Terror in Cyberspace

Gabriel Weimann

Dr. Gabriel Weimann (Weimann@soc.haifa.ac.il) is a Full Professor of Communication at Haifa University, Israel, and at the School of International Service, American University, Washington, D.C. He is a former Senior Fellow at the United States Institute of Peace (USIP), Washington, D.C. His recent book, *Terror on the Internet: The New Arena, the New Challenges*, was published in Washington, D.C., in 2006.

Introduction

The growing presence of modern terrorism on the Internet is at the nexus of two key trends: the democratization of communications driven by user-generated content on the Internet and the modern terrorists' growing awareness of the Internet's potential for their purposes. The Internet has long been a favorite tool of terrorists. Decentralized and providing almost perfect anonymity, the Internet cannot be subjected to control or restriction and allows access to anyone who wants it. Large and small terrorist groups have their own web sites and use this medium to spread propaganda, to raise funds and launder money, to recruit and train members, to communicate and conspire, and to plan and launch attacks. Al Qaeda, for example, now operates hundreds of web sites, and many more appear every year. Besides web sites, modern terrorists rely on e-mail, chatrooms, e-groups, forums, and virtual message boards, as well as resources like YouTube, Facebook, and Google Earth.

Fighting online terrorism raises the issue of countermeasures and their cost. Since the advent of the Internet, counterterrorism and security services all over the world have seen the Internet as both a danger and a useful instrument. Official statements have warned us of the ability of modern terrorists to use the Internet both for global communications as well as for cyber-attacks on crucial facilities and infrastructure. Recently, many security services and agencies have begun focusing on monitoring the Internet, on tracking down the terrorists using it, and on learning from the terrorists' Internet messages. These security services have made numerous attempts, some secret and some not, to apply various systems and defense mechanisms against terrorists on the Internet. We will review some of these efforts and then examine their cost in terms of civil liberties.

The Theater of Terror Conceptualization

From its early days, terror has combined psychological and theatrical aspects: the word "terror" comes from the Latin word "*terrere*" which means "to frighten" or "to scare."

During the "popular" phase of the French Revolution in September 1793, the "Reign of Terror" was officially declared and activated, and 16,000 people were guillotined; but executions of those labeled "internal enemies" of France took place throughout the country, and about 20,000 to 40,000 people were killed. Executions were conducted before large audiences and were accompanied by sensational publicity, thus spreading the intended fear. In the same way, but on a much larger scale, contemporary terrorists have new opportunities for exerting mass psychological impact as a result of technological advances in communications. During the 1970s, academic observers remarked increasingly on the theatrical proficiency with which terrorists conducted their operations. As Jenkins concluded his analysis of international terrorism, "Terrorism is aimed at the people watching, not at the actual victims. Terrorism is a theater."[1]

Modern terrorism can be understood in terms of the production requirements of theatrical engagements. Terrorists pay attention to script preparation, cast selection, sets, props, role-playing, and minute-by-minute stage management. Just as compelling stage plays or ballet performances require full attention to detail, the media orientation in terrorism also requires full attention to detail to be effective. Terrorist theory gradually realized the potential of the mass media. Acts of terrorism were perceived more and more as means of persuasion and psychological warfare, in which the victim was "the skin on a drum beaten to achieve a calculated impact on a wider audience."[2] The most powerful and violent performance in the modern "theater of terror" was the September 11, 2001 attack on American targets. Osama bin Laden discussed the twin attacks in November 2001. Referring to the suicide terrorists, whom he called "vanguards of Islam," bin Laden marveled: "Those young men said in deeds,

[1] BRIAN M. JENKINS, INTERNATIONAL TERRORISM: A NEW MODE OF CONFLICT (1975).

[2] ALEX P. SCHMID & JANNY DE GRAAF, VIOLENCE AS COMMUNICATION: INSURGENT TERRORISM AND THE WESTERN NEWS MEDIA (1982).

in New York and Washington, speeches that overshadowed other speeches made everywhere else in the world. The speeches are understood by both Arabs and non-Arabs, even Chinese."[3]

In her study *The Terrorist Calculus Behind 9-11*, Brigitte Nacos argued that bin Laden considered terrorism first and foremost as a vehicle to dispatch messages—"speeches" in bin Laden's words. With respect to the events of September 11, 2001, specifically, bin Laden concluded that Americans in particular had heard and reacted to the intended communication.[4] The psychological impact on the targeted population was not lost on bin Laden and his associates. In commenting on the impact of the terrorist attack on the American enemy, the al Qaeda leader remarked with obvious satisfaction, "There is America, full of fear from north to south, from west to east. Thank God for that." Moreover, Nacos argues that, by striking hard at America, the terrorists forced the media to explore al Qaeda grievances in ways that far transcended the quantity and narrow focus of the precrisis coverage of the terrorists' grievances.[5] Media coverage of Islam-related issues changed in a rather dramatic fashion after al Qaeda's attacks on September 11, 2001, when the U.S. media tried to answer the question President Bush posed in his speech before a joint session of the U.S. Congress: "Why do they hate us?" In the process, the perpetrators of the violence achieved perhaps their most important media-dependent goal—to publicize their causes, grievances, and demands.

