CHAPTER 6

Teaching Terrorism: Dimensions of Information and Technology

JAMES J. F. FOREST

In April 1999, after visiting an Internet cafe in the Victoria district of London, a young man downloaded two books—*The Terrorists' Handbook* and *How to Make Bombs, Book Two*—from a seemingly ordinary website.[1] Following the instructions provided in these texts, he packed a plastic pipe with flash powder he had removed from various fireworks and sealed the pipe with glue. This was put into a box surrounded by around 1,500 nails of differing sizes, which would act as shrapnel when the pipe was detonated. He added a modified timer and two battery-powered electrical igniters (which would serve as detonators), placed the device inside a sports bag, took a taxi to Brixton, South London, and left the bag on the corner of busy Electric Avenue. The explosion occurred at 5:25 P.M., injuring fifty people. The following Saturday, a second explosion took place, this time in Brick Lane, an East London neighborhood. The same type of device was used, this time injuring thirteen. Less than a week later, an explosion ripped apart the Admiral Duncan pub in Soho, London, at approximately 6:10 P.M. The pub had been full of Friday evening patrons; three were killed, four needed amputations, twenty-six suffered serious burns, and another fifty-three were injured in other ways.

Thanks to a series of tips to Scotland Yard, David Copeland's terrifying nail bombing campaign ended while the dead and maimed were still being counted from the wreckage of the Admiral Duncan pub. At his trial, Copeland told police that he was a Nazi, and that he hoped the explosions would "set fire to the country and stir up a racial war." The media focus on the trial of this young engineer from Farnborough, Hampshire, brought considerable public attention to the widespread availability of online resources like *The Terrorists' Handbook* and *How to Make Bombs, Book*

Two. Both titles are still easily accessible; a search for the keyword phrase "terrorist handbook" on the popular Google search engine found over 423,000 matches. One site gives instructions on how to acquire ammonium nitrate, Copeland's "first choice" of explosive material.

Most of the chapters in this volume address physical aspects of terrorist training, from the training camps in places like Afghanistan, Indonesia, and Syria to the various psychological and sociological forces involved in transforming a new recruit into a capable terrorist. This chapter explores a more virtual realm of terrorist learning, exploring the print and online materials that exist through which an individual can learn the skills and operational knowledge required for conducting successful terrorist attacks without necessarily affiliating with a particular terrorist-oriented group.

This discussion is placed within the context of the primacy of information—without appropriate operational knowledge, a would-be terrorist is limited in his or her capabilities to conduct a successful attack. Before the advent of the Internet, access to such forms of operational knowledge was fairly limited. In contrast, today it is accessible worldwide; at the touch of a keyboard, the click of the mouse, anyone—regardless of age, ethnicity, or intelligence level—can learn how to conduct a terrorist attack. Our understanding of the terrorist world must therefore include the dimensions of information and technology.

Two Types of Useful Information for Terrorism

Like terrorism, information can be seen as a primary tool to change behavior or bring about some action on either an individual or group level. There are basically two types of information useful to developing the would-be terrorist: *motivational* (most often of an ideological nature), and *operational* (that which provides strategic and tactical capabilities). Put another way, motivational/ideological information usually addresses the central question of *why* an individual or group seeks to use violent means to achieve political, social, and/or religious goals, while operational information addresses the question of *how* to most effectively use violent means for achieving these goals.

Motivational knowledge is typically disseminated in oral, print, and online formats, and largely deals in the realms of psychological, social, cultural, intellectual, and emotional development. Acquiring this knowledge (or indoctrination) is seen as vital to developing an individual's will to kill, and is addressed at length in Volume I of this publication.[2] However, it can be argued that operational information—a much more action-oriented realm of learning—arguably presents the greatest present danger to the civilized world. Motivational knowledge without operational capability is far less harmful than operational knowledge (with or without motivation). In

contrast, operational knowledge—the skill to kill—is the primary key to any terrorist's capability to achieve his or her objectives.

