www.techweb.com/wire/story/TWB20040420S0011>;  
Internet; accessed 23 April 2004.

<sup>80</sup> Martyn Williams, "Slammer was Fastest Spreading Worm Yet," *PC World*, 3 February 2003; [home page on-line]; available from:  
<http://www.pcworld.com/news/article/0,aid,109163,00.asp>;  
Internet; accessed 23 April 2004.

<sup>81</sup> Moore 1.

<sup>82</sup> "Symantec Security Response - CodeRed II," *Symantec.com*, 13 June 2003; [home page on-line]; available from:  
<http://securityresponse.symantec.com/avcenter/venc/data/codered.ii.html>; Internet; accessed 23 April 2004.

<sup>83</sup> "Symantic Security Response - W32.Netsky.Z@mm," *Symantec.com*, 21 April 2004; [home page on-line]; available from:  
<http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.z@mm.html>; Internet; accessed 23 April 2004.

<sup>84</sup> "Virus Tutorial," *Muslim Hackers Club*, No date, Retrieved via Archive.org; [home page on-line]; available from:  
[http://web.archive.org/web/20020203021658/www.ummah.net/mhc/virus\\_tut.html](http://web.archive.org/web/20020203021658/www.ummah.net/mhc/virus_tut.html); Internet; accessed 24 April 2004.

<sup>85</sup> "Sophos Virus analysis:W32/Toal-A," *Sophos.com*, No Date; [home page on-line]; available from:  
<http://www.sophos.com/virusinfo/analyses/w32toala.html>  
Internet; accessed 24 April 2004.

<sup>86</sup> Ibid.

<sup>87</sup> "Symantec Security Response - VBS.Melhack.B," *Symantec.com*, 17 September 2002; [home page on-line]; available from:  
<http://securityresponse.symantec.com/avcenter/venc/data/vbs.melhack.b.html>; Internet; accessed 24 April 2004.

<sup>88</sup> Dan Verton, "Pro-Iraq Hacker Threatens Virus Outbreak," *Computerworld*, 20 November 2002; [home page on-line]; available from:

<http://www.pcworld.com/news/article/0,aid,107205,00.asp>;  
Internet; accessed 24 April 2004.

<sup>89</sup> Raslan Sharif, "Cyber-terrorist or publicity seeker?" *The Star Online*, 7 January 2004; [home page on-line]; available from: <http://star-techcentral.com/tech/story.asp?file=/2003/1/7/itfeature/rlqaedahack&sec=itfeature>; Internet; accessed 24 April 2004.

<sup>90</sup> Verton 2002.

<sup>91</sup> "Will Malaysia Emerge as a Pro-Al Qaeda Cyber Terrorist Haven?" *iDefense.com*, 16 October 2003; [home page on-line]; available from: [http://www.odefense.com/application/poi/display?id=68&type=global\\_threat&flashstatus=false](http://www.odefense.com/application/poi/display?id=68&type=global_threat&flashstatus=false); Internet; accessed 24 April 2004.

<sup>92</sup> Brian Krebs, "Web Sites Vandalized with Antiwar Messages," *Washington Post*, 20 March 2003, retrieved via mirror at SecurityFocus.com; [home page on-line]; available from: <http://www.securityfocus.com/news/3288>; Internet; accessed 3 May 2004.

<sup>93</sup> Kevin Mitnick and William Simon, *The Art of Deception*, (Indianapolis: Wiley Publishing, 2002).

<sup>94</sup> "Zone-H.org Digital Attacks Archive - Ion," *Zone-H.org*, 3 May 2004; [home page on-line]; available from: [http://www.zone-h.org/en/defacements/filter/filter\\_defacer=Ion/](http://www.zone-h.org/en/defacements/filter/filter_defacer=Ion/); Internet; accessed 3 May 2003.

<sup>95</sup> "Zone-H.org Digital Attacks Archive - Ir4Dex," *Zone-H.org*, 3 May 2004; [home page on-line]; available from: [http://www.zone-h.org/en/defacements/filter/filter\\_defacer=Ir4dex/](http://www.zone-h.org/en/defacements/filter/filter_defacer=Ir4dex/); Internet; accessed 3 May 2003.

<sup>96</sup> "Zone-H.org Top Attackers," *Zone-H.org*, 3 May 2004; [home page on-line]; available from: <http://www.zone-h.org/en/hallofshame>; Internet; accessed 3 May 2004.

<sup>97</sup> "Zone-H.org Digital Attacks Archive - Ir4Dex," *Zone-H.org*, 3 May 2004; [home page on-line]; available from: [http://www.zone-h.org/en/defacements/filter/filter\\_defacer=Ir4dex/](http://www.zone-h.org/en/defacements/filter/filter_defacer=Ir4dex/); Internet; accessed 3 May 2003.

<sup>98</sup> Krebs 2003.

<sup>99</sup> The text of their defacement was unaltered; only graphics were removed. "Defacement," *Zone-H.org*, 8 March 2004; [home page on-line]; available from: <http://www.zone-h.org>

h.org/en/defacements/mirror/id=1126414; Internet; accessed 3 May 2004.

