PART V

Cyber Terrorism: The "New" Face of Terrorism

JOHNSON, OLIVIA

9110

Chapter 29

The Dark Side of the Web: Terrorists' Use of the Internet

Kelly Damphousse
University of Oklahoma

Kelly Damphousse, **Ph.D.,** is Associate Dean in the College of Arts and Sciences and Presidential Professor of Sociology at the University of Oklahoma. He earned his Ph.D. in Sociology from Texas A&M University in 1994. His research career has included studies of terrorism, homicide, drugs/crime nexus, Satanism, and several justice-related evaluation projects. He served as the Site Director of the Oklahoma City and Tulsa ADAM sites from 1998 to 2004 and has been Associate Director of "The American Terrorism Study" since 1994.

Abstract

This chapter examines how terrorists have used the Internet to communicate with a "world wide" audience. We begin by defining terrorism and placing the need for communication to a wide audience in context. Terrorists have traditionally communicated with people outside their organization to express their views, seek support, and raise money. Just as the Internet has become an increasingly important tool to society, terrorists have begun to use the Internet to achieve their goals. Indeed, terrorists were early adopters of the Internet, using bulletin boards and newsgroups before the advent of the browser-based Internet. The Internet is an extraordinary medium for the advancement of terrorist ideology because it is relatively inexpensive and attracts a large audience. The Internet also provides an outstanding tool for communicating with current and potential group members. Finally, the Internet provides access to vital information that can be used to injure terrorist targets (like governments) or to collect reconnaissance information to plan attacks. The chapter describes the proliferation of terrorists on the Internet and the ways that terrorists may use the Internet to perform acts of terrorism. Finally, we show how the Internet is being used to "counter" terrorism.

INTRODUCTION

This chapter addresses the use of the Internet by **terrorists** and those who mean to counter their activities. Before we go too far, though, we need to understand what is meant when we use the word "terrorist." For many of the people we examine in this chapter, the term is meaningless. On one extreme, these people see themselves as "freedom fighters" that are organized against an oppressive and more powerful regime (Ross 2006). It might surprise you, for example, to think

that George Washington and his fellow "patriots" were considered to be rebels (or "terrorists") by the English government. On another extreme, terrorists might think that they are only exercising their right to express themselves about a controversial issue (Hoffman 1998). Thus, someone who is opposed to **abortion** and publishes a list of abortion clinic addresses may only feel like they are "pointing toward evil," and not creating "hit lists" for which they might be criminally liable (Macavinta 1999).

Terrorism scholars have spent years trying to define terrorism and there about as many definitions of terrorism as there are scholars (Hoffman 1998). One simple definition provided by the United States government—the definition used by the FBI—states that terrorism is "the unlawful use of force and 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" (28 Code of Federal Regulations Section 0.85). The two key issues in most such definitions are (1) the use of force and (2) a political motivation.

As we will see, however, this definition is problematic regarding terrorists' use of the Internet. While creating a Web page may be politically motivated, it is certainly not a *use* of force. Indeed, it is often not even a *threatened* use of force. So, by definition, most uses of the Internet by terrorists are not terrorist acts, *per se*, but may be best described as acts that are *ancillary* to terrorism—acts that support terrorist activities (Smith, Damphousse, and Roberts 2006). Many times, for example, terrorists only use the Internet to air their grievances, something that such groups have done throughout the history of terrorism. Indeed, one might say that is the whole *point* of terrorism: to draw attention to a problem. Terrorists "want to impress. They play to and for an audience, and solicit audience participation" (Hacker 1976, xi). Thus, the Internet can be seen as just one more way of communicating with an audience, joining the **communiqué**, the poster, the placard, and the soapbox. The impact of the Internet on the ability of terrorists to communicate is enormous, of course, given its ability to reach such a wide audience so quickly. Interestingly, the Internet has given potential terrorists a tool that may preclude terrorism acts. In the pre-Internet era, a violent act was probably the only way to "get the word out." The Internet now gives politically frustrated groups a voice that does not *require* violence.

But if we stop there, we fail to recognize that the Internet also gives terrorists another weapon in its arsenal. Herein we observe a tremendous irony: as society becomes increasingly dependent on the Internet, it also becomes increasingly vulnerable to attack via the Internet. Thus, terrorists not only use the Internet to *communicate* with society, they may also use the Internet to *attack* society.

Terrorists also face a paradox when they decide to use the Internet because their new tool, like bomb parts and fingerprints, can be used by investigators to identify the attackers. In addition, the Internet can be used by **counter-terrorism** actors to warn citizens about potential terrorism threats and to seek information that can aid in the capture of the terrorists. This is the same problem that terrorists face when they use the media. "Just as the media is a tool of the terrorist, it is pernicious to the terrorist groups too. It helps an outraged public to mobilize its vast resources and produces information that the public needs to pierce the veil of secrecy all terrorist groups require" (Rapoport 1996, viii). Making their cause public brings greater attention to the terrorist, which may result in eventual capture and arrest. Thus, the way that terrorists use the Internet can make them more vulnerable to capture.

Terrorist groups described in this chapter are composed of three types: (1) groups that hate certain types of *people* (e.g., blacks, Jews, and women) (2) groups that oppose certain

types of *aspects of social life* (e.g., affirmative action, abortion, technology, and immigration), and (3) groups that oppose governments (e.g., Irish Republican Army and the **Republic of Texas**). While the ultimate focus of each of these protest groups may differ, there is certainly some overlap between the two types of groups in terms of behavior, strategy, membership, and etiology (Lofland 1996). A cautionary note is in order. We use the term "terrorist group" guardedly because we recognize that some groups that are described in this chapter might only be *potential* terrorist groups—that is, they have not committed any criminal act. At the same time, these groups are still interesting because of their marked potential for (1) engaging in terrorist acts or (2) providing for others the incentive to engage in violence (Damphousse and Smith 1997). Thus, this paper assesses the different ways that terrorist groups use the Internet (both as a manner of communicating with a wider audience and as a form of attack) and how the use of the Internet makes the terrorists vulnerable to capture. We start by discussing the need for communication by terrorist groups and then describe how terrorists and counter-terrorists use the Internet.

TERROR AND COMMUNICATION

If you consider the life course of terrorist groups, you realize that most groups started because their founding members were frustrated by some "problem" (Ross 2006). In some cases, they may have tried to "fix" the problem via legitimate means (e.g., through the political or legal system) while in other cases, they may not have felt empowered to make a change at all. At some point, the members decided that the only way that they can change the current situation is to react violently. As von Clausewitz wrote nearly 200 years ago, "War is the continuation of politics by other means" (von Clausewitz 1832/1976). By extension, terrorism is also a continuation of politics. The difference is that wars are fought between "states" while terrorism is conducted (mostly) by nonstate actors.

Terrorist groups in particular, engage in behaviors designed to send messages to outsiders. Violence, therefore, can be seen as an attempt by terrorist groups to call attention to some "problem" that needs to be "fixed" (Herman 1982; Rubenstein 1987). Indeed, some have suggested that terrorism could not even exist without the ability to communicate with people outside of the skirmish, calling to mind the proverbial "tree falling in the forest with no one to hear it" (Schmid and Graaf 1982). Acts of violence by terrorists can be considered indirect efforts at communication whereby the terrorists use the news media to inform the public about the motives of the group, in an effort to give "violent voice to the voiceless, and to awaken their sleeping brethren to the necessity of mass action" (Rubenstein 1989, 323). Hoffman (1998) details, for example, the impact of the media coverage of hijacking of an Israeli *El Al* airliner in 1968 and the killing of Israeli athletes at the Munich Olympic games in 1972 as watershed events that resulted in increased international attention to the "Palestinian question" (Said 1979).

Less extreme, though more direct, measures have also been taken by protest groups to get their message out. In general, this tactic is referred to as **propaganda** (Wright 1990). Propaganda is used by protest groups to inform the general public (or other more specific groups) about some problem in an effort to make them "feel the urgency, the necessity of some action, its unique characteristics, . . . [and] what to do" (Ellul 1969, 208). Traditionally, protest groups have used the printed word (via leaflets, fliers, posters, and newsletters) to

inform others about their cause (Wright 1990). More recently, terrorist groups used faxes to communicate with each other and with selected outsiders (e.g., media and academics). The problem with the use of these media is the relatively high cost and limited scope of coverage. There is little "bang for the buck" when much of the material is discarded by uninterested members of the public.

Protest groups experimented with the use of short wave radio for a time (and still continue to do so, to a lesser extent), but access to a larger audience was still restricted. The next advance that allowed greater access to the general public was made possible by the increased popularity of nationally syndicated talk radio programs. It was talk radio that first allowed members of protest groups to be able to discuss their concerns with a host and (presumably) a national audience. Conservative talk radio shows that allowed/fostered the discussion of topics that angered groups of individuals blossomed in the late 1980s. Still, access to a wide audience by the protest groups was somewhat limited as was the information that could be provided. Even worse, the information was also limited in that it was in verbal format; easily discarded and easily forgotten. While members of protest groups were able to communicate easily with each other and with a limited sympathetic audience, they were still unable to get their message to the "uncommitted audience" (Wright 1990).

THE EVOLUTION OF REVOLUTION

The advent of the World Wide Web (as we know it) in the mid-1990s provided protest groups with access to a mode of communication that was relatively inexpensive, patently "permanent," was in text and image format, and was accessible to almost anyone in the world. To the extent that antigovernment groups were among the first to make use of the Internet for propaganda use, the information revolution coincided with the conservative revolution in an ironic twist. The Internet had been developed in the late 1960s by the federal government (United States Department of Defense) to allow for the sharing of computer files between research scientists located around the country. The irony is that the project initially developed by the federal government was now being used by protest groups to encourage its downfall.

Terrorists were not latecomers to the computer age. In fact, discussion lists (listservs), bulletin board systems, and **newsgroups** had been actively used by such groups in the decade before the browser-based Internet came into existence. The least private of these early technologies was the newsgroups and **bulletin boards**, where messages ("articles") are posted to servers that are available to most anyone who has access to the site. These were the precursors to the currently in vogue Web log (blog) and networking sites. Electronic bulletin boards began in the late 1970s but they are essentially extinct now. A bulletin board normally was composed of a local group of computer users who were interested in a certain topic. Since people were accessing the bulletin board through the phone line, the expense of a long distance phone call resulted in most bulletin boards being used locally. Indeed, it was common back then for members of a bulletin board group to meet in person. Throughout the 1980s, right wing terrorist groups and activists were heavy users of such bulletin boards. Registered users could post comments, files, and software to the bulletin board system (BBS) so that others could access them. The advent of Internet browser software led to the ultimate near-demise of the BBS.

Newsgroups were similar to bulletin boards but they provided greater access to a wide range of people beyond the local area. Newsgroups were eventually divided into different topical hierarchies in 1986 to provide order to the rapidly expanding system ("comp.*" for computers discussions, "sci.*" for discussions about sciences, etc.). The "alt.*" hierarchy was created as a catchall category for topics that did not fit the other seven hierarchies. Over time, the "alt.*" designation became synonymous with "alternative" groups including Satanists, wiccans, and illicit drug enthusiasts. Included in this category were several politically defiant groups such as alt.activism.militia, alt.society.anarchy. Eventually, many antigovernment groups were using the newsgroup technology to communicate with each other. In time, a myth suggested that alt.* stood for "Anarchists, Lunatics and Terrorists" (Salus 1995). These public forums consist of individuals posting comments or questions and allowing others to post responses in a series of "threads." Newsgroups are monitored by an administrator who can drop "inappropriate" posts to the group or delete posts when interest in the topic as waned. The problem with using newsgroups, however, was that they were relatively easy for the government and others to monitor.

Listservs, first developed in 1984, are relatively more private than bulletin boards and newsgroups, but controlling who is part of the list can be difficult. Listservs use the e-mail system as a means of communication among people with a shared interest. In most cases, a moderator operates the listserv by creating a list of e-mail addresses of people who wish to be part of the "list." Interested members subscribe to the list and receive e-mail messages from every subscriber who submit an e-mail to the listserv. Upon receipt of the e-mail, the recipient can either reply to the rest of the listserv or to the individual.

These "asynchronous" communication processes are now being replaced by real-time applications called "**chat rooms**" (e.g., Internet Relay Chat and MUDs—Multi-User Dungeons). These programs allow groups of individuals to instantly communicate with each other via their computers. In recent years, simple text-based messages have been supplemented with video and voice protocols that allow users to see and hear each other, eliminating the need to type messages.

