Terrorist Use of the Internet
And
Related Information Technologies

A Monograph
by

Lt Col Patrick S. Tibbetts
U.S. Air Force

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas
AY 01-02

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Lt Col Patrick S. Tibbetts

Title of Monograph: Terrorist Use of the Internet and Related Information Technologies

Approved by:

_____ Monograph Director
Mr. Timothy L. Thomas

_____ Director, School of
COL James K. Greer, MMAS Advanced Military Studies

_____ Director, Graduate Degree
Philip J. Brookes, Ph.D. Program

Abstract

Terrorist Use of the Internet and Related Information Technologies, by Lt Col Patrick S. Tibbetts, U.S. Air Force, 64 pages.

Research Question: how will U.S. national security policy be affected by terrorist exploitation of the Internet and related information technologies?

Information operations are nothing new; they have been used in military operations throughout the history of conflict. Arguably, however, the combination of breakneck speed of technological advances in information management systems and evolving threats to U.S. national security are redefining forever the nature of warfare. Some proponents have seen the great promise of information operations as the capability to mitigate, if not eliminate, the fog and friction of war by "seeing all." Consequently, current information operations doctrine seems to be focused squarely on the advantages of using leading edge technologies to obtain real-time intelligence, surveillance and reconnaissance, thus creating a "common operating picture" of a more or less traditional battlefield. However, as the recent terrorist attacks in New York and Washington illustrate, we will likely continue to face significant threats from elusive, unconventional enemies operating in the shadows of a nontraditional "battlefield." Moreover, because of the proliferation of cheap, dual-use information technology, these enemies may possess now, or acquire in the future, the technical expertise and hardware to further their own political agendas, harass and frustrate U.S. attempts to conduct information operations (perhaps even to the extent of negating U.S. information superiority altogether), or directly attack the U.S. infrastructure or population. Information technology has thus given terrorists their own ability to "see all" on their own traditional battlefield: the populations and civilian infrastructure of the nations they wish to influence or destroy.

In order to answer the research question, the monograph will examine how transnational actors use the Internet and related information technologies to further their interests, with special emphasis on unconventional warfare and the profound influence of accessible advanced technology. To this end, it will document current and future methods and technologies that terrorist organizations are either using or could potentially use in information warfare against the United States. These include exploitation of the Internet and related information technologies: 1) for surreptitious command, control and communications; 2) to gain access to information of all types; 3) as a ubiquitous source of funding; 4) as a source of offensive information operations capability, including psychological operations, cyber and physical attack of communications nodes, and cyber attacks of critical infrastructure, and 5) for publicity and propaganda. The monograph will discuss the implications of these capabilities, and suggest enhancement of U.S. and friendly intelligence capabilities (particularly information sharing and human intelligence), immigration reform, and leveraging Western information technology superiority as priorities in the war against terrorism.

Table of Contents

Chapter One: Introduction

The events of September 11, 2001, marked a significant turning point in the history of the United States. The attacks on the World Trade Center and the Pentagon -- carried out by operatives of the Al Qaeda organization, who entered the country legally -- demonstrated once and for all that the United States is not invulnerable to attack on its own soil. The fact that the attacks were conducted by terrorists, using ingenious, asymmetric means against the most technologically and militarily sophisticated society in the world -- the world's last remaining superpower -- has generated increased study of terrorist organizations, their objectives and methods, as well as vigorous attempts to determine what factors led to their success.

The various failures of U.S. national security policy that contributed to this tragedy may have been few or numerous; they are not yet fully understood, and will undoubtedly take considerable time to identify, analyze and correct. Moreover, this effort will not be made any easier by the knowledge that the precise method of attack had already been predicted long before the event itself.[1] Nonetheless, it is apparent that the United States is at war, and definitely not with a traditional opponent. Instead of a set piece, military versus military confrontation, America finds itself challenged by a shadowy, non-state, networked and adaptive opponent who can remain invisible until the time comes to accomplish his mission.

This new type of opponent, while lacking the sophisticated military hardware the United States possesses, still has at his disposal significant capabilities with which to attack or facilitate attacks on American interests worldwide. Some of these capabilities involve using the Internet and related information technologies to facilitate achievement of their objectives. Although not necessarily an exhaustive list, the Internet provides terrorist groups with the following opportunities and capabilities:

---

[1] See, for example, Stephen Sloan, "Terrorism and Asymmetry," *Challenging the United States*

1) surreptitious command, control and communications capabilities;
2) enhanced access to information of all types;
3) a ubiquitous source of funding, money laundering, and electronic transfers;
4) a means to conduct asymmetric, offensive information operations, and
5) global publicity and recruiting.

This monograph examines all of these capabilities and opportunities, which in combination afford terrorist organizations with ample means to achieve competence in, if not mastery of, what Alberts, Gartska and Stein have called "network-centric warfare." This mode of warfare

> focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders' intent.[2]

Although the implications of these developments are not altogether clear, at least with respect to national security policy, it is nonetheless evident that the U.S. will need to adjust to the new threat. Because information technology gives terrorist organizations global power and reach without necessarily compromising their invisibility, the U.S. must enhance its own capabilities to reveal and effectively target terrorist cells and operatives wherever they hide, as well as prevent those outside of the country from entering. To this end, an effective U.S. response will require, at the very least:

> 1) a more networked approach to defense, involving interagency and international cooperation of unprecedented scope, particularly in the field of intelligence and information sharing;
>
> 2) extensive immigration reform to identify and eliminate the vulnerable seams in U.S. borders, and
>
> 3) a definite commitment to fully leverage American technological superiority, especially in Internet and related information technologies.

Symmetrically and Asymmetrically: Can America Be Defeated? (Carlisle Barracks, Pennsylvania: U.S. Army War College, July 1998), p. 180.

[2] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare:Developing and Leveraging Information Superiority* (Washington, D.C.: DoD C4ISR Cooperative Research Program, 1999), p.

Chapter Two: Surreptitious Command, Control and Communications

Current military literature makes much of U.S. technological superiority, particularly the Western lead in computer technology and its inherent advantages in command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR). Distinguished thinkers such as former U.S. Air Force Chief of Staff Ronald R. Fogleman see these technological advances as creating a revolution in military affairs: one that will provide near-perfect battlefield information to commanders at all echelons, enhancing military capability to find and destroy valuable enemy targets at stand off distances.[3] Like most technological advances throughout history, however, C4ISR technologies have proliferated: they are no longer a Western monopoly. Because they are so widely available, and because developed information societies are so dependent upon them, the strengths of Internet and computer technologies in general -- including automated information processing, global communications interconnectivity, and other capabilities -- are arguably even more useful to transnational and non-state actors than they are to industrialized nation-states. Although the United States is currently in a position of technological advantage, this proliferation of cheap, dual-use software allows entities with otherwise modest means to conduct command and control globally, in real time, and with considerable security. Using this technology, terrorist organizations can and do achieve secure, real-time command and control by exploiting the utility of Internet-based applications themselves, by using encryption to prevent unauthorized disclosure of information in stored and transmitted electronic files, and by using information hiding methods to conceal the relevant content of certain types of files.

[3] Ronald R. Fogleman, "Information Operations: The Fifth Dimension of Warfare," 1995 [online]; available from <http://www.defenselink.mil/speeches/1995/s19950425-fogleman.html> (accessed 24 September 2001).

The Internet as a Terrorist Command and Control Tool

The first method exploits the various built-in tools that make the Internet useful in the first place. For example, members of terrorist groups, with the use of fraudulent or non-existent credit card numbers, can open an unlimited number of Internet accounts with national Internet service providers such as America Online (AOL). Even without an AOL account, terrorists can create an AOL Instant Messenger (AIM) account on a short-term or ad hoc basis with a phony e-mail address.[4] Offenders can use these tools for real-time communication to coordinate their activities with little chance of interception: until it is too late to stop them. Then, once the current operation is complete, they can discard these bogus AIM accounts merely by uninstalling the software and formatting the computer's hard drive to erase all evidence that it was ever there. Usually, the service providers eventually cancel these accounts once they are ascertained to be fraudulent; however, in order to be a threat they only need to be active long enough to suit a short-term purpose.

Terrorist organizations also use existing Internet chat rooms and e-mail to plan and coordinate operations.[5] Many chat rooms are available for anonymous login, and can be accessed from cyber cafes, libraries or other Internet connections not traceable to a suspected terrorist group or member. Free e-mail hosting is also popular and available from a variety of sources. Not only do terrorist organizations use existing Internet services, they have constructed dedicated communications networks that utilize e-mail, the Internet and electronic bulletin boards (EBBs) to conduct seamless information processing and communications, both internal and external.[6] When used in conjunction with any of a number of features available on the Internet --

---

[4] The relative ease and unobtrusiveness of the AIM registration process is apparent at the AIM Home Page. See _____, "AOL Instant Messenger Home Page," *America Online Incorporated*, no date [online]; available from <http://www.aim.com/> (accessed 4 December 2001).
[5] Dorothy E. Denning, "Cyberterrorism," 24 August 2000 [online]; available from <http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc> (accessed 7 January 2002).
[6] Ibid.

anonymous mailers such as Send Fake Mail,[7] or re-mailer utilities such as Jack B. Nymble[8] -- e-mail can be a powerful, responsive short-term tool to accomplish command and control tasks in a relatively secure manner.

Terrorist Information Security

Encryption and information hiding technologies currently available allow almost anyone with an Internet connection to achieve high levels of security for selected files, communications or even whole systems. Numerous means exist by which terrorist organizations can effectively scramble and conceal messages or files. These methods include use of easily obtainable, dual-use technology, including digital steganography and other information-masking techniques. Dating back at least to ancient Greece, steganography is not a new science. Digital steganography, however, is relatively new. Its purpose is to hide digital information, sometimes within completely unrelated types of files. It is related to digital watermarking, which inserts information (usually copyright data) into digital material in an effort to protect Internet graphics and other files that are susceptible to copyright infringement. However, this technology can also support terrorist groups in that its main purpose is to conceal "a message where that hidden message is the object of the communication; for example, sending a satellite photograph hidden in another image."[9] Although these digital signatures are not easily detected without appropriate software and technical expertise, they are in widespread use. The important point is the same procedure may also be used to insert hidden messages into virtually any digital file extant on the Internet.

---

[7] _____, "Send Fake Mail," *Sendfake-mail.com*, no date [online]; available from <http://www.sendfake-mail.com/> (accessed 17 November 2001).
[8] _____, "Jack B. Nymble v2," *Potato Software*, no date [online]; available from <http://www.bigfoot.com/~potatoware/jbn2/> (accessed 17 November 2001).
[9] Neil F. Johnson and Shushil Jajodia, "Steganalysis of Images Created Using Current Staganographic Software," 1998 [online]; available from <http://www.isse.gmu.edu/~njohnson/ihws98/jjgmu.html> (accessed 12 November 2001). Originally published in *Lecture Notes in Computer Science, Vol. 1525*, (Springer-Verlag, 1998), pp. 273-289.

Terrorists also have access to what is generally termed "strong" encryption capability. Originally developed in the United States, this type of encryption is used legally for a number of purposes; chiefly, to support secure socket layer Internet communications, thus providing significant protection from fraud for those merchants and consumers engaged in electronic commerce. Since this form of encryption utilizes so many variables in its key, it is virtually unbreakable; the computing power required to decrypt a message protected with 1024-bit encryption within a reasonable period of time, for example, would require thousands of times the current number of computers in existence today.[10] Although this technology is a boon to those legitimate activities requiring secure communications over the Internet, its ready availability makes it a powerful security tool for terrorist command, control and communications.[11] Terrorists can also use the same encryption technology to conceal real-time Internet voice communications. Pretty Good Privacy (PGP) author Phil Zimmermann has published a secure Internet telephony program called PGPfone, which uses strong encryption protocols based on PGP as well as speech compression technology to allow any user to convert his or her computer into a virtual STU-III device.[12]

An interesting analog of encryption software hides messages within the text of ordinary e-mail. *Spammimic*, offered by Spammimic.com, is one example. Unlike tools that perform true file encryption, *Spammimic* hides the text of a short message into what appears to be run-of-the-mill "spam:" a pejorative reference to unsolicited, bulk commercial e-mail.[13] Spammimic.com explains the advantages of this method as follows:

> There is [sic] tons of spam flying around the Internet. Most people can't delete it fast enough. It's virtually invisible. This site gives you access to a program that will encrypt

---

[10] Hal Abelson et al., "Questions and Answers about MIT's Release of PGP 2.6," 2 June 1994 [online]; available from <http://web.mit.edu/afs/net/mit/jis/www/pgpfaq.html> (accessed 14 November 2001).
[11] One encryption program in widespread use, Pretty Good Privacy (PGP), is available from a number of sites online; see _____, "The International PGP Home Page," no date [online]; available from <http://www.pgpi.org/>.
[12] Jeffrey L. Schiller, "PGPfone Home Page," 10 June 1997 [online]; available from <http://web.mit.edu/network/pgpfone/> (accessed 10 November 2001).
[13] Its non-digital equivalent is Class A Bulk mail, also known as "junk mail" in the United States.

> a short message into spam. Basically, the sentences it outputs vary depending on the message you are encoding. Real spam is so stupidly written it's sometimes hard to tell the machine written spam from the genuine article.[14]

Spammimic thus appears to be the digital equivalent of a null cipher; that is, an unencrypted message concealed within innocuous-appearing text. It is relatively easy to "crack" a null cipher, but *Spammimic's* significance lies not in the simplicity of its code. Potentially, anyone with an Internet connection and rudimentary, "cut-and-paste" computer skills can use this tool to hide secret messages amongst the millions of "spam" e-mails sent daily throughout the world. As e-mail volume increases over time, the challenge of detecting potential terrorist communications using this method becomes daunting indeed. One research firm estimates that unsolicited commercial e-mail volume in the United States alone will reach 200 billion per year by 2004.[15] Moreover, as Spammimic's creators point out, "there are terrific tools…for encrypting your mail. If somebody along the way looks at the mail they can't understand it. But they do know you are sending encrypted mail to your pal."[16] Using *Spammimic* allows users to avoid the telltale hallmarks of data encryption in e-mails containing sensitive information, thus lowering the possibility they will attract the unwanted attention or suspicion of law enforcement and intelligence agencies.

A side benefit of digital cryptography is its potential as a tool for extortion and blackmail. Since cryptographic technology is available free to anyone with an Internet connection, it is entirely possible to fashion computer viruses which encrypt selected files on a targeted hard drive, rendering them useless to anyone without the key. Depending on the sensitivity or value of the encrypted files, this type of scheme could generate significant resources for the perpetrator in terms of hard cash, or in-kind transfers of goods and services vital to a terrorist organization's

---

[14] _____, "Explanation," *Spammimic.com*, no date [online]; available from <http://www.spammimic.com/explain.shtml> (accessed 1 January 2002).
[15] _____, "E-mail Landscape," *Iconocast Inc.*, no date [online]; available from <http://www.iconocast.com/dotcom/marketing/e-mail.html> (accessed 7 Jan 2002).
[16] _____, "Explanation," *Spammimic.com*, no date [online]; available from <http://www.spammimic.com/explain.shtml> (accessed 1 January 2002).

operations.[17] (This monograph addresses additional terrorist uses of computer and Internet technology as a means to finance operating expenses in Chapter Four, "Ubiquitous Source of Funding.")

The implications of these capabilities are enormous. With this technology, terrorists can now exercise discreet -- even secure -- command and control of paramilitary forces at global distances. Since their command and control apparatus is no longer constrained by the limits of geography, line-of-sight communications, or the speed of the fastest available courier, they can now project lethal force across continents, with more precision and better coordination, and hence better chance of spectacular success. In addition, cheap, readily available encryption technology compounds the already significant difficulties in monitoring even "in the clear" digital Internet communications. One factor is its sheer size and scope; the Internet is becoming more pervasive on a daily basis, and crosses international borders. It also encompasses a wide variety of communication capabilities, such as e-mail, instant messaging, chat rooms, electronic bulletin boards, and real-time streaming video. Finally, just as they must with every other communications medium, governments of free societies must make convincing arguments to address the privacy concerns of Internet users in order to implement effective countermeasures. For these reasons, the Internet is not as susceptible to traditional law enforcement methods of intercepting communications, such as wiretapping or other forms of surveillance.[18]

---

[17] Michael Wilson, "Terrorism in a New World," *Emergency Response and Research Institute*, 1994 [online]; available from <http://www.emergency.com/evo-revo.htm> (accessed 7 Jan 2002).
[18] Serena Chan and L. Jean Camp, "Towards Coherent Regulation of Law Enforcement Surveillance in the Network Society," 2001 [online]; available from <http://itc.mit.edu/rpcp/member/seminar/chan_031501.pdf> (accessed 16 December 2001).

