UNITED STATES INSTITUTE OF PEACE www.usip.org

SPECIAL REPORT

1200 17th Street NW • Washington, DC 20036 • 202.457.1700 • fax 202.429.6063

Gabriel Weimann

www.terror.net

How Modern Terrorism Uses the Internet

Summary

- The great virtues of the Internet—ease of access, lack of regulation, vast potential audiences, and fast flow of information, among others—have been turned to the advantage of groups committed to terrorizing societies to achieve their goals.
- Today, all active terrorist groups have established their presence on the Internet. Our scan of the Internet in 2003–4 revealed hundreds of websites serving terrorists and their supporters.
- Terrorism on the Internet is a very dynamic phenomenon: websites suddenly emerge, frequently modify their formats, and then swiftly disappear—or, in many cases, seem to disappear by changing their online address but retaining much the same content.
- Terrorist websites target three different audiences: current and potential supporters; international public opinion; and enemy publics.
- The mass media, policymakers, and even security agencies have tended to focus on the exaggerated threat of cyberterrorism and paid insufficient attention to the more routine uses made of the Internet. Those uses are numerous and, from the terrorists' perspective, invaluable.
- There are eight different ways in which contemporary terrorists use the Internet, ranging from psychological warfare and propaganda to highly instrumental uses such as fundraising, recruitment, data mining, and coordination of actions.
- While we must better defend our societies against cyberterrorism and Internet-savvy terrorists, we should also consider the costs of applying counterterrorism measures to the Internet. Such measures can hand authoritarian governments and agencies with little public accountability tools with which to violate privacy, curtail the free flow of information, and restrict freedom of expression, thus adding a heavy price in terms of diminished civil liberties to the high toll exacted by terrorism itself.

About the Report

Terrorists fight their wars in cyberspace as well as on the ground. However, while politicians and the media have hotly debated the dangers that cyberterrorism poses *to* the Internet, surprisingly little is known about the threat posed by terrorists' use *of* the Internet. Today, as this report makes plain, terrorist organizations and their supporters maintain hundreds of websites, exploiting the unregulated, anonymous, and easily accessible nature of the Internet to target an array of messages to a variety of audiences. Gabriel Weimann identifies no fewer than eight different ways in which terrorists are using the Internet to advance their cause, ranging from psychological warfare to recruitment, networking to fundraising. In each case, the report not only analyzes how the Internet can facilitate terrorist operations but also illustrates the point with examples culled from an extensive exploration of the World Wide Web.

Gabriel Weimann is a senior fellow at the United States Institute of Peace and professor of communication at Haifa University, Israel. He has written widely on modern terrorism, political campaigns, and the mass media. This report distills some of the findings from an ongoing, six-year study of terrorists' use of the Internet.

Special Report 116 March 2004

Contents

Introduction

The story of the presence of terrorist groups in cyberspace has barely begun to be told. In 1998, around half of the thirty organizations designated as "Foreign Terrorist Organizations" under the U.S. Antiterrorism and Effective Death Penalty Act of 1996 maintained websites; by 2000, virtually all terrorist groups had established their presence on the Internet. Our scan of the Internet in 2003–4 revealed hundreds of websites serving terrorists and their supporters. And yet, despite this growing terrorist presence, when policymakers, journalists, and academics have discussed the combination of terrorism and the Internet, they have focused on the overrated threat posed by cyberterrorism or cyberwarfare (i.e., attacks on computer networks, including those on the Internet) and largely ignored the numerous uses that terrorists make of the Internet every day.

In this report we turn the spotlight on these latter activities, identifying, analyzing, and illustrating ways in which terrorist organizations are exploiting the unique attributes of the Internet. The material presented here is drawn from an ongoing study (now in its sixth year) of the phenomenon, during which we have witnessed a growing and increasingly sophisticated terrorist presence on the World Wide Web. Terrorism on the Internet, as we have discovered, is a very dynamic phenomenon: websites suddenly emerge, frequently modify their formats, and then swiftly disappear—or, in many cases, seem to disappear by changing their online address but retaining much the same content. To locate the terrorists' sites, we have conducted numerous systematic scans of the Internet, feeding an enormous variety of names and terms into search engines, entering chat rooms and forums of supporters and sympathizers, and surveying the links on other organizations' websites to create and update our own lists of sites. This is often a herculean effort, especially because in some cases (e.g., al Qaeda's websites) locations and contents change almost daily.