The globalization of access to information technology has had a dramatic impact on the dissemination of this type of knowledge. As Bruce Hoffman aptly observed, "Using commercially published or otherwise readily accessible bomb-making manuals and operational guides to poisons, assassinations and chemical and biological weapons fabrication . . . the 'amateur' terrorist can be just as deadly and destructive as his more 'professional' counterpart."[3] In essence, operational knowledge can be seen as the most vital tool in the terrorist's toolkit, which accounts for why the would-be terrorist most often tends to seek out these sorts of information resources.

One can generate quite an extensive list of the types of strategic or tactical information terrorists need to acquire before conducting a successful attack. At the terrorist group level, required information includes how to organize cells, how to communicate between and among the organization's members, and how to get and exchange funds. In addition, a group—as well as a nonaffiliated individual seeking the ability to conduct a terrorist attack—may need to acquire information on document falsification, sabotage, target vulnerability assessment, and artillery training. Some terrorists need to learn how to move from one location to another without detection; how to mount rocket launchers in the beds of pickup trucks; how and where to launder money; how to successfully conduct a kidnapping; how to conduct target identification, surveillance and reconnaissance; how and where to build camouflage-covered trenches; and how to covertly communicate with other members of a group or network—for example, the use of personal messengers (particularly on horseback, motorcycle, or bicycle) rather than electronic communications, or changing frequencies when using electronic communications in battle.

A terrorist may also need certain kinds of information to help him or her decide what types of weapons will be most effective for a particular attack (and how they must be assembled, transported and used). Specialized information is needed to learn how to effectively fire handguns, machineguns, and rocket-propelled grenade launchers, or how to assemble bombs and TNT from the plastic explosive C4.[4] In many cases, surveillance and planning is needed for securing escape routes once the attack has been carried out. Terrorists must learn the nuances of securing organizational assets, planning the roles and responsibilities of members involved in the attack, identifying risks to the operation, and examining the advantages of using certain kinds of vehicles over others—for example, al Qaeda's use of Toyota Corollas for transporting militants and weapons on windy mountainous roads. Information for conducting urban warfare is also useful to the would-be terrorists, through which they can learn how to block roads, storm buildings, and attack the infrastructure of a country—including elec-

trical power plants, airports, railroads, large corporations, and military installations.[5]

A terrorist's search for operational information is not limited to attacks of a physical nature. Indeed, as described later in this chapter, cyberterrorist attacks require a specialized mix of knowledge. While highly technical knowledge is required to successfully use the Internet to shut down power plants, banking systems, or other cyberterrorist targets, a successful terrorist must also have a solid understanding of human behavior, public policies, emergency awareness procedures, and so forth.

In sum, the skills and abilities of the would-be terrorist are developed through the acquisition of an array of operational information. As described in many of the chapters of this volume, this individual can acquire this information through formal training camps by joining any number of terrorist organizations, including al Qaeda, the FARC, Hizballah, or Jemaah Islamiyah. However, training for terrorism can also take place through many forms of distance education—defined as instruction (typically asynchronous) provided through print or electronic means to individuals in a geographic location separate from the instructor(s).[6]

Print and Electronic Sources of Information for Learning Terrorism

Throughout most of the nineteenth and twentieth centuries, the distribution of literature complemented face-to-face contact as primary vehicles for both recruitment and training of new supporters of terrorist organizations. Books and magazines have always played a particularly important role in disseminating both motivational/ideological knowledge and operational knowledge to new and potential terrorists worldwide. One of the earliest prominent examples was Carlos Marighella's book *The Liberation of Brazil*, portions of which were widely translated and employed by Latin American and European terrorists.[7] In one chapter of his book, entitled "Handbook of Urban Guerilla Warfare," Marighella encouraged physical training and manual skills, as well as the mastery of small arms and explosives, and stated that only a guerrilla who had passed initial tests should be selected for additional training or tasking.[8] In Northern Ireland, the Provisional Irish Republican Army produced a manual called *The Green Book*, covering ideology as well as basic military training for new recruits, weaponry, explosives, and battle tactics.[9]

In the world of the jihadists, prominent books include Sayyid Qutb's *Under the Umbrella of the Koran*, which underscored the importance of monotheism in Islam,[10] and his *Signposts along the Road*, in which he damned Western and Christian civilization and urged jihad against the enemies of Islam.[11] Qutb's teachings have had considerable influence over

Osama bin Laden and informed the writings of his deputy, Ayman al-Zawahiri, as reflected in his book *Knights Under the Banner of the Prophet*.[12] Another influential Islamic scholar was Sheik Abdullah Azzam, whose books on jihad include *Join the Caravan*, *Signs of Ar-Rahman in the Jihad of the Afghan*, *Defense of the Muslim Lands*, and *Lovers of the Paradise Maidens*. Azzam's combat experiences in the Palestinian territories and Afghanistan contributed to the unique reverence given to his writings by Islamist radicals.