<sup>100</sup> Bunt 41.

<sup>101</sup> "Parliament suicide attack stuns India," *BBC*, 13 December 2001; [home page on-line]; available from: [http://news.bbc.co.uk/1/hi/world/south\\_asia/1708853.stm](http://news.bbc.co.uk/1/hi/world/south_asia/1708853.stm); Internet; accessed 3 May 2004.

<sup>102</sup> "Sharon's website hacked," *BBC*, 31 January 2001; [home page on-line]; available from: [http://news.bbc.co.uk/1/hi/world/middle\\_east/1145929.stm](http://news.bbc.co.uk/1/hi/world/middle_east/1145929.stm); Internet; accessed 3 May 2004.

<sup>103</sup> Bunt 43.

<sup>104</sup> Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. J. Arquilla and D. Ronfeldt (Santa Monica: Rand Corporation, 2001), 239-288.

<sup>105</sup> A mirrored copy of the defacement, which occurred in August 2002, was saved at <http://www.mrnick.binary9.net/riaa/>; accessed 3 May 2004.

<sup>106</sup> "Cracker Group Breaches GAO Servers," *Security Wire Digest*, 13 December 2001; [home page on-line]; available from: <http://infosecuritymag.techtarget.com/2001/dec/digest13.shtml>; Internet; accessed 3 May 2004.

<sup>107</sup> Dorothy Denning, "Cyberterrorism," Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, 23 May 2000.

<sup>108</sup> Scott Berinato, "The Truth about Cyberterrorism," *CIO Magazine*, 15 March 2002; [home page on-line]; available from: <http://www.cio.com/archive/031502/truth.html>; Internet; accessed 4 May 2004.

<sup>109</sup> Bruce Schneier, "The Risks of Cyberterrorism," *Crypto-Gram*, 15 June 2003; [home page on-line]; available from: <http://www.schneier.com/crypto-gram-0306.html#1>; Internet; accessed 4 May 2004.

<sup>110</sup> *Ibid.*

<sup>111</sup> Berinato.

<sup>112</sup> Denning 2000.

<sup>113</sup> Richard Forno, "Shredding the Paper Tiger of Cyberterrorism," *Security Focus*, 25 September 2002; [home page on-line]; available from: <http://www.securityfocus.com/columnists/111>; Internet; accessed 4 May 2004.

<sup>114</sup> Joshua Green, "The Myth of Cyberterrorism," *Washington Monthly*, November 2002; [home page on-line]; available from: <http://www.washingtonmonthly.com/features/2001/0211.green.html>; Internet; accessed 4 May 2004.

<sup>115</sup> Pollitt, 1997.

<sup>116</sup> Sandor Vegh, "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking," *First Monday* 7 10 (2002); [e-journal] [http://www.firstmonday.dk/issues/issue7\\_10/vegh/](http://www.firstmonday.dk/issues/issue7_10/vegh/) (accessed 4 May 2004).

<sup>117</sup> "Cyberterrorism: Is the Nation's Critical Infrastructure Adequately Protected?" Hearing before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations of the U.S. House of Representatives Committee on Government Reform, 24 July 2002, Serial No. 107-217.

<sup>118</sup> "Eligible Receiver," *Global Security.org*, 9 June 2002; [home page on-line]; available from: <http://www.globalsecurity.org/military/ops/eligible-receiver.htm>; Internet; accessed 4 May 2004.

<sup>119</sup> John Christensen, "Bracing for guerilla warfare in cyberspace," *CNN*, 6 April 1999; [home page on-line]; available from: <http://edition.cnn.com/TECH/specials/hackers/cyberterror>; Internet; accessed 4 May 2004.

<sup>120</sup> Kenneth Bacon, Department of Defense News Briefing, 16 April 1998; [home page on-line]; available from: [http://www.defenselink.mil/news/Apr1998/t04161998\\_t0416asd.html](http://www.defenselink.mil/news/Apr1998/t04161998_t0416asd.html); Internet; accessed 4 May 2004.

<sup>121</sup> General Campbell, quoted in Stephen Hildreth, "Cyberwarfare," Congressional Research Services, 15 November 2000; [home page on-line]; available from: [http://www.globalsecurity.org/security/library/report/crs/R L30735\\_001115.pdf](http://www.globalsecurity.org/security/library/report/crs/R L30735_001115.pdf); Internet; accessed 4 May 2004.

<sup>122</sup> "Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences," United States General Accounting Office, October 1999, 9; [home page on-line]; available from: <http://www.senate.gov/~y2k/documents/991004crit.pdf>; Internet; accessed 4 May 2004.

<sup>123</sup> Bradley Ashley, "Anatomy of Cyberterrorism: Is America Vulnerable?" Unpublished Paper for U.S.A.F. Air War College, 27 February 2003, 27; [home page on-line];

available from:

<http://www.au.af.mil/au/awc/awcgate/awc/ashley.pdf>;

accessed 4 May 2004.