These early computer links were important for planning and the transmission information between terrorist group members who were physically separated. But this medium was accessible to only a limited audience (mostly people who were active computer users and interested in the topic). The advent of the browser and "worldwide" access to these new Web pages changed the importance of the Internet for terrorist groups. For the first time, activists had access to people from all walks of life who were potential members, supporters, and contributors to their cause. Unfortunately for the protest groups, potential enemies also had access to the information that they made public. How protest groups and their opponents use the Internet is discussed in the following sections. But before detailing the activities of protesters on the Internet, it is necessary to provide some background regarding how the Internet works to make communication via the computer more accessible to a larger group of people.

Before the advent of Web browsers like Netscape and Internet Explorer, access to the Internet was available only to people who were technologically advanced. Knowledge of several programs was required to perform simple tasks like sharing files and sending an e-mail message. The creation of Web browsers solved most of these problems because of introduction of hypertext markup language (html). Even so, Web developers were required to learn a relatively complex software program and language to be able to create a Web page. Advances in technology over time eliminated that hurdle and now, anyone with access to the Internet

can create a Web page or site. Indeed, the availability of networking sites like Facebook, Xanga, and MySpace has made even the requirement for a Web page almost obsolete. If you want to let people know about your cause, you simply register at one of these networking sites and create a "group." Like-minded people from around the world can join your "group" and everyone can post information that is accessible to the world (or just to your "friends"). A recent search from my Facebook page, for example, revealed seven "groups" that express support for the **Earth Liberation Front** (ELF). These networking programs are incredibly easy to learn such that 12-year-old children are more than proficient in their use (www.comScore.com, retrieved June 12, 2007).

This system was made even more accessible in 1993 when browsers were developed that allowed computer users to interact with other computers through a graphical interface. With the Mosaic browser (and subsequently others like Netscape, FoxFire, Safari, and Explorer), novice users were able to access the Web pages created by terrorists. Over time, the graphical interface of the home pages became increasingly sophisticated, supplementing the images and text with sound and video. People using video-sharing sites like YouTube or on private Web sites, for example, can now easily access excerpts of speeches and videos. In addition to merely visiting Web sites, advances in software development has allowed people with no formal computer training to be able to create Web pages, giving them access to literally millions of people around the world. The decreasing cost of personal computers was associated with an increased access to the Internet and modem speed resulting in an incredible increase in Internet activity. From 1993 to 1997, the number of Web sites grew from almost zero to just under 5 million. By the middle of 2007, the Netcraft Web Survey reported that there were more than 123 million Web sites. Unfortunately, this incredible tool that has changed our world in so many ways is also being used to harm us. The goal of this chapter is to describe how terrorist groups can use the Internet to further their cause.

Method of Study

The data presented in this paper were compiled over the course of a 12-year research project starting in 1995 that was originally designed to examine how terrorist groups used the Internet to communicate with each other (Damphousse and Smith 1997). As the Internet evolved, we discovered that terrorists' use of the Internet evolved along with it. Each advance in Internet technology was adopted by terrorist groups to their advantage. The data collection began by the researchers conducting Internet searches via the Yahoo search engine for the virtual presence of specific known terrorist groups (e.g., KKK, FALN, and Aryan Nations). We discovered that it was not sufficient to search for "terrorism" since these groups don't always think of themselves as "terrorists"—so the searches had to be more creative. For example, an early search on the word "terrorism" yielded 68 "hits," most of which had to do with new stories about terrorists. Back in 1995, a search on Yahoo for the word "**Aryan**," however, yielded only nine Web sites, each of which was directly related to Aryan Nations groups. Other search engines yielded different Web pages. Using AltaVista, for example, resulted in over 3,700 pages with the word "Aryan."

Times and the Internet have changed. A search on the word "Aryan" in 2007 using Google yielded over 3.5 million hits (the first being the ubiquitous Wikipedia definition). Obviously, just using a search engine is not efficient. So we found other locations were found

by conducting searches for militia groups and by following links from one site to another. We discovered that a site maintained by one white supremacist group often provides links to several other similar Web sites. Thus, we followed the links located at each of the Web sites that we catalogued (and all the links on the subsequent Web sites). Each of the locations we visited was bookmarked for ease of later access and then visited regularly over the course of the 12-year period. We conducted crude content analyses of these pages, looking for patterns and trends in the way that these groups used the Internet. In addition, we scanned electronic news Web sites to see how the media was covering the topic of "terrorists and the Internet." In retrospect, we wish that we had done a better job making copies of Web sites given the frequency with which these Web sites disappeared. Unfortunately, much of the raw data has disappeared over time. Still, we believe that we understand how terrorist groups have used the Internet over the past 12 years. We discuss these tactics in the following section.

The Internet as Tool for Protest Groups

Previous examinations of how terrorists use the Internet have suggested as many as eight categories of usage (Weiman 2005). In the following sections, we provide examples of nine ways that terrorist groups can use the Internet. Some of these categories are based on exclusive properties of the Internet such as the potential ease of reaching millions of people. Some categories simply aid terrorists groups accomplish their goals. The final set of categories suggests ways that terrorists can use the Internet to attack their targets, the "**Cyber terrorism**" that has caused such concern (Collin 1996).

Leaderless Resistance and Propaganda

Until the 1980s, most terrorist groups exhibited a militaristic, hierarchical structure that allowed leaders to communicate directly with their followers. Over time, however, counter-terrorist efforts evolved such that law enforcement used this structure against the group as an entity. Instead of just prosecuting those who were involved in the terrorist incident, the FBI targeted the entire group, especially its leaders. Thus, the goal of the U.S. government became the "beheading" of the terrorist group. Lower-level operatives who were arrested for a terrorist act were offered attractive plea arrangements in exchange for testifying against their leaders. This resulted in leaders being held criminally culpable for the acts of their followers and in the eventual demise of many terrorist groups (Smith and Damphousse 1998).

To counter this strategy, terrorists groups began to change their tactics. One possible option would have been the creation of a cellular structure, where a leader coordinates independent cells. This strategy reduces damage to the entire terrorist structure but continues to put the leader at risk. A more suitable option emerged in the early 1990s that has come to symbolize the contemporary terrorism structural strategy, what Michael Barkun (1994, 1997) has referred to as "uncoordinated violence" strategies.

Ironically, the most prominent of these strategies, "**leaderless resistance**," evolved from unsuccessful federal prosecutions in the late 1980s. Following the acquittal of extreme right-wing group leaders in the 1988 Fort Smith, Arkansas trial, Louis Beam spent months devising a plan to minimize civil and criminal liability for group leaders. Following the siege at Ruby Ridge, Idaho in 1992, Beam publicly called for the implementation of "leaderless resistance" at a meeting of extreme right-wing adherents in Estes Park, Colorado (Beam 1992).

Copies of Beam's document abound on the Internet, including Beam's own Web site (http://www.louisbeam.com/leaderless.htm).

Beam's call to change was indeed prescient. He was aware that, even if people are motivated to engage in violent acts by the awareness of a problem, they still need training, information, and some direction. He saw the importance of the computer as vital cog in this new leadership strategy. "Organs of information distribution such as newspapers, leaflets, *computers, etc., which are widely available to all*, keep each person informed of events, allowing for a planned response that will take many variations. No one need issue an order to anyone. Those idealists truly committed to the cause of freedom will act when they feel the need" (Beam 1992, 2, emphasis added). Thus, terrorists who have adopted this new "indirect action" strategy can "lead" without putting themselves at risk of criminal prosecution. The Internet provides the best option for such "leaders" to guide "followers" in future actions, providing a rationale for "direct action" and information about successful tactics and potential targets. Using the Internet allows followers to receive their marching orders without the leader ever knowing who the follower is.

The majority of the sites that we observed, for example, had sections that described the purported "problem" (e.g., immigration, gay and minority rights, and excessive taxation and government control) in great detail to show how society was deteriorating. The use of vivid imagery was designed to appeal to each reader's sensitivity. Frequently, the Web pages provided anecdotal "atrocity" stories like the moral entrepreneurs of other such moral panics (Victor 1993). For example, the "**Waco Holocaust Electronic Museum**" Web page suggested that the siege at the Branch Davidian compound was only part of a continuing pattern of attacks by federal law enforcement agencies against the Christian right (http://www.public-action.com/SkyWriter/WacoMuseum/, accessed February 27, 2006). To further incite passion about the threat of the government to the church, the "curator" provided links to the autopsy reports of the Waco victims, including grisly photographs of the victims of the fiery end of the siege. Bear in mind that it was frustration about the Waco siege and its outcome that motivated (in part) **Timothy McVeigh** to bomb the Oklahoma City federal building in 1995.

Other Web sites offer similarly graphic text. The Watchman newsletter was hosted by a white supremacist Web site called stormfront.org.[1] The following text relates a race-related atrocity story to seemingly unrelated events at Ruby Ridge, Waco, and Oklahoma City in a thinly veiled call for action.

"As I was preparing to mail this double issue of 'The Watchman' an event took place in the Chicago area which demands comment. Three black animals butchered a White woman and her young White children, one by torture and then cut her open to remove the half-breed baby she was pregnant with . . . It seems that they were using her as an incubator to breed a light-skinned child, and decided to eliminate her, having no further need for her reproductive ability. The one who removed the little bastard was a negress nurse who used her medical training to carry out her part in the crime . . . it is becoming more apparent with every day that passes that *unless the White Race rises up against their tormentors in a consuming fury, we will instead be consumed by them*. I do not hate these people as individuals but only a fool would believe that we will ever live together in peace. Events like this, as well as Waco, the Randy Weaver massacre and Oklahoma City portend a darkening future for America and it is

[1]The newsletter is not longer available because—according to the Stormfront Web site—the editor (Mark Thomas) was thought to have become an informant for the government.

becoming increasingly clear that *unless heroic measures are taken without delay*, there will be no future for us or our children" (http://www2.stormfront.org/watchman/index.html, retrieved on February 6, 1996, emphasis added).

Recruiting

The primary job of all terrorist leaders is to recruit members into their group. The traditional way of doing this is by inflaming the passion of potential followers so that they become willing to engage in activities that they would normally find repugnant—to move them from the "propaganda of word" to the "propaganda of deed" (Stafford 1971). In the past, this task was accomplished through the publication of books and pamphlets (e.g., Marx and Engels 1848/1964). In the information age of terrorism, the Internet provides the best way of showing potential new members that they have been lulled into a complacency (a false consciousness) that threatens to destroy them. As opposed to books on the subject, the Internet is free to potential members have nothing to invest to learn about the problem. The Internet also offers greater coverage than pamphlets and yelling from the street. It is also private, so that both the "speaker" and the "listener" are safe from observation during their "conversation." The following quote which appeared on the now defunct Web site called "The Patriot's Soapbox" demonstrates this line of reasoning:

> If there is one thing I want to accomplish by publishing these thoughts on the Internet, it is to stimulate you American slaves out there to WAKE UP and become sovereign Americans again. While you were slumbering, watching television, drinking beer, being amused, your 'servants' captured and enslaved you, and became your 'masters'. You could be free, but you are entangled in a Web of deceit: lies, fictions and frauds committed by your friendly public servants. (http://www.geocities.com/CapitolHill/1781/, retrieved February 14, 1996)

More contemporary examples include Web sites that are devoted to the question of abortion. Pro-life advocates worry that the very *act* of abortion has been so watered down that citizens are not offended by the act. A recent controversial tactic has been the use of large shocking photographs of aborted fetuses on billboards and 18-wheeler trailers "as a way to educate people about the realities of abortion" to that potential recruits can fully appreciate the issue at hand (Baez 2006, 1). These tactical uses of images find a natural home on the Internet and several Web sites have been created based on the same principle. The antiabortion Web page abort73.com, for example, includes a sophisticated video that begins "If ignorance is bliss, turn back now. But if you are ready to lift the curtain on one of the greatest injustices history has even known, you've come to the right place . . . while contemporary media outlets cover-up the carnage, an entire industry grows rich off of a strategically uninformed clientele . . . we dare you to know" (http://www.abort73.com/, retrieved June 1, 2007). The Web site provides statistics on the number of abortions completed each year along with graphic pictures and videos of fetuses and procedures.

It would be a stretch to call this a "terrorist" Web site but there are other sites that can capitalize on such sites to encourage direct action. A Web site called "The Nuremburg Trials" (http://www.christiangallery.com/atrocity/, retrieved June 1, 2007), for example, provides a list of abortion clinic, their respective addresses, and pictures that have been taken by "abortioncams." The impact of such Web sites has been observed in U.S. courts. In a 2003 federal criminal complaint, for example, Stephen Jordi was recorded telling an informant that "he had

ordered over the Internet a book known for its 'prolific terrorist ties' and had visited the '**Army of God**' Web site . . . (www.christiangallery.com). This Web site has been called a 'hit list' for abortion clinics and providers" (*USA v. Stephen Jordi* 2003, 6–7).