In terms of U.S.-based domestic terrorist groups, one of the most oft-cited sources of motivational/ideological knowledge is *The Turner Diaries*. Written by William Pierce—a former physics professor and, at the time, the founding leader of the white supremacist group The National Alliance—and published under the pseudonym Andrew MacDonald, the book describes a fictional civil war in the United States in which white Aryans fight what the author and other right-wing extremists call the Zionist Occupation Government (ZOG), killing blacks and Jews indiscriminately. The dramatic highlights are the ruthless destruction of American cities to pave the way for the dream of a white America and a white world come true.[13] Since its publication in 1980, the book has influenced a whole generation of right-wing extremists, from Christian Identity adherents to Neo-Nazis, Klansmen, militia, and survivalist activists. *The Turner Diaries* was a favorite book of Oklahoma City bomber Timothy McVeigh, who used the description of the FBI headquarters' destruction as a blueprint for his real-life terror attack.[14]

While a significant majority of the publications in the terrorist world deal with the motivational/ideological realm of knowledge (most often of a religious and/or political flavor), the increasing proliferation of operationally-focused magazines and training manuals is cause for some concern. Al Qaeda's occasionally-published magazine *Mu'askar al-Battar* (The al-Battar Training Camp), features essays on military training amid a plethora of appeals for Muslims to join the fight. Issue 19, released October 2004, includes advice on survival techniques in the wild, the care and use of a revolver, and instruction in map reading and orientation.

Other jihadi periodicals, many linked to al Qaeda, include *Voice of Jihad* (in print and online circulation since 2000) and *Tora Bora*, the May 2004 issue of which included an analysis of Pakistan's campaign in the Waziristan province and an extended article on "The Secret of Success in Battle." In Algeria, a new magazine appeared in May 2004 (*Al-Jama'a*, or "The Group") which noticeably imitates al Qaeda publications. Posted on the website of the *Groupe Salafiste pour la Predication et le Combat* (GSPC), the first issue of this publication was large on motivational/ideological knowledge, but short on operational knowledge.[15] Another periodic jihadist publication, the "In the Shadow of the Lances" series, first appeared after 9/11. As of mid-2003, there have been nine installments, the majority of which were written by al Qaeda spokesman Sulaiman Abu Gaith and were

largely focused on motivational/ideological knowledge transfer, while the fifth and sixth installments were written by Saif al-Adel (believed to be a high-ranking member of al Qaeda's military operations) and provided tactical lessons learned from the battle against U.S. forces in Afghanistan.[16]

Other prominent sources of operational knowledge include *The Anarchist Cookbook* and *The Mujahideen Poisons Handbook*. The latter was written by Abdel Aziz in 1996 and "published" on the official Hamas website, detailing in twenty-three pages how to prepare various homemade poisons, poisonous gases, and other deadly materials for use in terrorist attacks.[17] The *Terrorist's Handbook*, published by "Chaos Industries and Gunzenbombz Pyro Technologies," offers ninety-eight pages of step-by-step operational knowledge.[18] But the multivolume *Encyclopedia of the Afghan Jihad*, written in Arabic and distributed on paper and on CD-ROM, is perhaps one of the most oft-cited terrorist training manuals in existence today. It contains a wealth of operational knowledge for new terrorists, covering topics such as recruitment of new members, discharging weapons, constructing bombs, and conducting attacks. Specific examples are included, such as how to put small explosive charges in a cigarette, a pipe, or a lighter in order to maim a person; drawings of simple land mines that could be used to blow up a car (not unlike the improvised explosive devices seen most recently in Iraq); and radio-controlled devices that could be used to set off a whole truckload of explosives, like those used to destroy the U.S. embassies in Kenya and Tanzania in August 1998.