<sup>124</sup> Christopher Joyner and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework," *European Journal of International Law* 12 5 (2001), 825-865.

<sup>125</sup> Verton 21-22.

<sup>126</sup> "Blue Cascades Infrastructure Interdependencies Tabletop Exercise Final Report," *Pacific Northwest Economic Region Partnership for Regional Infrastructure Security*, 18 July 2002; [home page on-line]; available from: <http://www.pnwer.org/pris/CascadesReport.htm>; Internet; accessed 4 May 2004.

<sup>127</sup> Ibid.

<sup>128</sup> "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," U.S.-Canada Power System Outage Task Force (USCPSOTF), April 2004, 17; [home page on-line]; available from: <http://reports.energy.gov/BlackoutFinal-Web.pdf>; Internet; accessed 4 May 2004.

<sup>129</sup> Kirk Semple, "Bush says there is no sign of Terrorism," *New York Times*, 14 August 2003; [home page on-line]; available from: [http://www.nytimes.com/2003/08/14/nyregion/14WIRE\\_POWER.html?ex=1083902400&en=fd6dc4935d3626d&ei=5070](http://www.nytimes.com/2003/08/14/nyregion/14WIRE_POWER.html?ex=1083902400&en=fd6dc4935d3626d&ei=5070); Internet; accessed 4 May 2004.

<sup>130</sup> USCPSOTF 17.

<sup>131</sup> Approximately 50 million people in 2 Canadian provinces and 8 American states were affected.

"August 2003 Blackout," U.S. Department of Energy Office of Electric Transmission and Distribution, No Date; [home page on-line]; available from: <http://www.electricity.doe.gov/news/blackout.cfm?section=news&level2=blackout>; Internet; accessed 4 May 2004.

<sup>132</sup> Brian Fonseca, "IT Role Cited in Blackout," *eWeek*, 19 April 2004; [home page on-line]; available at: <http://www.eweek.com/article2/0,1759,1570096,00.asp>; Internet; accessed 4 May 2004.

<sup>133</sup> Kevin Anderson, "US 'fears al-Qaeda hack attack,'" *BBC* 27 June 2002; [home page on-line]; available at: <http://news.bbc.co.uk/2/hi/science/nature/2070706.stm>; Internet; accessed 5 May 2004.

<sup>134</sup> Patrick Tyler and Don Van Natta Jr., "Militants in Europe Openly Call for Jihad and the Rule of Islam," *New York Times*, 26 April 2004; [home page on-line]; available from:  
<http://www.nytimes.com/2004/04/26/international/europe/26EURO.html?ex=1083902400&en=870b31dd30c22e64&ei=5070>;  
Internet; accessed 5 May 2004.

<sup>135</sup> Press Release, "Muslim Demonstration Shakes the Heart of London," *Al-Muhajiroun*, 5 May 2004; [home page on-line]; available from: [http://www.al-muhaajiroun.com/press\\_release/050504\\_demo\\_pr.htm](http://www.al-muhaajiroun.com/press_release/050504_demo_pr.htm); Internet; accessed 5 May 2004.

<sup>136</sup> "The Vision of al-Muhajiroun," *Al-Muhajiroun.com*, No Date; [home page on-line]; available from:  
[http://www.al-muhaajiroun.com/about\\_us/vision.html](http://www.al-muhaajiroun.com/about_us/vision.html)  
Internet; accessed 5 May 2002.

<sup>137</sup> Author Interview, 5 May 2004. The source asked not to be named.

<sup>138</sup> Eric Lichtblau, "Report Warns of Infiltration by Al Qaeda in U.S. Prisons," *New York Times*, 5 May 2004; available from:  
<http://www.nytimes.com/2004/05/05/national/05CHAP.html?ex=1084334400&en=28a95a3f8ae91efd&ei=5062&partner=GOOGLE> ;  
Internet; accessed 5 May 2004.

<sup>139</sup> Kyle Olson, "Aum Shinrikyo: Once and Future Threat?" *Emerging Infectious Diseases* 5 4 (1999).

<sup>140</sup> Timothy Robinson and Kenneth Bredemeier, "5 Scientologists Get Jail Terms for Conspiring to Rob, Bug and Spy on U.S.," *Washington Post*, 7 December 1979.

<sup>141</sup> Sean Webby, "Tip from Mtn. View sparked online terror probe," *Mercury News*, 27 June 2002; [home page on-line]; available from:  
<http://www.siliconvalley.com/mld/siliconvalley/3554398.htm>;  
Internet; accessed 5 May 2004.

<sup>142</sup> Information Bulletin 02-001, "Terrorist Interest in Water Supply and SCADA Systems," U.S. National Infrastructure Protection Center, 30 January 2002; [home page on-line]; available from:  
<http://www.nipc.gov/publications/infobulletins/2002/ib02-001.htm>; Internet; accessed 5 May 2004.

<sup>143</sup> Kelli Arena and David Ensor, "U.S. infrastructure information found on al Qaeda computers," *CNN*, 27 June 2002; [home page on-line]; available from:

<http://www.cnn.com/2002/US/06/27/alqaeda.cyber.threat/>;  
Internet; accessed 1 June 2004.