Communication with the Audience

Historically, terrorists have followed attacks by issuing a communiqué—often through the media—that lets the "audience" know why the attack occurred. Indeed, the very rationale for committing a violent act is to gain public attention (Hoffman 1998). The media was used because it was the best way to reach a large audience. Having access to the Internet allowed terrorists to bypass the media to speak directly to the audience. The takeover of the Japanese embassy in Peru in 1996 by the **Túpac Amaru Revolutionary Movement** (MRTA) provides the first know example of a terrorist group using the Internet to communicate with the people of the world. Over the course of the four-month long crisis, MRTA hostage-takers provided statements and electronic videos on their now defunct Web site: http://burn.ucsd.edu/~ats/mrta.htm (the Web site was retrieved at http://www.nadir.org/nadir/initiativ/mrta/ on May 24, 2007). Tellingly, the text of the communiqués was presented English (as well as in Spanish and Japanese), showing the importance they placed on reaching out to the western world. The Web site also included Italian, Turkish, and Serbian language versions. Clearly, the terrorist group seeks to communicate with a wider audience than those with whom it battles.

Federal authorities have come to realize that one threat of the Internet is its ability to allow a large number of people who would never have otherwise met to be able to communicate with each other. Thus, an individual in Idaho who hates African-Americans can create a home page to exhibit this hatred. People living in Florida can visit this home page and read the material placed there. If the Florida readers are impressed with the page, they can add the Idaho Web address to a list of "hot" links making Idaho page now available to people who visit the Florida page. The advent of networking sites has made this kind of interaction much more possible. The importance of the Web for this capacity is exhibited in the following quote found on a right-wing Web site:

> The net is the most powerful free speech forum that has ever existed. Support all efforts to keep it uncensored. Wild claims of your children being carted away by Internet pedophiles, etc. are meant to frighten the unaware. The Internet terrifies the powers that be because they are no longer in control of the information that you can receive. Through the Internet one can set up a Web page and state his opinion to the world, literally. Everyone in the world who is interested in that subject can then access that page and read that opinion for themselves. How unbelievable! We no longer have to wait to be told what someone or some group is saying. We can now get it straight from the horse's mouth. Well, expect the world control freaks to move to crush this situation. (http://207.15.176.3:80/cause/, retrieved on February 16, 1997)

Some terrorist groups use the Internet as a method of communicating with the group as a whole. The Republic of Texas was a secessionist group that planned to re-claim Texas from the federal government and overturn the de facto (State) government. During the late 1990s, they held their meetings in small cities all over Texas. Because many members were not able to attend every meeting, the meeting minutes were published on the group's Web page. The group also published all of its press releases (communiqués) on the Web site and an interpretation

of previous events that involved the group. Even more amazing, the Web site published a list of the officers of the Republic, making it very easy for the government to know who to watch. The Web site was also used for emergency purposes at times. When federal agents arrested an "ambassador," for example, an urgent alert was placed on the Web asking citizens to call the local, state, and federal law enforcement agencies demanding his release. Their original extensive Web site is no longer available electronically but one faction of the group has created a similar Web site that continues to list members of the "provisional government" and meeting minutes—although it takes a while to find it if you don't know where to look (http://www.texaspublicrecord.net/gov/index.shtml, retrieved on June 15, 2007). The new site includes the 2003 Declaration of Independence signed by more than 40 signatories.

Further efforts at the coalescing of like-minded individuals and groups have evolved into a page with a more social than political agenda. A "pro-white" record label called Resistance Records (http://www.resistance.com/, retrieved on May 24, 2007) produces and sells music suitable for those with pro-Aryan attitudes. At one time, a white power group named Alpha hosted a Web page (http://www.alpha.org, retrieved on November 21, 1996) that included "Aryan Dating Page." The "lifestyles" Web site is no longer available but it allowed men and women (white and nongay) to meet over the Internet via the posting of pictures contact information for available and interested men and women. A similar Web site with a focus on "white dating" (http://www.allwhitedating.com/, retrieved April 14, 2003) was created in 2002. Aryans who are looking to find compatible love interests can to the **Stormfront** Web site (http://www.stormfront.org/forum/, retrieved June 1, 2007), which evolved from an ordinary Web site to a forum host site. Along with a "white singles" forum, people can log in to running discussions on subjects like poetry, religion, health and fitness, and white nationalism. In addition, the Web site provides access to "Stormfront Radio," a white supremacist Internet radio station that plays right-wing oriented music and provides social commentary.

e-ffiti

The nature of Internet use is that happening upon one or another Web page is usually not a planned event but more a matter of happenstance. Indeed, one of the problems with performing research about terrorists on the Internet is that it is easy to get distracted by following interesting links. But anyone who has wasted a few hours surfing the Web is familiar with the results—it is not difficult to end up far removed from where you ever intended to go. This feature of the Internet works to the advantage of terrorist groups who want to inflict harm on others through the written word or "art" work. This is especially relevant for hate groups that are focused on race or ethnicity. As a result, an African-American who happened upon the Alpha (http://www.alpha.org, retrieved on December 12, 1996) home page would understandably be shocked and offended by reading the following messages scrolling at the bottom of the screen: "African American, what a joke, why not just call them what they are? N*****S! America for Whites, Africa for blacks, ship those apes back to those trees, send them n*****s back! Ring that bell, jump for joy, White mans day is here, no more n****r civil rights, led by n****r queers! Who needs N*****s?"

Likewise, a more recent Web site called Tightrope (http://www.tightrope.cc/forum/, retrieved June 12, 2006), which is highlighted by an image of a raised fist holding a noose, has a page dedicated to jokes aimed at African Americans and Jews and provides a set of racist

songs available for download in mp3 format. In a similar vein, the several Aryan Web pages, such as White Revolution—Nebraska (http://www.whiterevolution-ne.org/, retrieved June 1, 2007) proclaim allegiance to a sacred 14-word code of honor ("We Must Secure The Existence Of Our People And A Future For White Children!") that is portrayed prominently on most of the pages. T-shirts, posters, and bumper stickers showing the **14 words** in different formats are readily available over the Web.

But race is not the only feature attacked on the Web by Aryans. The White Aryan Resistance Web page (http://www.resist.com/, retrieved June 1, 2007) exhibits cartoons and a joke book attacking both gays and Jews. The use of stereotypic humor is a common phenomenon appearing on many of these sites. The Web site also provides contact information for "prisoners of war," white power supporters who are currently serving time in federal prison.

Support Activities

Terrorist groups are normally self-sufficient (with the exception of state-sponsored terrorists) with the result being that they have to raise money in order to sustain their activities. One way many groups do this is by engaging in "preincident activities" such as bank robbery and fraud (Smith and Damphousse 1996). The Internet provides a legal way to seek external funding. The Internet's reach into millions of homes and the ease of collecting money using credit card services like PayPal makes such fund raising relatively easy (and much safer). Thus, many terrorist Web sites include the option of buying merchandise such as books and T-shirts while other sites simply plea for donations to support the efforts. The pleas used on these pages are usually addressed to "fellow travelers" who might be motivated to aid the group's need to replace failing equipment or to sustain the membership. The request for funds is often associated with a desire to provide a better service to the user. In 1996, for example, an author left the following message for his followers: "Many people have told us how they cannot access our Web site much of the time, this is due to lack of funding. Our Web site is run on an old and slow machine that allows only two people at any time to be on the site. The site is now receiving between 50 and 100 users per day with not a second of idle time. That 50–100 per day can be improved to hundreds of white people per day worldwide accessing great writings of white leaders and learning more about the movement for White Power. We must upgrade and improve our equipment a.s.a.p. Every white man or woman who can not access our site may not return to try again becoming a lost soul" (http://www.alpha.org, retrieved December 12, 1996).

Other times, the efforts at fund raising display the personal hardships endured by the host that are the result of efforts to be a "good citizen." Thus, the editor of *The Watchman* newsletter wrote in desperation "Your prayers and financial support are urgently needed at this time. I am currently under tremendous attack and the threat of criminal prosecution. In the last six months I have lost my disability allowance, had many of my belongings stolen by the feds and am being driven from my home of 18 years. I have six children and staggering legal bills. Without a miracle, I am going under, and if the feds have their way, to prison. I have given my life to this struggle on faith, without regard to the consequences to my self or even my family. Our future is in God's hands and they are attached to your forearms. We are unable to cash checks without using a bank account that could be seized at any time by the feds. Postal Money Orders made out to XXXX are best and they protect your privacy as well.

Please help us to survive and continue the struggle for His Kingdom at The watchman (http://www2.stormfront.org/watchman/, retrieved August 15, 1996)."

This plea for funds on the Internet is not limited to American terrorists. **The Shining Path**—a Peruvian terror group—regularly posts messages to its Web site urging supporters to export the revolutionary message by hawking "revolutionary" products like T-shirts, posters, and videos (http://www.csrp.org/index.html, retrieved May 12, 2007).

The Web as Weapon

The possibility that the Web will be used to conduct acts of terrorism has increased dramatically since its inception. Indeed, since corporations who are the victims of computer crime are wont to dealt with virtual invasions discretely, it is likely that there is much more cyber terrorism occurring than currently known. There are three possible threats from protest groups using the Internet to perform acts of terrorism. First, protest groups can gain access to other home pages and either deface them, or change them to provide alternative information. There are already several examples of this kind of "**hactivism**" occurring. Perhaps one of the most infamous early incidents was the defacing of the home page of the Central Intelligence Agency (CIA). On September 18, 1996, a Swedish protest group called "Power Through Resistance" vandalized the home page of the CIA. The group changed the title of the page to the "Central Stupidity Agency," and added several links to nongovernment home pages such as Playboy. Earlier, hackers had renamed the Department of Justice home page the "Department of Injustice." Although no sensitive material was available to the attackers, the fact that individuals on another continent were able to sabotage these sensitive and heavily protected Web sites is evidence of the potential for remote activity.

A second way that protest groups can use the Web as a weapon is through the impairment (or at least threatened impairment) of vital government or corporate communication processes. It is not difficult, for example, to imagine a protest group "hacking" its way into the computer system that controls the power supply to an area and then threatening to cut off power unless some demand is carried out. In fact, such a problem has occurred in Japan where groups attacked the commuter train computer system (Devost, Houghton, and Pollard 1996). The threat is even greater if one considers the impact such a threat would have on the operation of a nuclear facility. Related, protest groups could directly access financial institutions and perform account transfers, resulting in the theft of huge amount of funds. The relative ease of impairment of other computers is evidenced by the large growth in computer viruses (which "infect" computer with programs designed to destroy software or data) in the past several years. As society infrastructure becomes increasingly dependent on computers and the importance of remote access (which provides the necessary portal for terrorists), the chances of such an attack increase dramatically.

Finally, there is increasing concern among governments that information housed on their computers may be accessed by unauthorized individuals. In 1994, a British youth was arrested for suspicion in a case where a military base in New York was impaired for over a month (Wilson 1996). There are two potential problems here. First, opposition groups may more easily gain intelligence information. Second, and perhaps more deadly, false or illegitimate commands could be delivered to military forces, ordering them to unwittingly perform some terrorist act.

The fears associated with these types of virtual attacks have created a new industry of software and hardware solutions including virus protections and firewalls that are designed to protect vulnerable and important computer systems from attack. These programs are designed to only allow legitimate users access to the information housed on corporate or agency computers (Alpert 1996). In general, firewalls are designed to inspect each attempt to access a computer network. Those users who attempt to get into the network without authorization are rejected.

Virtual Reconnaissance

It is not just the publication of Web pages and the ease of communication that makes the Internet so useful to terrorists. The Internet has spawned increasingly complex sets of tools that can be used to aid terrorist efforts. These tools can aid terrorist efforts at reconnaissance—where they seek detailed information about selected targets. For example, there is increasing concern about the use of Google Earth by terrorist groups. The free and easy-to-use program provides a "bird's eye view" of potential terrorism targets by simply typing in an address or the name of a location. It has been well documented that the group that was planning the May 2007 attack on JFK Airport had used Google Earth to obtain detailed information on the airport and the location of the jet fuel tanks. Ordinary street maps would have provided some limited information but the aerial photos available from Google Earth provided the group with unparalleled information—the kind of data once only available to technologically advanced governments. To counter this tool, governments have asked Google Earth to "blur" the photos of sensitive areas, but a recent search by the author provided startlingly clear and detailed photos of airports, U.S. military bases in Europe, and symbolically important national monuments.