The report begins by sketching the origins of the Internet, the characteristics of the new medium that make it so attractive to political extremists, the range of terrorist organizations active in cyberspace, and their target audiences. The heart of the report is an analysis of eight different uses that terrorists make of the Internet. These range from conducting psychological warfare to gathering information, from training to fundraising, from propagandizing to recruiting, and from networking to planning and coordinating terrorist acts. In each instance, we offer concrete examples drawn from our own research, from cases reported in the media, and from contacts with Western intelligence organizations. Although the bulk of the report amounts to a strong argument for the political, intelligence, and academic communities to pay much more attention to the dangers posed by terrorists' use of the Internet, the report concludes with a plea to those same communities not to overreact. The Internet may be attractive to political extremists, but it also symbolizes and supports the freedom of thought and expression that helps distinguish democracies from their enemies. Effective counterterrorist campaigns do not require, and may be undermined by, draconian measures to restrict Internet access.

Modern Terrorism and the Internet

Paradoxically, the very decentralized network of communication that the U.S. security services created out of fear of the Soviet Union now serves the interests of the greatest foe of the West's security services since the end of the Cold War: international terror. The roots of the modern Internet are to be found in the early 1970s, during the days of the Cold War, when the U.S. Department of Defense was concerned about reducing the vulnerability of its communication networks to nuclear attack. The Defense Department decided to decentralize the whole system by creating an interconnected web of computer networks. After twenty years of development and use by academic researchers, the Internet

quickly expanded and changed its character when it was opened up to commercial users in the late 1980s. By the mid-1990s, the Internet connected more than 18,000 private, public, and national networks, with the number increasing daily. Hooked into those networks were about 3.2 million host computers and perhaps as many as 60 million users spread across all seven continents. The estimated number of users in the early years of the twenty-first century is over a billion.

As it burgeoned, the Internet was hailed as an integrator of cultures and a medium for businesses, consumers, and governments to communicate with one another. It appeared to offer unparalleled opportunities for the creation of a forum in which the "global village" could meet and exchange ideas, stimulating and sustaining democracy throughout the world. However, with the enormous growth in the size and use of the network, utopian visions of the promise of the Internet were challenged by the proliferation of pornographic and violent content on the web and by the use of the Internet by extremist organizations of various kinds. Groups with very different political goals but united in their readiness to employ terrorist tactics started using the network to distribute their propaganda, to communicate with their supporters, to foster public awareness of and sympathy for their causes, and even to execute operations.

By its very nature, the Internet is in many ways an ideal arena for activity by terrorist organizations. Most notably, it offers

By its very nature, the Internet is in many ways an ideal arena for activity by terrorist organizations.

- easy access;
- little or no regulation, censorship, or other forms of government control;
- potentially huge audiences spread throughout the world;
- anonymity of communication;
- fast flow of information;
- inexpensive development and maintenance of a web presence;
- a multimedia environment (the ability to combine text, graphics, audio, and video and to allow users to download films, songs, books, posters, and so forth); and
- the ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source for stories.

An Overview of Terrorist Websites

These advantages have not gone unnoticed by terrorist organizations, no matter what their political orientation. Islamists and Marxists, nationalists and separatists, racists and anarchists: all find the Internet alluring. Today, almost all active terrorist organizations (which number more than forty) maintain websites, and many maintain more than one website and use several different languages.

Today, almost all active terrorist organizations . . . maintain websites, and many maintain more than one website and use several languages.

As the following illustrative list shows, these organizations and groups come from all corners of the globe. (This geographical categorization, it should be noted, reveals the geographical diversity but obscures the fact that many groups are truly transnational, and even transregional, in character.)

- *From the Middle East,* Hamas (the Islamic Resistance Movement), the Lebanese Hezbollah (Party of God), the al Aqsa Martyrs Brigades, Fatah Tanzim, the Popular Front for the Liberation of Palestine (PFLP), the Palestinian Islamic Jihad, the Kahane Lives movement, the People's Mujahedin of Iran (PMOI—Mujahedin-e Khalq), the Kurdish Workers' Party (PKK), and the Turkish-based Popular Democratic Liberation Front Party (DHKP/C) and Great East Islamic Raiders Front (IBDA-C).
- *From Europe,* the Basque ETA movement, Armata Corsa (the Corsican Army), and the Irish Republican Army (IRA).

- *From Latin America,* Peru's Tupak-Amaru (MRTA) and Shining Path (Sendero Luminoso), the Colombian National Liberation Army (ELN-Colombia), and the Armed Revolutionary Forces of Colombia (FARC).
- *From Asia,* al Qaeda, the Japanese Supreme Truth (Aum Shinrikyo), Ansar al Islam (Supporters of Islam) in Iraq, the Japanese Red Army (JRA), Hizb-ul Mujehideen in Kashmir, the Liberation Tigers of Tamil Eelam (LTTE), the Islamic Movement of Uzbekistan (IMU), the Moro Islamic Liberation Front (MILF) in the Philippines, the Pakistan-based Lashkar-e-Taiba, and the rebel movement in Chechnya.

Content

What most sites do* not *feature is a detailed description of their violent activities.