<sup>144</sup> "What is SCADA?" The Geek FAQ, No Date; [home page on-line]; available from: <http://www.geek-faq.com/data-networks/scada.shtml>; Internet; accessed 5 May 2004.

"IEEE Std C37.1-1994 - IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control," IEEE Working Group C3 - Electric Network Control Systems Standards, 17 July 2003; [home page on-line]; available from: [http://grouper.ieee.org/groups/sub/wgc3/c371\\_mn.htm](http://grouper.ieee.org/groups/sub/wgc3/c371_mn.htm); Internet; accessed 5 May 2004.

<sup>145</sup> Scott Berinato, "Debunking the Threat to Water Utilities," CIO Magazine, 15 March 2002; [home page on-line]; available from: [http://www.cio.com/archive/031502/truth\\_sidebar2.html](http://www.cio.com/archive/031502/truth_sidebar2.html); Internet; accessed 5 May 2004.

<sup>146</sup> Erbschloe 188.

<sup>147</sup> Heath Kelly, "QUT researchers uncover major technology flaw," Queensland University of Technology Press Release, 18 May 2004; [home page on-line]; available from: <http://www.news.qut.edu.au/cgi-bin/WebObjects/News.woa/wa/goNewsPage?newsEventID=2489>; Internet; accessed 19 May 2004.

<sup>148</sup> John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)" *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. J. Arquilla and D. Ronfeldt (Santa Monica: Rand Corporation, 2001), 1-25.

<sup>149</sup> Ibid.

<sup>150</sup> Elissa Lee and Laura Leets, "Persuasive Storytelling by Hate Groups Online," *American Behavioral Scientist* 45 6 (2002) 927-957.

<sup>151</sup> John Stanton, "Terror in Cyberspace," *American Behavioral Scientist* 45 6 (2002) 1017-1032.

<sup>152</sup> Michael Whine, "Cyberspace--A new medium for Communication, Command and Control by Extremists," *Studies in Conflict and Terrorism* 22 3 (1999) 231-246.

<sup>153</sup> Brian Levin, "Cyberhate," *American Behavioral Scientist* 45 6 (2002) 958-988.

<sup>154</sup> Raymond Franklin, "The Hate Directory," 2004; [home page on-line]; available from: <http://www.bcpl.net/~rfrankli/hatedir.pdf>; Internet; accessed 3 May 2004.

<sup>155</sup> Sara Steen, "Assessing the Public's Demands for Hate Crime Penalties," *Justice Quarterly* 21 1 (2004), 51-125.

<sup>156</sup> Mark Juergensmeyer, *Terror in the Mind of God* (Berkeley: University of California Press, 2000), 182.

<sup>157</sup> Bob Fick, "Idaho jurors mull whether grad student was aiding terrorists," *Associated Press*, 3 June 2004.

<sup>158</sup> Italics inserted for consistency.

"FAQs about Azzam Publications," *Azzam.com*, No Date. Retrieved via archive.org; [home page on-line]; available from:

<http://web.archive.org/web/20010807202216/http://azzam.com/html/faqsazzam.htm>; Internet; accessed 4 May 2004.

<sup>159</sup> "'In the Hearts of Green Birds' Order Page," *Azzam.com*, No Date. Retrieved via archive.org; [home page on-line]; available from:

<http://web.archive.org/web/20010808011239/http://azzam.com/html/productsgreenbirds.htm>; Internet; accessed 4 May 2004.

<sup>160</sup> "Abu Thabit Ad-Daheishi," *Azzam.com*, March 2000. Retrieved via Archive.org; [home page on-line]; available from:

<http://web.archive.org/web/20010629110529/www.azzam.com/html/storiesabuthabitdaheishi.htm>; Internet; accessed 4 May 2004.

<sup>161</sup> Juergensmeyer 191.

<sup>162</sup> Rex Hudson, "The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?" *United States Library of Congress Federal Research Division*, 1999, 50.

<sup>163</sup> Ibid.

<sup>164</sup> "USA Today Admits Reporter Plagiarized," *CNN*, 19 March 2004; [home page on-line]; available from: <http://www.cnn.com/2004/US/03/19/usatoday.reporter.ap/>; Internet; accessed 4 May 2004.

<sup>165</sup> "Decode Al-Qaeda stego-communications," *Politechbot.com*, 10 July 2002; [home page on-line]; available from: <http://www.politechbot.com/p-03735.html>; Internet; accessed 4 May 2004.

<sup>166</sup> "Stegograms found on azzam.com," *Politechbot.com*, 10 July 2002; [home page on-line]; available from: <http://www.politechbot.com/p-03747.html>; Internet; accessed 4 May 2004.

<sup>167</sup> Jonathon Galt, "Letter to the ISP of Azzam.com," *Personal Website*, 10 April 2002; [home page on-line];

available from: <http://uk.geocities.com//johnnathanrgalt/>; Internet; accessed 4 May 2004.