The Terrorist Production

The emergence of media-oriented terrorism led several communication and terrorism

[3] *See* SCHMID & DE GRAAF, *supra* note 2. The quotes are taken from the translations of a videotape, presumably made in mid-November 2001 in Afghanistan.

[4] Brigitte L. Nacos, *The Terrorist Calculus Behind 9-11: A Model for Future Terrorism?*, 26 STUD. CONFLICT & TERRORISM 1 (2003).

[5] *Id.*

scholars to reconceptualize modern terrorism within the framework of symbolic communication production: "As a symbolic act, terrorism can be analyzed much like other mediums of communication, consisting of four basic components: transmitter (terrorist), intended recipient (target), message (bombing, ambush) and feedback (reaction of target audience)."[6] In fact, Ralph Dowling suggested applying the concept of "rhetoric genre" to modern terrorism and argued that "[t]errorists engage in recurrent rhetorical forms that force the media to provide the access without which terrorism could not fulfill its objectives."[7] Furthermore, some terrorist events have become "terrorist spectaculars"[8] that can best be analyzed by "media event" conceptualization.[9]

The growing importance of publicity and mass media to terrorist organizations is revealed both by the diffusion of media-oriented terrorist acts as well as by the tactics of more media-minded modern terrorists.[10] It is clear that media-wise terrorists plan their actions with the media as a major consideration. They select targets, location, and timing according to media preferences, and try to satisfy the media's criteria for newsworthiness, timetables, and deadlines. Terrorists prepare visuals for the media, such as video clips of their actions, taped interviews and declarations of the perpetrators, films, press releases (PRs), and video news releases (VNRs). Modern terrorists feed the media directly and indirectly with

---

[6] Phillip A. Karber, *Urban Terrorism: Baseline Data and a Conceptual Framework*, 52 SOC. SCI. Q. 521, 527–33 (1971).

[7] Ralph E. Dowling, *Terrorism and the Media: A Rhetorical Genre*, 36 J. COMM. 12, 14 (1986).

[8] J. Bowyer Bell, *Terrorist Scripts and Live-Action Spectaculars*, 17 COLUM. JOURNALISM REV. 47, 50. (1978).

[9] Gabriel Weimann, *Media Events: The Case of International Terrorism*, 31 J. BROADCASTING & ELECTRONIC MEDIA 21, 31 (1987) (analyzing media events and terrorist spectaculars).

[10] BRIGITTE L. NACOS, MASS-MEDIATED TERRORISM 9–10 (2002); GABRIEL WEIMANN & CONRAD WINN, THE THEATER OF TERROR: MASS MEDIA AND INTERNATIONAL TERRORISM (1994).

propaganda material often disguised as news items. Terrorists also monitor the coverage of materials they provide to the media and examine closely various media organizations' reports. Terrorists' pressure on journalists takes many forms, from open and friendly hosting to direct threats, blackmail, and even murder of journalists. Finally, terrorist organizations may also operate their own media—television channels (Al-Manar of the Hezbollah), news agencies, newspapers and magazines, radio channels, video and audio cassettes, and, recently, web sites.

The New Arena: Terror on the Internet

Post-modern terrorists take advantage of the fruits of globalization and modern technology—especially the most advanced communication technologies—to plan, coordinate, and execute their deadly campaigns. No longer geographically constrained within a particular territory, or politically or financially dependent on a particular state, they rely on advanced communication such as the Internet. Terrorism and the Internet are related in two ways: First, the Internet is a forum for both terrorist groups and individual terrorists to spread their messages of hate and violence, to communicate with one another and with their supporters and sympathizers, and even to launch psychological warfare against their enemies. Second, individuals and groups attack computer networks, including those on the Internet, in what has become known as "cyberterrorism" or "cyberwarfare." Currently, terrorists use and abuse the Internet for their own benefit more than they attack it.