Chapter Three: Enhanced Access to Information

Information technology is revolutionizing research of all kinds -- academic, corporate, professional and nefarious. The sheer volume of information available to anyone with an Internet connection is staggering: a University of California at Berkeley study found the total content of all Web-accessible information in the year 2000 included over 7,500 terabytes of data comprising over 550 billion documents. The same study revealed that the "surface" Web alone was growing at a rate of *7.3 million pages per day* in 2000.[19] With any of the dozens of Internet search engines and directories available, it is easier than ever for researchers to pinpoint specific information quickly. This has also affected intelligence collection, since ready access to open-source information has increased commensurately; as Steele points out, "the vast majority of usable, relevant information necessary to support policymakers, acquisition managers, and commanders is available in unclassified form from private sector sources," including the Internet.[20] The increased availability of information has been a boon not just to legitimate researchers, or even to friendly intelligence specialists: it is also available to those whose agendas are less noble. Terrorists can and do use the power of the Internet to obtain a wealth of data on potential targets, as well as technical know-how on the construction and employment of a variety of conventional and unconventional weapons.

Targeting Tools

One source of targeting data that terrorists can exploit is commercial satellite imagery. There are numerous sources of geospatial data available on the Web. Many are of limited utility or are restricted access sites, but there are also several sources of commercially available satellite

---

[19] Peter Lyman and Hal R. Varian, "How Much Information," 2000 [online]; available from <http://www.sims.berkeley.edu/research/projects/how-much-info/internet.html> (accessed 22 September 2001).

[20] Robert D. Steele, "Information Peacekeeping: The Purest Form of War," in *Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?* (Carlisle Barracks, Pennsylvania: U.S. Army War College Strategic Studies Institute, July 1998), pp. 157-158.

imagery with sufficient resolution to serve as targeting or planning tools. Space Imaging, Incorporated is probably the best-known provider of high-resolution commercial satellite photography. Their IKONOS satellite was the first commercial satellite to deliver one-meter resolution black-and-white, and four-meter resolution color images.[21] However, DigitalGlobe is poised to take the lead in this arena in 2002 with its QuickBird satellite, which will deliver seventy-centimeter resolution black-and-white, and 280-centimeter resolution color images.[22]

In addition to these two companies, there are at least five others, some of which are actually resellers of archived imagery, that offer some type of space imagery on the Internet, either free or for very low prices.[23] For example, as late as January 2002 -- long after the September 11 attacks -- the author was able to download one-meter resolution images of the Pentagon, the Washington Monument, and the U.S. Capitol from the TerraServer Web site.[24]

Precise intelligence on high-visibility targets is only one advantage of this technology. High-resolution satellite imagery can also give terrorists an unacceptable level of insight into our own antiterrorism and counterterrorism efforts. Recognizing the threat to military operations posed by commercially available intelligence sources focused on Afghanistan since September 11, the National Imagery and Mapping Agency (NIMA) has already purchased all rights to Afghanistan

---

[21] _____, "Geo 1m and 4m Frequently Asked Questions," *Space Imaging Incorporated*, no date [online]; available from <http://www.spaceimaging.com/carterra/geo/prodinfo/geo_faq.htm> (accessed 17 December 2001).

[22] _____, "DigitalGlobe Overview," *DigitalGlobe*, no date [online]; available from <http://www.digitalglobe.com/?goto=about> (accessed 21 December 2001).

[23] See _____, "ImageNet," *Core Software Technology*, no date [online]; available from <http://www.imagenet.com/info.html>; _____, "High-Resolution Satellite Imagery," *PlanGraphics, Incorporated*, 2000 [online]; available from <http://www.plangraphics.com/satellite.htm>; _____, "The GEMI Store Online," *GEMI Corporation*, 2000 [online]; available from <http://www.eomonline.com/CommonGEMI/Aboutus/about.htm>; _____, "Satellite Photos, Aerial Photography, and Images," *TerraServer.Com*, no date [online]; available from <http://www.terraserver.com/>, and ____, "SPOT Image Corporation Home Page," *SPOT Image Corporation*, no date [online]; available from <http://www.spot.com/> (all URLs accessed 22 December 2001).

[24] Imagery of the Pentagon, the Washington Monument and the U.S. Capitol was still available online on 15 January 2002 at the following URLs, respectively: http://terraserver.homeadvisor.msn.com/image.asp?S=10&T=1&X=1608&Y=21522&Z=18&W=0; http://terraserver.homeadvisor.msn.com/image.asp?S=10&T=1&X=1617&Y=21532&Z=18&W=0, and http://terraserver.homeadvisor.msn.com/image.asp?S=10&T=1&X=1628&Y=21532&Z=18&W=0.

imagery from Space Imaging's IKONOS satellite, and has expressed interest in obtaining material from DigitalGlobe's QuickBird as well. NIMA's agreement with Space Imaging guarantees rights to this imagery in perpetuity; essentially, this means that third parties, including the media, cannot legally gain access to these materials without explicit U.S. government permission.[25]

Detailed information on U.S. infrastructure available on the Internet is not limited to high-resolution space imagery, however. Terrorists can also obtain maps, diagrams and other information on a variety of public utilities, national historic landmarks, population-dense facilities such as shopping centers and malls, transportation hubs, and other potential targets. One particularly alarming example is the wealth of information on U.S. nuclear reactors, including specific information on containment facilities, available to anyone with an Internet connection. Prior to the events of September 11, 2001, some of this information was actually available on government Web sites. For example, broken links to reactor locations and maps, as well as statistics, diagrams and other plant-specific data, still exist online at the Nuclear Regulatory Commission web site.[26] Links to similar information at the Yucca Mountain nuclear waste repository Web site result in a security notice specifying the removal of certain types of technical information, including maps.[27]

Notwithstanding the events of September 11, however, descriptions and maps of transportation routes for high-level nuclear waste in Nevada are still available online. Potential terrorist actors can easily access information about the routes themselves, as well as shipping

---

[25] Michael R. Gordon, "Pentagon Corners Output of Special Afghan Images," *The New York Times*, 18 October 2001 [online]; available from <http://206.181.245.163/ebird/e20011019pentagon.htm> (accessed 4 November 2001).

[26] See United States Nuclear Regulatory Commission , "NRC - What's New," no date [online]; available from <http://www.nrc.gov/site-help/new-content.html>, and " NRC: Schedule for Rebuilding NRC's Web Site," no date [online]; available from <http://www.nrc.gov/site-help/new-content/rebuild-schedule.html> (both URLs accessed 17 January 2002).

[27] See U.S. Department of Energy, Office of Civilian Radioactive Waste Management, "Maps," no date [online]; available from <http://www.ymp.gov/reference/maps/index.htm> (accessed 28 December 2001).

origins and destinations.[28] Also, although the U.S. government has removed much of the more sensitive information from its Web sites, alternative sources of similar content still exist. The Animated Software Company's Web site has off-topic documents containing locations, status, security procedures and other technical information concerning dozens of U.S. reactors.[29] The Virtual Nuclear Tourist site contains similar information; this site is particularly detailed on specific security measures that may be implemented at various nuclear reactor locations worldwide.[30]

Technical Information on Weapons Construction

Although the Internet is thus a source of intelligence for terrorist groups, planning or targeting information derived from the Internet is practically useless to an enemy that lacks the means to strike targets. This fact may help to explain why information about United States critical infrastructure has always been more or less transparent on the Web; in recent history, the only entities capable of striking vital targets on U.S. soil have been nation-states, which are themselves easier to target than shadowy terrorist organizations, and which in any event would risk full-scale retaliation for any act of aggression within the U.S. itself. The explosion of the Internet, however, has also made technical knowledge -- including the science of weapons of mass destruction -- readily available. Of particular concern in this regard is the proliferation of "how to" web pages devoted to explaining the technical intricacies of homemade bombs, which can in many cases be constructed using lethal combinations of otherwise innocuous materials. Much of this information has been available in print media since at least the late 1960s, with the

---

[28] State of Nevada, "Nuclear Waste Transportation Routes - U.S.," no date [online]; available from <http://www.state.nv.us/nucwaste/states/us.htm> (accessed 14 December 2001).

[29] _____, "List of Nuclear Power Plants in America," *The Animated Software Company*, no date [online]; available from <http://www.animatedsoftware.com/environm/no_nukes/nukelist1.htm> (accessed 11 December 2001).

[30] Joseph Gonyeau, "Joseph Gonyeau's Virtual Nuclear Tourist: Nuclear Plants Around the World," no date [online]; available from <http://www.nucleartourist.com/> (accessed 12 December 2001). Plant security data was available on this site at <http://www.nucleartourist.com/areas/security.htm> (accessed 12 December 2001).

publication of William Powell's *The Anarchist Cookbook* and other, similar titles. Today, there are numerous Internet documents with such information. As early as April 1997, the Department of Justice had concluded that the availability of this information played a significant role in facilitating terrorist and other criminal acts:

> It is readily apparent from our cursory examination that anyone interested in manufacturing a bomb, dangerous weapon or weapon of mass destruction can easily obtain detailed instructions for fabricating and using such a device. Available sources include not only publications from the so called underground press but also manuals written for legitimate purposes, such as military, agricultural, industrial and engineering purposes. Such information is *also readily available to anyone with access to a home computer equipped with a modem* [italics mine].[31]

The author's own Web research revealed that, despite Congressional efforts to put the lid on sensitive information of this kind, even a cursory search of the Web revealed dozens of documents containing bomb making techniques and procedures.[32] Moreover, information on crude weapons construction is not limited to garden-variety pipe bombs, Molotov cocktails, or other, similar devices. A single search of the Web with the Google search engine, using search terms "how to build a nuclear weapon" revealed a minimum of five sites with detailed information on the construction of a crude nuclear device.[33] Although the challenge of building a true fissile device while maintaining secrecy is daunting, the challenge of building a so-called

---

[31] U.S. Department of Justice, "Report On The Availability of Bombmaking Information, the Extent to Which Its Dissemination Is Controlled by Federal Law, and the Extent to Which Such Dissemination May Be Subject to Regulation Consistent With the First Amendment to the United States Constitution," April 1997 [online]; available from <http://cryptome.org/abi.htm> (accessed 20 November 2001).

[32] See _____, "Anarchist Cookbook, Terrorist Handbook," no date [online]; available from <http://come.to/anarchy> (accessed 21 November 2001), which contains online versions of *The Anarchist Cookbook* and *The Terrorist Handbook*. For pipe bomb making instructions, see _____, "Contact Pipe Bomb," 2001 [online]; available from <http://www.totse.com/en/bad_ideas/ka_fucking_boom/162267.html> and _____, "Manual of the Anarchist, Vol I," 4 January 1985 [online]; available from <http://www.etext.org/CuD/Misc/anarch>.

[33] See _____, "How to Build a Thermonuclear Bomb," *About, Incorporated*, no date [online]; available from <http://physics.about.com/c/ht/00/07/How_Build_Thermonuclear_Bomb0964152140.htm>; _____, "Let's Build a Nuke," no date [online]; available from <http://home.clara.net/nybbles/oldestuff/vik/nuke/index2.html>; _____, "Atomic Bomb Design," no date [online]; available from <http://www.accutek.com/%7Emoistner/nuclear1.htm>; Carey Sublette, "Introduction to Nuclear Weapon Physics and Design," 20 February 1999 [online]; available from <http://nuketesting.enviroweb.org/hew/Nwfaq/Nfaq2.html>, and Carey Sublette, "Engineering and Design of Nuclear Weapons," 20 February 1999 [online]; available from <http://nuketesting.enviroweb.org/hew/Nwfaq/Nfaq4.html> (all URLs accessed 3 December 2001).

"dirty bomb" is not as difficult. In what is perhaps the most chilling current scenario, terrorists could easily obtain techniques, even from legitimate web sites, for building radiological weapons.[34] Such weapons may be less physically destructive than true fissile weapons, but they could kill or injure thousands if detonated in a population-dense environment. More importantly, their capacity for spreading fear -- what is arguably the ultimate terrorist objective -- could be even more potent than the attacks on the World Trade Center and the Pentagon.

The feasibility of these threats should not be underestimated. Recently captured materials indicate that the terrorist organization Al Qaeda not only compiled information on "home-grown explosives," but also was actively pursuing data and technical expertise necessary to pursue nuclear, chemical and biological weapons programs.[35] Moreover, according to Ken Katzman, a terrorism analyst for the Congressional Research Service, much of the material in these captured documents was probably downloaded from the Internet.[36] Therefore, it is also important to note that removal of technical information from the public domain is no guarantee of safeguarding it; in essence, this effort is akin to "closing the barn door after the cow has escaped." Terrorist intelligence and technical data obtained prior to September 11 can be archived, stored and distributed surreptitiously irrespective of government or private attempts to squelch its presence on the Internet. Indeed, these materials can be loaded onto offshore or other international Web servers that cannot be affected by regulatory practices, rendering useless any attempt to halt their spread outside the reach of American law enforcement.

---

[34] _____, " News Reports Confirm PSI TECH's Radiological 'Dirty Bomb' Scenario as Possible Terrorist Weapon," *PSI TECH International, Incorporated*, 4 December 2001 [online]; available from <http://www.remoteviewing.com/news/120401.html> (accessed 19 December 2001).

[35] Mike Boettcher and Ingrid Arnesen, "Al Qaeda Documents Outline Serious Weapons Program," *CNN*, 25 January 2002 [online]; available from <http://www.cnn.com/2002/US/01/24/inv.al.qaeda.documents/> (accessed 28 January 2002).

[36] David Ruppe, "Terror Manual," *ABC News*, 18 September 2001 [online]; available from <http://abcnews.go.com/sections/world/DailyNews/binladenterror_000918.html> (accessed 5 October 2001).

Chapter Four: Ubiquitous Source Of Funding

A terrorist organization, like any other entity, requires resources to conduct operations; obviously, the greater the pool of resources from which it can draw, the greater its capability to act. As President George W. Bush remarked shortly after the second attack on the World Trade Center, "money is the life-blood of terrorist operations."[37] Information technology and the Internet are providing terrorist organizations with new, lucrative sources of funding in their ongoing efforts to finance larger, more destructive, and more politically significant operations. This, combined with various techniques available on the Internet to launder funds derived from a variety of sources, is therefore cause for some measure of genuine concern. The ability to instantaneously and globally transfer funds is one of the features that make information technologies so useful and responsive to business and consumer demands; indeed, it is one of the strengths of an information-based economy. Ironically, the various methods of funds transfer available today also provide terrorist organizations with the same connectivity advantages that individuals, businesses and government agencies enjoy. The use of these sources of funding by paramilitary and extremist groups on the Internet, including terrorist organizations, runs the gamut from conspicuous marketing campaigns to clandestine money laundering efforts.

Direct Solicitation of Funds

Some of these groups, for example, have an unabashed presence on the Internet; they openly declare their purposes and policies, and solicit funds for their operating expenses from like-minded individuals and groups, all in plain sight. For example, the African People's Socialist Party (a.k.a. International People's Democratic Uhuru Movement) has a web site at http://www.npdum.com, which contains a printable page individuals can use to pledge monthly

[37] _____, "Bush Calls Halt to Terror Funding," *BBC News*, 24 September 2001 [online]; available from <http://news.bbc.co.uk/hi/english/world/americas/newsid_1560000/1560942.stm> (accessed 3 October

donations in a manner similar to Combined Federal Campaign contributions.[38] The Lebanese Forces Party's web site, at http://www.lebanese-forces.org, has an online store where contributors can purchase books, CDs, clothing, flags and other paraphernalia.[39] The Liberation Tigers of Tamil Eelam, commonly referred to as Tamil Tigers, also have an online store at http://www.eelamweb.com, although donors are instructed to send a certified check or money order to an address in Canada, payable to the World Tamil Movement.[40] The World Church of the Creator, a white supremacist group based in Illinois, also has a Web site at http://www.wcotc.com/index.shtml, which includes a PayPal link for donations. The site also has an online store where donors can purchase literature, clothing, membership materials, audio and video merchandise, and even portraits of the group's founder.[41]

The proliferation and ease of use of e-mail also provides terrorist groups the option to use commercial "spam" to generate income. As more individuals get connected to the Internet, the potential pool of online donors grows commensurately. For example, the total number of Internet users worldwide grew to almost 309 million in January 2002, with U.S. users accounting for nearly fifty eight percent of that number.[42] Of all Internet activity, e-mail is the most widely used Internet resource among U.S. citizens; one research firm estimates that forty five percent of Americans use e-mail regularly.[43] Also, Internet use is growing in the U.S. by about two million

---

2001).