In a similar vein, the advent of the Internet created a huge information vacuum that governments seemed overly willing to fill. In the early days of the Internet, it was common for local, state, and federal governments to feel compelled to "put it on the Web." Thus, many documents and much information that should never have been made public were put on the Internet. This information included electrical grids, maps of water supplies, emergency response plans. As a witness testified before the Little Hoover Commission on California State Government Organization and Economy one month after the 9/11 attacks, "One cautionary note, however, is that we used available sources of information to identify and characterize the critical physical infrastructure of the state. The same information we accessed is available to individuals and terrorist groups, who may use it as a road map for designing cyber disruptions, decide which critical systems to target, and when to target them" (Riley 2001, 5). It was only after vulnerability studies were conducted after the 9/11 attacks that governments became aware of how susceptible they were to having their own information used against them. As a result of a careful reexamination of the public's right to know and the need for security, governments are working on removing much of this vulnerable information from the Internet.

Terrorism Strategy Depository (e-libris)

Terrorists often learn from other terrorists and it is not uncommon for raids on terrorist compounds to uncover copies of terrorist "manuals" and other material that can either encourage the terrorist action or show how to perform certain acts. These books range from

"how to" books that describe how to build a bomb to books on successful terrorism strategies. Examples include *Military Studies in the Jihad Against the Tyrants* (allegedly used by members of Al-Qaeda), the *Mini-manual of the Urban Guerrilla* by (Marighella 1970), *The Anarchist's Cookbook* (Powell 1970) and ***The Turner Diaries*** (MacDonald 1978) by William Luther Pierce. Pierce's book provided the framework for McVeigh's bombing of the Murrah Building in Oklahoma City. Each of these books and others like them are widely available on the Internet. The latter three are likewise available for purchase at the Amazon bookstore Web site. Interestingly, Powell has posted a statement on several Web sites (including Amazon.com) disavowing the book he wrote when he was a teenager. Since he does not own the copyright, he has no power to stop its continued publication. Even if he did, it is very likely that his work (and the copycats it spawned) would continue to be available on the Internet indefinitely.

Coordination of Direct Action

Like all tactical units, communication among participants and between leaders and participants is vital. The ability to communicate by e-mail and, more recently, by instant messaging, greatly enhances terrorist operations. The problem for terrorists, of course, is the difficulty in keeping "private" anything that is sent by e-mail. Thus, terrorists are increasingly using **encryption** technologies that can keep the message safe from prying eyes. During the 2004 trial of Abdelghani Mzoudi, who was on trial in Germany for his alleged role in the 9/11 attacks, included testimony from a former Iranian intelligence operative who stated that Mzoudi had been trained to encrypt e-mail messages in Iran (Boston 2004).

Encryption software uses a mathematical algorithm that can scramble and then unscramble a message that is sent from one person to another through the use of a "key." If an e-mail were intercepted, it would be meaningless without the ability to decode it. The ability to communicate secretly via e-mail is a major advance for terrorist groups and a cause for great concern. In the days following 9/11, for example, policymakers called for restrictions on encrypting software once law enforcement agencies reported the use of the software by the attackers. Suggested changes included the outright ban of encryption software availability for the public to the requirement that software companies create a "back door" into the encryption code so that the government can better monitor communication between suspected terrorists (Knight 2001).

Industry experts have suggested, however, that there is no way of stopping the use of encryption software, especially since it would be available from Web sites outside of the US. In addition, experts point to the greater likelihood that terrorists would use **steganography** (i.e., "covered writing") where messages are hidden in plain sight. Ancient examples of steganography include tattooing information on a bald head that is eventually covered by the growth of hair. The microdot technology invented during the cold war also allowed information to be "hidden" on the period at the end of a typed sentence. In the electronic world, steganography takes advantage of how digital pictures are created. Briefly, a digital picture is composed of a series of pixels that represent one of the three primary colors. The more pixels in a picture, the sharper the image and the bigger the file size. Steganographic encoding software embeds the message within these pixels and a user who receives the picture (and a decoding key), can extract the image or the message from the digital photo. Steganography programs like S-tools for Windows can also use sound files (*.wav) to hide information (Johnson and Jajodia 1998).

DISCUSSION: TERRORISM IN A FLAT WORLD

Last month, I was riding in a van in central Oklahoma going 70 miles per hour when I checked my e-mail on my cell phone. I noticed that I had received an e-mail from my boss who was waiting out a rainstorm at an archeological dig in northern Italy. I replied to his request and then sent an instant message to my assistant asking her to handle the problem. Later that same day, when we got lost on the way to an event, I accessed Google Maps from my cell phone to find our way. Later, I e-mailed a picture of the event to my daughter. This "flattening of the world" has changed our lives forever (Friedman 2005). Instant access to the Internet and all that it provides also makes the task of a terrorist even easier. All of the things that the Internet provides for terrorists are now available almost anywhere in the world at almost any time—something that was unthinkable to most people just 15 years ago.

The World Wide Web is being used by protest groups in America (and around the world) to deliver their message in ways never dreamed possible before 1980. Access to the Web has allowed protest groups to proselytize more individuals than ever before. They have also become better able to communicate with each other (for political and social ends). They are also in a better position to attract funding from people with whom they would not otherwise have contact. The most serious threat, however, appears be the potential of actual terrorist acts committed via the Web. The presence of protest groups on the Web has spawned a new aspect of terrorism/counter-terrorism previously never imagined—the explosion of "citizen counter-terrorists."

Just as the Internet benefits terrorist groups, it can also increase their vulnerability. Using the Internet gives the government an opportunity to monitor their activities. One recent example occurred in China, where search engine giant Yahoo provided the e-mail addresses of political dissidents to the Chinese government (Sinn 2007). Indeed, the Chinese government has required Internet companies doing business in the country to participate in self-censorship or have censored the Web site unilaterally (Zittrain and Edilman 2003). This has resulted recently in the Internet photo company Flickr being blocked in China, apparently because photos offensive to the Chinese government were linked to the site (Perez 2007).

Other nonstate actors also use the Internet to interrupt terrorist behavior. We usually consider "counter-terrorists" as being the purview of government agencies, the military, and special terrorism task forces. The mission of these organizations is to gather intelligence about potential terrorist groups and to inform the public, when necessary, about their threat. Some social/civic groups and private individuals, however, have created Web sites whose primary function is to publicize the operations of protest type groups. The "Klanwatch" project operated by the **Southern Poverty Law Center** and the **Anti-Defamation League**, for example, focuses upon making available information about the **Ku Klux Klan** and other anti-Semitic activities. These two organizations have continued these activities in cyberspace, operating home pages that describe activities of terrorist groups. Also available at these home pages are opportunities to purchase literature describing the history of the militia groups and other terrorist groups.

What is unique with the advent of the Internet, however, is the proliferation of Web sites that have been created by private citizens who have made it their mission to document both pro- and anti-terrorism pages. A common example of civilian counter-terrorism on the Internet is the "Police Officer's Internet Directory" home page, hosted by a Boston police

officer. This page provided little independent commentary, but included a large number of links to pro- and antiprotest groups throughout the early 1990s (e.g., "Hate Groups, Terrorists, & Radicals"). The commentary supplied by the host was limited to suggesting that the sites provided on the page were offensive and may be unpleasant to view. By the mid-2000s, the Web site had expanded beyond just focusing on terrorist and became a key source about all things police-related—including counter-terrorism (see http://www.officer.com, retrieved November 12, 2006).

One of the most progressive of these early citizen counter-terrorism pages was called "The **Militia Watchdog**," which grew out of a Usenet FAQ (frequently asked questions). In this location, the host (an historian who is an expert on the history of the militia in America) tracked news about terrorist groups and provides links to, and commentary about, the home pages of various protest groups. The page provided "patriot profiles" (thick descriptions of contemporary militia groups), essays (e.g., description of gun show activities), collection of news articles about terrorists (e.g., the militia follies), and special reports about events such as federal elections. By 2000, the author became an employee for the anti-defamation league and the Militia Watchdog page "died," although the archives are still available (http://www.adl.org/mwd/default.asp, retrieved on August 15, 2001).

Perhaps the most interesting development along these lines is the formation of counter-counter-terrorism on the Web. At least two home pages have been created that challenge the information provided on the Militia Watchdog and other similar pages: "[The author of the Militia Watchdog] is feeding the paranoia of the mass population, fueled by the news media, that the patriots and militias are somehow planning to commit terrorist acts. [He] and his traitorous counterparts in the government and in the media have yet to prove there to be a link between the militias and the **Oklahoma City Bombing**. Having recently re-viewed footage of the initial 2 hours following the bombing in Oklahoma City, simple things I noticed REFUTE the claims to a 4,800 pound truck bomb full of cow manure! Rather, the basic evidence supports an INTERNAL blast blowing out from INSIDE the building" (http://www.execpc.com/~warning/dogpound.html, retrieved on February 20, 1996).

Increasingly sophisticated tools to monitor and investigate terrorists on the Internet are currently being developed. Researchers at the University of Arizona, for example, have developed an algorithm that will allow investigators to monitor Internet chat rooms and be able to determine who is participating in the conversation (Zhou et al. 2005). The software creates a visual pattern that distinguishes among users. The algorithm is based on word pattern usage. Since people are habitual, when we write, we tend to use certain combinations of words in ways that are different from other people. The software is designed to conduct **authorship analysis**, allowing the users to determine the word-use patterns and then recognize when they are used. Thus, the text-based messages that terrorists use to communicate with each other create virtual "fingerprints" that allow investigators to know who is participating. Even more, the researchers are developing virtual "spiders" that can crawl throughout the World Wide Web looking for the identified terrorists as they move from chat room to chat room.

Clearly, the use of the Internet by terrorist groups and those who oppose them is a phenomenon that bears continued observation. The impact of the citizen counter-terrorists on the propaganda and fundraising efforts of the protest groups is uncertain at this time. The fact that counter-counter-terrorism home pages have begun to spring up is evidence that the effect is beginning to be noticed.

The creation of the Internet has been referred to as the beginning of the information revolution. How fitting, then, that the political revolutionaries of our time were among the first to make the most creative use of it. What is interesting is that the term "leaderless resistance" may take on a new meaning in this age of generating information and then making it available to the world. Serious implications await discussion concerning the liability of those whose home pages (filled with anger, hate, and protest) become the catalyst for some violent action by an unknown actor. The Oklahoma City bombing, for example, has been compared to activities described in *The Turner Diaries* (MacDonald 1978), which is now also available on the Web. It remains to be seen if the federal government will begin prosecuting individuals who foment rage while attempting to shield themselves via the leaderless resistance strategy.

In essence, individuals who operate home pages perform essentially one-way communication with other people. The information provided on the Internet is of a special case. Much like leaflets of old, the information is distributed to individuals only indirectly. That is, propaganda about the excesses of government—or some other threat—is distributed rather anonymously, where the reader and the writer may never meet. The authors of the information in the home page can claim that they did not intend for readers to take any specific action. It is certain that the Internet will continue to play an important role in how terrorist groups operate—just as the Internet has become so essential to the rest of the world.

KEY TERMS

14 words
Abortion
Anti-Defamation League
Army of God
Aryan
Authorship analysis
Bulletin boards
Chat rooms
Communiqué
Counter-terrorism
Cyber terrorism
Earth Liberation Front
Encryption
Hactivism
Ku Klux Klan
Leaderless resistance
Militia Watchdog
Newsgroups
Oklahoma City bombing
Propaganda
Republic of Texas
Southern Poverty Law Center
Steganography
Stormfront
Terrorist
The Shining Path
The Turner Diaries
Timothy McVeigh
Túpac Amaru Revolutionary Movement
Waco Holocaust Electronic Museum

REFERENCES

Alpert, B. November 1996. On fire: Fear of hackers should keep the computer firewall market smokin'. *Barrons*: 25.

Baez, A. 2006. Anti-abortion photos spark rally, debate: National organization sets up graphic panels depicting aborted fetuses in Arbor. Retrieved May 25, 2006, from http://www.dailynexus.com/article.php?a=11829

Barkun, M. 1994. *Religion and the Racist Right: The Origins of the Christian Identify Movement*. Chapel Hill, NC: University of North Carolina Press.

Barkun, M. 1997. Changing U.S. domestic threats. Presentation to the International Conference on Aviation Safety and Security, Washington, DC.

Beam, L. 1992. Leaderless resistance. Presentation made to leaders of the extreme right, October 23, 1992, Estes Park, Colorado. First published in *Seditionist* 12: 1–3.

Boston, W. 2004. Witness-box weirdness. Retrieved February 8, 2004, from http://www.time.com/time/magazine/article/0,9171,901040209-586265,00.html

Collin, B. 1996. The future of cyberterrorism: Where the physical and virtual worlds converge. Retrieved May 2, 1997, from 11th Annual International Symposium on Criminal Justice Issues Web site: http://www.acsp.uic.edu/OICJ/CONFS

Damphousse, K. R., and B. L. Smith. 1997. "The Internet: A terrorist medium for the 21st century." In *The Future of Terrorism: Violence in the New Millennium,* edited by H. Kushner, 208–24. Thousand Oaks, CA: Sage.