<sup>168</sup> In a previous study, the author traced the path Azzam.com took until it was eventually completely closed down.

Dino Bozonelos and Galen Stocking, "The effects of Counter-terrorism on Cyberspace: A Case Study of Azzam.com," *Journal of the Institute of Justice and International Studies* 3 (2003), 88-98.

<sup>169</sup> "Farewell Message from Azzam Publications (mirror)," Azzam.com 20 November 2001. Retrieved via Google cache; [home page on-line]; available from: <http://64.233.167.104/search?q=cache:W4P92cH6lAwJ:www.as-sahwah.com/viewarticle.php%3FarticleID%3D756+%22Farewell+message+from+azzam%22&hl=en>; Internet; accessed 4 May 2004.

<sup>170</sup> Aaron Weisburd, *Internet Haganah*; [home page on-line]; available at <http://haganah.rkka.org/haganah/index.html>; Internet; accessed 2 May 2004.

<sup>171</sup> Aaron Weisburd, Author Interview, 6 May 2004. Conducted via e-mail.

<sup>172</sup> Ibid.

<sup>173</sup> The Council of American-Islamic Relations (CAIR) maintains a website that tracks Pipes' comments that it deems offensive or display "a troubling bigotry toward Muslims and Islam."

"Who is Daniel Pipes?" CAIR, No Date; [home page on-line]; available from: [http://www.cair-net.org/misc/people/daniel\\_pipes.html](http://www.cair-net.org/misc/people/daniel_pipes.html); Internet; accessed 4 May 2004.

<sup>174</sup> Ralph Salmi, Cesar Majul, and George Tanham, *Islam and Conflict Resolution* (Lanham: University Press of America, 1998), 195-6.

<sup>175</sup> Daniel Pipes, "What is Jihad?" originally published by *New York Post*, 31 December 2002; [home page on-line]; available from: <http://www.danielpipes.org/article/990>; Internet; accessed 4 May 2004.

<sup>176</sup> "'Zionism is behind Terrorist Actions in the Kingdom,'" *Little Green Footballs*, 3 May 2004; [home page on-line]; available from: [http://littlegreenfootballs.com/weblog/?entry=10912\\_Zionism\\_is\\_Behind\\_Terrorist\\_Actions\\_in\\_the\\_Kingdom](http://littlegreenfootballs.com/weblog/?entry=10912_Zionism_is_Behind_Terrorist_Actions_in_the_Kingdom); Internet; accessed 4 May 2004.

<sup>177</sup> "Islamic Murderbot Gets 32 Years," *Little Green Footballs*, 3 May 2004; [home page on-line]; available from: [http://littlegreenfootballs.com/weblog/?entry=10909\\_Islamic\\_Murderbot\\_Gets\\_32\\_Years](http://littlegreenfootballs.com/weblog/?entry=10909_Islamic_Murderbot_Gets_32_Years); Internet; accessed 4 May 2004.

<sup>178</sup> "Religion of RPGs," *Little Green Footballs*, 3 May 2004; [home page on-line]; available from: [http://littlegreenfootballs.com/weblog/?entry=10907\\_Religion\\_of\\_RPGs](http://littlegreenfootballs.com/weblog/?entry=10907_Religion_of_RPGs); Internet; accessed 4 May 2004.

<sup>179</sup> Discussion comment; [home page on-line]; available from: <http://littlegreenfootballs.com/weblog/?entry=10922#c0007>; Internet; accessed 4 May 2004.

<sup>180</sup> Discussion comment; [home page on-line]; available from: <http://littlegreenfootballs.com/weblog/?entry=10913#c0051>; Internet; accessed 4 May 2004.

<sup>181</sup> Discussion comment; [home page on-line]; available from: <http://littlegreenfootballs.com/weblog/?entry=10922#c0021>; Internet; accessed 4 May 2004.

<sup>182</sup> Supra 171.

<sup>183</sup> An earlier version of this section was presented by the author at the 2002 International Studies Association annual conference in Las Vegas, NV.

<sup>184</sup> Johnson, Neil F. and Jajodia, Sushil. Exploring Steganography: Seeing the Unseen. *IEEE Computer* (1998): 26-34.

<sup>185</sup> Norman, Bruce, *Secret Warfare*, (Washington DC: Acropolis Books Ltd., 1973).

<sup>186</sup> Jackson, Brian A. "Technology Acquisition by Terrorist Groups: Threat Assessment Informed By Lessons from Private Sector Technology Adoption." *Studies in Conflict & Terrorism* Vol 24 Issue 3 (2001): 183-213.

<sup>187</sup> StegoArchive.com. Steganography Software: Windows; [home page on-line]; available from: <http://members.tripod.com/steganography/setgo/software.html>

<sup>188</sup> Google.com; Internet search engine; [home page on-line]; available from: <http://www.google.com>; Internet.

<sup>189</sup> Walker, Jill. "The Political Economy of Linking On the Web." *Proceedings of the Thirteenth Conference on Hypertext and Hypermedia* (2002):72-73.