[38] _____, "NPDUM Sustainer Drive," *International People's Democratic Uhuru Movement*, no date [online]; available from <http://www.npdum.com/sd_pledge_form.htm> (accessed 11 October 2001).

[39] _____, "LF Store," *Lebanese Forces Party*, no date [online]; available from <http://www.lebanese-forces.org/store/lfshop.htm> (accessed 13 October 2001). Note: this online store uses the PayPal electronic funds network for funds transfers.

[40] _____, "Eelamweb Online Store," *EelamWeb*, no date [online]; available from <http://www.eelamweb.com/shop/> (accessed 16 October 2001).

[41] _____, "World Church of the Creator Educational Items," *World Church of the Creator*, no date [online]; available from <http://www.wcotc.com/items> (accessed 25 January 2002).

[42] _____, "Traffic Patterns: Top Online Properties of January 2002," *INT Media Group, Incorporated*, January 2002 [online]; available from <http://cyberatlas.internet.com/big_picture/traffic_patterns/article/0,,5931_971121,00.html> (accessed 10 February 2002).

[43] _____, "Geographics: U.S. Internet Population Continues to Grow," *INT Media Group, Incorporated*, 6 February 2002 [online]; available from <http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_969541,00.html> (accessed 10

new users per month.[44] As Internet user demographics become clearer and better defined, terrorist groups -- either themselves, or through proxies with plausible deniability -- will be able to target those users who have demonstrated sympathy or sensitivity to certain particular causes or social issues, and solicit private donations from individuals fitting the right "profile" whenever they desire. It is reasonable to conclude, therefore, that they will account for at least a portion of worldwide commercial e-mail volume. When coupled with effective misinformation or disinformation about the true purposes, goals, and activities of a particular group, commercial e-mail solicitations have the potential to contribute significantly to a terrorist organization's publicity objectives, as well as their finances.

Use of Private Organizations as Fronts

While some groups conduct their Internet activities openly, other organizations are known or suspected of using charities, legitimate or illegitimate, as fronts for their financing. An overall decrease in visible state-sponsored terrorism has resulted in a greater proportion of terrorist support coming from the general public. In fact, "public support for terrorist groups has become the most essential element in fund-raising and the main source of finances,"[45] despite the fact that the general public is not always aware of the ultimate recipients of their money The well-publicized investigation of the Holy Land Foundation for Relief and Development (HLFRD), and the subsequent seizure of its assets, was only one of numerous actions taken by the Bush administration in the wake of the World Trade Center attack to disrupt alleged financing schemes of this sort. One alarming revelation, according to a Federal Bureau of Investigation memorandum, was the use of charitable donations to fund annuities for the families of Hamas suicide bombers in Israel and Palestine. Allegedly, HLFRD's support provides "a constant flow of suicide volunteers and buttresses a terrorist infrastructure heavily reliant on moral support of

---

February 2002).
[44] Ibid.
[45] Yael Shahar, "Tracing bin Laden's Money: Easier Said Than Done," 21 September 2001 [online];

the Palestinian populace."[46] At one time the HLFRD had a Web site, but as of this writing it is no longer available[47].

Benevolence International Foundation[48] and Global Relief Foundation[49], whose assets were also frozen in December 2001, continue to operate online and have pages providing numerous tools for potential donors, including online donation by credit card, wire transfer, online checking, and other methods. The International Islamic Relief Organization, allegedly founded by Usama bin Laden's brother-in-law, has a continuing presence on the Internet[50]. Ostensibly, this organization was created to "alleviate the suffering of human beings worldwide," and conducts "humanitarian activities in more than 120 countries in different parts of the world."[51] Its web site provides a mailing address in Saudi Arabia, as well as an e-mail address and voice, FAX and TELEX numbers, but the site itself does not specifically solicit private donations.

Abuse of Unregulated Modes of Funds Transfer

As pervasive as open and direct forms of online solicitation are, even when using a legitimate-appearing front, some terrorist groups may choose to maintain a more clandestine presence on the Internet. Since the e-commerce industry in general is as yet largely unregulated, there are several Internet avenues that are susceptible to terrorist manipulation for funds transfer, money laundering, and illicit exchange schemes. Online auction providers such as eBay or

---

available from <http://www.ict.org.il/articles/articledet.cfm?articleid=387> (accessed 27 October 2001).
[46] Lisa Getter, "FBI Tied Islamic Charity to Calls to Kill Israelis," *The Los Angeles Times*, 6 December 2001 [online]; available from <http://www.latimes.com/news/nationworld/world/la-120601holy.story> (accessed 11 December 2001).
[47] _____, "Holy Land Foundation for Relief and Development Home Page," *Holy Land Foundation for Relief and Development*, no date [online]; previously available from <http://www.hlf.org> (accessed 6 December 2001). Subsequent attempts to access the site after HLFRD assets were frozen were repeatedly unsuccessful.
[48] _____, "Donate through BIF," *Benevolence International Foundation*, no date[online]; available from <http://www.benevolence.org/donate.htm> (accessed 28 January 2002).
[49] _____, "Help Now," *Global Relief Foundation*, no date [online]; available from <http://www.grf.org/helpnow.html> (accessed 28 January 2002).
[50] Vincent Cannistraro, "Testimony before the House Committee on International Relations," 3 October 2001 [online]; available from <http://www.house.gov/international_relations/cann1003.htm> (accessed 28 November 2001).
[51] _____, "Welcome," *International Islamic Relief Organization*, 1996 [online]; available from

Yahoo! Auctions, for example, may unwittingly provide the means for terrorist and other criminal organizations to transfer funds while attracting little or no unwanted attention to their activities. The author's research into eBay auctions, for example, revealed numerous instances of attempted sales of online video game accounts, or the copyrighted material therein. Frequently, attempted sales were disguised as a different offer entirely using ingenious legal or semantic devices. One such auction offered a set of second-hand video game software for $200.00, which was available brand-new from the publisher for $39.99.[52] Although this particular transaction by itself is not illegal, closer inspection of the terms of the offer revealed that the seller was in fact attempting to sell the game characters that he had created and advanced during his time playing the game, in violation of copyright law and the end user license agreement accompanying the software.[53]

While copyright infringement is hardly as serious a transgression as terrorist financing, this example illustrates how disreputable individuals and groups can exploit a pervasive, unregulated Internet economy. Terrorist operatives can open an account with an online auction provider, offer any item at all -- a motor vehicle, a coin collection, or even a cookie recipe, to cite a ridiculous example -- and "sell" it to a trusted agent who knows where to look for this particular item. Whether actual goods or services are delivered after the electronic exchange takes place is immaterial; the important point is that the funds are transferred. The advantage, then, of using an unregulated online auction provider is that nobody need know exactly what goods or services changed hands, or if in fact anything other than cash changed hands at all. Lost in the huge volume of daily, anonymous transactions, moderately sized parcels of cash can thus easily be transferred and effectively laundered by anyone with an Internet connection.

<http://www.arab.net/iiro/> (accessed 15 January 2002).

[52] _____, "eBay item 1327313247," *eBay Incorporated*, [online]; available from <http://cgi.ebay.com/aw-cgi/eBayISAPI.dll?ViewItem&item=1327313247> (accessed 28 January 2002). Auction items on the eBay Web site are frequently added and removed, so the durability of this link is questionable.

[53] _____, "Terms of Service," *Sony Online Entertainment Incorporated*, 2002 [online]; available from <http://www2.station.sony.com/en/termsofservice.jsp> (accessed 28 January 2002).

International electronic payments between legitimate businesses have been available for a number of years through a variety of official and unofficial organizations, such as the Society for Worldwide Interbank Financial Telecommunication.[54] With the increasing popularity of the Internet and development of financial services networks outside of the conventional banking industry, it has become easier than ever for individuals, charities and small businesses to collect and disburse funds electronically. Acting as fronts for terrorist organizations, any of these entities can easily exploit such networks to push resources when and where they are needed to finance terrorist operations. Depending on local and national laws, such transactions can prove to be virtually untraceable. For example, numerous countries permit the existence of anonymous corporations and shell banks that are completely unregulated and in some cases immune to foreign prosecution.[55] Even in a country like America, with fairly robust banking laws, online financial services provide opportunities for funds transfer and money laundering. One company known as PayPal, for example, has a network of over twelve million registered users who use the system to make payments on online auction and other e-commerce sites, as well as for professional services rendered.[56] Again, since this industry is as yet unregulated, the potential for exploitation by criminal entities is very real.

Shortly after the World Trade Center attacks, the Organisation For Economic Co-Operation And Development's Financial Action Task Force recognized serious deficiencies in anti-money laundering procedures within the international banking system and adopted eight recommendations designed to thwart terrorist fund raising and distribution. Although the recommendations are non-binding, they illustrate that the international community is only beginning to perceive the relative ease with which criminal entities are able to conduct all kinds

---

[54] _____, "This is SWIFT," *Society for Worldwide Interbank Financial Telecommunication*, no date [online]; available from <http://www.swift.com/index.cfm?item_id=1182> (accessed 26 January 2002).
[55] Yael Shahar, "Tracing bin Laden's Money: Easier Said Than Done," 21 September 2001 [online]; available from <http://www.ict.org.il/articles/articledet.cfm?articleid=387> (accessed 27 October 2001).
[56] _____, "About Us," *PayPal Corporation*, 2002 [online]; available from <http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/about-outside> (accessed 3 January 2002).

of transactions in today's global, electronic financial environment, as well as the potential difficulties to be encountered in responding to the problem.[57]

[57] Organisation For Economic Co-Operation And Development, Financial Action Task Force on Money Laundering, "Special Recommendations on Terrorist Financing," 31 October 2001 [online]; available from <http://www1.oecd.org/fatf/pdf/SRecTF_en.pdf>.

Chapter Five: Offensive Information Operations

Terrorist offensive information operations[58] can take many forms, including but not limited to 1) attacks on the information system itself, in the form of physical or cyber attack of critical communications nodes; 2) cyber attacks against control systems for critical parts of national infrastructure, resulting in varying degrees of physical damage, and 3) psychological attacks on individuals and groups. The Internet's pervasiveness and interconnectivity results in difficult to manage vulnerabilities that terrorists can and do seek out. Moreover, the widespread availability of potentially disruptive dual-use software facilitates terrorist offensive information operations.

Internet Vulnerability

The vulnerability of the Internet was probably not foreseen at its creation, for a number of reasons. Originally, the Internet was designed to enhance information sharing among a select group of trusted users. Indeed, its open architecture, which creates its susceptibility to exploitation, has always been an intentional feature. The more porous the medium, the more rapidly it can disseminate information; or, as stated succinctly by one observer, "part of the difficulty in securing the Internet's infrastructure and protecting it from ancillary attacks lies in its structure, which was designed to facilitate communication, not thwart invaders."[59] The Internet continues to be a soft terrorist target, despite advances in computer network security, because it remains vulnerable. The National Security Agency, in its series of "Eligible Receiver" exercises in 1996, noted that almost two-thirds of all federal government computers systems were not

[58] "Offensive information operations," as used in this monograph, does not portray the general U.S. understanding of the phrase as "attack of enemy information operations capabilities." No attempt is made to redefine the term beyond that contained in U.S. Department of Defense joint doctrine. See _____, Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998 [online]; available from <http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf> (accessed 17 September 2001).

[59] Mike Brunker, "Will Hackers or Spies Knot the Net," *MSNBC News*, 23 July 1996 [online]; available from <http://www.msnbc.com/news/177668.asp> (accessed 3 October 2001).

secure.[60] Although some progress has been made since then in improving Internet and computer security in both the public and private sectors, the news is not entirely good. The CERT Coordination Center, for example, provides several indicators of Internet vulnerability to hacking or other malicious activity; their most recent report indicates the number of annual Internet security incidents grew exponentially from 1988 to 2001.[61] The Internet thus continues to be vulnerable to terrorist offensive information operations.

Attacks on the Information System

Despite its vulnerabilities, the Internet is a robust system in that it is "self-healing." Because the Internet is networked, information can follow a variety of paths and thus circumvent discontinuities in the system, irrespective of whether they are intentionally caused. While this characteristic is one of the Internet's great strengths, there are nonetheless critical system nodes that are susceptible to cyber attack, and the disruption or destruction of these nodes can cause widespread loss of connectivity. In a 1998 report on Internet vulnerabilities, the director of education for the International Computer Security Association stated that "when you attack a network you can attack the channels, but the channels are multiple in the Net … but you can also attack the control structures that determine things like addressing and how information gets transferred through the Net. And in those circumstances, I think you have a real problem."[62] One example of this type of attack involves targeting routers, domain-name servers and other information hubs with denial-of-service attacks. If properly orchestrated and coordinated, these types of attacks can bring the entire Internet down for a short period of time.[63]

---

[60] Robert J. Perillo Jr., "Eligible Receiver Excercise [sic] Shows Vulnerability," 22 December 1997 [online]; available from <http://www.infowar.com/civil_de/civil_022698b.html-ssi> (accessed 29 September 2001).
[61] Carnegie Mellon University, Software Engineering Institute, "CERT/CC Statistics 1988-2001," 10 January 2002 [online]; available from < http://www.cert.org/stats/> (accessed 15 January 2002).
[62] Mike Brunker, "Will Hackers or Spies Knot the Net," *MSNBC News*, 23 July 1996 [online]; available from <http://www.msnbc.com/news/177668.asp> (accessed 3 October 2001).
[63] Ibid.

The Internet is susceptible not only to cyber attack, but also to physical attack. If the targets are selected carefully, physical attacks can in fact achieve even more dramatic results than cyber attacks. A relatively small number of well-placed bombs could achieve significant disruption if the attacker knows where to strike, and does so in a coordinated manner against multiple targets simultaneously. The widespread use of fiber optic cable, while vastly increasing the rate of data transmission on the Internet, creates a similar physical vulnerability:

> One of the hardest attacks to guard against is the low-tech approach -- known in security circles as the "backhoe attack." "Just go in and cut the fiber [optic cable] … most of the domestic Internet and all of Europe is connected [at an Internet exchange point in Virginia], so you could wipe out everything for days. If you cut several times in several different places, you could wipe it out for weeks.[64]

This continuing vulnerability, moreover, is taking place in an environment where the hacker's knowledge base and tool kit are becoming increasingly more available to anyone with access to an Internet connection. For example, in April 1999 there were an estimated 30,000 web sites devoted to hacking; many of these sites allow users to download disruptive utilities and other software, as well as provide a forum for discussion of hacking tips and techniques.[65] In an article about the potential for cyber terrorism on the Internet, computer security expert Rob Clyde commented that "you no longer have to have knowledge, you just have to have the time … you just download the tools and the programs. It's the democratization of hacking. And with these programs … they can click on a button and send [virtual] bombs to your network, and the systems will go down."[66]

Cyber Attacks on Critical Control Systems

Despite the challenges and unnecessary costs posed by the cyber threat to the Internet itself, potential attacks, even if well orchestrated, are merely nuisances in the long term. Defacement of public Web sites is certainly little more than electronic graffiti, while taking the entire system

---

[64] Ibid.
[65] John Christensen, "Bracing for Guerrilla Warfare in Cyberspace," *CNN*, 6 April 1999 [online]; available from <http://www.cnn.com/TECH/specials/hackers/cyberterror/> (accessed 12 October 2001).

down, even for an extended period of time, would constitute at worst a significant disruption; it is unlikely to generate mass casualties, for example, or catastrophic physical or economic damage. In any event, it is arguable that terrorist groups have a vested interest in maintaining rather than disrupting Internet connectivity, if they come to rely upon it for their own purposes. Cyber attacks on critical control systems, however, are much more potentially devastating, and achievable without disruption to the Internet at large. As Vetter and Perlstein have pointed out, advanced industrial societies may have unforeseen vulnerabilities associated with weak nodes in their technological infrastructures, or with the complexity and interdependence of the systems themselves. Attacks on these vulnerabilities, even by a small group of determined terrorists with the requisite expertise, "could have far-reaching consequences."[67]

Much of the current concern in the area of critical control systems lies in a type of software-facilitated, distributed control system known as a Supervisory Control and Data Acquisition (SCADA) system. SCADA software is used in computer networks to control and monitor machines and other equipment in a variety of industrial settings, including electrical power production and distribution, water treatment and distribution, manufacturing, petroleum exploration and drilling, and nuclear energy applications. The software accesses data about the state of actuators, valves, motors, electrical relays, and other machine components, and can in fact be used to control these devices remotely over a wide geographical area. Additionally, it is used to report alarm or emergency conditions extant in industrial equipment, and make that information available for access to any or all client computers on the network.[68] The chief utility of SCADA systems is that they allow personnel to monitor and control equipment distributed over a large area or in remote locations from a convenient central facility, reducing administrative and logistical costs.