What is the content of terrorist sites? Typically, a site will provide a history of the organization and its activities, a detailed review of its social and political background, accounts of its notable exploits, biographies of its leaders, founders, and heroes, information on its political and ideological aims, fierce criticism of its enemies, and up-to-date news. Nationalist and separatist organizations generally display maps of the areas in dispute: the Hamas site shows a map of Palestine, the FARC site shows a map of Colombia, the LTTE site presents a map of Sri Lanka, and so forth. Despite the ever-present vocabulary of "the armed struggle" and "resistance," what most sides do *not* feature is a detailed description of their violent activities. Even if they expound at length on the moral and legal basis of the legitimacy of the use of violence, most sites refrain from referring to the terrorists' violent actions or their fatal consequences—this reticence is presumably inspired by propagandist and image-building considerations. Two exceptions to this rule are Hezbollah and Hamas, whose sites feature updated statistical reports of their actions ("daily operations") and tallies of both "dead martyrs" and "Israeli enemies" and "collaborators" killed.

Audiences

Whom do the Internet terrorists target at their sites? An analysis of the content of the websites suggests three different audiences.

- *Current and potential supporters.* Terrorist websites make heavy use of slogans and offer items for sale, including T-shirts, badges, flags, and videotapes and audiocassettes, all evidently aimed at sympathizers. Often, an organization will target its local supporters with a site in the local language and will provide detailed information about the activities and internal politics of the organization, its allies, and its competitors.
- *International public opinion.* The international public, who are not directly involved in the conflict but who may have some interest in the issues involved, are courted with sites in languages other than the local tongue. Most sites offer versions in several languages. ETA's site, for instance, offers information in Castilian, German, French, and Italian; the MRTA site offers Japanese and Italian in addition to its English and Spanish versions; and the IMU site uses Arabic, English, and Russian. For the benefit of their international audiences, the sites present basic information about the organization and extensive historical background material (material with which the organization's supporters are presumably already familiar).

Judging from the content of many of the sites, it appears that foreign journalists are also targeted.

Judging from the content of many of the sites, it appears that foreign journalists are also targeted. Press releases are often placed on the websites in an effort to get the organization's point of view into the traditional media. The detailed background information is also very useful for international reporters. One of Hezbollah's sites specifically addresses journalists, inviting them to interact with the organization's press office via-email.

- *Enemy publics*. Efforts to reach enemy publics (i.e., citizens of the states against which the terrorists are fighting) are not as clearly apparent from the content of many sites. However, some sites do seem to make an effort to demoralize the enemy by threatening attacks and by fostering feelings of guilt about the enemy's conduct and motives. In the process, they also seek to stimulate public debate in their enemies' states, to change public opinion, and to weaken public support for the governing regime.

How Terrorists Use the Internet

We have identified eight different, albeit sometimes overlapping, ways in which contemporary terrorists use the Internet. Some of these parallel the uses to which everyone puts the Internet—information gathering, for instance. Some resemble the uses made of the medium by traditional political organizations—for example, raising funds and disseminating propaganda. Others, however, are much more unusual and distinctive—for instance, hiding instructions, manuals, and directions in coded messages or encrypted files.

Psychological Warfare

Terrorism has often been conceptualized as a form of psychological warfare, and certainly terrorists have sought to wage such a campaign through the Internet. There are several ways for terrorists to do so. For instance, they can use the Internet to spread disinformation, to deliver threats intended to distill fear and helplessness, and to disseminate horrific images of recent actions, such as the brutal murder of the American journalist Daniel Pearl by his captors, a videotape of which was replayed on several terrorist websites. Terrorists can also launch psychological attacks through cyberterrorism, or, more accurately, through creating the fear of cyberterrorism. "Cyberfear" is generated when concern about what a computer attack *could* do (for example, bringing down airliners by disabling air traffic control systems, or disrupting national economies by wrecking the computerized systems that regulate stock markets) is amplified until the public believes that an attack *will* happen. The Internet—an uncensored medium that carries stories, pictures, threats, or messages regardless of their validity or potential impact—is peculiarly well suited to allowing even a small group to amplify its message and exaggerate its importance and the threat it poses.

Terrorism has often been conceptualized as a form of psychological warfare, and certainly terrorists have sought to wage such a campaign through the Internet.

Al Qaeda combines multimedia propaganda and advanced communication technologies to create a very sophisticated form of psychological warfare. Osama bin Laden and his followers concentrate their propaganda efforts on the Internet, where visitors to al Qaeda's numerous websites and to the sites of sympathetic, aboveground organizations can access prerecorded videotapes and audiotapes, CD-ROMs, DVDs, photographs, and announcements. Despite the massive onslaught it has sustained in recent years—the arrests and deaths of many of its members, the dismantling of its operational bases and training camps in Afghanistan, and the smashing of its bases in the Far East—al Qaeda has been able to conduct an impressive scare campaign. Since September 11, 2001, the organization has festooned its websites with a string of announcements of an impending "large attack" on U.S. targets. These warnings have received considerable media coverage, which has helped to generate a widespread sense of dread and insecurity among audiences throughout the world and especially within the United States.