<sup>190</sup> Images available from: [www.freeservers.co.uk](http://www.freeservers.co.uk)

<sup>191</sup> Upham, Derek. Readme.jsteg, Included in the software package Jsteg. January 2000.

<sup>192</sup> Compuserve, Incorporated. Graphics Interchange Format (sm) Version 89a; July 1990; [home page on-line]; available from: <http://www.w3.org/Graphics/GIF/spec-gif89a.txt>; Internet.

<sup>193</sup> Johnson, Neil F., and Jajodia, Sushil. "Steganalysis of Images Created Using Current Steganography Software." *Lecture Notes in Computer Science* 1525 (1998):273-289.

<sup>194</sup> ANSI (American National Standards Institute), ANSI X3.4-1986. American National Standard for Information Systems – Coded Character Sets – 7-bit American National Standard Code for Information Interchange (7-bit ASCII). [New York]: ANSI, 1986.

<sup>195</sup> Provos, Neils, Stegdetect Help file, Included in the software package Stegdetect, December 2001.

<sup>196</sup> Amaratunga, K, "A Fast Wavelet Algorithm for the Reduction of Color Information," Technical Report, Department of Civil and Environmental Engineering, MIT, 1997.

<sup>197</sup> WestField, A, and Pfitzmann, A. "Attacks on Steganographic Systems." *Information Hiding* (1999):29-46.

<sup>198</sup> Niels Provos, Peter Honeyman: "Detecting Steganographic Content on the Internet." *CITI Technical Report* (2001):1-11.

<sup>199</sup> See *Supra* 19.

<sup>200</sup> N. J. Hopper, J. Langford, and L. van Ahn, Provably secure steganography." *Advances in Cryptology: CRYPTO* (2002).

<sup>201</sup> Distributed.net press release. Distributed.net completes rc5-64 project (list announcement). <<http://www.distributed.net/pressroom/news-20020926.html>> September 2002.

<sup>202</sup> FCC 02-231 "In the Matter of Digital Broadcast Copyright Protection," January 2002; [home page on-line]; available from: [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-02-231A1.txt](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-231A1.txt); Internet; accessed 5 May 2004.

<sup>203</sup> Fisk, G., Fisk, M, Papadopoulos, C., and Neil, J. "Eliminating Steganography in Internet Traffic with Active Wardens." 5<sup>th</sup> International Workshop on Information Hiding. October 2002.

<sup>204</sup> J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and gray-scale images," *IEEE Multimedia (Multimedia and Security)* , (2001):27-41.

<sup>205</sup> See *Supra* 25.

<sup>206</sup> See especially Naas et al. vs. Anonymizer, Inc., et al., (2003) in which an Internet Service Provider was held liable for communications conducted through their services.

<sup>207</sup> Kevin Poulson, "U.S. Defends Cybercrime treaty," *Security Focus*, 23 April 2004; [home page on-line]; available from: <http://www.securityfocus.com/news/8529>; Internet; accessed 5 May 2004.

<sup>208</sup> President Bush, letter to the U.S. Senate, 17 November 2003. Contained in Press Release, "Bush Asks Senate Approval to Ratify Convention on Cybercrime," *United States Department of State*, 18 November 2003; [home page on-line]; available from: <http://usinfo.state.gov/gi/Archive/2003/Nov/18-773753.html>; Internet; accessed 5 May 2004.

<sup>209</sup> "FBI launches Love Bug inquiry," *BBC*, 5 May 2000; [home page on-line]; available from: <http://news.bbc.co.uk/1/hi/sci/tech/736974.stm>; Internet; accessed 5 May 2004.

<sup>210</sup> "Jane Wakefield, "Man Accused of Love Bug hack goes free," *ZDNet*, 27 September 2000; [home page on-line]; available from: <http://www.zdnetindia.com/news/stories/4089.html>; Internet; accessed 5 May 2004.

<sup>211</sup> "Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime," *United States Department of Justice*, 10 November 2003; [home page on-line]; available from: <http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm>; Internet; accessed 5 May 2004.

<sup>212</sup> "Critical Foundations: Protecting America's Infrastructures," *President's Commission on Critical Infrastructure Protection*, October 1997.

<sup>213</sup> Bill Clinton, "Presidential Decision Directive-63," *United States White House*, 22 May 1998; [home page on-line]; available from: <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>; Internet; accessed 5 May 2004.

<sup>214</sup> *Ibid.*

<sup>215</sup> *Ibid.*

<sup>216</sup> Press Release, "Commerce Secretary Mineta Announces New Information Technology (IT) Information Sharing and Analysis Center (ISAC)," *United States Department of*

Commerce, 16 January 2001; [home page on-line]; available from:

<http://www.ntia.doc.gov/ntiahome/press/2001/itsac011601.htm>; Internet; accessed 5 May 2004.

<sup>217</sup> "Membership," *Information Technology Information Sharing and Analysis Center (IT-ISAC)*, No Date; [home page on-line]; available from: <https://www.it-isac.org/membership.php>; Internet; accessed 5 May 2004.