---

[66] Ibid.
[67] Harold J. Vetter and Gary R. Perlstein, *Perspectives on Terrorism* (Pacific Grove, California: Brooks/Cole Publishing Company, 1991), p. 181.
[68] _____, "What is SCADA," *Modular SCADA Limited*, no date [online]; available from

The very convenience that makes SCADA systems efficient, however, also creates vulnerabilities. While usually deployed on a closed, isolated local area network for security reasons, some studies show they are being connected to the Internet at large with greater frequency, mostly due to remote access constraints and corporate information demands.[69] Additional vulnerabilities can arise from too much information about the network being available to the general public, insecure network architecture, lack of fully enforceable security protocols, or poor security management practices.[70]

The chief threats posed by hacking into SCADA networks include disrupting or completely shutting down electrical power grids, water treatment and distribution, and other industrial processes. It is also possible to alter or mask valid emergency alarms in industrial equipment. Failing to recognize an emergency condition, operators might not perform the appropriate emergency procedures, thus allowing the emergency condition to worsen before it is detected and corrected; ultimately, it might by then be too late to prevent serious damage, personal injury or deaths. An even more threatening scenario, however, might involve making one type of condition display as an alarm for a completely different emergency situation: in this case, an operator who reacts with an incorrect emergency procedure might compound the problem rather than solve it.

Psychological Attacks[71]

While terrorist information attacks directly against the Internet and other U.S. infrastructure are indeed potentially formidable, the worst long-term damage may be psychological -- either

---

<http://www.modular-scada.co.uk/what-is-scada.htm> (accessed 30 November 2001).

[69] Dion Stempfly, "Common Vulnerabilities in Operational Networks," *Presentation to the Energy Information Technology Conference and Exposition*, 14 January 2002 [online]; available from <http://www.energyitexpo.com/presentations/stempfley.pdf> (accessed 3 February 2002).

[70] _____, "Understanding SCADA System Security Vulnerabilities," *Riptech, Incorporated*, January 2001 [online]; available from <http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf> (accessed 26 November 2001).

[71] The psychological impact of terrorist information operations, while emphasized in this chapter, is equally pertinent to terrorist publicity concepts. See Chapter Six, Publicity.

from the psychological effects of physical attacks, or via the effects of purely psychological attacks. Hoffman has found that terrorist acts almost always seek to convey a message; the more shocking and frightening the terrorist act, the greater the impact of the message.[72] In this process, which seeks to influence domestic and international public opinion, terrorist psychological attacks can also inflict significant damage on the U.S. and global economy, for a relatively small investment of resources. The psychological effects of physical attacks, for example, can potentially be more damaging than the initial violence. In some cases, the intended effect of a physical attack can be more psychological than physical, while other types of attacks, especially those enabled or accomplished through means of information technology, are almost purely psychological.

The terrorist attacks on the World Trade Center and other targets on September 11, 2001 had demonstrably adverse psychological effects, some of which were far removed from the actual scenes of violence. Charles Marmar, professor and vice chair of the department of psychiatry at the University of California at San Francisco, and associate chief of staff at the San Francisco Veterans Affairs Medical Center, estimated that between 70,000 and 100,000 people in New York City alone were at high risk for post-traumatic stress disorder, by observing the destruction from a nearby vantage point, by losing a relative or close friend in the disaster, or due to other factors. The psychological costs of 9/11 could ultimately rival its physical destruction:

> Before the terrorist attacks on the World Trade Center and the Pentagon, anxiety-related disorders cost the U.S. $42 billion a year in medical and work-related losses. Now mental health professionals can only make educated estimates of how many more of us will be affected in the near future, although they have begun studying the problem.[73]

A similar phenomenon can be observed with the intentional placement of anthrax-laced letters within the U.S. mail system. This incident, following almost on the heels of the 9/11 attacks, has been referred to as a "scare" with good reason: with no disrespect to those American

---

[72] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), p. 131.
[73] Sarah Graham, "9/11: The Psychological Aftermath," *Scientific American*, 12 November 2001 [online]; available from <http://www.sciam.com/explorations/2001/111201anxiety/> (accessed 13 December 2001).

innocents who were affected, the primary effect of the anthrax release was psychological. Dr John Gearson, senior lecturer in defense studies at King's College, London, put the threat of such biological attacks in perspective, dismissing its physical dimension while highlighting its psychological potency:

> The anthrax scare continues to grow and around the world people feel more vulnerable than at any time since the height of the Cold War as they face the threat of bio-chemical terrorist attack. Government officials struggle to reassure the public, while conflicting and lurid reports from an excited, and directly targeted, media do little to calm the situation. … But we are not particularly good at risk assessment at the best of times and this should caution us in the current climate of fear and uncertainty. In the two weeks since the anthrax scare began to sweep the USA more than a thousand Americans have died in car accidents, but the roads have not been shut down.[74]

It is clear that both of these recent attacks have caused, if not fear, at least serious concern among U.S. citizens. The mere threat of another September 11-style incident was enough to reduce airline passenger miles significantly, thus weakening major airlines and the U.S. economy in general: airline revenues after 9/11 dropped from almost $33 billion to just over $20 billion, a decrease of approximately thirty eight percent.[75] The threat of biological terrorism likewise sparked more than a 100 percent increase in traffic to the Centers for Disease Control and Prevention Web site; in October 2001, it registered more than 9.1 million unique "hits," the most of any Federal government site in that time frame.[76]

The power of the Internet to inculcate fear is not limited, however, to its ability to facilitate and create synergy with lethal physical attacks. Terrorists can also use information technology to communicate frightening messages without any specific linkage to a physical act of destruction. Even if such messages do not create widespread panic, they can result in significant economic costs to Internet users and providers. One example is the use of e-mail hoaxes to spread

---

[74] John Gearson, "Anthrax Is Mostly in the Mind," *BBC News*, 19 October 2001 [online]; available from <http://news.bbc.co.uk/hi/english/uk/newsid_1608000/1608377.stm> (accessed 7 November 2002).
[75] _____, "Terror Attacks Seen Costing 1.6 Million Jobs," *MSNBC News*, 11 January 2002 [online]; available from <http://www.msnbc.com/news/685854.asp> (accessed 26 January 2002).
[76] Centers for Disease Control and Prevention, Division of Media Relations, "CDC Releases New Bioterrorism Web Resources for Clinicians, Lab Professionals, Public," 18 January 2002 [online]; available from <http://www.cdc.gov/od/oc/media/pressrel/r020118.htm> (accessed 27 January 2002).

disinformation, in an attempt to create widespread panic. The virtue of e-mail hoaxes is they can be targeted precisely at specific organizations. The U.S. Department of Energy, on its Computer Incident Advisory Capability Web site, lists a variety of e-mail hoaxes targeted against such disparate organizations as the U.S. government, commercial fast-food chains, discount store chains, and other entities. Although the likelihood of widespread panic resulting from an e-mail hoax is probably not high, the costs in lost time and bandwidth can range in the millions of dollars.[77]

[77] U.S. Department of Energy, Computer Incident Advisory Capability, "CIAC Internet Hoax Information," 25 December 2001 [online]; available from <http://hoaxbusters.ciac.org/HBHoaxIndex.html> (accessed 27 December 2001).

Chapter Six: Publicity

Terrorists use a variety of techniques to broadcast their message. Usually, this is because they wish to be seen not as criminals, but as liberators, or other instigators of positive change. Clearly, depending on one's point of view, terrorist organizations can be seen in either light; hence, it has been stated innumerable times that "one man's terrorist is another man's freedom fighter."[78] At least in part because of this problem -- which is essentially one of perspective -- scholars have repeatedly encountered difficulty in defining terrorism.[79] Still, there is general agreement that terrorists usually have a political, cultural or religious agenda they wish to implement. To achieve their objectives, moreover, they frequently choose actions that maximize their visibility in the media, thereby drawing attention to the cause or causes they espouse. As Hoffman asserts, "without the media's coverage the [terrorist] act's impact is arguably wasted, remaining narrowly confined to the immediate victim(s) of the attack rather than reaching the larger 'target audience' at whom the terrorists' violence is actually aimed."[80]

To this end, terrorists have historically relied very heavily on organized media, including newspapers, periodicals, television, and radio, to communicate their motives and aims in what they hope to be positive ways. In order to secure favorable publicity, terrorist groups have frequently attempted to form "good relationships with the press [that] are often cultivated and nurtured over a period of years."[81] By the late 1990s, however, a series of trends had developed that was beginning to affect the relationship of terrorists and the media. One of these trends is the growing incidence of terrorist attacks on the very media personnel and institutions they seek to

---

[78] *Impassim.*
[79] See Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction,* Chapter One: Terrorism and History (New York: Oxford University Press, 2000), and Bruce Hoffman, *Inside Terrorism,* Chapter One: Defining Terrorism (New York: Columbia University Press, 1998).
[80] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), p.132.
[81] Raphael F. Perl, "Terrorism, the Media, and the Government: Perspectives, Trends, and Options for Policymakers," 22 October 1997 [online]; available from <http://www.fas.org/irp/crs/crs-terror.htm> (accessed 29 September 2001).

influence.[82] One explanation of this seeming contradiction between terrorist ends and means lies in the advent of the Internet. Legitimate businesses have been using the Web to build awareness and credibility with the public for years; with little investment, terrorist groups can now do the same, and are working harder towards developing solid online presences to further their political ambitions. As the Webmaster of the Zapatista Army of National Liberation's unofficial site stated, "the crisis in Chiapas will not be solved in Cyberspace; yet, the Internet can be a powerful tool for activism and information dissemination (hence, the page's existence)."[83] Indeed, terrorist organizations can arguably affect public opinion through the Internet in even more thoroughgoing ways than is possible using conventional print or broadcast media.

The Internet as Terrorist Publicity Tool

The Internet provides some benefits to terrorists over conventional media in influencing public perception of their organizations or objectives. For example, terrorist Web publishers have complete freedom to control the content of their publicity; they need not depend on journalists or editors from the conventional media, upon whom they cannot necessarily rely not to misrepresent portions of the message, or place them out of context. To a lesser extent, they can also determine which "audience" sees what content. Current versions of Web browsers, including Netscape and Internet Explorer, support JavaScript functions allowing Internet servers to know which language is set as the default for a particular client's computer.[84] Hence, a browser set to use English as the default language can be redirected to a site optimized for publicity aimed at Western audiences, while one set to use Arabic as the default can be redirected to a different site tailored toward Arab or Muslim sensibilities.

---

[82] Ibid.
[83] Justin Paulson, "About the New www.ezln.org Site," January, 2001 [online]; available from <http://www.ezln.org/acerca.en.html> (accessed 17 December 2001).
[84] Michael Edwards, "More Sniffing for Browsers, Virtual Machines, and Operating Systems," 25 June 1998 [online]; available from <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndetect/html/sniffing2.asp> (accessed 17 November 2001).

These capabilities allowing editorial discretion and customized messages based on the audience affords terrorists great flexibility in the prosecution of their information war. However, it is nonetheless necessary to have sufficient numbers of personnel properly trained in required computer skills to achieve desired Web effects. In this regard, the quality of terrorist Web content is highly variable; in some cases, Web sites sponsored by or sympathetic to terrorist issues are amateurish at best, but professional sites with high production values are becoming more common. Moreover, terrorist propaganda on the Internet can be overt, such as on "official" Web sites where the organization itself claims responsibility for content, or covert, such as on "unofficial" sites published by sympathetic individuals or organizations with no visible, direct ties to the terrorist organization itself. Consequently, at least some terrorist organizations active on the Internet appear to demonstrate more sophistication and sensitivity to particular target audiences than might be commonly appreciated. That is, the messages and images they contain may vary dramatically, depending on the target audience.

Examples of these distinctions abound on the Internet. The official Hamas site contains imperfections typical of amateur Web publishing efforts, such as broken links, misspellings, and HTML "gizmos" which do more to distract than draw attention to important topics[85]. Many documents linked to this site portray images of graphic violence, presumably in an effort to inspire feelings of outrage. The OBM-Network site -- Internet home of Al-Muhajiroun leader Sheikh Omar Bakri Muhammad -- is more professionally done than Hamas' site, although broken links are also evident here.[86] Multiple links from this site and its sister site, Al-Muhajiroun, also lead to documents with images of graphic violence.[87] The higher end of Web publishing

---

[85] _____, "The Islamic Resistant Movement (Hamas)," no date [online]; available from <http://www.palestine-info.com/hamas/index.htm> (accessed 22 November 2001).

[86] _____, "OBM Network," no date [online]; available from <http://www.obm.clara.net/index.html> (accessed 24 January 2002).

[87] See _____, "OBM Network," no date [online]; available from <http://www.almuhajiroun.com/events/detail2.php?image=crime.jpg> (accessed 29 December 2001). This URL contains a series of video stills depicting an alleged murder of a Palestinian, in full color, by Israeli police. Also, see _____, "Iraq: The Murder Continues," *Al-Muhajiroun*, no date [online]; available from <http://www.almuhajiroun.com/lnews/special-%20iraq.php> (accessed 29 December 2001). This URL

standards, at least in terms of aesthetics, is represented by the Euskal Herria Journal Web site,[88] a New York-based publication supporting Basque independence with links to Euskadi Ta Askatasuna (ETA). This site does not, incidentally, contain images of graphic violence.

Although it is impossible to divine intent from a survey of Web sites alone, it is safe to state that terrorist propaganda on the Web takes many forms, and can be tailored to a variety of audiences. For example, content can be targeted specifically at those who are already "true believers": that is, those whose perception of the organization is already positive, whose perception of the "enemy" is already negative, or both. Propaganda on such sites can be intended to reinforce that belief. On other sites, content can be oriented more toward persuading "unbelievers" of the correctness of the terrorists' point of view. Although inducing a radical change of belief on the part of an opponent would obviously be beneficial, the chief benefit from these sites would be convincing the "fence-sitters": those who have not formed an opinion, or who have mixed feelings about issues important to the terrorists. For example, it may be easier to persuade educated Western audiences with facts rather than with imagery. If the goal is to recruit suicide bombers, images of graphic violence interspersed with half-truths and religious dogma may be more appropriate.

The Internet as Terrorist Recruiting Tool

Although publicity is in part image-creation and image-maintenance, it also involves garnering active support for the terrorist organization and its objectives. Whereas conventional media has and will continue to supply avenues for the first two, the Internet allows terrorist organizations to solicit and receive support directly from its online audience. Its "always on" nature, as well as its ability to present unadulterated content to specific audiences, makes the Web an attractive choice as a terrorist recruiting tool.

---

contains graphic pictures of children in Iraq with horrible birth defects: blamed, of course, on the United States and United Kingdom.