Devost, M., B. Houghton, and N. Pollard. 1996. Information terrorism: Can you trust your toaster? Retrieved May 2, 1997, from The Terrorism Research Center Web site: http://www.Terrorism.com

Ellul, J. 1969. *Propaganda: The Formation of Men's Attitudes*. New York: Alfred A. Knopf.

Friedman, T. L. 2005. *The World Is Flat: A Brief History of the Twenty-First Century*. New York: Farrar, Straus and Giroux.

Hacker, F. J. 1976. *Crusaders, Criminals, Crazies: Terror and Terrorism in Our Time.* New York: W. W. Norton.

Herman, E. 1982. *The Real Terror Network: Terrorism in Fact and Propaganda*. Boston: South End Press.

Hoffman, B. 1998. *Inside Terrorism.* New York: Columbia University Press.

Johnson, N. F., and S. Jajodia. February 1998. Steganography: Seeing the unseen. *IEEE Computer*: 26–34.

Knight, W. 2001. Controlling encryption will not stop terrorists. Retrieved September 30, 2001, from http://www.newscientist.com/article.ns?id=dn1309

Lofland, J. 1996. *Social Movement Organizations: Guide to Research on Insurgent Realities*. New York: Aldine de Gruyter.

Macavinta, C. 1999. Abortion "hit list" slammed in court. Retrieved February 2, 1999, from CNET News Web site: http://news.com.com/2100-1023-221054.html

MacDonald, A. 1978. *The Turner Diaries*. Arlington, VA: National Alliance.

Marighella, C. 1970. *Mini-Manual of the Urban Guerrilla.* NP: New World Liberation Front.

Marx, K., and F. Engels. 1848/1964. *The Communist Manifesto*, translated by P. M. Sweezy. New York: Monthly Review Press.

Perez, J. C. 2007. Flickr photos being blocked in China: Is Yahoo's photo tool being censored? Retrieved June 12, 2007, from http://www.pcadvisor.co.uk/news/index.cfm?newsid=9683

Powell, W. 1970. *The Anarchist's Cookbook.* New York: Lyle Stuart, Inc.

Rapoport, D. 1996. Editorial: The media and terrorism—Implications of the Unabomber case. *Terrorism and Political Violence* 8 (1): i–ix.

Riley, K. J. 2001. Statement of Jack Riley before the Little Hoover Commission. Retrieved December 1, 2002, from Little Hoover Commission on California State Government Organization and Economy Web Site: http://www.lhc.ca.gov/lhcdir/disaster/RileyOct01.pdf

Ross, J. I. 2006. *Political Terrorism: An Interdisciplinary Approach*. New York: Peter Lang.

Rubenstein, R. 1987. *Alchemists of Revolution: Terrorism in the Modern World*. New York: Basic Books.

Rubenstein, R. 1989. "Rebellion in America: The fire next time." In *Violence in America: Protest, Rebellion and Reform*, edited by T. R. Gurr, 167–82. Newbury Park, CA: Sage.

Said, E. 1979. *The Question of Palestine*. New York: First Vintage Books.

Salus, P. 1995. *Casting the Net: From ARPAnet to Internet and Beyond.* Reading, MA: Addison-Wesley Professional.

Schmid, A., and J. Graaf. 1982. *Violence as Communication: Insurgent Terrorism and the Western News Media.* Beverly Hills: Sage.

Sinn, D. 2007. Yahoo weighs in on free speech in China. Retrieved on June 12, 2007, from Associated Press Web site: http://www.ap.org

Smith, B., and K. Damphousse. 1996. Punishing political offenders: The effect of political motive on federal sentencing decisions. *Criminology* 34 (3): 289–321.

Smith, B., and K. Damphousse. 1998. Terrorism, politics, and punishment: A test of structural contextual theory and the liberation hypothesis. *Criminology* 36 (1): 67–92.

Smith, B., K. Damphousse, and P. Roberts. 2006. Final technical report: Pre-incident indicators of terrorist incident: The identification of behavioral, geographic, and temporal patterns of preparatory conduct. Washington, DC: Office of Justice Programs.

Stafford, D. 1978. *From Anarchism to Reformism.* Toronto: University of Toronto Press.

USA v. Stephen Jordi. 2003. Criminal complaint in case number 03-CR-60259.

Victor, J. 1993. *Satanic Panic: The Creation of a Contemporary Legend*. Chicago: Open Court.

von Clausewitz, C. 1832/1976. *On War*. Princeton, NJ: Princeton University Press.

Weiman, G. 2005. How modern terrorism uses the Internet. *Journal of International Security Affairs* 8: 1–10.

Wilson, D. 1996. 40 million potential spies. Retrieved on May 23, 1996, from http://www.cnn.com/US/9605/23/internet.spying/index.html

Wright, J. 1990. *Terrorist Propaganda: The Red Army Faction and the Provisional IRA, 1968–86*. New York: St. Martin's Press.

Zhou, Y., E. Reid, J. Qin, H. Chen, and G. Lai. 2005. US domestic extremist groups on the Web: Link and Content Analysis. *IEEE Intelligent Systems* 20 (5): 44–51.

Zittrain, J., and B. Edilman. 2003. Internet filtering in China. *Internet Computing* 7 (2): 70–77.

Chapter 30

Cyber Terrorism: Problems, Perspectives, and Prescription

P. Madhava Soma Sundaram, K. Jaishankar
Manonmaniam Sundaranar University, India

Dr. P. Madhava Soma Sundaram (Madhavan) is the reader and head of the Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli, India. Madhavan holds masters' degree in criminology and Ph.D. in criminology from the University of Madras. His doctorate work is in the field of victimology, focusing on fear of crime. Madhavan has authored one book and several articles/papers, chapters in books, editorials, book reviews, project reports, monographs in journals and magazines. He is the founding editor-in-chief of "Crime and Justice Perspective"—the official organ of the Criminal Justice Forum (CJF), India, and the founding editor of the *International Journal of Criminal Justice Sciences*. He serves in the International Editorial Advisory Board of the *International Journal of Cyber Criminology*. In recognition of his contribution in the growth of criminology in India, Madhavan was conferred the title of Fellow of Indian Society of Criminology (FISC) by the Indian Society of Criminology (ISC) for 2001. His areas of specialization are juvenile justice, victimology, child protection, and social defense.

Dr. K. Jaishankar is a lecturer in the Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli, India. He is the founding editor-in-chief of the *International Journal of Cyber Criminology* and the founding editor of "Crime and Justice Perspective"—the official organ of the Criminal Justice Forum (CJF), India, and the founding managing editor of the *International Journal of Criminal Justice Sciences*. He serves in the International Editorial boards of *Journal of Social Change* (USA), *Electronic Journal of Sociology* (Canada), *Crime, Punishment and Law: An International Journal* (USA), *Journal of Physical Security* (USA), and *Graduate Journal of Social Science* (UK). He is the national focal point for India for the International Police Executive Symposium's working paper series and expert of world police database at www.coginta.com. He is a co-investigator of the International Project on Cyber bullying funded by SSHRC, Canada involving eight countries, along with the principal investigator Dr. Shaheen Shariff, McGill University. He is a pioneer in developing the new field, cyber criminology, and is the proponent of "space transition theory," which gives an explanation for the criminal behavior in cyberspace. He is a recognized expert in the field of cyber criminology and invited by various universities in U.S. to deliver lectures on his space transition theory of cyber crimes. His areas of academic competence are cyber criminology, crime mapping, GIS, communal violence, victimology, policing, and crime prevention.

Abstract

The Internet has brought revolutionary changes to the world. One of the greatest changes has been the growing connectivity between all "corners" of the world via the Internet. In many ways, this has been a boon to humanity. However, there is also a dark side to this achievement.

A prime example of this negative side has been the rapid spread of computer viruses. The world becomes more dependent on the myriad activities carried out via the Internet, and a potential exists for much more serious consequences of this dark side of the Internet, including events related to cyber terrorism. This chapter examines cyber terrorism, one of the major negative consequences of the Internet. It also examines the potential impact of cyber terrorism, its possible methods, its prevention, and control.

INTRODUCTION

Indeed, the world is undergoing a second industrial revolution. Information technology today touches every aspect of life, irrespective of one's location on the globe. Daily activities are affected in form, content, and time by the computer. Businesses, governments, and individuals all receive the many benefits of this information revolution. While providing tangible benefits in time and money, the computer has also had an impact on everyday life, as computerized routines replace mundane human tasks. More and more businesses, industries, economies, hospitals, and governments are becoming dependent on computers. Computers are not only used extensively to aid in the performance of industrial and economic functions in society, but are also to perform many functions upon which human life itself depends. Computers are also used to store confidential data of a political, social, economic, or personal nature. They assist in the improvement of economies and of living conditions in all countries. Communications, organizational functioning, and scientific and industrial progress have developed so rapidly with computer technology that our way of living has irreversibly changed.

Defining Cyber Crimes

Defined broadly, the term "computer crime" could reasonably include a wide variety of criminal offenses, activities, or issues. The potential scope is even larger when using the frequent companion or substitute term "computer-related crime." Given the pervasiveness of computers in everyday life, even in the lives of those who have never operated a computer, there is almost always some nontrivial nexus between crime and computers. This is especially the case when factoring in the extensive use of computers in evidence, investigations, and court administration (Lewis 2002; Gregory 2000; Post 2000; Sprols and Byars 1998).

Nevertheless, something far less than such a panoramic view of "computer crime" comes to mind, when the term is used. Moreover, as the phrase is evolving into a term of art, the narrower set of meanings has become more prevalent in the literature. One noteworthy example is the FBI National Computer Crime Squad's (NCCS) (ISTS 2001) list of crime categories it investigates: Intrusions of the Public Switched Network (the telephone company)

- major computer network intrusions
- network integrity violations
- privacy violations
- industrial espionage
- pirated computer software
- other crimes where the computer is a major factor in committing the criminal offense

What is Cyber Terrorism?

A spectrum of criminal acts may be conducted via the Internet, ranging from cyber espionage and **information warfare** carried out by foreign governments to **cyber crimes** carried out by smaller groups or individuals. Although **cyber terrorism** may be carried in conjunction with cyber espionage or cyber crime, it is considered distinct from the two entities. Cyber terrorism combines both cyberspace and terrorism and it is the use of intentional violence against computer systems that support or protect the health of human communities or the information stored in these systems. Unlike cyber espionage, virtually all instances of cyber terrorism to date have been carried out by organized factions unconnected to world governments. Often, cyber terrorism is aimed at coercing a population or its government to accede to certain political or social objectives. In addition, cyber terrorism usually is more extensive and destructive than is simple cyber crime. As a result, cyber terrorism either harms the health of human communities or generates a fear of this harm.

Cyber terrorism still is in its infancy. Although there have been numerous cyber-terrorist events, there have been no large-scale incidents affecting large geographic areas. Despite the challenge of producing damage of this magnitude, the potential for large-scale, cyber-terrorist events increases as the Internet continues to expand. Furthermore, cyber terrorism may be used to:

1. help plan other terrorist activities
2. soften a target prior to a physical attack
3. generate more fear and confusion concurrent with other terrorist acts

Defining Cyber Terrorism

If one views cyber terrorism in a narrow sense, it essentially becomes an extension of traditional terrorism into the realm of information technology. Although there is no internationally agreed-upon definition of traditional terrorism *per se*, central characteristics include politically or otherwise motivated use of violence directed at civilians, by a group or individual, in order to influence public perceptions (Conway 2002). Terrorism in this sense can and does apply to the cyberworld. There is clearly the potential for individuals with political and/or religious motivations to make use of information technology **tools** to abuse, tamper, or corrupt information technology–based data or control processes, which could result in severe injury or death.

It is first important to note that no single definition of the term "terrorism" has yet gained universal acceptance. Additionally, no single definition for the term "cyber terrorism" has been universally accepted as well. In addition, labeling a computer attack as "cyber terrorism" is problematic, because it is often difficult to determine the intent, identity, or the political motivations of a computer attacker with any certainty until long after the event has occurred (Wilson 2003).

There are some emerging concepts, however, that may be combined to help build a working definition for cyber terrorism. Internationally, terrorism is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience. The term "international

terrorism" means terrorism involving citizens or the territory of more than one country. The term "terrorist group" means any group practicing, or that has significant subgroups that practice, international terrorism[1] (U.S. Department of State 2003).