Al Qaeda combines multimedia propaganda and advanced communication technologies to create a very sophisticated form of psychological warfare.

Despite the massive onslaught it has sustained in recent years . . . al Qaeda has been able to conduct an impressive scare campaign.

Interestingly, al Qaeda has consistently claimed on its websites that the destruction of the World Trade Center has inflicted psychological damage, as well as concrete damage, on the U.S. economy. The attacks on the Twin Towers are depicted as an assault on the trademark of the U.S. economy, and evidence of their effectiveness is seen in the weakening of the dollar, the decline of the U.S. stock market after 9/11, and a supposed loss of confidence in the U. S. economy both within the United States and elsewhere. Parallels are drawn with the decline and ultimate demise of the Soviet Union. One of bin Laden's recent publications,

posted on the web, declared that "America is in retreat by the Grace of Almighty and economic attrition is continuing up to today. But it needs further blows. The young men need to seek out the nodes of the American economy and strike the enemy's nodes."

Publicity and Propaganda

Terrorists now have direct control over the content of their message . . . [enabling them] to manipulate their own image and the image of their enemies.

The Internet has significantly expanded the opportunities for terrorists to secure publicity. Until the advent of the Internet, terrorists' hopes of winning publicity for their causes and activities depended on attracting the attention of television, radio, or the print media. These traditional media have "selection thresholds" (multistage processes of editorial selection) that terrorists often cannot reach. No such thresholds, of course, exist on the terrorists' own websites. The fact that many terrorists now have direct control over the content of their message offers further opportunities to shape how they are perceived by different target audiences and to manipulate their own image and the image of their enemies.

Most terrorist sites emphasize two issues: the restrictions placed on freedom of expression and the plight of comrades who are now political prisoners.

As noted earlier, most terrorist sites do not celebrate their violent activities. Instead, regardless of the terrorists' agendas, motives, and location, most sites emphasize two issues: the restrictions placed on freedom of expression and the plight of comrades who are now political prisoners. These issues resonate powerfully with their own supporters and are also calculated to elicit sympathy from Western audiences that cherish freedom of expression and frown on measures to silence political opposition. Enemy publics, too, may be targets for these complaints insofar as the terrorists, by emphasizing the antidemocratic nature of the steps taken against them, try to create feelings of unease and shame among their foes. The terrorists' protest at being muzzled, it may be noted, is particularly well suited to the Internet, which for many users is *the* symbol of free, unfettered, and uncensored communication.

Terrorist sites commonly employ three rhetorical structures, all used to justify their reliance on violence. The first one is the claim that the terrorists have no choice other than to turn to violence. Violence is presented as a necessity foisted upon the weak as the only means with which to respond to an oppressive enemy. While the sites avoid mentioning how the terrorists victimize others, the forceful actions of the governments and regimes that combat the terrorists are heavily emphasized and characterized with terms such as "slaughter," "murder," and "genocide." The terrorist organization is depicted as constantly persecuted, its leaders subject to assassination attempts and its supporters massacred, its freedom of expression curtailed, and its adherents arrested. This tactic, which portrays the organization as small, weak, and hunted down by a strong power or a strong state, turns the terrorists into the underdog.

A second rhetorical structure related to the legitimacy of the use of violence is the demonizing and delegitimization of the enemy. The members of the movement or organization are presented as freedom fighters, forced against their will to use violence because a ruthless enemy is crushing the rights and dignity of their people or group. The enemy of the movement or the organization is the real terrorist, many sites insist: "Our violence is tiny in comparison to his aggression" is a common argument. Terrorist rhetoric tries to shift the responsibility for violence from the terrorist to the adversary, which is accused of displaying its brutality, inhumanity, and immorality.

A third rhetorical device is to make extensive use of the language of nonviolence in an attempt to counter the terrorists' violent image. Although these are violent organizations, many of their sites claim that they seek peaceful solutions, that their ultimate aim is a diplomatic settlement achieved through negotiation and international pressure on a repressive government.

Data Mining

The World Wide Web alone offers about a billion pages of information, much of it free—and much of it of interest to terrorist organizations.