[88] _____, "Euskal Herria Journal: a Basque Journal," no date [online]; available from <http://www.ehj-

Although a central Internet clearinghouse for terrorist recruitment -- the "Monster.com" of terrorism, so to speak -- does not yet exist, some extremist organizations already exploit the technology specifically for this purpose on their official Web sites. A 2001 study on Internet extremist group recruitment found that, although they have achieved only modest success, hate groups such as the Hammerskin Nation, the National Alliance, Stormfront, Aryan Nations, and the Word Church of The Creator are all interested in using the Web for recruiting members, including proselytizing minors.[89] Other radical or extremist groups or their political analogs also recruit actively on the Web. For example, the African People's Socialist Party Web site contains a page providing instructions for gaining membership, sponsoring new members, and creating local chapter affiliates.[90] Sinn Fein's Web site not only encourages people to join local or regional branches of Sinn Fein internationally, but also provides an e-mail newsletter service.[91] The Lebanese Forces Party has recently solicited volunteers to serve as French translators for its Web site, as well as managers for its advertising, forums, and links areas.[92]

Another popular recruiting aid for terrorist groups has been videotapes, as evidenced by recent discoveries of brutally graphic recruiting tapes in conventional formats.[93] As digital video

---

navarre.org/index.html> (accessed 22 November 2001).

[89] Beverly Ray and George E. Marsh II, "Recruitment by Extremist Groups on the Internet," February 2001 [online]; available from <http://www.firstmonday.dk/issues/issue6_2/ray/> (accessed 7 November 2001). See also _____, "World Church of the Creator - Children's Site," *World Church of the Creator*, no date [online]; available from <http://www.wcotc.com/kids/> (accessed 9 November 2001); _____, "White Pride for Kids," *Stormfront*, no date [online]; available from <http://kids.stormfront.org/> (accessed 7 November 20010, and _____, "Aryan Nations Youth Action Corps," *Aryan Nations*, no date [online]; available from <http://www.aryan-nations.org/youthcorps.html>.

[90] _____, "What_You_Can_Do_Now," *International People's Democratic Uhuru Movement*, no date [online]; available from <http://www.inpdum.com/what_you_can_do_now.htm> (accessed 11 October 2001).

[91] _____, "Sinn Fein Home Page," *Sinn Fein*, no date [online]; available from <http://www.sinnfein.ie/> (accessed 7 November 2001).

[92] _____, "LF Backoffice," *Lebanese Forces Party*, 2 December 2000 [online]; available from <http://www.lebanese-forces.org/backoffice.htm> (accessed 14 October 2001).

[93] See Diana Ellis, "Terrorist Recruitment Video Links bin Laden, Cole," *Seattle Post-Intelligencer*, 20 June 2001 [online]; available from <http://seattlepi.nwsource.com/national/28167_binladen20.shtml> (accessed 6 November 2001); _____, "Spain Shows Suspect Terrorist Haul," *CNN*, 14 November 2001 [online]; available from <http://www.cnn.com/2001/WORLD/europe/11/14/inv.spain.videos/> (accessed 22 November 2001), and Jason Burke, "You Have to Kill in the Name of Allah Until You Are Killed," *The Observer*, 27 January 2002 [online]; available from <http://www.observer.co.uk/islam/story/0,1442,640288,00.html> (accessed 30 January 2002).

recording devices become less expensive, digital "tapes" can easily supplant old-fashioned analog tapes, simply because digital video files are easier to distribute. Digital formats such as Windows Media Player, Real Player, and QuickTime are more accessible because the Internet does not recognize international boundaries. In countries with freedom of speech laws, it is very difficult to quash distribution of such content on the Internet, however illegal or unsavory the subject matter. Distribution of digital video is thus more resistant to interception efforts by state agencies, as well as more available in general, since anyone with an Internet connection can download the relevant content. Moreover, technology also exists for reformatting conventional recruiting videotapes into Internet-friendly formats for Web publication or electronic transfer. A number of different software utilities facilitate conversion of VHS and other conventional formats to digital files recognizable by computer video applications, including Adobe's Premiere 6.0; thus, conversion and electronic distribution of current and future terrorist recruiting tapes is possible now, for relatively small investment of resources.[94]

[94] _____, "Digital Video Primer Brochure," *Adobe Systems Incorporated*, 2002 [online]; available from <http://www.adobe.com/support/salesdocs/8e96.htm> (accessed 12 January 2002).

Chapter Seven: Conclusions And Recommendations

Terrorist organizations can use the Internet and related information technology in a variety of ways to achieve their purposes. They can exercise command, control and communications over global distances, in real time, and often with considerable security. They can effectively coordinate among individual cells, taking full advantage of the strengths of a networked organization. They can even coordinate with other groups, such as rogue states, like-minded terrorist organizations, and sympathetic nongovernmental organizations, to achieve enhanced synergy in their operations. They can solicit donations, as well as move and launder funds. They can collect and distribute intelligence, technical data, doctrine, tactics, and procedures. They can conduct offensive information operations, including psychological operations, physical and cyber attacks against friendly C4I systems and nodes, and cyber attack and exploitation of critical state infrastructure that is heavily dependent on computer, and especially Internet, technology. All of these capabilities transcend international boundaries, and are frequently difficult to fight directly, particularly in nations with freedom of speech laws. Indeed, each of them capitalizes on the porous nature of liberal, democratic societies, as well as their increasing dependence on information technology in the normal, day-to-day course of human affairs. Simply put, current information technology enables terrorists to practice netwar, and affords them unprecedented freedom of action.

Meeting the challenge of these threats is not going to be simple, inexpensive, or painless. The war on terrorism will likely be long, as well as arduous; indeed, there may be no way to win the war on terrorism decisively. The paradigm of conflict has shifted away from confrontation between monolithic nation-states, and towards smaller, nastier wars between a variety of regional, national and sub-national participants. Network centric warfare blurs the distinction between military and law enforcement actions, leading some to believe that it is not possible to resolve

conflicts by defeating the "criminal element," terrorist or otherwise, in global society; rather, the only reasonable objective is to "control the level of violence and destruction to some level of international social tolerance."[95] The only thing that is abundantly clear is that the national security implications of these threats are legion, and only time will tell exactly how thoroughgoing the required changes will be. For the military, they will undoubtedly have an impact on organization, doctrine, training, equipment, and level of support provided to civil agencies.

Although a comprehensive review of all possible implications and associated responses is quite beyond the scope of this monograph, some obvious approaches include reassessing the content of U.S. government Web sites, development of information deterrence or "info tech watch" programs, refining awareness of how terrorists exploit U.S. freedom of access, legal systems, and objectivity through use of information technologies, and developing a more sophisticated understanding of the culture of information terrorism itself: terrorist information acquisition and dissemination processes, decision-making protocols, targeting methodologies, financial support apparatuses, and even their cultural or social rationale for acting.

At the strategic political level, however, the best bang for the U.S. buck will probably involve changes in intelligence collection and dissemination, immigration policy, and exploitation of innovative or evolving information technologies. Because of the ability of terrorist groups to remain invisible until they wish to be seen, coupled with their ability to project power globally, the chief tasks in the war on terror must be to physically locate cells and individual operatives, then targeting them or keeping them out of the country. Defeating the networked terrorist threat will thus require an exceptional level of effort in enhancing friendly intelligence capabilities, shoring up immigration loopholes, and leveraging the United States' already considerable information technology superiority to increase security. Moreover, because of the comprehensive

[95] Leonard Sullivan Jr., "Meeting the Challenges of Regional Security," 1 February 1994 [online]; available from <http://carlisle-www.army.mil/usassi/ssipubs/pubs94/chalnges/chalnges.pdf> (accessed 27 September

effects of the information revolution on society, these areas are all interrelated; therefore, progress will have to be measured in part by how well efforts in each category are integrated to complement each other.

Enhancing Intelligence Capability

Arguably, the single biggest challenge facing the United States today with respect to terrorist threats is enhancing its already formidable intelligence capabilities. Although better intelligence will not necessarily lead to better threat assessments,[96] the threats posed by pervasive information technology are becoming clearer. Because it moves globally at the speed of light, information technology enables and facilitates the operations of networked organizations composed of geographically dispersed "sleeper" cells; it allows terrorists to move openly without attracting attention -- at least in liberal, Western democracies -- while simultaneously strengthening their ability to attack in a coordinated fashion, from a distance, and at a place and time of their choosing. The worldwide efforts of the Al Qaeda organization, coordinating with like-minded groups in a violent confrontation with the West, are but one particularly striking example. For these reasons, finding, tracking and targeting terrorist cells is essential to combating them. The United States can accomplish this objective in part by enhancing intelligence capability across the board, but particularly in intelligence sharing and human intelligence.

One way the United States can increase the value of the intelligence it collects is to ensure it gets into the hands of relevant users in a timely manner. Against a networked adversary that exploits the advantages of information technology, an intelligence collection and dissemination system with minimal obstacles is not a mere convenience: it is essential, perhaps even of paramount importance. As terrorist organizations increasingly adopt the network form, states and

---

2001).

[96] Some experts see the "intelligence failure" leading to the September 11 attacks to be one of misplaced priorities and misallocation of resources, based on partisan political agendas. See, for example, Joseph Cirincione, "Defending America," *Georgetown Journal of International Affairs*, Winter/Spring 2002 [online]; available from <http://cfdev.georgetown.edu/publications/journal/ws02cirincione.pdf> (accessed

other entities attempting to combat terrorism may very well have to become less hierarchical and more networked to be successful, if for no other reason than "it takes networks to fight networks."[97] Consequently, government agencies must themselves become less hierarchical and more networked, and develop ways to better facilitate information sharing of all types. An adequate system will facilitate sharing horizontally, vertically, and across the spectrum of federal, state and local organizations that depend on accurate and timely intelligence and other information to support decision-making processes.

At every echelon, the United States has not always done a good job of interagency coordination, including intelligence sharing. As early as 1997, the General Accounting Office concluded that the Federal government, in its efforts to combat terrorism, had no instruments or policies in place to ensure effective cooperation among interested agencies, accurate prioritization of requirements, or elimination of redundant activities and capabilities.[98] Predictably then, despite a sophisticated electronic intelligence umbrella, terrorists were able to penetrate American defenses with seeming aplomb, prompting some experts to place the blame for the September 11 attacks squarely on poor interagency coordination. According to this view, the problem is not necessarily an insufficient amount of intelligence collected, nor is it a deficiency in collection methods; it is more "a failure of national [agency] coordination," according to former National Security Agency official John Garber. "This is a large and extremely well-coordinated attack. In spite of our best efforts to coordinate intelligence collection on terrorists, this is a massive failure of national cooperation."[99]

---

8 March 2002).

[97] Ian O. Lesser et al., *Countering the New Terrorism*, (RAND Corporation, 1999), pp. 55-56 [online]; available from <http://www.rand.org/publications/MR/MR989/MR989.chap3.pdf> (accessed 18 October 2001). Lesser and his colleagues also point out that "hierarchies have a difficult time fighting networks," and "whoever masters the network form first and best will gain major advantages."

[98] Government Accounting Office, *Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination*, GAO/NSIAD-98-39, 1 December 1997 [online]; available from <http://www.gao.gov/archive/1998/ns98039.pdf> (accessed 28 September 2001).

[99] Dan Verton and Bob Brewin, "Companies Warned About Possible Cyberattacks," *CNN*, 13 September, 2001 [online]; available from <http://www.cnn.com/2001/TECH/internet/09/13/cyber.terrorism.idg/index.html?related> (accessed 2

Fortunately, changes are either underway or on the horizon to achieve better "cross talk" between intelligence users. Certain provisions of the Patriot Act, for example, will permit broader discretionary intelligence sharing between and among Federal agencies.[100] Another, more technical measure can provide the capability to electronically link disparate intelligence databases. The state of Pennsylvania had already installed such a network -- Justice Network, or JNET -- prior to the World Trade Center and Pentagon attacks, and actually used it successfully during its investigation of the crash of United Airlines Flight 93.[101] According to JNET developer KPMG Consulting, this system is able to link existing intelligence databases without modification, and within a secure environment. An all-inclusive system similar to JNET, sponsored at the Federal level but including relevant players at all levels, could conceivably allow law enforcement agencies in San Francisco, for example, to share intelligence with a military special forces team on the other side of the globe *immediately and in real time*, and vice-versa.

Because it is often a perishable commodity, agencies at all levels need this capability to respond to useful information as soon as possible; hence, they need access to all-source intelligence with minimal delay. At the very least, database linking can afford quicker analysis and response times for all agencies; potentially, it can also provide more accurate analysis, since all the relevant pieces of the intelligence "puzzle" can be readily available to multiple analysts. Moreover, systems such as JNET can and do include databases not just from the intelligence and law enforcement communities, but also from public health entities -- effectively enhancing disaster preparedness and response capabilities as well as intelligence sharing.[102] When coupled with Bush administration efforts to coordinate responses to terrorism through the newly created

---

October 2001).

[100] U.S. House of Representatives, H.R. 3162, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001," Section 203 [online]; available from <http://thomas.loc.gov/cgi-bin/query/D?c107:1:./temp/~c107fr5TN1:e25931:> (accessed 17 November 2001).

[101] Ibid.

[102] _____, "KMPG Consulting - Homeland Security Authority - JNET Solution," *KMPG Consulting, Incorporated*, no date [online]; available from <http://www.kpmgconsulting.com/solutions/homeland_security/defense_authority.html> (accessed 14

Office of Homeland Security -- which, perhaps not coincidentally, is tasked to "identify priorities" and "coordinate efforts for collection and analysis of information within the United States regarding threats of terrorism"[103] -- database-sharing systems can significantly increase U.S. capability to find and thwart terrorist cells, as well as individual operatives.

At the same time, because of the global nature of the terrorist threat, the United States cannot focus on internal intelligence sharing at the expense of intelligence sharing with external entities. In their study of what they call the "Afghan Alumni," Shay and Schweitzer contend that the threat posed by terrorist organizations such as Al Qaeda is not a concern of Western civilization alone, but is shared with moderate Muslim nations and countries with significant Islamic minorities. For this reason among others, they determined that the only way to defeat Al Qaeda and like-minded transnational groups is through a comprehensive system of international cooperation, particularly with respect to intelligence:

> The widespread distribution of the "Afghan Alumni" and the lack of an institutionalized and centralized system makes [sic] it difficult to penetrate their ranks and foil their activities. This makes international intelligence cooperation between potential victims of the "Afghan Alumni" even more imperative. The purpose of such cooperation is to create a database and monitor the movements of Afghan activists throughout the world.[104]

No single agency or nation can expect satisfactory results if they go it alone in a war against a networked, global opponent. Whatever other options the United States and its allies consider in their response to the terrorist threat, it is clear that effective cooperation within and between friendly intelligence communities is essential to success.

Although national and international coordination is crucial to exploiting available intelligence, there must first be a sufficient quantity of all-source intelligence with which to work.

December 2001).

[103] George W. Bush, "Executive Order Establishing the Office of Homeland Security and the Homeland Security Council," 8 October 2001 [online]; available from <http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html> (accessed 15 October 2001).

[104] Shaul Shay and Yorum Schweitzer, "The 'Afghan Alumni' Terrorism: Islamic Militants Against the Rest of the World," 6 November 2000 [online]; available from <http://www.ict.org.il/articles/articledet.cfm?articleid=140> (accessed 12 October 2001). See also Boaz Ganor, "Fundamental Premises for Fighting Terrorism," 16 September 2001 [online]; available from <http://www.ict.org.il/articles/articledet.cfm?articleid=383> (accessed 12 October 2001).

Joint Publication 2-0, *Doctrine for Intelligence Support to Joint Operations*, recognizes the necessity of a wide range of intelligence sources, including human intelligence (HUMINT), to ensure accuracy of information as well as counter enemy operational security and deception practices.[105] Nonetheless, the United States has fallen behind in both the quantity and quality of its HUMINT capabilities, at least at the strategic level, opting instead to rely on technical solutions. Some scholars such as Robert D. Steele characterize this trend as a "rush to spend billions on technology, while routinely ignoring the challenges and opportunities inherent in human collection, open source collection, foreign area expertise, and human all-source analysis.[106] The Central Intelligence Agency (CIA) in particular has been slow to adapt from the Cold War standard of dependence on elaborate, electronic surveillance and reconnaissance systems. As early as 1994, Congress was investigating ways to make the CIA more relevant in a post-Cold War world. In what was to become a wholesale reevaluation of the agency, Pennsylvania Senator Arlen Specter contemplated its "total overhaul" while others questioned whether the CIA was even necessary or relevant.[107] Moreover, since the mid-1970s HUMINT has been more or less relegated to the back burner of CIA operations, in part because of the Church and Pike Committees' revelations of CIA foreign assassination plots and other, so-called "dirty tricks."[108] General Hugh Shelton, retired Chairman of the Joint Chiefs of Staff, recently commented that the subsequent desire to "get out of the human intelligence business" was in large measure responsible for the alleged intelligence failures surrounding the September 11 attacks.[109]

---

[105] _____, *Joint Publication 2-0, Doctrine for Intelligence Support to Joint Operations*, 9 March 2000 [online]; available from <http://www.dtic.mil/doctrine/jel/new_pubs/jp2_0.pdf> (accessed 22 October 2001), p. II-2.