Caruso (2002) has provided an official definition for cyber terrorism in the United States. "Cyberterrorism—meaning the use of cybertools to shut down critical national infrastructures (such as energy, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population—is clearly an emerging threat." Denning's (1999) definition of cyber terrorism is slightly more elaborate:

> Cyberterrorism refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Though these attacks occur in cyberspace, they still exhibit the four elements common to all acts of terrorism:

1. *Premeditated and not simply acts born of rage*: Cyber-terrorist attacks are premeditated and must be planned since they involve the development or acquisition of software to carry out an attack.
2. *Political and designed to impact political structure*: Computer terrorism is an act that is intended to corrupt or destroy a computer system (Galley 1996). Cyber terrorists are hackers with a political motivation; their attacks can impact political structure through this corruption and destruction.
3. *Targeted at civilians and civilian installations*: Cyber-terrorist attacks often target civilian interests. Denning (2000) defines cyber terrorism as an attack that results in violence against persons or property, or at least that causes enough harm to generate fear.
4. *Conducted by ad hoc groups as opposed to national armies*: Cyber terrorism is sometimes distinguished from cyber warfare or information warfare, which are computer-based attacks orchestrated by agents of a nation or state.

Cyber warfare is another term that is often used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same (Hildreth 2001). Cyber warfare and information warfare employ information technology as an instrument of war to attack an adversary's critical computer systems (Hirsch, Kett, and Trefil 2002). Schwartau (1996) has proposed three categories for classifying information warfare: (1) personal information warfare, (2) corporate information warfare, and (3) global information warfare.

[1]The U.S. government has employed this definition of terrorism for statistical and analytical purposes since 1983.

Personal information warfare involves computer-based attacks on data about individuals. It may involve such things as disclosing or corrupting confidential personal information, such as those in medical or credit files. Corporate information warfare may involve industrial espionage or disseminating misinformation about competitors over the Internet. Global information warfare is aimed at a country's critical computer system infrastructure. The goal is to disrupt the country by disabling systems, such as energy, communication, or transportation.

Magnitude of the Problem

Some experts (Caruso 2001; Copeland 2000; Conway 2002; Hoopes 2005) have observed that terrorist organizations may begin to change their use of computer technology:

- Seized computers belonging to terrorist organizations indicate its members are now becoming familiar with hacker tools that are freely available over the Internet.
- As computer-literate youth increasingly join the ranks of terrorist groups, what may be considered radical today will become increasingly more mainstream in the future.
- A computer-literate leader may bring increased awareness of the advantages of an attack on information systems that are critical to an adversary, and will be more receptive to suggestions from other, newer computer-literate members.
- Once a new tactic has won widespread media attention, it likely will motivate other rival groups to follow along the new pathway.
- Potentially serious computer attacks may be first developed and tested by terrorist groups using small, isolated laboratory networks, thus avoiding detection of any preparation before launching a widespread attack.

Potential Cyber Terrorists

Cyber terrorism potentially can be carried out by anyone with access to the Internet. This includes anyone with a computer (and a modem), and as the technology becomes more sophisticated, may include anyone with cellular phones, wireless personal digital assistant (PDAs), and other wireless, handheld devices. The next cyber terrorist may be a world away or right next door as long as they have Internet access and the requisite knowledge. Accordingly, cyber terrorists may be domestic or foreign, with few limits on their actual location.

Cyber terrorists may act alone, as members of terrorist groups, or as proxies for terrorist groups. For example, in Hanover, Germany, in the 1980s, criminal hackers hired out their services to a terrorist group. Potential cyber terrorists also may include disgruntled current or former employees of a variety of private or public institutions. Cyber terrorists are likely to be very comfortable using computers and the Internet. In everyday life, people use the tools that they know and are comfortable with, including tools for criminal or destructive activities. As the Internet becomes an increasingly more central part of daily life, future terrorists increasingly will be more likely to use the Internet to plan and carry out terrorist activities. Why endanger one's life with explosives or weapons of mass destruction when you can sit in front of a computer and attack your enemy with almost total anonymity?

Today, most criminal hacking, or "cracking," is accomplished by one of three methods: (1) DoS (denial of service), in which the attacker overloads the server and shuts the system down; (2) actual destruction of information (although erasure of information usually is difficult to do effectively if their backup systems are in place); and (3) alteration of information, or "spoofing" (which is more difficult to safeguard against, but also can be mitigated with the use of backup systems).

Hackers are able to access computers via a number of routes, including poorly protected passwords, liberal access privileges, or dormant accounts of former employees. Hacking is facilitated by laxly enforced security policies (Copeland 2000). Currently, "parasites" are of great concern as a type of cyber attack. Parasites are small computer programs that remain in computer systems and slowly corrupt the system and its backups, thus, damaging the information in the system. These parasitic programs can cause systems to perform the wrong tasks. They also can spoof data, thus causing record alterations with troublesome effects.

Much of the basic knowledge needed to carry out acts of cyber terrorism is readily available through the Internet. Many hacking tools can be downloaded freely from the Internet through quick and easy searches. The beginner requires only knowledge of English and the capability to follow directions. However, in order to crack the better-protected computer systems ("hardened systems"), more extensive knowledge is required. This includes several years of experience with computer languages (e.g., C, C++, Perl, and Java); an understanding of general UNIX and NT systems administration, local-area network/wide-area network theory, remote access and common security protocols, and sufficient time would be required. Much of this advanced education and training is available over the Internet or may be obtained through readily available classes at public educational facilities (Galley 1996).

Cyber Terrorism: The Dynamics

Galley (1996) discusses three types of attacks against computer systems: (1) physical, (2) syntactic, and (3) semantic. A physical attack uses conventional weapons, such as bombs or fire. A syntactic attack uses virus-type software to disrupt or damage a computer system or network. A semantic attack is a more subtle approach. Its goal is to attack users' confidence by causing a computer system to produce errors and unpredictable results.

Syntactic attacks are sometimes grouped under the term "malicious software" or "malware." These attacks may include viruses, worms, and Trojan horses. One common vehicle of delivery for malware is e-mail.

Semantic attacks involve the modification of information or dissemination of incorrect information (Schneier 2000). Modification of information has been perpetrated even without the aid of computers, but computers and networks have provided new opportunities to achieve this process. In addition, the dissemination of incorrect information to large numbers of people quickly is facilitated by such mechanisms as e-mail, message boards, and Web sites.

There are five basic steps traditionally used by computer hackers to gain unauthorized access, and subsequently take over computer systems. These five steps may be used to plan a computer attack for purposes of cyber crime or cyber espionage, and may be employed for purposes of cyberterror (Wilson 2003). The steps are frequently automated through use of special hacker tools that are freely available to anyone via the Internet.

Step 1: Reconnaissance

In the first step, hackers employ extensive preoperative surveillance to find out detailed information about an organization that will help them gain later unauthorized access to computer systems. The most common method is social engineering, or tricking an employee into revealing sensitive information (such as a telephone number or a password). Other methods include dumpster diving, or rifling through an organization's trash to find sensitive information (such as floppy disks or important documents that have not been shredded). This step can be automated if the attacker installs in an office computer, a virus, worm, or "Spy ware" program that performs surveillance and then transmits useful information, such as passwords, back to the attacker. "Spy ware" is a form of malicious code that is quietly installed in a computer without user knowledge when a user visits a malicious Web site. It may remain undetected by firewalls or current antivirus security products, while monitoring keystrokes to record Web activity or collect snapshots of screen displays and other restricted information for transmission back to an unknown third party.

Step 2: Scanning

Once in possession of special restricted information, or a few critical phone numbers, an attacker performs additional surveillance by scanning an organization's computer software and network configuration to find possible entry points. This process can be quite slow, sometimes lasting months, as the attacker looks for several vulnerable openings into a system.

Step 3: Gaining Access

Once the attacker has developed an inventory of software and configuration vulnerabilities on a target network, he or she may quietly take over a system and network by using a stolen password, to create a phony account, or by exploiting a vulnerability that allows them to install a malicious Trojan Horse, or automatic "bot" that will await further commands sent through the Internet.

Step 4: Maintaining Access

Once an attacker has gained unauthorized access, he or she may secretly install extra malicious programs that allow them to return as often as they wish. These programs, known as "Root Kits" or "Back Doors," run unnoticed and can allow an attacker to secretly access a network at will. If the attacker can gain all the special privileges of a system administrator, then the computer or network has been completely taken over, and is "owned" by the attacker. Sometimes the attacker will reconfigure a computer system, or install software patches to close the previous security vulnerabilities just to keep other hackers out.

Step 5: Covering Tracks

Sophisticated attackers desire quiet, unimpeded access to the computer systems and data they take over. They must stay hidden to maintain control and gather more intelligence, or to refine preparations to maximize damage. The "Root Kit" or "Trojan Horse" programs often allow the attacker to modify the log files of the computer system, or to create hidden files to help avoid detection by the legitimate system administrator. Security systems may not detect the unauthorized activities of a careful intruder for a long period of time.

CYBER TERRORISM: THE TOOLS

Cyber terrorists use various tools and methods to unleash terrorism. Some of the major tools and methodologies are:

a. Hacking

"Hacking" is a generic term for all forms of unauthorized access to a computer or a computer network. Many technologies, the major ones being packet sniffing, tempest attack, password cracking, and buffer overflow facilitate hacking (Nagpal 2002).

- ***Packet Sniffing***

  When information is sent over computer networks, it gets converted into hex and broken into lots of packets. Each packet is identified by a header, which contains the source, destination, size of packet, total number of packets, serial number of that packet, etc. If a hacker wants to see this information, he uses packet sniffing technology that reconverts the data from hex to the original. This technology is like putting the equivalent of a phone tap on a computer. Sniffing can be committed when a packet leaves the source or just before it reaches the destination. For this, the hacker would need to know only the IP address (the unique number that identifies each computer on a network). A packet sniffer can log all the files coming from a computer. It can also be programmed to give only a certain type of information (e.g. only passwords).

- ***TEMPEST (Transient Electromagnetic Pulse Emanation Standard)***

  This technology allows someone not in the vicinity to capture the electromagnetic emissions from a computer and thus view whatever is on the monitor. A properly equipped car can park near the target area and pick up everything shown on the screen. There are some fonts that remove the high-frequency emissions, and thus severely reduce the ability to view the text on the screen from a remote location. Shielding computer equipment and cabling can avoid this attack.

- ***Password Cracking***

  A password is a type of secret authentication word or phrase used to gain access. Passwords have been used since Roman times. Internal to the computer, passwords have to be checked constantly. Therefore, all computers try to "cache" passwords in memory so that each time a password is needed the user does not need to be asked. If someone hacks into the memory of a computer, he can sift the memory or page files for passwords. Password crackers are utilities that try to "guess" passwords. One way, the dictionary attack, involves trying out all the words contained in a predefined dictionary of words. Readymade dictionaries of millions of commonly used passwords can be freely downloaded from the Internet. Another form of password cracking attack is "brute force" attack. In this attack, all possible combinations of letters, numbers, and symbols are tried out one by one till the password is found out.

- ***Buffer Overrun***

  Also known as buffer overrun, input overflow, and unchecked buffer overflow, this is probably the simplest way of hacking a computer. It involves input of excessive data into a computer. The excess data "overflows" into other areas of the computer's memory. This allows the hacker to insert executable code along with the input, thus enabling the hacker to break into the computer.

b. Trojans

Similar to the wooden horse, of the Troy War, in ancient Greece, a Trojan horse program pretends to do one thing while actually doing something completely different, but damages the software in a computer. Trojans are of various types, the important ones are:

- ***Remote Administration Trojans***

  They let a hacker access the victim's hard disk, and perform many functions on his computer (copy files, shut down his computer, open and close his CD-ROM tray, etc.).

- ***Password Trojans***

  Trojans search the victim's computer for passwords and then send them to the attacker or the author of the Trojan. There are Trojans for every kind of password. These Trojans usually send the information back to the attacker via e-mail.

- ***Privileges-Elevating Trojans***

  These Trojans are usually used to fool system administrators (the system administrator is considered the king of the network as he has the maximum privilege on the network). They can either be bound into a common system utility or pretend to be something harmless and even quite useful and appealing. Once the administrator runs it, the Trojan will give the attacker more privileges on the system.

- ***Key Loggers***

  These Trojans log all of the victim's keystrokes on the keyboard (including passwords), and then either save them on a file or occasionally e-mail them to the attacker. Key loggers usually do not take much disk space and can masquerade as important utilities, thus making them very hard to detect.