The Internet may be viewed as a vast digital library. The World Wide Web alone offers about a billion pages of information, much of it free—and much of it of interest to terrorist organizations. Terrorists, for instance, can learn from the Internet a wide variety of

details about targets such as transportation facilities, nuclear power plants, public buildings, airports, and ports, and even about counterterrorism measures. Dan Verton, in his book *Black Ice: The Invisible Threat of Cyberterrorism* (2003), explains that "al-Qaeda cells now operate with the assistance of large databases containing details of potential targets in the U.S. They use the Internet to collect intelligence on those targets, especially critical economic nodes, and modern software enables them to study structural weaknesses in facilities as well as predict the cascading failure effect of attacking certain systems." According to Secretary of Defense Donald Rumsfeld, speaking on January 15, 2003, an al Qaeda training manual recovered in Afghanistan tells its readers, "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy."

The website operated by the Muslim Hackers Club (a group that U.S. security agencies believe aims to develop software tools with which to launch cyberattacks) has featured links to U.S. sites that purport to disclose sensitive information such as code names and radio frequencies used by the U.S. Secret Service. The same website offers tutorials in creating and spreading viruses, devising hacking stratagems, sabotaging networks, and developing codes; it also provides links to other militant Islamic and terrorist web addresses. Specific targets that al Qaeda–related websites have discussed include the Centers for Disease Control and Prevention in Atlanta; FedWire, the money-movement clearing system maintained by the Federal Reserve Board; and facilities controlling the flow of information over the Internet. Like many other Internet users, terrorists have access not only to maps and diagrams of potential targets but also to imaging data on those same facilities and networks that may reveal counterterrorist activities at a target site. One captured al Qaeda computer contained engineering and structural features of a dam, which had been downloaded from the Internet and which would enable al Qaeda engineers and planners to simulate catastrophic failures. In other captured computers, U.S. investigators found evidence that al Qaeda operators spent time on sites that offer software and programming instructions for the digital switches that run power, water, transportation, and communications grids.

Specific targets that al Qaeda–related websites have discussed include the Centers for Disease Control and Prevention in Atlanta [and] FedWire, the money-movement clearing system maintained by the Federal Reserve Board.

Numerous tools are available to facilitate such data collection, including search engines, e-mail distribution lists, and chat rooms and discussion groups. Many websites offer their own search tools for extracting information from databases on their sites. Word searches of online newspapers and journals can likewise generate information of use to terrorists; some of this information may also be available in the traditional media, but online searching capabilities allow terrorists to capture it anonymously and with very little effort or expense.

Fundraising

Like many other political organizations, terrorist groups use the Internet to raise funds. Al Qaeda, for instance, has always depended heavily on donations, and its global fundraising network is built upon a foundation of charities, nongovernmental organizations, and other financial institutions that use websites and Internet-based chat rooms and forums. The Sunni extremist group Hizb al-Tahrir uses an integrated web of Internet sites, stretching from Europe to Africa, which asks supporters to assist the effort by giving money and encouraging others to donate to the cause of jihad. Banking information, including the numbers of accounts into which donations can be deposited, is provided on a site based in Germany. The fighters in the Russian breakaway republic of Chechnya have likewise used the Internet to publicize the numbers of bank accounts to which sympathizers can contribute. (One of these Chechen bank accounts is located in Sacramento, California.) The IRA's website contains a page on which visitors can make credit card donations.

The IRA's website contains a page on which visitors can make credit card donations.

Internet user demographics (culled, for instance, from personal information entered in online questionnaires and order forms) allow terrorists to identify users with sympathy

Internet user demographics . . . allow terrorists to identify users with sympathy for a particular cause or issue.

for a particular cause or issue. These individuals are then asked to make donations, typically through e-mails sent by a front group (i.e., an organization broadly supportive of the terrorists' aims but operating publicly and legally and usually having no direct ties to the terrorist organization). For instance, money benefiting Hamas has been collected via the website of a Texas-based charity, the Holy Land Foundation for Relief and Development (HLF). The U.S. government seized the assets of HLF in December 2001 because of its ties to Hamas. The U.S. government has also frozen the assets of three seemingly legitimate charities that use the Internet to raise money—the Benevolence International Foundation, the Global Relief Foundation, and the Al-Haramain Foundation—because of evidence that those charities have funneled money to al Qaeda.

In another example, in January 2004, a federal grand jury in Idaho charged a Saudi graduate student with conspiring to help terrorist organizations wage jihad by using the Internet to raise funds, field recruits, and locate prospective U.S. targets—military and civilian—in the Middle East. Sami Omar Hussayen, a doctoral candidate in computer science in a University of Idaho program sponsored—ironically—by the National Security Agency, was accused of creating websites and an e-mail group that disseminated messages from him and two radical clerics in Saudi Arabia that supported jihad.

Recruitment and Mobilization

Recruiters . . . roam online chat rooms and cybercafes, looking for receptive members of the public, particularly young people.