[106] Robert D. Steele, "Information Peacekeeping: The Purest Form of War," in *Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?* (Carlisle Barracks, Pennsylvania: U.S. Army War College Strategic Studies Institute, July 1998), p. 144.

[107] Tim Weiner, "Congress Decides to Conduct Study of Need for C.I.A.," *The New York Times*, 28 September 1994 [online]; available from <http://www.nytimes.com/library/national/092894real-cia.html> (accessed 14 October 2001).

[108] Gerald K. Haines, "Looking For a Rogue Elephant: The Pike Committee Investigations and the CIA," *Studies in Intelligence*, Winter 1998-1999 [online]; available from <http://www.cia.gov/csi/studies/winter98-99/art07.html> (accessed 20 October 2001).

[109] Stephen H. Baker and Christopher Hellman, "Terrorism and Military Priorities," 26 October 2001

Since then, the clarion-call for increased HUMINT has been virtually incessant; this has resulted in governmental efforts to substantially augment intelligence spending, including a planned "five-year effort" to address intelligence shortfalls with emphasis on "correcting deficiencies in human intelligence."[110]

While any effort augmenting its inadequate HUMINT capability is a step in the right direction, the United States faces a long, difficult road in terms of the timeline required to realize concrete benefits. As President George W. Bush stated in his 2002 State of the Union address, "time is not on our side;" this is true not only because of the dangers of increased proliferation of weapons of mass destruction.[111] Adequate HUMINT capability, particularly one deployed against a networked non-state actor, takes time and effort to cultivate. It does not instantaneously materialize, as it were, out of whole cloth. Robert J. Heibel, former Deputy Chief of Counterterrorism for the Federal Bureau of Investigation, related the situation succinctly in his remarks following the September 11 attacks:

> If the perpetrators are in fact Islamic extremists, by the very nature of their organization, there's a real law enforcement security penetration problem. In all likelihood they grew up together, they are related somehow, members of the same tribe and they have a common fervor and hate for Western society. It is not just a matter of saying "let's put five agents undercover and penetrate the group." It is a very difficult operation. It takes a great deal of planning and preparation.[112]

How much "planning and preparation" is a subject of debate; however, most sources have suggested that it could take many years for the CIA to assemble the assets and build the organization required to insert reliable agents into, for example, a single radical Islamic terrorist

---

[online]; available from <http://www.cdi.org/terrorism/military-priorities.cfm> (accessed 6 November 2001).

[110] U.S. Senate Select Committee on Intelligence, "Report on Intelligence Authorization for FY 2002," 19 September 2001 [online]; available from <http://www.infowar.com/class_2/01/class2_091901c_j.shtml> (accessed 12 November 2001). Note: specific details of the budget authorization recommended by the committee are classified, and not included in this report.

[111] George W. Bush, "State of the Union Address," *White House Office of the Press Secretary*, 29 January 2002 [online]; available from <http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html> (accessed 1 February 2002).

[112] _____, "Robert Heibel: Intelligence and Counterterrorism," *CNN*, 12 September 2001 [online]; available from <http://www.cnn.com/2001/COMMUNITY/09/12/heibel/index.html> (accessed 21 September 2001).

network.[113] Still, increased HUMINT capability is an investment the United States must make despite the costs, simply because reliance only on electronic intelligence will not be sufficient to achieve its objectives. Imagery intelligence (IMINT) is frequently limited by a number of factors, particularly weather and terrain. Moreover, all forms of electronic intelligence, including measurement and signature intelligence (MASINT) and signals intelligence (SIGINT), typically reveal where an enemy *is* (or, perhaps more often, where an enemy *was*). Even so, they cannot reliably and in all cases determine precise enemy locations, much less predict activity or intentions.[114] HUMINT, whether collected from infiltrators or informants, is an essential element of an all-source intelligence apparatus, particularly for accurately predicting where an enemy *will be*. This capability is especially important to ensure success in foiling terrorist attacks, including employment of weapons of mass destruction:

> There is simply no other way to acquire the kind of insider information America needs for its defense. HUMINT provides intimate knowledge of the capabilities of our potential enemies that will help America prepare the necessary defenses. More importantly, HUMINT provides the best information on our potential enemies' intentions and could offer us the only warning of an impending attack or the only clue as to a devastating attack's perpetrators and sponsors.[115]

The benefits of enhanced HUMINT capability are not limited to finding and targeting terrorists themselves, however; they apply equally well to disrupting terrorist financial networks. Good HUMINT is necessary to cut off terrorist funding and money-laundering efforts, particularly where there are no electronic transfers to trace. Although electronic funds transfers are appealing for a number of previously examined reasons, other methods of accomplishing unregulated transactions are also available. One example is the *hawala* system, which has been in use throughout South Asia and the Middle East for centuries. The *hawala* system is cash-only,

---

[113] Evan Thomas, "Intelligence: Gearing Up For a Shadow Struggle," *MSNBC News*, 8 October 2001 [online]; available from <http://www.msnbc.com/news/635934.asp> (accessed 20 October 2001).
[114] The international effort to locate and capture drug kingpin Pablo Escobar is illustrative of the limitations of electronic intelligence. See Mark Bowden, *Killing Pablo* (New York: Atlantic Monthly Press, 2001), particularly pp. 208-211.
[115] Chris Quillen, "State-Sponsored WMD Terrorism: A Growing Threat," 2000 [online]; available from <http://www.terrorism.com/analysis/quillen-wmd-terrorism.pdf> (accessed 17 September 2001).

informal and anonymous, with few record keeping conventions; indeed, records are usually destroyed upon completion of the transaction.[116] Moreover, thorough examination of the sheer volume of financial transactions worldwide -- electronic or otherwise -- is a daunting challenge, and probably not cost effective. "Catching terrorists 'is not something you're going to do by looking at the haystack of financial transactions,' says Treasury Secretary Paul H. O'Neill. 'It comes from intelligence' that provides banks and allies with targeted accounts to watch."[117]

Immigration Reform

One of the most important beneficiaries of enhanced intelligence sharing and HUMINT will be Federal immigration authorities. The September 11 hijackers, according to most accounts, all entered the United States legally, effectively exploiting what has historically been a porous border with limited obstacles to entry. Prior identification of the culprits as Al Qaeda operatives -- based on timely collection and dissemination of intelligence -- could have prevented their entry, and thus the tragedies that ensued in New York, Washington and Pennsylvania. However, the immigration process in the United States is in some ways deficient in and of itself; therefore, immigration reform is also important in a thoroughgoing program to counter the terrorist threat.

Part of the U.S. immigration problem is organizational. As recently as December 23, 2001, issuance of most U.S. visas was the responsibility of the State Department's Bureau of Consular Affairs;[118] regulation of immigration and border control procedures, however, were under the purview of the Justice Department's Immigration and Naturalization Service.[119] This organizational setup has prompted numerous experts, including Steven A. Camarota, Director of

---

[116] Kevin Anderson, "Hawala System Under Scrutiny," *BBC News*, 8 November 2001 [online]; available from <http://news.bbc.co.uk/hi/english/business/newsid_1643000/1643995.stm> (accessed 7 December 2001).
[117] Mike McNamee, Amy Borrus, Heather Timmons, and David Fairlamb, "A Hard Slog for Financial 'Special Forces,'" *BusinessWeek*, 26 November 2001.
[118] U.S. Department of State, Bureau of Consular Affairs, "Mission of the Bureau of Consular Affairs," no date [online]; available from <http://travel.state.gov/mission.html> (accessed 23 December 2001).
[119] U.S. Department of Justice, Immigration and Naturalization Service, "INS Mission and Strategies: Mission, Strategies, and Performance," 13 November 2001 [online]; available from

Research for the Center for Immigration Studies, to see an inherent conflict of interest between the two functions:

> …it is difficult to imagine two less complementary functions than diplomacy and immigration enforcement. The diplomat's goal of promoting cooperation and compromise is sometimes in conflict with the gatekeeper's goal of exposing fraud and ensuring compliance with the law. This systemic mismatch is likely to persist regardless of management changes and may only be remedied by transferring all visa-issuing responsibilities overseas to the INS or perhaps a new "Visa Corps."[120]

Repairing whatever shortcomings exist in visa-issuance procedures, of course, will do nothing to stem the flow of illegal aliens who waltz across U.S. borders without any documentation at all. Hence, additional personnel and resources are required for border and port-of-entry security agencies such as the INS, Border Patrol and Customs Service. Also, because of the historically open borders the United States has shared with Canada and Mexico, cooperation with those two nations will be essential in creating integrated North and Central American security networks, not only to intercept terrorist operatives attempting to enter the continent, but also to foil possible efforts to import weapons of mass destruction. Sound objectives of such integration would include shutting down or disrupting drug- and migrant-smuggling operations, intelligence sharing, law enforcement cooperation, and swift implementation of joint enforcement procedures.[121]

For all of these initiatives, technology can expedite and facilitate change, although historical attempts to implement technological solutions to immigration problems have been less than completely successful. As early as 1994, the U.S. Commission on Immigration Reform called for a computerized registry, based on the Social Security Account Number, to verify work

---

<http://www.ins.gov/graphics/aboutins/insmission/index.htm> (accessed 23 December 2001).

[120] Steven A. Camarota, "Immigration and Terrorism: Testimony Prepared For the Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information," 12 October 2001 [online]; available from <http://www.cis.org/articles/2001/sactestimony1001.html> (accessed 16 November 2001).

[121] Doris Meissner, "After the Attacks: Protecting Borders and Liberties," *Carnegie Endowment for International Peace Policy Brief*, 8 November 2001, pp. 5-6 [online]; available from <http://www.ceip.org/files/pdf/PolicyBrief8.pdf> (accessed 19 December 2001).

authorizations for immigrants on work visas.[122] Subsequent Congressional attempts to institute a national identification card system for immigrants on work and student visas was passed by the House of Representatives, but failed a Senate vote.[123] Creation of an automated system for entry-exit tracking of immigrants should receive new emphasis now, in light of the events of September 11. Easy ways around the current entry-exit tracking system abound; under the current system, there is no way to know, reliably and with precision, whether short-term immigrants have actually left the country, particularly if they travel by land.[124] One way to increase confidence in the system would be to institute a comprehensive, electronic visa system such as the one currently fielded by Australia. According to Australia's Department of Immigration and Multicultural and Indigenous Affairs, its Electronic Travel Authority visas are automatically tracked and recorded in a national database, which not only simplifies entry-exit tracking, but is also convenient for the traveler.[125]

The U.S. Congress is currently contemplating legislation to address some of these concerns. House Resolution 3525 authorizes implementation of electronic visa files (section 301), an integrated entry and exit data system (section 202 and 303), and identification documents for "certain" newly admitted aliens (section 309). Further, it prescribes 200 additional INS inspectors and 200 additional investigative personnel, along with their associated support staffs, per fiscal year in 2002 through 2006 (section 101).[126] Swift Senate consideration and passage of these provisions is necessary.

---

[122] U.S. Commission on Immigration Reform, "U.S. Immigration Policy: Restoring Credibility," 1994 [online]; available from <http://www.utexas.edu/lbj/uscir/exesum94.html> (accessed 20 December 2001). The Commission reiterated this recommendation in its subsequent 1997 report: see "Becoming an American: Immigration and Immigrant Policy," September 1997, p. 40 [online]; available from <http://www.utexas.edu/lbj/uscir/becoming/ex-summary.pdf> (accessed 20 December 2001).
[123] American Civil Liberties Union, "House Vote on HR 2202," 1996 [online]; available from http://www.aclu.org/vote-guide/House_HR2202A.html> (accessed 22 December 2001).
[124] Mark Krikorian, "It's Time to Plug Our Leaky Borders," *City Journal*, Autumn 2001 [online]; available from <http://www.city-journal.org/html/11_4_its_time_to_plug.html> (accessed 23 December 2001).
[125] Australian Department of Immigration and Multicultural & Indigenous Affairs, "Internet Visa Services Australia: What is an ETA," no date [online]; available from <http://www.eta.immi.gov.au/ETAAus2En.html> (accessed 29 December 2001).
[126] U.S. House of Representatives, H.R. 3525, "Enhanced Border Security and Visa Entry Reform Act of

Leveraging Technological Superiority

Technological solutions such as those contemplated by House Resolution 3525 are not limited to immigration fixes. As the United States becomes more and more an information culture, information technology superiority will continue to be one of its strong suits. Not surprisingly, technological innovation will therefore continue to play a role in the war on terrorism. Further developments in automated weapons and sensing platforms will certainly contribute; civil liberties concerns notwithstanding, next-generation Internet surveillance capabilities such as the recently acknowledged Magic Lantern program will also be required.[127] However, key components of a near-term friendly strategy to exploit information technology should also include leveraging capabilities to provide better information security and physical security.

As previously discussed, the Internet's origins have much to do with its vulnerability. Because its precursor, ARPANET, was a closely held asset shared among a small group of trusted users, it was "originally designed for openness and flexibility, not for security."[128] This open architecture has carried over as the Internet has grown, resulting in the vulnerabilities discussed in Chapter Five; moreover, despite widespread knowledge of these vulnerabilities, computer security practices are highly variable in terms of quality, efficacy and level of enforceability. In the near term, part of the solution to network vulnerability will be administrative rather than technological: the United States must encourage cooperative efforts among government and private users to increase understanding of and adherence to generally accepted computer security practices. Differences in computer security policy, as well as unevenly applied and enforced

---

2001," 19 December 2001 [online]; available from <http://thomas.loc.gov/cgi-bin/query/D?c107:1:./temp/~c107OvvKIU::> (accessed 27 December 2001).

[127] Dan Verton, "Feds Boost Online Surveillance Activity," *Computerworld*, 10 December 2001 [online]; available from <http://www.computerworld.com/storyba/0,4125,NAV47_STO66430,00.html> (accessed 16 December 2001).

[128] Thomas A. Longstaff et al., "Security of the Internet," February 1998 [online]; available from <http://www.cert.org/encyc_article/tocencyc.html#History> (accessed 14 October 2001). Originally published in *The Froehlich/Kent Encyclopedia of Telecommunications, Volume 15* (New York: Marcel

policies, create seams that are subject to attack by malicious elements. Hence, standardization is a necessary feature of comprehensive computer network security. Although there is no such thing as zero risk, an intensive program to implement uniform computer security practices is essential to make the Internet as secure as it can possibly be. In addition, "high-value" systems -- such as those employing SCADA software for control of critical infrastructure -- must be confined to closed networks inaccessible through the Internet at large, at least until adequate technological solutions to address security concerns are developed.