- ***Destructive Trojans***

  These Trojans can destroy the victim's entire hard drive, encrypt, or just scramble important files. Some might seem like joke programs, while they are actually destroying every file they encounter.

c. Computer Viruses

A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a copy of it. Viruses are very dangerous, in that they spread faster than being stopped, and even the least harmful of viruses could be fatal. For example, a virus that stops a hospital life support computer could be catastrophic.

d. Computer Worms

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections). Unlike viruses, worms do not need to attach themselves to a host program. There are two types of worms: *host computer worms* and *network worms.*

e. E-mail-Related Crimes

E-mail has emerged as the world's most preferred form of communication. Like any other form of communication, criminals also misuse e-mail. The ease, speed, and relative anonymity of e-mail have made it a powerful tool for criminals. Some of the major e-mail-related crimes are e-mail spoofing, spreading Trojans, viruses, and worms; e-mail bombing, threatening e-mails, defamatory e-mails, and so forth.

f. Denial of Service Attacks (DoS)

Denial of Service (DoS) attacks are aimed at denying authorized persons access to a computer or computer network. These attacks may be launched using a single computer or millions of computers across the world. In the latter scenario, the attack is known as a distributed denial of service (DDoS) attack. The main reason for the vulnerability of computer systems to DoS attacks is the limited nature of computer and network resources, be it bandwidth, processing power, storage capacities, or other resources. DoS attacks pose another challenge, namely timely detection and source identification. These attacks are usually launched from "innocent" systems that have been compromised by the attackers. All the attacker need to do, to launch a DDoS attack is install a Trojan in many computers, gain control over them, and then employ them in sending a lot of requests to the target computer.

g. Cryptography

A disturbing trend that is emerging nowadays is the increasing use of encryption, high frequency encrypted voice/data links, steganography (steganography, literally meaning covered writing, involves the hiding of data in another object; it can be used to hide text messages within image and audio files) etc., by terrorists and members of organized crime cartels. Notable examples are those of Osama bin Laden,[2] Ramsey Yousef,[3] Leary,[4] the Calicartel,[5] the Dutch underworld[6] and the Italian mafia.

[2]The alleged mastermind behind the September 11 attacks on the World Trade Center in the United States is believed to use steganography and 512-bit encryption to keep his communication channels secure.

[3]He was behind the bombing the World Trade Center in the USA in 1993 and an aircraft belonging to Manila Air in 1995.

[4]He was sentenced to 94 years in prison for setting off firebombs in the New York (USA) subway system in 1995. Leary had developed his own algorithm for encrypting the files on his computer.

[5]This cartel is reputed to be using sophisticated encryption to conceal their telephone communications, radios that distort voices, video phones which provide visual authentication of the caller's identity, and instruments for scrambling transmissions from computer modems.

[6]Dutch organized crime syndicates use PGP and PGPfone to encrypt their communications. They also use palmtop computers installed with Secure Device, a Dutch software product for encrypting data with IDEA. The palmtops serve as an unmarked police/intelligence vehicles database.

Weapons of Mass Annoyance[7]

A detailed examination of some of the scenarios for attacks on critical infrastructures helps place cyberattacks more accurately in a strategic or national security context.

- Dams used for water storage and for power generation are often cited as a likely target for cyber attack. Analysts in the United States believe that "by disabling or taking command of the floodgates in a dam, for example, or of substations handling 300,000 volts of electric power, an intruder could use virtual tools to destroy real-world lives and property" (Gellman 2002).
- Assuming that a terrorist could find vulnerability in a water supply system that would allow him to shut down one city's water for a brief period, this vulnerability could be exploited to increase the damage of a physical attack (by denying fire fighters access to water; DeNileon 2001).
- Many analyses have cyber terrorists shutting down the electrical power system. One of the better cyber-security surveys found that power companies are a primary target for cyber attacks and that 70 percent of these companies had "suffered a severe attack" in the first 6 months of 2002 (Riptech 2002).
- Interference with national air traffic systems to disrupt flights, shut down air transport, and endanger passenger and crews is another frequently cited cyber threat. The high level of human involvement in the control and decision-making process for air traffic reduces the risk of any cyber attack.
- Manufacturing and economic activity are increasingly dependent on computer networks, and cyber crime and industrial espionage are new dangers for economic activity. However, the evidence is mixed as to the vulnerability of manufacturing to cyber attack. A virus in 2000 infected 1,000 computers at Ford Motor Company. Ford received 140,000 contaminated e-mail messages in 3 hours before it shut down its network. E-mail service was disrupted for almost a week within the company (Keith 2000).
- Cyber attacks are often presented as a threat to military forces and the Internet has major implications for espionage and warfare. Information warfare covers a range of activities of which cyber attacks may be the least important (Buchan 1999).
- Terrorist groups like Al Qaeda do make significant use of the Internet, but as a tool for intra-group communications, fund-raising, and public relations. Cyber terrorist could also take advantage of the Internet to steal credit card numbers or valuable data to provide financial support for their operations.
- Terrorist groups are likely to use the Internet to collect information on potential targets, and intelligence services can not only benefit from information openly available on the Web but, more importantly, can benefit from the ability to clandestinely penetrate computer networks and collect information that is not publicly available.
- The financial costs to economies from cyber attack include the loss of intellectual property, financial fraud, damage to reputation, lower productivity, and third-party liability (*The Financial Times* 2002; Swartz 2001; *Sunday Herald Sun* 2001).

[7]Weapons of mass annoyance: a phrase originated by Stewart Baker.

- India and Pakistan have engaged in a long-term dispute over Kashmir. The dispute moved into cyberspace when pro-Pakistan hackers began repeatedly attacking computers in India. The number of attacks has grown yearly: 45 in 1999, 133 in 2000, and 275 by the end of August 2001 (Vatis 2002). At least one of these groups, the Pakistan Hackers Club, has also attacked American assets, namely, Web sites maintained by the U.S. Department of Energy and the U.S. Air Force.
- The Israel–Palestine conflict saw its first cyber attacks in October 2000 when some Israeli teenagers launched DoS attacks against computers maintained by the Palestinian terrorist organizations Hezbollah and Hamas (Kraft 2000). Anti-Israel hackers responded almost immediately and crashed several Israeli Web sites by flooding them with bogus traffic. Among the Israeli sites attacked by the Palestinians were sites belonging to the Knesset (parliament), Israeli Defense Forces, the Foreign Ministry, and the Bank of Israel.
- Some of the other possible situations are given below:

HYPOTHETICAL SITUATIONS

Several commentators discussing the capabilities of cyberterrorists have posited numerous hypothetical situations where cyberterrorists attack critical infrastructures within the United States.

Situation 1: A possible cyber terrorist attack could target children through a cereal manufacturer. A cyber terrorist could hack into the manufacturer's production computer and change the iron content to be added to the cereal. The cyber terrorist tells the computer to add 80 percent iron to the cereal instead of two percent. Many children eat the cereal and become very ill or possibly even die. Although several experts agree that this is a possible situation, many argue that the plan's success is unlikely.

Situation 2: A possible cyber terrorist attack could target airline passengers through the air traffic control tower of an airport. The cyber terrorist hacks into the computer system of the air traffic control tower and adds false information about the airplane's location, speed, etc., causing the air traffic controller to give the airplane pilot wrong information. The airplane then crashes into another plane, or into the ground, depending on the misinformation.

Situation 3: A cyber terrorist will place computerized bombs all throughout a city. These bombs will transmit a code to one another, and can be detonated by a timer or a computer. The bombs are also programmed to explode if one of the other bombs is disarmed.

Situation 4: A cyber terrorist disrupts bank software, interrupts financial transactions, and hacks into the stock market, deleting and changing stock prices. The cyber terrorist also introduces false information to the media concerning corporate mergers, stock prices, and corporate earnings. The disinformation causes a rapid decrease in stock prices, a loss of market capitalization, and a destabilization of the market. The citizenry lose faith in the economic systems and economic destabilization is achieved.

Situation 5: A cyber terrorist hacks into a pharmacy chain's computer network and changes information regarding drug interaction information. A large number of the elderly receive different medications, which have negative combined effects. Many become ill and some die.

—Adapted from Pollitt 2000.

Potential Effects

Cyber terrorism has the potential to greatly affect the healthcare infrastructure of a modern society. In many countries, as healthcare systems have become rapidly more dependent on the Internet, a number of instances of cyber crimes against healthcare systems already have been reported. While to date, most cyber crimes have been minor, they likely are harbingers of acts to come. Areas of particular concern to healthcare facilities include the potential for cyber terrorism–related events to erase or alter computerized medical, pharmacy, or health insurance records.

Cyber terrorism also may target other institutions that directly or indirectly affect the health of communities. Industries or public service agencies at particular risk of cyber terrorism include: (1) water supplies; (2) electrical power supplies; (3) emergency services; (4) telecommunications systems; (5) transportation systems; (6) banking and financial systems; and (7) government.

There have been numerous attacks against these infrastructures. Hackers have invaded the public phone networks, compromising nearly every category of activity, including switching and operations, administration, maintenance, and provisioning (OAM&P). They have crashed or disrupted signal transfer points, traffic switches, OAM&P systems, and other network elements. They have planted "time bomb" programs designed to shut down major switching hubs, disrupted emergency services throughout the eastern seaboard, and boasted that they have the capability to bring down all switches in Manhattan. They have installed wiretaps, rerouted phone calls, changed the greetings on voice mail systems, taken over voice mailboxes, and made free long-distance calls at their victims' expense—sticking some victims with phone bills in the hundreds of thousands of dollars. When they cannot crack the technology, they use "social engineering" to con employees into giving them access.

Cyber terrorism against the telecommunications system may have critical implications for the public health of communities. From the healthcare system perspective, attacks against the telecommunications system not only have the potential to disrupt the flow of health information, but also the multiple logistical systems upon which the operations of healthcare facilities depend (e.g., the acquisition of supplies). From the public safety perspective, cyber attacks against the telecommunications system may disrupt crucial information-sharing networks. For example, in March 1997, a teenage hacker penetrated and disabled a telephone company computer that provided service to the Worcester Airport in Massachusetts, cutting off service to the airport control tower, fire department, security, and weather service for 6 hours.

Public safety may be affected adversely by cyber terrorism in other ways. For example, in 1992, a disgruntled former employee of Chevron Corporation's emergency alert network, hacked into computers in New York and San Jose, California and reconfigured the firm's emergency alert system so that it would fail during an event. The disabled system was not discovered until an emergency arose at the Chevron refinery in Richmond, California, and the adjacent community could not be notified during an accidental chemical release. During the 10-hour period in which the system was down, thousands of people in 22 states and six areas in Canada with Chevron facilities went without the Chevron emergency alert system. As suggested above, hackers also have attacked traffic regulation systems, disrupting traffic lights, with the potential for an increase in motor vehicle collisions.

Cyber attacks against the essential services, such as the water and electrical supply systems, comprise another major area of concern. Hospitals and communities alike are highly dependent on water and only can subsist for limited periods without water. Fortunately, the majority of water system authorities in the United States are protected against cyber attacks

by supervisory control and data acquisition (SCADA) systems, though these systems may be still circumvented by other means. While hospitals in the United States almost always have back-up generators should the electrical supply system fail, communities almost always are immediately vulnerable. The longer a community remains without power, the more likely it is to suffer food and selected medication spoilage due to loss of refrigeration and deaths due to medical equipment failure (i.e., ventilators outside of hospitals).

Finally, cyber terrorism also can cause environmental contamination, with the potential for adverse health effects in the community. For example, in 2000, a perpetrator in Australia allegedly penetrated the Maroochy Shire Council's computer system and used radio transmissions to create overflows of raw sewage into the Sunshine Coast, causing widespread contamination. By extrapolation, a dedicated terrorist group could use cyber terrorism to cause more widespread, more enduring, or more toxic environmental contamination, with an almost incalculable impact on public health.

Cyber Terrorism and Civil Aviation

One of the methods where cyber terrorism has distinct but dangerous consequence is in the field of the civil aviation. This image of civil aviation as a potential target for cyber terrorists is a chilling one, but it paints a worst-case scenario that, in many respects, misses the point about cyber terrorism.

The range of potential perpetrators and intentions in the civil aviation environment is probably the most troubling aspect of this new reality. The availability on the Internet of easy-to-use tools to disable, disrupt, or corrupt systems is astonishing. In addition, the anonymity provided by the Internet may facilitate or encourage individuals to engage in activity or behavior that they otherwise avoid, and there is little likelihood of being caught. Several high-profile cases involving concerted attacks directed against American government systems were what appears to be the work of thrill-seeking teenagers. The civil aviation environment, therefore, is one of multiple, often unknown attackers, and a wide array of targets, whereas cyber terrorism per se represents a small but potential growth area.

Prevention and Control

Up-to-date **computer security** systems and firewalls, personal vigilance, and adherence to best-practice guidelines are essential in maintaining the security of computer systems. While the knowledge of how to hack into a computer system is readily available on the Internet, this same knowledge also allows system managers to understand how better to protect their systems. In addition, the Internet offers many resources, which can assist in protecting computer systems from cyber attacks. Nevertheless, even with the best security systems, safety measures can be rendered ineffective by lapses in security-conscious behavior.