The Internet can be used not only to solicit donations from sympathizers but also to recruit and mobilize supporters to play a more active role in support of terrorist activities or causes. In addition to seeking converts by using the full panoply of website technologies (audio, digital video, etc.) to enhance the presentation of their message, terrorist organizations capture information about the users who browse their websites. Users who seem most interested in the organization's cause or well suited to carrying out its work are then contacted. Recruiters may also use more interactive Internet technology to roam online chat rooms and cybercafes, looking for receptive members of the public, particularly young people. Electronic bulletin boards and user nets (issue-specific chat rooms and bulletins) can also serve as vehicles for reaching out to potential recruits.

Some would-be recruits, it may be noted, use the Internet to advertise themselves to terrorist organizations. In 1995, as reported by Verton in *Black Ice,* Ziyad Khalil enrolled as a computer science major at Columbia College in Missouri. He also became a Muslim activist on the campus, developing links to several radical groups and operating a website that supported Hamas. Thanks in large part to his Internet activities, he came to the attention of bin Laden and his lieutenants. Khalil became al Qaeda's procurement officer in the United States, arranging purchases of satellite telephones, computers, and other electronic surveillance technologies and helping bin Laden communicate with his followers and officers.

Potential recruits are bombarded with religious decrees and anti-American propaganda, provided with training manuals on how to be a terrorist, and . . . given specific instructions on how to make the journey to Iraq.

More typically, however, terrorist organizations go looking for recruits rather than waiting for them to present themselves. The SITE Institute, a Washington, D.C.–based terrorism research group that monitors al Qaeda's Internet communications, has provided chilling details of a high-tech recruitment drive launched in 2003 to recruit fighters to travel to Iraq and attack U.S. and coalition forces there. Potential recruits are bombarded with religious decrees and anti-American propaganda, provided with training manuals on how to be a terrorist, and—as they are led through a maze of secret chat rooms—given specific instructions on how to make the journey to Iraq. In one particularly graphic exchange in a secret al Qaeda chat room in early September 2003 an unknown Islamic fanatic, with the user name "Redemption Is Close," writes, "Brothers, how do I go to Iraq for Jihad? Are there any army camps and is there someone who commands there?" Four days later he gets a reply from "Merciless Terrorist." "Dear Brother, the road is wide open for you—there are many groups, go look for someone you trust, join him, he will be the protector of the Iraqi regions and with the help of Allah you will become one of the

Mujahidin." "Redemption Is Close" then presses for more specific information on how he can wage jihad in Iraq. "Merciless Terrorist" sends him a propaganda video and instructs him to download software called Pal Talk, which enables users to speak to each other on the Internet without fear of being monitored.

Many terrorist websites stop short of enlisting recruits for violent action but they do encourage supporters to show their commitment to the cause in other tangible ways. "How can I help the struggle: A few suggestions," runs a heading on the Kahane Lives website; "Action alert: What you can do" is a feature on the Shining Path's website. The power of the Internet to mobilize activists is illustrated by the response to the arrest of Abdullah Ocalan, leader of the Kurdish terrorist group the PKK. When Turkish forces arrested Ocalan, tens of thousands of Kurds around the world responded with demonstrations within a matter of hours—thanks to sympathetic websites urging supporters to protest.

Networking

Many terrorist groups, among them Hamas and al Qaeda, have undergone a transformation from strictly hierarchical organizations with designated leaders to affiliations of semi-independent cells that have no single commanding hierarchy. Through the use of the Internet, these loosely interconnected groups are able to maintain contact with one another—and with members of other terrorist groups. In the future, terrorists are increasingly likely to be organized in a more decentralized manner, with arrays of transnational groups linked by the Internet and communicating and coordinating horizontally rather than vertically.

Terrorists are increasingly likely to be organized . . . [as] arrays of transnational groups linked by the Internet and communicating and coordinating horizontally rather than vertically.

Several reasons explain why modern communication technologies, especially computer-mediated communications, are so useful for terrorists in establishing and maintaining networks. First, new technologies have greatly reduced transmission time, enabling dispersed organizational actors to communicate swiftly and to coordinate effectively. Second, new technologies have significantly reduced the cost of communication. Third, by integrating computing with communications, they have substantially increased the variety and complexity of the information that can be shared.

The Internet connects not only members of the same terrorist organizations but also members of different groups. For instance, dozens of sites exist that express support for terrorism conducted in the name of jihad. These sites and related forums permit terrorists in places such as Chechnya, Palestine, Indonesia, Afghanistan, Turkey, Iraq, Malaysia, the Philippines, and Lebanon to exchange not only ideas and suggestions but also practical information about how to build bombs, establish terror cells, and carry out attacks.