<sup>218</sup> "Member List," *IT-ISAC*, No date; [home page on-line]; available from: <https://www.it-isac.org/memberlist.php>; Internet; accessed 5 May 2004.

<sup>219</sup> "Alert Archive," *IT-ISAC*, last update 27 January 2004; [home page on-line]; available from: <https://www.it-isac.org/publicalerts.php>; Internet; accessed 5 May 2004.

<sup>220</sup> "May 2004 Web Server Survey Finds 50 Million Sites," *Netcraft*, 3 May 2004; [home page on-line]; available from: [http://news.netcraft.com/archives/2004/05/03/may\\_2004\\_web\\_server\\_survey\\_finds\\_50\\_million\\_sites.htm](http://news.netcraft.com/archives/2004/05/03/may_2004_web_server_survey_finds_50_million_sites.htm); Internet; accessed 5 May 2004.

<sup>221</sup> "US-CERT Cyber Security Bulletin SB04-119," *United States Computer Emergency Readiness Team (US-CERT)*, 28 April 2004; [home page on-line]; available from: <http://www.us-cert.gov/cas/body/bulletins/SB04-119.pdf>; Internet; accessed 5 May 2004.

<sup>222</sup> "The National Strategy to Secure Cyberspace," *United States Government*, February 2003, vii.

<sup>223</sup> Ibid viii.

<sup>224</sup> Ibid x.

<sup>225</sup> Ibid 21-24.

<sup>226</sup> Ibid 27-35.

<sup>227</sup> Ibid 37-42.

<sup>228</sup> Ibid 43-48.

<sup>229</sup> Ibid 49-52.

<sup>230</sup> Robert Lemos and Declan McCullagh, "Cybersecurity plan lacks muscle," *News.com*, 19 September 2002; [home page on-line]; available from: [http://news.com.com/2100-1023-958545.html?tag=fd\\_lede](http://news.com.com/2100-1023-958545.html?tag=fd_lede); Internet; accessed 6 May 2004.

<sup>231</sup> James Dempsey, "CDT's Comments on draft cybersecurity strategy," *Center for Democracy and Technology Press Release*, 18 November 2002; [home page on-line]; available from: <http://www.cdt.org/security/critinfra/021118nssc.shtml>; Internet; accessed 6 May 2004.

<sup>232</sup> Bruce Schneier, "National Strategy to Secure Cyberspace," *Crypto-Gram Newsletter*, 15 October 2002; [home page on-line]; available from: <http://www.schneier.com/crypto-gram-0210.html#1>; Internet; accessed 6 May 2004.

<sup>233</sup> A few other prominent articles or essays expressing concern over the *Strategy*:

Marcus Ranum, "Federal Cybersecurity: Get a Backbone," *The Internet Security Conference Insight Newsletter*, 24 September 2002; [home page on-line]; available from: <http://www.tisc2002.com/newsletters/414.html>; Internet; accessed 6 May 2004.

George Smith, "A cybersecurity sleeping pill," *Security Focus*, 23 September 2002; [home page on-line]; available from: <http://www.securityfocus.com/columnists/110>; Internet; accessed 6 May 2004.

Robert Vamosi, "My Plan for fixing software flaws," *ZDNet*, 2 October 2002; [home page on-line]; available from: [http://reviews-zdnet.com.com/4520-6033\\_16-4207625.html](http://reviews-zdnet.com.com/4520-6033_16-4207625.html); accessed 6 May 2004.

<sup>234</sup> Gail Hamilton, quoted in Andrew Zangrilli, "20 Questions with a Security Expert," *Modern Practice*, December 2002; [home page on-line]; available from: [http://practice.findlaw.com/archives/20questions\\_1202.html](http://practice.findlaw.com/archives/20questions_1202.html); Internet; accessed 6 May 2004.

<sup>235</sup> US-CERT.

<sup>236</sup> IT-ISAC Alert Archive.

<sup>237</sup> Cyber Security Research and Development Act, H.R. 3395, 7 February 2002.

<sup>238</sup> Homeland Security Act of 2002, H.R. 5005, 19 November 2002.

<sup>239</sup> Donald Rumsfeld, Testimony before the 9/11 Commission. 23 March 2003.

<sup>240</sup> "MIPT/Ad-Hoc Query," Rand-Oklahoma City National Memorial Institute for the Prevention of Terrorism, 24 November 2003; [home page on-line]; available from: [http://db.mipt.org/sch\\_det\\_crit.cfm](http://db.mipt.org/sch_det_crit.cfm); Internet; accessed 6 May 2004.