Although network vulnerability -- and thus information security -- is at some level a user and agency responsibility, there are also technological efforts underway to increase the Web's intrinsic security without impairing its openness or flexibility. One such initiative is Next-Generation Internet Protocol. This proposed standard would use cryptographic techniques to provide host authentication, as well as positive identification of authorized users. Although completion of work on the new protocol is years away -- including a planned multi-year phase-in period -- it is hoped that it will provide more intrinsic security.[129]

Automated systems can also contribute to physical security in a variety of ways. Biometrics -- the use of unique physiological or behavioral characteristics for positive identification of individuals -- has been either explored or in use in a variety of states and countries. The Texas Department of Public Safety, for example, has taken thumbprints of licensed drivers for decades, and has recently begun capturing thumbprint images electronically in the process of issuing new and renewal licenses and identification cards.[130] Recently, the Netherlands and other countries have been exploring the use of electronic iris and facial scans for positive identification of

---

Dekker Inc., 1997), pp. 231-255.
[129] Ibid.
[130] Texas Department of Public Safety, "Thumbprint Capture for Driver Licenses and Identification Cards," no date [online]; available from <http://www.txdps.state.tx.us/administration/driver_licensing_control/license_issuance/thumbprints.htm> (accessed 24 December 2001).

immigrants, in part based on the inadequacy of passport photographs as a means of positive identification.[131]

The ability to distinguish between community members and outsiders is, in some ways, a basic need of any society. Positive identification of friend and foe, however, becomes an essential requirement for a society in conflict, even if civil liberties are perceived to be at stake. To this end, aggressive development of biometric systems has several distinct virtues. First, they are no more intrusive, physically or legally, than photography or conventional fingerprinting. Second, the spiraling growth of electronic transactions -- such as online driver license renewals, visa applications, and various forms of electronic commerce -- make reliable, positive electronic identification important for individual as well as collective security. Finally, in addition to positive identification, biometrics can also provide negative identification: or, in the words of biometrics researcher Jim Weyman, proof that "you are not who you say you are not." This feature is critical to protect against attempts to fraudulently obtain multiple driver licenses or other documents that could facilitate terrorist operations within U.S. borders.[132]

Perhaps the best feature of a biometrics system, if properly integrated, is that it requires little or no intrinsic security, since it compares live subjects to recorded data. Computer security expert Dorothy Denning argues that fears of biometric data counterfeiting or other criminal "workarounds" are unfounded, and in fact miss the point of biometrics entirely:

> What makes biometrics successful is not secrecy, but rather the ability to determine "liveness." I can easily distinguish the living, flesh-and-blood you from a statue or photograph of you, or even someone wearing a costume and mask that looks like you. … If I don't know you at all, I might ask for a photo ID. But I would use such a photo only because I lack knowledge of your appearance. I authenticate you by comparing your live face against the photo, not by comparing one photo against another. … The same principle applies in the digital world. Your biometric prints need not be kept secret, but the validation process must check for liveness of the readings.[133]

---

[131] Joris Evers, "Dutch Government Uses Biometrics to ID Immigrants," *CNN*, 19 April 2001 [online]; available from <http://www.cnn.com/2001/TECH/ptech/04/19/biometric.ID.idg/index.html> (accessed 23 December 2001).
[132] Mary Behr, "Q&A: Where Is Everybody," *ZDNet Reviews*, 21 May 2001 [online]; available from <http://www.zdnet.com/products/stories/reviews/0,4161,2762280,00.html> (accessed 22 December 2001).
[133] Dorothy E. Denning, "Why I Love Biometrics: It Is "Liveness," Not Secrecy, That Counts," January

Information technology is used in other ways to bolster physical security. Remotely panning video cameras and other surveillance devices have been in use for years on U.S. Air Force installations, particularly during the Cold War when nuclear-armed aircraft maintained strip alert. In the private sector, they continue to be used in mercantile applications in an attempt to thwart incidents of shoplifting and armed robbery; in some jurisdictions, cameras capture license plate numbers of speeding vehicles, providing law enforcement with an automated tool to punish offenders. Recently, hybrid arrangements that incorporate elements of surveillance and in-transit visibility systems have been suggested as a means of providing advance warning of the contents of shipping containers bound for the U.S., as well as alerts of possible en route tampering, using Global Positioning System satellites and secure ship-to-shore communications.[134] The continuing need to enhance physical security in the face of a networked terrorist adversary will require similar innovative applications of information technology in the future.

Last, but not least, are promising future technologies related to information warfare. Edward Waltz has cataloged a variety of potential emerging capabilities, including collection, processing, dissemination/presentation, offensive and defensive technologies that may have a considerable positive impact on U.S. information dominance in the long term. Some of the more interesting capabilities include intelligent, unattended ground sensors, hyperspectral, integrated aperture sensing, ultraspectral and all-spectral sensing, distributed operating systems with mediated, heterogeneous databases, digital organisms, quantum computing and storage, and a host of other possibilities.[135] Of course, this is not to say that technological innovation is a panacea. No application of technology will wholly preclude terrorist operations; some groups, for example, are

---

2001 [online]; available from <http://www.infosecuritymag.com/articles/january01/columns_logoff.shtml> (accessed 26 December 2001).

[134] Dan Verton, "IT Key to Antiterror Defenses at Nation's Sea Ports," *Computerworld*, 16 January 2002 [online]; available from <http://www.computerworld.com/storyba/0,4125,NAV47_STO67422,00.html> (accessed 21 January 2002).

[135] See Edward Waltz, *Information Warfare: Principles and Operations* (Boston, Massachusetts: Artech House, Incorporated, 1998), pp. 365-379.

known to be using combinations of low- and high-tech methods to exercise command, control and communications.[136] Nonetheless, a failure to exploit the United States' overwhelming technological superiority would be a serious error.

[136] Daniel Sieberg, "Bin Laden Exploits Technology to Suit His Needs," *CNN*, 21 September 2001 [online]; available from <http://www.cnn.com/2001/US/09/20/inv.terrorist.search/index.html> (accessed 5 October 2001).

Bibliography

Abelson, Hal, Jeff Schiller, Brian LaMacchia, and Derek Atkins. "Questions and Answers about MIT's Release of PGP 2.6," 2 June 1994. [Online]; available from <http://web.mit.edu/afs/net/mit/jis/www/pgpfaq.html> (accessed 14 November 2001).

American Civil Liberties Union. "House Vote on HR 2202," 1996. [Online]; available from http://www.aclu.org/vote-guide/House_HR2202A.html> (accessed 22 December 2001).

Anderson, Kevin. "Hawala System Under Scrutiny." *BBC News*, 8 November 2001. [Online]; available from <http://news.bbc.co.uk/hi/english/business/newsid_1643000/1643995.stm> (accessed 7 December 2001).

Australian Department of Immigration and Multicultural & Indigenous Affairs. "Internet Visa Services Australia: What is an ETA," no date. [Online]; available from <http://www.eta.immi.gov.au/ETAAus2En.html> (accessed 29 December 2001).

Baker, Stephen H. and Christopher Hellman. "Terrorism and Military Priorities," 26 October 2001. [Online]; available from <http://www.cdi.org/terrorism/military-priorities.cfm> (accessed 6 November 2001).

Behr, Mary. "Q&A: Where Is Everybody?" *ZDNet Reviews*, 21 May 2001. [Online]; available from <http://www.zdnet.com/products/stories/reviews/0,4161,2762280,00.html> (accessed 22 December 2001).

Boettcher, Mike and Ingrid Arnesen. "Al Qaeda Documents Outline Serious Weapons Program." *CNN*, 25 January 2002. [Online]; available from <http://www.cnn.com/2002/US/01/24/inv.al.qaeda.documents/> (accessed 28 January 2002).

Bowden, Mark. *Killing Pablo* (New York: Atlantic Monthly Press, 2001).

Brunker, Mike. "Will Hackers or Spies Knot the Net?" *MSNBC News*, 23 July 1996. [Online]; available from <http://www.msnbc.com/news/177668.asp> (accessed 3 October 2001).

Burke, Jason. "You Have to Kill in the Name of Allah Until You Are Killed." *The Observer*, 27 January 2002. [Online]; available from <http://www.observer.co.uk/islam/story/0,1442,640288,00.html> (accessed 30 January 2002).

Bush, George W. "Executive Order Establishing the Office of Homeland Security and the Homeland Security Council," 8 October 2001. [Online]; available from <http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html> (accessed 15 October 2001).

Bush, George W. "State of the Union Address," *White House Office of the Press Secretary*, 29 January 2002 [online]; available from <http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html> (accessed 1 February 2002).

Camarota, Steven A. "Immigration and Terrorism: Testimony Prepared For the Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information," 12 October 2001. [Online]; available from <http://www.cis.org/articles/2001/sactestimony1001.html> (accessed 16 November 2001).

Cannistraro, Vincent. "Testimony before the House Committee on International Relations," 3 October 2001. [online]; available from <http://www.house.gov/international_relations/cann1003.htm> (accessed 28 November 2001).

Carnegie Mellon University, Software Engineering Institute. "CERT/CC Statistics 1988-2001," 10 January 2002. [Online]; available from < http://www.cert.org/stats/> (accessed 15 January 2002).

Centers for Disease Control and Prevention, Division of Media Relations. "CDC Releases New Bioterrorism Web Resources for Clinicians, Lab Professionals, Public," 18 January 2002. [Online]; available from <http://www.cdc.gov/od/oc/media/pressrel/r020118.htm> (accessed 27 January 2002).

Chan, Serena and L. Jean Camp. "Towards Coherent Regulation of Law Enforcement Surveillance in the Network Society," 2001. [Online]; available from <http://itc.mit.edu/rpcp/member/seminar/chan_031501.pdf> (accessed 16 December 2001).

Christensen, John. "Bracing for Guerrilla Warfare in Cyberspace." *CNN*, 6 April 1999. [Online]; available from <http://www.cnn.com/TECH/specials/hackers/cyberterror/> (accessed 12 October 2001).

Cirincione, Joseph. "Defending America." *Georgetown Journal of International Affairs*, Winter/Spring 2002. [Online]; available from <http://cfdev.georgetown.edu/publications/journal/ws02cirincione.pdf> (accessed 8 March 2002).

Denning, Dorothy E. "Cyberterrorism," 24 August 2000. [Online]; available from <http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc> (accessed 7 January 2002).

Denning, Dorothy E. "Why I Love Biometrics: It Is "Liveness," Not Secrecy, That Counts," January 2001. [Online]; available from <http://www.infosecuritymag.com/articles/january01/columns_logoff.shtml> (accessed 26 December 2001).

Edwards, Michael. "More Sniffing for Browsers, Virtual Machines, and Operating Systems," 25 June 1998. [Online]; available from <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndetect/html/sniffing2.asp> (accessed 17 November 2001).

Ellis, Diana. "Terrorist Recruitment Video Links bin Laden, Cole." *Seattle Post-Intelligencer*, 20 June 2001. [Online]; available from <http://seattlepi.nwsource.com/national/28167_binladen20.shtml> (accessed 6 November 2001).

Evers, Joris. "Dutch Government Uses Biometrics to ID Immigrants." *CNN*, 19 April 2001. [Online]; available from <http://www.cnn.com/2001/TECH/ptech/04/19/biometric.ID.idg/index.html> (accessed 23 December 2001).

Fogleman, Ronald R. "Information Operations: The Fifth Dimension of Warfare," 1995. [Online]; available from <http://www.defenselink.mil/speeches/1995/s19950425-fogleman.html> (accessed 24 September 2001).

Gearson, John. "Anthrax Is Mostly in the Mind." *BBC News*, 19 October 2001. [Online]; available from <http://news.bbc.co.uk/hi/english/uk/newsid_1608000/1608377.stm> (accessed 7 November 2002).

Getter, Lisa. "FBI Tied Islamic Charity to Calls to Kill Israelis." *The Los Angeles Times*, 6 December 2001. [Online]; available from <http://www.latimes.com/news/nationworld/world/la-120601holy.story> (accessed 11 December 2001).

Gonyeau, Joseph. "Joseph Gonyeau's Virtual Nuclear Tourist: Nuclear Plants Around the World," no date. [Online]; available from <http://www.nucleartourist.com/> (accessed 12 December 2001).

Gordon, Michael R. "Pentagon Corners Output of Special Afghan Images." *The New York Times*, 18 October 2001. [Online]; available from http://206.181.245.163/ebird/e20011019pentagon.htm (accessed 4 November 2001).

Graham, Sarah. "9/11: The Psychological Aftermath." *Scientific American*, 12 November 2001. [Online]; available from <http://www.sciam.com/explorations/2001/111201anxiety/> (accessed 13 December 2001).

Haines, Gerald K. "Looking For a Rogue Elephant: The Pike Committee Investigations and the CIA." *Studies in Intelligence*, Winter 1998-1999. [Online]; available from <http://www.cia.gov/csi/studies/winter98-99/art07.html> (accessed 20 October 2001).

Hoffman, Bruce. *Inside Terrorism* (New York: Columbia University Press, 1998).

Johnson, Neil F. and Shushil Jajodia. "Steganalysis of Images Created Using Current Staganographic Software," 1998. [Online]; available from <http://www.isse.gmu.edu/~njohnson/ihws98/jjgmu.html> (accessed 12 November 2001). Originally published in *Lecture Notes in Computer Science, Vol. 1525*, (Springer-Verlag, 1998), pp. 273-289.

Krikorian, Mark. "It's Time to Plug Our Leaky Borders." *City Journal*, Autumn 2001. [Online]; available from <http://www.city-journal.org/html/11_4_its_time_to_plug.html> (accessed 23 December 2001).

Laqueur, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (New York: Oxford University Press, 2000).

Lesser, Ian O., Bruce Hoffman, John Arquilla, David F. Ronfeldt, Michele Zanini, and Brian Michael Jenkins. *Countering the New Terrorism* (RAND Corporation, 1999). [Online]; available from <http://www.rand.org/publications/MR/MR989/MR989.chap3.pdf> (accessed 18 October 2001).

Longstaff, Thomas A., James T. Ellis, Shawn V. Hernan, Howard F. Lipson, Robert D. McMillan, Linda Hutz Pesante, And Derek Simmel. "Security of the Internet," February 1998. [Online]; available from <http://www.cert.org/encyc_article/tocencyc.html#History> (accessed 14 October 2001). Originally published in *The Froehlich/Kent Encyclopedia of Telecommunications, Volume 15* (New York: Marcel Dekker Inc., 1997), pp. 231-255.

Lyman, Peter and Hal R. Varian, "How Much Information," 2000. [Online]; available from <http://www.sims.berkeley.edu/research/projects/how-much-info/internet.html> (accessed 22 September 2001).

McNamee, Mike, Amy Borrus, Heather Timmons, and David Fairlamb, "A Hard Slog for Financial 'Special Forces.'" *BusinessWeek*, 26 November 2001.

Meissner, Doris. "After the Attacks: Protecting Borders and Liberties." *Carnegie Endowment for International Peace Policy Brief*, 8 November 2001. [Online]; available from <http://www.ceip.org/files/pdf/PolicyBrief8.pdf> (accessed 19 December 2001).

Organisation For Economic Co-Operation And Development, Financial Action Task Force on Money Laundering. "Special Recommendations on Terrorist Financing," 31 October 2001. [Online]; available from <http://www1.oecd.org/fatf/pdf/SRecTF_en.pdf>.

Paulson, Justin. "About the New www.ezln.org Site," January, 2001. [Online]; available from <http://www.ezln.org/acerca.en.html> (accessed 17 December 2001).

Perillo, Robert J., Jr. "Eligible Receiver Excercise [sic] Shows Vulnerability," 22 December 1997. [Online]; available from <http://www.infowar.com/civil_de/civil_022698b.html-ssi> (accessed 29 September 2001).

Perl, Raphael F. "Terrorism, the Media, and the Government: Perspectives, Trends, and Options for Policymakers," 22 October 1997. [Online]; available from <http://www.fas.org/irp/crs/crs-terror.htm> (accessed 29 September 2001).

Quillen, Chris. "State-Sponsored WMD Terrorism: A Growing Threat," 2000. [Online]; available from <http://www.terrorism.com/analysis/quillen-wmd-terrorism.pdf> (accessed 17 September 2001).

Ray, Beverly and George E. Marsh II, "Recruitment by Extremist Groups on the Internet," February 2001. [Online]; available from <http://www.firstmonday.dk/issues/issue6_2/ray/> (accessed 7 November 2001).

Ruppe, David. "Terror Manual." *ABC News*, 18 September 2001. [Online]; available from <http://abcnews.go.com/sections/world/DailyNews/binladenterror_000918.html> (accessed 5 October 2001).

Schiller, Jeffrey L. "PGPfone Home Page," 10 June 1997. [Online]; available from <http://web.mit.edu/network/pgpfone/> (accessed 10 November 2001).

Shahar, Yael. "Tracing bin Laden's Money: Easier Said Than Done," 21 September 2001. [Online]; available from <http://www.ict.org.il/articles/articledet.cfm?articleid=387> (accessed 27 October 2001).

Shay, Shaul and Yorum Schweitzer. "The 'Afghan Alumni' Terrorism: Islamic Militants Against the Rest of the World," 6 November 2000. [Online]; available from <http://www.ict.org.il/articles/articledet.cfm?articleid=140> (accessed 12 October 2001). See also Boaz Ganor, "Fundamental Premises for Fighting Terrorism," 16 September 2001 [online]; available from <http://www.ict.org.il/articles/articledet.cfm?articleid=383> (accessed 12 October 2001).

Sloan, Stephen. "Terrorism and Asymmetry." *Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?* (Carlisle Barracks, Pennsylvania: U.S. Army War College, July 1998).