In the United States, Tom Metzger, the guru of the "lone wolf" or "leaderless resistance" model of activism, has provided right-wing extremist groups with strategic guidance for several decades. Through his *White Aryan Resistance* (WAR) monthly newspaper, books, a telephone hotline, a website, and a weekly e-mail newsletter (*Aryan Update*), Metzger's work can be seen as the operational-knowledge counterpart to the motivational/ideological knowledge contribution of the *Turner Diaries*. His primary contribution to the field of terrorist knowledge has been in advocating individual or small-cell underground activity, as opposed to above-ground membership organizations. He argues that individual and cellular resistance leaves behind the fewest clues for law enforcement authorities, decreasing the chances that activists will end up getting caught. Specific guidelines for this strategy include act alone and leave no evidence, do not commit robbery to obtain operating funds, act silently and anonymously, do not deface your body with identifiable tattoos, understand that you are expendable, and whatever happens, do not grovel.[19] While Metzger intended his operational knowledge to improve the capabilities of like-minded racists, some observers have noted its salience for (and adoption by) other terrorist-minded groups as well.

Another U.S.-focused terrorism resource is the *Field Manual for Free Militia*, which is available on the web.[20] This manual contains sections such

as "Principles Justifying the Arming and Organizing of a Militia," which lays out a theological justification for the ideals and goals of the Christian Militia movement. Another section of the manual provides advice for buying and using weapons and other equipment considered necessary for violent confrontation with enemies of the movement. Christian militiamen are encouraged to acquire a medium- to high-power semiautomatic rifle with a magazine that is detachable, camouflaged clothing, protective gear needed in direct combat (like helmets and flak jackets), and basic radio equipment that would be necessary to keep a small force of men in contact during a battle.[21] Thus, like the al Qaeda manual and other jihadist resources described earlier, this popular Christian Militia publication contains both motivational/operational learning and operational training.

Beyond the printed word, terrorists are discovering what many Western institutions of higher learning have already recognized: CD-ROMS, video recordings, and other forms of multimedia offer powerful vehicles for motivational and operational knowledge transfer. Even audio recordings are useful; Osama bin Laden is said to have been considerably influenced by the tape recordings of fiery sermons by Abdullah Azzam, a Palestinian and a disciple of Qutb.[22]

However, perhaps no source of operational information is more important today than the Internet. Indeed, the global spread of Internet connectivity provides such a powerful medium for terrorists to engage in distance learning activities that some websites can truly be called—as in the words of Israeli terrorism researcher Gabriel Weimann—"virtual training camps."[23] For example, two "Jihad in Chechnya" websites (azzam.com and kavkaz.org) offer an array of motivational and tactical support to terrorist organizations, particularly through photo and video libraries. Much of the information found in the *Encyclopedia of the Afghan Jihad* volumes is now available on many websites and in multiple languages. The website of the French Anonymous Society (*Société Anonyme*) offers a two-volume *Sabotage Handbook* online, with sections on topics such as planning an assassination and antisurveillance methods.[24]

The invention and increasing availability of online language translation tools also offers a unique and important dimension to the transfer of knowledge in the terrorism world. With these tools, the U.S. Army website—which offers scores of publicly available field manuals on everything from conducting psychological operations to sniper training and how to install Claymore antipersonnel mines—can be translated online and used to educate non-English speaking terrorist-minded individuals. Further, the ability to rapidly transfer new information in electronic form to a global audience, simultaneously and in multiple languages, presents additional challenges to those seeking to curb the ability of terrorist organizations to train new members.