Sharing Information

The World Wide Web is home to dozens of sites that provide information on how to build chemical and explosive weapons. Many of these sites post *The Terrorist's Handbook* and *The Anarchist Cookbook,* two well-known manuals that offer detailed instructions on how to construct a wide range of bombs. Another manual, *The Mujahadeen Poisons Handbook,* written by Abdel-Aziz in 1996 and "published" on the official Hamas website, details in twenty-three pages how to prepare various homemade poisons, poisonous gases, and other deadly materials for use in terrorist attacks. A much larger manual, nicknamed "The Encyclopedia of Jihad" and prepared by al Qaeda, runs to thousands of pages; distributed through the Internet, it offers detailed instructions on how to establish an underground organization and execute attacks. One al Qaeda laptop found in Afghanistan had been used to make multiple visits to a French site run by the Société Anonyme (a self-described "fluctuating group of artists and theoreticians who work specifically on the relations between critical thinking and artistic practices"), which offers a two-volume *Sabotage Handbook* with sections on topics such as planning an assassination and antisurveillance methods.

The World Wide Web is home to dozens of sites that provide information on how to build chemical and explosive weapons.

This kind of information is sought out not just by sophisticated terrorist organizations but also by disaffected individuals prepared to use terrorist tactics to advance their idiosyncratic agendas. In 1999, for instance, a young man by the name of David Copeland planted nail bombs in three different areas of London: multiracial Brixton, the largely Bangladeshi community of Brick Lane, and the gay quarter in Soho. Over the course of three weeks, he killed 3 people and injured 139. At his trial, he revealed that he had learned his deadly techniques from the Internet, downloading *The Terrorist's Handbook* and *How to Make Bombs: Book Two*. Both titles are still easily accessible. A search for the keywords "terrorist" and "handbook" on the Google search engine found nearly four thousand matches that included references to guidebooks and manuals. One site gives instructions on how to acquire ammonium nitrate, Copeland's "first choice" of explosive material.

A search for the keywords "terrorist" and "handbook" on the Google search engine found nearly four thousand matches that included references to guidebooks and manuals.

In Finland in 2002, a brilliant chemistry student who called himself "RC" discussed bomb-making techniques with other enthusiasts on a Finnish Internet website devoted to bombs and explosives. Sometimes he posted queries on topics such as manufacturing nerve gas at home. Often he traded information with the site's moderator, whose messages carried a picture of his own face superimposed on Osama bin Laden's body, complete with turban and beard. Then RC set off a bomb that killed seven people, including himself, in a crowded shopping mall. The website frequented by RC, known as the Home Chemistry Forum, was shut down by its sponsor, a computer magazine. But a backup copy was immediately posted again on a read-only basis.

Planning and Coordination

Terrorists use the Internet not only to learn how to build bombs but also to plan and coordinate specific attacks. Al Qaeda operatives relied heavily on the Internet in planning and coordinating the September 11 attacks. Thousands of encrypted messages that had been posted in a password-protected area of a website were found by federal officials on the computer of arrested al Qaeda terrorist Abu Zubaydah, who reportedly masterminded the September 11 attacks. The first messages found on Zubaydah's computer were dated May 2001 and the last were sent on September 9, 2001. The frequency of the messages was highest in August 2001. To preserve their anonymity, the al Qaeda terrorists used the Internet in public places and sent messages via public e-mail. Some of the September 11 hijackers communicated using free web-based e-mail accounts.

Thousands of encrypted messages that had been posted in a password-protected area of a website were found by federal officials on the computer [of the man] who reportedly masterminded the September 11 attacks.

Hamas activists in the Middle East, for example, use chat rooms to plan operations and operatives exchange e-mail to coordinate actions across Gaza, the West Bank, Lebanon, and Israel. Instructions in the form of maps, photographs, directions, and technical details of how to use explosives are often disguised by means of steganography, which involves hiding messages inside graphic files. Sometimes, however, instructions are delivered concealed in only the simplest of codes. Mohammed Atta's final message to the other eighteen terrorists who carried out the attacks of 9/11 is reported to have read: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." (The reference to the various faculties was apparently the code for the buildings targeted in the attacks.)

Instructions . . . are often disguised by means of steganography, which involves hiding messages inside graphic files.