The Need for International Technical Coordination

Networked information systems are being rapidly adopted by governments and businesses worldwide to improve communications, operational control, and ultimately, competitiveness. Reliance on these systems, especially where the Internet exists as the primary infrastructure,

is likely to increase. It is a complex technical and political task for nations and their commercial enterprises to protect information assets and ensure that critical operations continue even if attacked. The growth of world markets and an increase in transnational mergers only serve to compound this complexity.

Governments are recognizing the need to protect their information and critical infrastructures in response to these threats and are responding accordingly. Some governments recognize that it is not sufficient to address only the local or national aspects of safeguarding information and critical infrastructures. Because attacks against the Internet typically do not require the attacker to be physically present at the site of the attack, the risk of being identified is significantly reduced. Besides the technological challenges this presents, the legal issues involved in pursuing and prosecuting intruders adds a layer of difficulty as they cross multiple geographical and legal boundaries. An effective solution can only come in the form of international collaboration.

In the area of law enforcement, the Internet constitutes a new patrol area in many respects. Unlike jurisdictions based on national and political borders, the digital information infrastructure does not have a central location in the physical world. So not only is responding to attacks difficult technically but also many of the accepted methods for practicing law enforcement are ineffective. Recent G8 (Group of Eight Advanced Industrial States) and OPEC (Organization of Petroleum Exporting Countries) activities are examples of increasing recognition of this international need. The problems that we must address to improve our critical information infrastructures require the involvement of diverse parties including governments, policy and lawmakers, law enforcement, software vendors, the research community, and practitioners such as FIRST (Forum of Incident Response and Security Teams) members who have experience responding to computer security incidents. Attempting to address the problems in one group without input and feedback from the others is likely to result in flawed or incomplete solutions. The U.S. government legislation (the Digital Millennium Act, 1998) resulting from the World Intellectual Property Organization (WIPO) treaty resulted in a flurry of panic throughout the Internet security community. Practitioners, researchers, software vendors, and incident response teams realized that aspects of their work that address security flaws to reduce risk to our critical infrastructures might become illegal under the proposed legislation. This was clearly not the original intent of the treaty or the resulting legislation. This is just one example of the urgent need for ongoing communication among policymakers, technologists, and others to ensure that future policies and agreements on a national and international scale are practical and effective.

Current Difficulties

Many network protocols that now form part of the information infrastructure were designed without computer security in mind. Without a secure infrastructure, it is difficult to avoid security problems and resolve computer security incidents. The combination of rapidly changing technology, expanding use, and new, often unimagined uses of the information infrastructure creates a volatile situation in which the nature of threats and vulnerabilities is difficult to assess and predict.

It is inexpensive (the cost of a personal computer and Internet access), quick (less than a minute), and easy (using freely available intruder tools) for anyone to launch attacks against

our critical information infrastructures. Conversely, it is expensive (international effort and funding), long-term (research, development, and deployment), and complex (technically and politically) to take the steps needed to *harden* the information infrastructure to make it less susceptible to attack, and to enable us to respond more effectively and efficiently when attacks do happen.

In general, incident response and computer security teams consist of practitioners and technologists who have a wealth of operational experience but lack authority to make policy and security decisions in their organizations. They also may have limited funding and lack professional recognition. This has negative consequences; a given team's organization may not allow enough staff to respond effectively to security incidents. Similarly, a team may not have sufficient authority to influence and ensure improved computer security and comprehensive response. Moreover, at this time, there is no infrastructure to support a coordinated global incident response effort, although there are a few components in place that can form the basis of this infrastructure.

A variety of issues must be addressed when considering how to promote an effective global incident response infrastructure. These include discussions about which organizations will coordinate and participate in the development effort, how current groups and forums can fit their mission and objectives into an agenda to create a global infrastructure, and what possible structures and mechanisms might be required and effective in the future.

Countering Cyber Terrorism

In order to counter this form of terrorism, it is required that the following actions need to be taken immediately. In order to prevent damage, risk analysis needs to be performed for the information systems of the target critical infrastructures, and measures will have to be implemented as needed according to the importance of the information system. It is also necessary to continually raise security level in each of the fields with critical infrastructure (Erbschloe 2001).

- Raising security level in private sector critical infrastructure fields.
- Communication and coordination systems for private sector, etc. Critical infrastructure groups build a communication and coordination system between operators associated with cyber terrorism countermeasures, while making use of existing communication mechanisms, to fulfill the following roles:
  - Collect, distribute, and share the common security information in the various fields, as well as the warning information
  - A communication system for when a cyber attack occurs, or when there is a danger of such an attack
  - Implement unified, centralized communications for the government and related agencies
- Communication and coordination systems with other critical infrastructure operators.
  - In cases of interconnection to other information systems and operators of important infrastructure in other fields through networks, develop, as needed, the communication and cooperation systems for cyber terrorism countermeasures.

- Establishing a communication and cooperation system for government The government, will have to fill the following roles in developing the communication and cooperation systems:
  - Collecting, distributing, and sharing security information and warning information
  - Collecting information when a cyber attack occurs, or when there is a danger of such an attack
  - Within government departments, communication with related agencies and the private sector critical infrastructure groups
- Establishing an emergency response plan:
  - To establish countermeasures and an emergency response plan in the event of a cyber attack, or when there is a danger of such an attack on the private sector critical infrastructure operators, investigate while making use of the communications systems established. Expected issues for the emergency response plan include communication, containment of damage, verification of safety, recovery (temporary measures), prevention of recurrence, etc.
  - The actions during an emergency will sometimes require a high-level judgment, so procedures like the emergency response plan will be determined so that the appropriate persons, having the proper authority and responsibility, can make decisions quickly.
- Promote research and development:
  - The government and private sector critical infrastructure operators will promote cooperation and communication between the government and the private sector on research of the technology, countermeasures, threat analysis, and development of the required technology to build a strong foundation against the threat of cyber terrorism.
- Add and revise legislation:
  - The government needs to consider changes to the law, such as the basic criminal law, from the perspective of maintaining safety for the telecommunications networks and international harmony.
- International cooperation:
  - Cyber attacks can be made without regard for national boundaries, so international cooperation and coordination is required in order to handle such attacks.
  - The government and private sector key infrastructure operators will work to accumulate information from information security organizations outside our country.
  - The government needs to promote cooperation with the international organizations related to cyber terrorism.
  - The government will have to work to strengthen international cooperation, information exchanges and shared training with the counterparts in other nations.

CONCLUSION

The threat posed by cyber terrorism has grabbed the attention of the mass media, the security community, and the information technology (IT) industry. Journalists, politicians, and experts in a variety of fields have popularized a scenario in which sophisticated cyber terrorists

electronically break into computers that control dams or air traffic control systems, wreaking havoc and endangering millions of lives (Wiemann 2004). Though, cyber terrorism has become the fancy word of today's terror lexicon, many argue that it does not pose the threat as it is perceived (Green 2002; Forno 2002; Wiemann 2004). In addition, some argue that it is a ploy created by the media (Green 2002; Forno 2002). Government officials in the United States, including Caruso (2001) argue that media has exaggerated the issue of cyber terrorism, but agree that cyber terrorism has a threat to the information infrastructure (Caruso 2002). Hence it is found that there are two alternative perspectives with regard to threat of cyber terrorism. Even though we do not see any threat of cyber terrorism, as the cyberspace is explored day by day, the threat of cyber terrorism might increase in the near future.

KEY TERMS

Cyber crimes
Cyber terrorism
Computer security
Information warfare
Tools

REFERENCES

Buchan, G. C. 1999. "Implications of information vulnerabilities for military operations." In *Strategic Appraisal: The Changing Role of Information in Warfare,* edited by K. Zalmay, J. P. White, A. W. Marshall, 283–323. Santa Monica: Rand.

Caruso, J. T. October 11, 2001. Inaccurate media reports of potential terrorist attack. Before the House Intelligence Subcommittee on Terrorism and Homeland Defense.

Caruso J. T. March 21, 2002. Combating terrorism: Protecting the United States. Before the House Subcommittee on National Security, Veterans Affairs, and International Relations.

Conway, M. 2002. What is cyberterrorism? *Current History* 101 (659): 436–42.

Copeland, T. E. 2000. *The Information Revolution and National Security.* Carlisle, PA: Strategic Studies Institute, United States Army War College.

DeNileon, G. P. 2001. The who, what, why, and how of counterterrorism issues. *Journal AWWA* 93 (5): 78–85.

Denning, D. 1999. "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy,* edited by A. John and D. Ronfeldt, 239–38. Santa Monica: Rand.

Denning, D. 2000. *Cyberterrorism.* Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Retrieved December 15, 2006, from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Erbschloe, M. 2001. *Information Warfare: How to Survive Cyberattacks*. New York: Osborne/McGraw-Hill.

Financial Times, The [London]. November 22, 2002. A long, hard look at the hackers: 14.

Forno, R. 2002. Shredding the paper tiger of cyberterrorism. Retrieved December 15, 2006, from http:// www.securityfocus.com/columnists/111

Galley, P. 1996. Computer terrorism: What are the risks? [English translation July 1, 1998, by Arif M. Janmohamed] Retrieved December 15, 2006, from http://home.worldcom.ch/pgalley/infosec/sts_en/

Gellman, B. June 27, 2002. Cyberattacks by Al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool. *Washington Post*.

Green, J. 2002. The myth of cyberterrorism. *Washington Monthly.* Retrieved December 15, 2006, from www.washingtonmonthly.com/features/2001/0211.green.html

Hildreth, S. 2001. Cyberwarfare [CRS Report for Congress]. Retrieved December 15, 2006, from http:// www.fas.org/irp/crs/RL30735.pdf

Hirsch, E., Jr., J. Kett, and J. Trefil. 2002. *The New Dictionary of Cultural Literacy.* 3rd ed. Boston: Houghton Mifflin.

Hoopes, N. August 16, 2005. New focus on cyberterrorism. At risk: Computers that run power grids, refineries. *Christian Science Monitor*. Retrieved April 26, 2006, from http://www.csmonitor.com/2005/0816/p01s02-stct.html

Institute for Security Technology Studies (ISTS) at Dartmouth College. September 22, 2001. *Cyberattacks During the War on Terrorism.* Hanover, NH.

Keith, B. May 8, 2000. With its e-mail infected, ford scrambled and caught up. *New York Times*.

Kraft, D. October 26, 2000. Islamic groups "attack" Israeli Web sites. Retrieved December 15, 2006, from http://www.landfield.com/isn/mail-archive/2000/Oct/0137.html

Lewis, J. A. 2002. Assessing the risks of cyberterrorism, cyber war and other cyber threats. *NATO Review* 49 (Winter): 16–18.

Nagpal, R. 2002. Cyberterrorism in the context of globalization. Paper presented at the II World Congress on Informatics and Law Madrid, Spain, September 2002. Retrieved December 15, 2006, from http://www.ieid.org/congreso/ponencias/Nagpal,%20Rohas.pdf

Pollitt, M. M. 2000. Cyberterrorism—Fact or fancy? Retrieved December 15, 2006, from www.cs.georgetown.edu/~denning/infosec/pollitt.htm

Post, J. M. 2000. From car bombs to logic bombs: The growing threat from information terrorism. *Terrorism and Political Violence* 12 (2): 97–122.

Riptech Internet Security Threat Report. 2002. Retrieved December 15, 2006, from http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf

Schneier, B. 2000. Semantic network attacks. *Communications of the ACM* 43 (12): 168.

Schwartau, W. 1996. *Information Warfare.* New York: Thunder's Mouth Press.

Sprols, J., and W. Byars. 1998. *Cyberterrorism*. Retrieved December 15, 2006, from http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/

Sunday Herald Sun [Melbourne]. November 18, 2001. How terror stalks the Web: 43.

Swartz, J. October 9, 2001. Experts fear cyberspace could be terrorists' next target. *USA Today*.

U.S. Department of State. 2003. Patterns of global terrorism, 2003. Retrieved December 15, 2006, from http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10220.htm

Vatis, M. 2002. Cyberattacks: Protecting America's security against digital threats. Discussion paper ESDP-2002-04, John F. Kennedy School of Government, Harvard University.

Wiemann, G. December 2004. Cyberterrorism: How real is the threat? Special Report No. 119. United States Institute of Peace. Retrieved December 15, 2006, from http://www.usip.org/pubs/specialreports/sr119.html

Wilson, C. 2003. Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress. CRS Report for Congress Congressional Research Service, The Library of Congress, U.S. Department of State.