Online computer games are another form of Internet-based training for

terrorism. Today, a whole variety of "first-person shooter" games—with violent graphics, depicting real-life scenarios in which the player is the central character, killing Jews and other racial minorities—can be obtained for free on the Internet.[25] As Madeleine Gruen notes, "a website associated with the racist organization National Alliance offers game titles and descriptions such as 'Shoot the Blacks' (Blast away the darkies as they appear), 'Nigger Hunt' (Safari in Africa: Kill all the Niggers you can) and 'Rattenjagt' (Kill the Jewish rats). Their strategy [in offering these games] is . . . to make them widely available on the web for free so that there can be no limit to the number of people exposed to the 'white power' message."[26]

The first computer game developed by a political Islamist group is called *Special Force*, and was launched in February 2003 by the Lebanese terrorist group Hizballah.[27] Another "first-person shooter" game, *Special Force* gives players a simulated experience of conducting Hizballah operations against Israeli soldiers in battles re-created from actual encounters in the south of Lebanon, and features a training mode where players can practice their shooting skills on targets such as Israeli Prime Minister Sharon and other Israeli political and military figures. The game can be played in Arabic, English, French, and Farsi, and is available on one of the Hizballah websites.[28] Mahmoud Rayya, a member of Hizballah, noted in an interview for the *Daily Star* that the decision to produce the game was made by leaders of Hizballah, and that "in a way, *Special Force* offers a mental and personal training for those who play it, allowing them to feel that they are in the shoes of the resistance fighters."[29]

According to terrorism analyst Madeleine Gruen, Hizballah's Central Internet Bureau developed the game in order to train children physically and mentally for military confrontation with their Israeli enemies.[30] By the end of May 2003, more than 10,000 copies of *Special Force* been sold in the United States, Australia, Lebanon, Syria, Iran, Bahrain, and United Arab Emirates. Games such as these, as Gruen notes, "are intended to dehumanize the victim and to diminish the act of killing." In essence, through simulating acts of violence, these games develop the players' skill to kill, without the players having to leave the comfort of their own home.

Websites operated by the global news media also play a role in teaching terrorism, each time they offer details of how a successful attack was carried out.[31] By offering online video clips of attacks and their aftermath, messages from prominent terrorist leaders (like Osama bin Laden or Abu Masab al-Zarqawi), and other types of information, these media websites are in essence providing a form of showcase for the display of both motivational and operational information.[32] Indeed, in some cases training for terrorism may in fact be an ultimate goal of providing such information—like, for example, the website of al-Manar (the Arabic word for beacon), a television station owned and operated by Hizballah. In other cases—such

as the satellite television networks al-Jazeera and al-Arabiya, whose websites are relatively less one-sided in their coverage of the Middle East crisis but are much more global in their appeal throughout the Islamic world[33]—the goals are more journalistic in nature. In either case, would-be terrorists can learn much from the television broadcasts and websites of such media outlets.

Overall, much of the terrorist-oriented uses of the web involve one-way dissemination of ideology. Most websites of concern play a similar role as pamphlets, doctrinal statements, or other literature that seeks to motivate terrorist-oriented sentiments. However, a limited (but growing) number of online information sources are providing operational capability-building knowledge, a means by which motivated terrorists can acquire the know-how to actually carry out a successful attack. This is particularly true when considering the threat of cyberterrorism.

Tools and Training for Conducting Cyberterrorist Attacks

Cyberterrorism refers to the convergence of cyberspace and terrorism.[34] The Naval Postgraduate School defines cyberterrorism as the unlawful destruction or disruption of digital property to intimidate or coerce people.[35] Mark Pollitt, special agent for the FBI, offers a more comprehensive definition: Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational or clandestine agents.[36] In 1996, the President's Commission on Critical Infrastructure Protection noted how the threat of cyberterrorism was changing the landscape of homeland security:

> In the past, we have been protected from hostile attacks on the infrastructures by broad oceans and friendly neighbors. Today, the evolution of cyberthreats have changed the situation dramatically. In cyberspace, national borders are no longer relevant. Electrons don't stop to show passports. Potentially serious cyber attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker.[37]

Clearly, the threat of a cyber attack is an important consideration for anyone working to improve national security, and deserves far more attention in the study of terrorism than has been seen to date. Indeed, much of the research literature on cyber attacks has been limited to focusing on criminal aspects, such as credit card theft, bank fraud, identity theft, or more generally, computer hacking.