State of Nevada. "Nuclear Waste Transportation Routes - U.S.," no date. [Online]; available from <http://www.state.nv.us/nucwaste/states/us.htm> (accessed 14 December 2001).

Steele, Robert D. "Information Peacekeeping: The Purest Form of War." *Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?* (Carlisle Barracks, Pennsylvania: U.S. Army War College Strategic Studies Institute, July 1998).

Stempfly, Dion. "Common Vulnerabilities in Operational Networks." *Presentation to the Energy Information Technology Conference and Exposition*, 14 January 2002. [Online]; available from <http://www.energyitexpo.com/presentations/stempfley.pdf> (accessed 3 February 2002).

Sublette, Carey. "Engineering and Design of Nuclear Weapons," 20 February 1999. [Online]; available from <http://nuketesting.enviroweb.org/hew/Nwfaq/Nfaq4.html> (accessed 3 December 2001).

Sublette, Carey. "Introduction to Nuclear Weapon Physics and Design," 20 February 1999. [Online]; available from <http://nuketesting.enviroweb.org/hew/Nwfaq/Nfaq2.html> (accessed 3 December 2001).

Sullivan, Leonard, Jr. "Meeting the Challenges of Regional Security," 1 February 1994. [Online]; available from <http://carlisle-www.army.mil/usassi/ssipubs/pubs94/chalnges/chalnges.pdf> (accessed 27 September 2001).

Texas Department of Public Safety. "Thumbprint Capture for Driver Licenses and Identification Cards," no date. [Online]; available from <http://www.txdps.state.tx.us/administration/driver_licensing_control/license_issuance/thumbprints.htm> (accessed 24 December 2001).

Thomas, Evan. "Intelligence: Gearing Up For a Shadow Struggle." *MSNBC News*, 8 October 2001. [Online]; available from <http://www.msnbc.com/news/635934.asp> (accessed 20 October 2001).

U.S. Commission on Immigration Reform. "U.S. Immigration Policy: Restoring Credibility," 1994. [Online]; available from <http://www.utexas.edu/lbj/uscir/exesum94.html> (accessed 20 December 2001).

U.S. Commission on Immigration Reform. "Becoming an American: Immigration and Immigrant Policy," September 1997. [Online]; available from <http://www.utexas.edu/lbj/uscir/becoming/ex-summary.pdf> (accessed 20 December 2001).

U.S. Department of Energy, Computer Incident Advisory Capability. "CIAC Internet Hoax Information," 25 December 2001. [Online]; available from <http://hoaxbusters.ciac.org/HBHoaxIndex.html> (accessed 27 December 2001).

U.S. Department of Energy, Office of Civilian Radioactive Waste Management. "Maps," no date. [Online]; available from <http://www.ymp.gov/reference/maps/index.htm> (accessed 28 December 2001).

U.S. Department of Justice. "Report On The Availability of Bombmaking Information, the Extent to Which Its Dissemination Is Controlled by Federal Law, and the Extent to Which Such Dissemination May Be Subject to Regulation Consistent With the First Amendment to the United States Constitution," April 1997. [Online]; available from <http://cryptome.org/abi.htm> (accessed 20 November 2001).

U.S. Department of Justice, Immigration and Naturalization Service. "INS Mission and Strategies: Mission, Strategies, and Performance," 13 November 2001. [Online]; available from <http://www.ins.gov/graphics/aboutins/insmission/index.htm> (accessed 23 December 2001).

U.S. Department of State, Bureau of Consular Affairs. "Mission of the Bureau of Consular Affairs," no date. [Online]; available from <http://travel.state.gov/mission.html> (accessed 23 December 2001).

U.S. Government Accounting Office. *Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination*, GAO/NSIAD-98-39, 1 December 1997. [Online]; available from <http://www.gao.gov/archive/1998/ns98039.pdf> (accessed 28 September 2001).

U.S. House of Representatives. H.R. 3162, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001," section 203. [Online]; available from <http://thomas.loc.gov/cgi-bin/query/D?c107:1:./temp/~c107fr5TN1:e25931:> (accessed 17 November 2001). Signed by the President and became public law 26 October 2001).

U.S. House of Representatives. H.R. 3525, "Enhanced Border Security and Visa Entry Reform Act of 2001," 19 December 2001. [Online]; available from <http://thomas.loc.gov/cgi-bin/query/D?c107:1:./temp/~c107OvvKIU::> (accessed 27 December 2001).

U.S. Nuclear Regulatory Commission. "NRC: Schedule for Rebuilding NRC's Web Site," no date. [Online]; available from <http://www.nrc.gov/site-help/new-content/rebuild-schedule.html> (accessed 17 January 2002).

U.S. Nuclear Regulatory Commission. "NRC - What's New," no date. [Online]; available from <http://www.nrc.gov/site-help/new-content.html> (accessed 17 January 2002).

U.S. Senate Select Committee on Intelligence. "Report on Intelligence Authorization for FY 2002," 19 September 2001. [Online]; available from <http://www.infowar.com/class_2/01/class2_091901c_j.shtml> (accessed 12 November 2001).

Verton, Dan and Bob Brewin. "Companies Warned About Possible Cyberattacks." *CNN*, 13 September 2001. [Online]; available from <http://www.cnn.com/2001/TECH/internet/09/13/cyber.terrorism.idg/index.html?related> (accessed 2 October 2001).

Vetter, Harold J. and Gary R. Perlstein. *Perspectives on Terrorism.* (Pacific Grove, California: Brooks/Cole Publishing Company, 1991.)

Waltz, Edward. *Information Warfare: Principles and Operations*. (Boston, Massachusetts: Artech House, Incorporated, 1998.)

Weiner, Tim. "Congress Decides to Conduct Study of Need for C.I.A." *The New York Times*, 28 September 1994. [Online]; available from <http://www.nytimes.com/library/national/092894real-cia.html> (accessed 14 October 2001).

Wilson, Michael. "Terrorism in a New World." *Emergency Response and Research Institute*, 1994. [Online]; available from <http://www.emergency.com/evo-revo.htm> (accessed 7 Jan 2002).

Sieberg, Daniel. "Bin Laden Exploits Technology to Suit His Needs." *CNN*, 21 September 2001. [Online]; available from <http://www.cnn.com/2001/US/09/20/inv.terrorist.search/index.html> (accessed 5 October 2001).

Verton, Dan. "IT Key to Antiterror Defenses at Nation's Sea Ports." *Computerworld*, 16 January 2002. [Online]; available from <http://www.computerworld.com/storyba/0,4125,NAV47_STO67422,00.html> (accessed 21 January 2002).

_____. "About Us." *PayPal Corporation*, 2002. [Online]; available from <http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/about-outside> (accessed 3 January 2002).

_____. "Anarchist Cookbook, Terrorist Handbook," no date. [Online]; available from <http://come.to/anarchy> (accessed 21 November 2001).

_____. "AOL Instant Messenger Home Page." *America Online Incorporated*, no date. [Online]; available from <http://www.aim.com/> (accessed 4 December 2001).

_____. "Aryan Nations Youth Action Corps." *Aryan Nations*, no date. [Online]; available from <http://www.aryan-nations.org/youthcorps.html>.

_____. "Atomic Bomb Design," no date. [Online]; available from <http://www.accutek.com/%7Emoistner/nuclear1.htm> (accessed 3 December 2001).

_____. "Bush Calls Halt to Terror Funding." *BBC News*, 24 September 2001. [Online]; available from <http://news.bbc.co.uk/hi/english/world/americas/newsid_1560000/1560942.stm> (accessed 3 October 2001).

_____. "Contact Pipe Bomb," 2001. [Online]; available from <http://www.totse.com/en/bad_ideas/ka_fucking_boom/162267.html>.

_____. "Digital Video Primer Brochure." *Adobe Systems Incorporated*, 2002. [Online]; available from <http://www.adobe.com/support/salesdocs/8e96.htm> (accessed 12 January 2002).

_____. "DigitalGlobe Overview." *DigitalGlobe*, no date. [Online]; available from <http://www.digitalglobe.com/?goto=about> (accessed 21 December 2001).

_____. "Donate through BIF." *Benevolence International Foundation*, no date. [Online]; available from <http://www.benevolence.org/donate.htm> (accessed 28 January 2002).

_____. "eBay item 1327313247." *eBay Incorporated*, no date. [Online]; available from <http://cgi.ebay.com/aw-cgi/eBayISAPI.dll?ViewItem&item=1327313247> (accessed 28 January 2002).

_____. "Eelamweb Online Store." *EelamWeb*, no date. [Online]; available from <http://www.eelamweb.com/shop/> (accessed 16 October 2001).

_____. "E-mail Landscape." *Iconocast Inc.*, no date. [Online]; available from <http://www.iconocast.com/dotcom/marketing/e-mail.html> (accessed 7 Jan 2002).

_____. "Euskal Herria Journal: a Basque Journal," no date. [Online]; available from <http://www.ehj-navarre.org/index.html> (accessed 22 November 2001).

_____. "Explanation." *Spammimic.com*, no date. [Online]; available from <http://www.spammimic.com/explain.shtml> (accessed 1 January 2002).

_____. "The GEMI Store Online." *GEMI Corporation*, 2000. [Online]; available from <http://www.eomonline.com/CommonGEMI/Aboutus/about.htm>.

_____. "Geo 1m and 4m Frequently Asked Questions." *Space Imaging Incorporated*, no date. [Online]; available from <http://www.spaceimaging.com/carterra/geo/prodinfo/geo_faq.htm> (accessed 17 December 2001).

_____. "Geographics: U.S. Internet Population Continues to Grow." *INT Media Group, Incorporated*, 6 February 2002. [Online]; available from <http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_969541,00.html> (accessed 10 February 2002).

_____. "Help Now." *Global Relief Foundation*, no date. [Online]; available from <http://www.grf.org/helpnow.html> (accessed 28 January 2002).

_____. "High-Resolution Satellite Imagery." *PlanGraphics, Incorporated*, 2000. [Online]; available from <http://www.plangraphics.com/satellite.htm>.

_____. "Holy Land Foundation for Relief and Development Home Page." *Holy Land Foundation for Relief and Development*, no date. [Online]; previously available from <http://www.hlf.org> (accessed 6 December 2001).

_____. "How to Build a Thermonuclear Bomb." *About, Incorporated*, no date. [Online]; available from <http://physics.about.com/c/ht/00/07/How_Build_Thermonuclear_Bomb0964152140.htm> (accessed 3 December 2001).

_____. "ImageNet." *Core Software Technology*, no date. [Online]; available from <http://www.imagenet.com/info.html>.

_____. "The International PGP Home Page," no date. [Online]; available from <http://www.pgpi.org/>.

_____. "Iraq: The Murder Continues." *Al-Muhajiroun*, no date. [Online]; available from <http://www.almuhajiroun.com/lnews/special-%20iraq.php> (accessed 29 December 2001).

_____. "The Islamic Resistant Movement (Hamas)." *Hamas*, no date. [Online]; available from <http://www.palestine-info.com/hamas/index.htm> (accessed 22 November 2001).

_____. *Joint Publication 2-0, Doctrine for Intelligence Support to Joint Operations*, 9 March 2000. [Online]; available from <http://www.dtic.mil/doctrine/jel/new_pubs/jp2_0.pdf> (accessed 22 October 2001), p. II-2.

_____. *Joint Publication 3-13, Joint Doctrine for Information Operations*, 9 October 1998. 0 [Online]; available from <http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf> (accessed 17 September 2001).

_____. "KMPG Consulting - Homeland Security Authority - JNET Solution." *KMPG Consulting, Incorporated*, no date. [Online]; available from <http://www.kpmgconsulting.com/solutions/homeland_security/defense_authority.html> (accessed 14 December 2001).

_____. "Let's Build a Nuke," no date. [Online]; available from <http://home.clara.net/nybbles/oldestuff/vik/nuke/index2.html> (accessed 3 December 2001).

_____. "LF Backoffice." *Lebanese Forces Party*, 2 December 2000. [Online]; available from <http://www.lebanese-forces.org/backoffice.htm> (accessed 14 October 2001).

_____. "LF Store." *Lebanese Forces Party*, no date. [Online]; available from <http://www.lebanese-forces.org/store/lfshop.htm> (accessed 13 October 2001).

_____. "List of Nuclear Power Plants in America." *The Animated Software Company*, no date. [Online]; available from <http://www.animatedsoftware.com/environm/no_nukes/nukelist1.htm> (accessed 11 December 2001).

_____. "Manual of the Anarchist, Vol I," 4 January 1985. [Online]; available from <http://www.etext.org/CuD/Misc/anarch>.

_____. "News Reports Confirm PSI TECH's Radiological 'Dirty Bomb' Scenario as Possible Terrorist Weapon." *PSI TECH International, Incorporated*, 4 December 2001. [Online]; available from <http://www.remoteviewing.com/news/120401.html> (accessed 19 December 2001).

_____. "NPDUM Sustainer Drive." *International People's Democratic Uhuru Movement*, no date. [Online]; available from <http://www.npdum.com/sd_pledge_form.htm> (accessed 11 October 2001).

_____. "OBM Network," no date. [Online]; available from <http://www.almuhajiroun.com/events/detail2.php?image=crime.jpg> (accessed 29 December 2001).

_____. "OBM Network," no date. [Online]; available from <http://www.obm.clara.net/index.html> (accessed 24 January 2002).

_____. "Robert Heibel: Intelligence and Counterterrorism." *CNN*, 12 September 2001. [Online]; available from <http://www.cnn.com/2001/COMMUNITY/09/12/heibel/index.html> (accessed 21 September 2001).

_____. "Satellite Photos, Aerial Photography, and Images." *TerraServer.Com*, no date. [Online]; available from <http://www.terraserver.com/>.

_____. "Sinn Fein Home Page." *Sinn Fein*, no date. [Online]; available from <http://www.sinnfein.ie/> (accessed 7 November 2001).

_____. "Spain Shows Suspect Terrorist Haul." *CNN*, 14 November 2001. [Online]; available from <http://www.cnn.com/2001/WORLD/europe/11/14/inv.spain.videos/> (accessed 22 November 2001).

_____. "SPOT Image Corporation Home Page." *SPOT Image Corporation*, no date. [Online]; available from <http://www.spot.com/> (all URLs accessed 22 December 2001).

_____. "Terms of Service." *Sony Online Entertainment Incorporated*, 2002. [Online]; available from <http://www2.station.sony.com/en/termsofservice.jsp> (accessed 28 January 2002).

_____. "Terror Attacks Seen Costing 1.6 Million Jobs." *MSNBC News*, 11 January 2002. [Online]; available from <http://www.msnbc.com/news/685854.asp> (accessed 26 January 2002).

_____. "This is SWIFT." *Society for Worldwide Interbank Financial Telecommunication*, no date. [Online]; available from <http://www.swift.com/index.cfm?item_id=1182> (accessed 26 January 2002).

_____. "Traffic Patterns: Top Online Properties of January 2002." *INT Media Group, Incorporated*, January 2002. [Online]; available from <http://cyberatlas.internet.com/big_picture/traffic_patterns/article/0,,5931_971121,00.html> (accessed 10 February 2002).

_____. "Understanding SCADA System Security Vulnerabilities." *Riptech, Incorporated*, January 2001. [Online]; available from <http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf> (accessed 26 November 2001).

_____. "Welcome." *International Islamic Relief Organization*, 1996. [Online]; available from <http://www.arab.net/iiro/> (accessed 15 January 2002).

_____. "What is SCADA?" *Modular SCADA Limited*, no date. [Online]; available from <http://www.modular-scada.co.uk/what-is-scada.htm> (accessed 30 November 2001).

_____. "What_You_Can_Do_Now." *International People's Democratic Uhuru Movement*, no date. [Online]; available from <http://www.inpdum.com/what_you_can_do_now.htm> (accessed 11 October 2001).

_____. "White Pride for Kids." *Stormfront*, no date. [Online]; available from <http://kids.stormfront.org/> (accessed 7 November 2001).

_____. "World Church of the Creator - Children's Site." *World Church of the Creator*, no date. [Online]; available from <http://www.wcotc.com/kids/> (accessed 9 November 2001).

_____. "World Church of the Creator Educational Items." *World Church of the Creator*, no date. [Online]; available from <http://www.wcotc.com/items> (accessed 25 January 2002).