## SELECTED BIBLIOGRAPHY

- Alexander, Yonah and Michael Swetnam. *Cyber Terrorism and Information Warfare: Threats and Responses*. Ardsley: Transnational Publishers, 2001.
- Amaratunga, K. "A Fast Wavelet Algorithm for the Reduction of Color Information." Technical Report, Department of Civil and Environmental Engineering, MIT, 1997.
- Anderson, Alison. "Risk, Terrorism, and the Internet." *Knowledge, Technology and Policy* 16 2 (2003), 24-34.
- Ballard, James, Hornik, Joseph and McKenzie, Douglas. "Technological Facilitation of Terrorism." *American Behavioral Scientist* 45 6 (2002), 989-1016.
- Bozonelos, Dino and Stocking, Galen. "The effects of Counter-terrorism on Cyberspace: A Case Study of Azzam.com." *Journal of the Institute of Justice and International Studies* 3 (2003), 88-98.
- "Critical Foundations: Protecting America's Infrastructures," *President's Commission on Critical Infrastructure Protection*, October 1997.
- Cyber Security Research and Development Act, H.R. 3395, 7 February 2002.
- "Cyberterrorism: Is the Nation's Critical Infrastructure Adequately Protected?" Hearing before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations of the U.S. House of Representatives Committee on Government Reform, 24 July 2002, Serial No. 107-217.
- Debrix, François. "Cyberterrorism and Media-Induced Fears: The Production of a Media Culture." *Strategies* 14 1 (2001).
- Denning, Dorothy. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." *Networks and Netwars: The Future of Terror, Crime and Militancy*, ed. Arquilla and Ronfeldt. Santa Monica: Rand Corporation, 2001.

- Denning, Dorothy. "Cyberterrorism." Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, 23 May 2000.
- Denning, Dorothy. "Cyberwarriors: Activists and Terrorists Turn to Cyberspace," *Harvard International Review* 23, 2 (2001)
- Dietrich, Sven, Long, Neil and Dittrich, David, "Analyzing Distributed Denial of Service Tools: The Shaft Case," *Proceedings of the Second ACM SIGCOMM Workshop on Internet Measurement, 2002*, 329-339.
- Fridrich, J., M. Goljan, and R. Du. "Detecting LSB steganography in color and gray-scale images." *IEEE Multimedia (Multimedia and Security)*. (2001):27-41.
- Jackson, Brian A. "Technology Acquisition by Terrorist Groups: Threat Assessment Informed By Lessons from Private Sector Technology Adoption." *Studies in Conflict & Terrorism* Vol 24 Issue 3 (2001): 183-213.
- Johnson, Neil F., and Jajodia, Sushil. "Steganalysis of Images Created Using Current Steganography Software." *Lecture Notes in Computer Science* 1525 (1998):273-289.
- Johnson, Neil F. and Jajodia, Sushil. Exploring Steganography: Seeing the Unseen. *IEEE Computer* (1998): 26-34.
- Joyner, Christopher and Lotrionte, Catherine "Information Warfare as International Coercion: Elements of a Legal Framework," *European Journal of International Law* 12 5 (2001), 825-865.
- Juergensmeyer, Mark, *Terror in the Mind of God* (Berkeley: University of California Press, 2000), 182.
- Lee, Elissa and Leets, Laura, "Persuasive Storytelling by Hate Groups Online," *American Behavioral Scientist* 45 6 (2002) 927-957.
- Levin, Brian, "Cyberhate," *American Behavioral Scientist* 45 6 (2002) 958-988.

- Lewis, James, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *Center for Strategic and International Studies*, December 2002.
- McGrath, Cam, "Politics: Activists Crusade Against e-Jihad," *Inter Press Service*, 12 April 2004.
- Norman, Bruce, *Secret Warfare*, (Washington DC: Acropolis Books Ltd., 1973).
- Provos, Niels and Honeyman, Peter: "Detecting Steganographic Content on the Internet." *CITI Technical Report* (2001):1-11.
- Ronfeldt, David and Arquilla, John, "What next for Networks and Netwars?," *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. J. Arquilla and D. Ronfeldt (Santa Monica: Rand Corporation, 2001), 311-361.
- Salmi, Ralph, Majul, Cesar and Tanham, George, *Islam and Conflict Resolution* (Lanham: University Press of America, 1998), 195-6.
- Schbley, Ayla, "Defining Religious Terrorism: A Causal and Anthological Profile," *Studies in Conflict & Terrorism* 26 (2003), 105-134.
- Shpiro, Shlomo, "Conflict Media Strategies and the Politics of Counter-terrorism," *Politics* 22 2 (2002), 76-86.
- Stanton, John, "Terror in Cyberspace," *American Behavioral Scientist* 45 6 (2002) 1017-1032.
- United States Federal Bureau of Investigation Definition of Terrorism, cited in Jonathon White, *Terrorism* (Stamford: Wadsworth Thomas Learning, 2002), 12.
- United States Department of State, *Patterns of Global Terrorism*, April 2004.
- WestField, A, and Pfitzmann, A. "Attacks on Steganographic Systems." *Information Hiding* (1999):29-46.

Whine, Michael, "Cyberspace - A new Medium for  
Communication, Command and Control by Extremists,"  
*Studies in Conflict and Terrorism* 22 3 (1999), 231-  
246.

Wolf, Jim, "First 'Terrorist' Cyber-attack Reported by  
U.S.," *Reuters*, May 5 1998.