Hacking is a general term used to describe a variety of creative techniques through which individuals seek to gain access to computer systems.[38] Some, like "denial of service attacks" or "e-mail bombs," are meant to break these systems, or at least keep them from doing what they ordinarily do. For example, a denial of service attack on a web server floods it with bogus requests for pages. The server spends so much time trying to process these requests that it cannot respond to legitimate requests and may crash. An e-mail bomb is similar, but targets a victim's mail server.[39] Both attacks serve as a form of virtual blockade, and can result in a loss of service, computer system degradation, and even general insecurity among computer users. In what some U.S. intelligence authorities characterized as the first known attack by terrorists against a country's computer systems, the Tamil Tigers (ethnic separatists considered one of the most lethal terrorist groups in the world) swamped the computers at Sri Lankan embassies with thousands of e-mail messages, clogging their network systems and "generating fear in the embassies."[40]

In addition to cyber attacks that flood and disable websites or e-mail servers with a barrage of data, computer users also face a daily threat from computer viruses, worms, Trojan horses and logic bombs—malicious computer programs designed by hackers and spread over the Internet to steal or destroy computer data. A virus is a program that can attach itself to a file, corrupt a computer's data files, replicate itself, and even try to use all of the computer's processing resources in an attempt to crash the machine. Worms invade a computer and steal its resources to replicate themselves and spread to other computers on the network. A Trojan horse appears to do one thing but does something else—the system may accept it as one thing, but upon execution it may release a virus, worm, or logic bomb. A logic bomb is an attack triggered by an event, like the computer clock reaching a certain date. It might release a virus or be a virus itself.[41] To complicate matters further, these types of attacks are often difficult to identify until after they have taken place, and identifying the culprit—figuring out who attacked you, and how—can take enormous amounts of time and energy. Developers of computer viruses, worms, and so forth are quite innovative and creative, causing no end of trouble for the virus protection industry.

While most cyber attacks of major significance have been relatively harmless forms of political protest—or at worst, an annoyance for computer network professionals to deal with—they have also occasionally caused significant economic and political trouble. For example, the CODE RED attack in 2001 infected 50,000 machines per hour, ultimately causing billions of dollars in damage.[42] During the Gulf War, Dutch hackers stole information about U.S. troop movements from U.S. Defense Department computers and tried to sell it to the Iraqis, who thought it was a hoax and turned them down.[43] In March 1997, a fifteen-year-old Croatian penetrated

computers at a U.S. Air Force base in Guam.[44] Government computers reportedly were crashed by terrorist groups during elections in Indonesia, Sri Lanka, and Mexico.[45]

In March 1994, two hackers, identified by the aliases Kuji and Datastream Cowboy, broke into the U.S. Air Force's lab in Rome, New York. Subsequent investigations led officials to Britain, and with the help of Scotland Yard it was discovered that Datastream Cowboy—a sixteen-year-old British student—had used various hacking techniques to access data from NATO headquarters, Goddard Space Flight Center, the South Korean Atomic Research Institution, and over a hundred other victims. Telecommunications networks in Colombia, Chile, the United States, and at least a half-dozen more countries were used as conduits for these attacks.[46] In February 1998, a number of Department of Defense networks were attacked by hackers using a well-known vulnerability in the Solaris (UNIX-based) computer system. The hackers probed, found, and exploited the vulnerabilities in the DOD computer network, planted a program to gather data, and then returned later to collect the data. Two high school students from California were eventually arrested, along with an eighteen-year-old Israeli accomplice.

To test the nation's defenses against a massive Internet-based attack, the National Security Agency hired thirty-five hackers in 1997 to launch simulated attacks on the U.S. electronic infrastructure, an exercise dubbed "Eligible Receiver."[47] The hackers gained access to thirty-six Department of Defense networks, "turned off" sections of the U.S. power grid (affecting cities like Los Angeles, Colorado Springs, St. Louis, Chicago, Detroit, and Tampa), "shut down" parts of the 911 emergency network in Washington, DC, and gained access to computer systems aboard a Navy cruiser at sea.[48] From this and other exercises, the U.S. government has learned that a coordinated cyber attack has the potential to bring down parts of the Internet, silence communications and commerce, paralyze federal agencies and businesses, hang up air traffic control systems, deny emergency 911 services, shut down water supplies, and interrupt power supplies to millions of homes.[49]