Since 9/11, U.S. security agencies have monitored a number of websites that they believe are linked to al Qaeda and appear to contain elements of cyberplanning (e.g., directions for operatives, information for supporters and activists, calls for action, threats, and links to other websites):

- alneda.com, which, until it was closed down in 2002, is said by U.S. officials to have contained encrypted information to direct al Qaeda members to more secure sites, featured international news about al Qaeda, and published a variety of articles, books, and fatwas (the latter typically declaring war on the United States, Christianity, or Judaism);

- assam.com, which served as a mouthpiece for jihad in Afghanistan, Chechnya, and Palestine;
- almuhrajiroun.com, which in the late 1990s and early 2000s urged sympathizers to assassinate Pakistani president Pervez Musharraf;
- qassam.net, a site that U.S. officials claim is linked not only to al Qaeda but also to Hamas;
- jihadunspun.net, which offered a thirty-six-minute video of Osama bin Laden lecturing, preaching, and making threats;
- 7hj.7hj.com, which aimed to teach visitors how to hack into Internet networks and how to infect government and corporate websites with "worms" and viruses;
- aloswa.org, which featured quotations from bin Laden and religious legal rulings justifying the attacks of 9/11 and other assaults on the West;
- drasat.com, run (some experts suspect) by a fictional institution called the Islamic Studies and Research Center and reported to be the most credible of dozens of Islamist sites posting al Qaeda news; and
- jehad.net, alsaha.com, and islammemo.com, which are alleged to have posted al Qaeda statements as well as calls for action and directions for operatives.

Conclusion

In a briefing given in late September 2001, Ronald Dick, assistant director of the FBI and head of the United States National Infrastructure Protection Center (NIPC), told reporters that the hijackers of 9/11 had used the Internet, and "used it well." Since 9/11, terrorists have only sharpened their Internet skills and increased their web presence. Today, terrorists of very different ideological persuasions—Islamist, Marxist, nationalist, separatist, racist—have learned many of the same lessons about how to make the most of the Internet. The great virtues of the Internet—ease of access, lack of regulation, vast potential audiences, fast flow of information, and so forth—have been turned to the advantage of groups committed to terrorizing societies to achieve their goals.

How should those societies respond? This is not the place to attempt anything like a definitive answer, but two things seem clear. First, we must become better informed about the uses to which terrorists put the Internet and better able to monitor their activities. As noted at the outset of this report, journalists, scholars, policymakers, and even security agencies have tended to focus on the exaggerated threat of cyberterrorism and paid insufficient attention to the more routine uses made of the Internet. Those uses are numerous and, from the terrorists' perspective, invaluable. Hence, it is imperative that security agencies continue to improve their ability to study and monitor terrorist activities on the Internet and explore measures to limit the usability of this medium by modern terrorists.

It is imperative that security agencies continue to improve their ability to study and monitor terrorist activities on the Internet.

Second, while we must thus better defend our societies against terrorism, we must not in the process erode the very qualities and values that make our societies worth defending. The Internet is in many ways an almost perfect embodiment of the democratic ideals of free speech and open communication; it is a marketplace of ideas unlike any that has existed before. Unfortunately, as this report has shown, the freedom offered by the Internet is vulnerable to abuse from groups that, paradoxically, are themselves often hostile to uncensored thought and expression. But if, fearful of further terrorist attacks, we circumscribe our own freedom to use the Internet, then we hand the terrorists a victory and deal democracy a blow. We must not forget that the fear that terrorism inflicts has in the past been manipulated by politicians to pass legislation that undermines individual rights and liberties. The use of advanced techniques to monitor, search, track, and analyze

While we must . . . better defend our societies against terrorism, we must not in the process erode the very qualities and values that make our societies worth defending.

For more information on this topic, see our website (www.usip.org), which has an online edition of this report containing links to related websites, as well as additional information on the subject.

communications carries inherent dangers. Although such technologies might prove very helpful in the fight against cyberterrorism and Internet-savvy terrorists, they would also hand participating governments, especially authoritarian governments and agencies with little public accountability, tools with which to violate civil liberties domestically and abroad. It does take much imagination to recognize that the long-term implications could be profound and damaging for democracies and their values, adding a heavy price in terms of diminished civil liberties to the high toll exacted by terrorism itself.

Of Related Interest

A number of other publications from the United States Institute of Peace address issues related to terrorism and to the Internet and other forms of information technology. ***Note:*** Most of our reports can be downloaded from our website at **www.usip.org/reports.**

Recent Special Reports on Terrorism

- *Terrorism in the Horn of Africa* (Special Report 113, January 2004)
- *Global Terrorism after the Iraq War* (Special Report 111, October 2003)
- *The Diplomacy of Counterterrorism: Lessons Learned, Ignored, and Disputed* (Special Report 80, January 2002)
- For terrorism and counterterrorism links, visit www.usip.org/library/topics/terrorism.html.

Recent Reports from the Virtual Diplomacy Initiative

- *Creating a Common Communications Culture: Interoperability in Crisis Management* (January 2004)
- *Net Diplomacy I (Beyond Foreign Ministries), II (Beyond Old Borders), and III (2015 and Beyond)* (August 2002)
- *Information Technology and Peace Support Operations* (July 2002)
- For more resources, visit www.usip.org/virtualdiplomacy/index.html.

United States Institute of Peace
1200 17th Street NW
Washington, DC 20036
www.usip.org