The global spread of the Internet presents attractive opportunities to would-be terrorists. Terrorists have obvious incentives to look for and exploit the weakest links in any system—including social systems. In most societies, the weakest links regarding Internet security are the average home users browsing the Internet, sending an e-mail to Uncle Joe with a photo of the new baby, checking a bank balance, and shopping for that latest U2 release. Malicious attacks against the average Internet user have become increasingly common, resulting in widespread computer crashes and many instances of credit card number theft, identity theft, and bank fraud, through which terrorist groups can gain funds to support their operations. Attacks of various types occur through cyberspace every day, even in the United

States; the world's greatest economic and military superpower cannot protect its citizens against a fourteen-year-old computer whiz in Malaysia. However, these small-scale attacks can also be seen as training exercises, whereby computer hackers develop the technical skills for future, more elaborate and complicated attacks—like that envisioned in the NSA's "Eligible Receiver" exercise. It is this latter point which causes the most concern for public and private security professionals worldwide.

While private firms like CERT and Symantec scramble to keep up with the evolution and proliferation of Internet viruses and newly invented hacking techniques, the U.S. government recently issued its first national strategy for securing cyberspace.[50] To its credit, this document highlights the importance of multinational cooperation, particularly since many of the most active websites are hosted in countries beyond those that are committed to the global war on terrorism. The National Strategy to Secure Cyberspace (2002) also emphasizes the nation's vulnerability, noting that "of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security." Indeed, the threat of cyberterrorism is quite real and is ignored at our peril. For this reason, government agencies and units have been established through North America and Europe to investigate cyber crimes and to work with the private sector to identify and fix critical vulnerabilities in cyberspace.

Unfortunately, as most technology-savvy observers will agree, a vast array of tools and information resources for learning terrorism are all around us. The Internet offers a rich source of information through which self-styled hackers or crackers can learn how to conduct a wide variety of cyber attacks against any private or public online entity. Each year, thousands of new websites with hacker tips and tools appear, along with dozens of publications and newsgroups.[51] An entire world of hacker support communities also exists online. The website chat forums of hacking groups—with names such as the Chaos Computer Club, the Cult of the Dead Cow, !Hispahak, L0pht Heavy Industries, Phrack, Pulhas, and Legion of the Underground—serve as places where members share ideas and experiences, sometimes even boasting of their exploits in a perverse form of one-upmanship. These online arenas for shared learning provide a useful source of information for the would-be cyberterrorist.

Today, thousands of websites provide detailed step-by-step instructions for conducting denial of service attacks, packet sniffing, password cracking, buffer overflow attacks, network vulnerability testing, and so forth. Visitors can download free software (like the SuperScan vulnerability scanning tool or the Ethereal packet sniffing program) for use in finding and exploiting vulnerabilities in virtually any type of computer or network system. Tools can also be found online for protecting an attacker's anonymity and for conducting encrypted communications, including the use of steganography—a

method known to be used by members of al Qaeda, whereby computer graphics and digital photos are used to hide data (such as the plans for future attacks), and can then be transferred openly over the Internet.[52]

According to a 1998 statement to Congress by Clark Staten, the executive director of the Emergency Response and Research Institute in Chicago, "Members of some Islamic extremist organizations have been attempting to develop a 'hacker network' to support their computer activities and even engage in offensive information warfare attacks."[53] As Israeli researcher Gabriel Weimann (2005) has noted, Islamic radical terrorists have an interest in conducting various forms of cyber attacks. In fact, Sheikh Abdul Aziz al-Alshaikh—the Grand Mufti of Saudi Arabia and the highest official cleric in the country—issued a special *fatwa* in December 2002 which in essence encourages Muslims "to send viruses to disable and destroy websites" that are deemed hostile to Islam.[54] It is thus unsurprising to find that the website of the Muslim Hackers Club offers tutorials in viruses, hacking strategies, and instructions and encouragement for exploiting various network vulnerabilities.[55] According to military analyst Timothy Thomas, "The website 7hj.7hj.com aims to teach Internet users how to conduct computer attacks . . . [and offers] a kind of database or encyclopedia for the dissemination of computer viruses, purportedly in the service of Islam."[56]

The Internet is also used for conducting surveillance on potential targets. One captured al Qaeda computer contained engineering and structural architecture features of a dam, enabling al Qaeda engineers and planners to simulate catastrophic failures.[57] In fact, an al Qaeda training manual recovered in Afghanistan informed its readers that "using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy."[58] Thus, in addition to the wide range of instructions and free software applications for hacking into websites, e-mail systems, banking transactions, etc., the Internet also provides the cyberterrorist with such open source documents as plans, building schematics, maintenance schedules, emergency preparedness plans, and others that can be useful in planning an attack.

Overall, cyber attacks require a specialized mix of knowledge, and much of it is easily available on the Internet. While highly technical knowledge is required to successfully use the Internet to shut down power plants, banking systems, or other cyberterrorist targets, a host of manuals, instructions, and tools are freely available to the would-be terrorist. With the increasingly interconnected infrastructure of the United States and other advanced economies, it is plain to see why terrorists would be attracted to the opportunities of cyber attacks, and for them, the capabilities made available by the Internet must surely bring a sinister smile to their face.

Conclusion

This chapter offers a fairly bleak prognosis for the global war on terrorism. Because of the vast—and growing—amounts of information available both in print and online, through which an individual can learn the tools of terror, we will likely never see the complete eradication of terrorism. Through a process of independent study and distance learning, an individual—with limited, if any, guidance from seasoned veterans of terrorist organizations—can acquire both the ideological and operational knowledge needed to become a somewhat effective terrorist. The situation is even more grim in the world of cyberspace, where the unique tools needed to conduct cyber attacks are freely available, and there is a large, supportive community of hackers ready and willing to teach the "newbie" how to use these tools.

Books and websites can thus be seen as valuable sources of terrorist learning—at least, a certain type of independent, self-directed type of learning. However, it is virtually impossible to do anything about their existence without resorting to the type of widespread government censorship that very few in the world would want to see. This produces a difficult dilemma for the governments of most nation-states in the global war on terrorism. Most countries recognize that it is counterproductive to allow the exchange of terrorist-related learning on their soil. Thus, training camps are found in only a small number of countries. However, many countries do not yet seem to recognize that training for terrorism may already be taking place in a virtual form under their very noses. By allowing terrorist-training websites to exist on Internet servers within their jurisdiction, these countries are in essence playing host to online centers of knowledge transfer in the terrorist world. How the United States (and the civilized world) should respond to the challenges raised in this chapter, without violating the democratic principles and civil liberties so crucial to our way of life, is one of the more important challenges of the twenty-first century.

Acknowledgments

The views expressed herein are those of the author and do not purport to reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense.

A large number of teachers, Ulema and scholars took part in the workshop on Counter Terrorism being held on Monday at Baluchistan University of Information Technology. The role of educators in shaping character of students was the main theme of discussions. The prime reason of organizing this workshop was to encourage and remind teachers their role in building peace, religious tolerance, and goodwill in students by educating them. The curriculum and lectures can play a vital role in eliminating extremist approach, barbarism and narrow mindedness from minds of students and change their percepti Concise, succinct, and provocative, Communicating Terror, Second Edition explores multiple rhetorical dimensions of terrorism, connects terrorism to communication theories, and helps readers understand how this violence creates a public discourse for multiple target audiences. Author Joseph S. Tuman uses fascinating case studies and examples as he explores both dissent terrorism and state terror and looks at terrorism from a communicative perspective. Presenting terrorism as a process of communication between terrorists Developing technologies that leap ahead of the terrorists requires vision and strategy, and a good strategy requires hard choices. It begins by establishing criteria for selecting the most crucial technological investments. In my mind, there should be three: Seeking out technologies that can contribute to building a true national system that addresses all the challenges of terrorism from intelligence and early warning to domestic counterterrorism and response.Â lethal ones or with electronic, psychological, and/or information warfare, making these other anti-terrorism tools more effective and discriminate. Research by the U.S. military suggests four areas of non-lethal weapons development that show particular promise. They are