The network of computer-mediated communication (CMC) is ideal for terrorists-as-communicators: it is decentralized, it cannot be subjected to control or restriction, it is not censored, and it allows free access to anyone. The structure of modern terrorist organizations makes computer-mediated communication even more important and useful for terrorists. The loosely knit network of cells, divisions, and subgroups typical to modern terrorists makes the Internet an ideal and necessary tool for inter- and intra-group networking. The rise of

virtually networked terrorist groups is part of a broader shift to what Arquilla and Ronfeldt have called "Netwar":

> *[N]etwar* refers to an emerging mode of conflict and crime at societal levels, involving measures short of traditional war in which the protagonists . . . are likely to consist of dispersed, small groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command. . . . [N]etwar differs from modes of conflict . . . in which the protagonists prefer formal, stand-alone, hierarchical organizations, doctrines, and strategies, as in past efforts, for example, to build centralized movements along Marxist lines.[11]

Web sites are only one of the Internet's services used by modern terrorists; there are many other facilities on the Internet—e-mail, chat rooms, e-groups, forums, virtual message boards—that terrorists use more and more. Many terrorist web sites are used for psychological campaigns against enemy states and their military forces. The verbal and graphic messages attempt to demoralize and scare the enemy or create feelings of guilt, doubt, and division. Terrorists use the Internet to post scary footage of executions, beheadings, fatal sniper attacks, and deadly bombings to frighten the enemy's troops. They also use the Internet to deliver threats and messages to enemy governments and enemy populations. The current literature offers anarray of works describing the ways that terrorists use the Internet.[12]

---

[11] John Arquilla, David Ronfeldt & Michele Zanini, *Networks, Netwar and Information-Age Terrorism*, *in* COUNTERING THE NEW TERRORISM 39, 47 (Ian O. Lesser et al. eds., 1999).

[12] GABRIEL WEIMANN, TERROR ON THE INTERNET: THE NEW ARENA, THE NEW CHALLENGES (2006); Maura Conway, *Terrorism and the Internet: New Media—New Threat?*, 59 PARLIAMENTARY AFF. 283, 283–92 (2006); Maura Conway, *Terrorist 'Use' of the Internet and Fighting Back*, 19 INFO. & SECURITY 9, 11–20 (2006); Kathy Crilley, *Information Warfare: New Battlefields, Terrorists, Propoganda and the Internet*, 53 ASLIB PROC. 250, 252–53 (2001); Tina Freiburger & Jeffrey S. Crane, *A Systematic Examination of Terrorist Use of the Internet*, 2 INT'L J. CYBER CRIMINOLOGY 309, 311–316 (2008); Phyllis B. Gerstenfeld, Diana R. Grant & Chau-Pu Chiang, *Hate Online: A Content Analysis of Extremist Internet Sites*, 3 ANALYSES SOC. ISSUES & PUB. POL'Y

The Advantages of the Internet for Modern Terrorism

The great virtues of the Internet—ease of access, lack of regulation, vast potential audiences, fast flow of information, multimedia applications and so forth, have been converted to the advantage of groups committed to terrorizing societies to achieve their goals. The Internet takes very little skill to use, has few regulations, provides a worldwide audience to whom information can be sent quickly at a low cost, and allows for user anonymity.[13] These design elements allow terrorists to engage in their activities with minimal risks.[14]

29, 34–41 (2003); Bruce Hoffman, RAND Corp., Testimony Before the H. Permanent Select Comm. on Intell., The Use of the Internet by Islamic Extremist (May 4, 2006), *in* RAND Corp. Testimony Series (2006), at 3–14, *available at* http://www.au.af.mil/au/awc/awcgate/congress/hoffman_testimony4may06.pdf ; Evan F. Kohlmann, *The Real Online Terrorist Threat*, 85 FOREIGN AFF. 115, 116–121 (2006); Irving Lachow & Courtney Richardson, *Terrorist Use of the Internet: The Real Story*, 45 JOINT FORCE Q. 100, 100–02 (2007); William Rosenau, *Waging the "War of Ideas," in* HOMELAND SECURITY HANDBOOK 1131 (David G. Kamien ed., 2006); Timothy L. Thomas, *Information-Age "De-Terror-ence,"* 82 MIL. REV. 32, 33–36 (2002); Timothy L. Thomas, *Al Qaeda and the Internet: The Danger of "Cyberplanning,"* 33 PARAMETERS 112, 112–123 (2003); GABRIEL WEIMANN, U.S. INST. PEACE, WWW.TERROR.NET: HOW MODERN TERRORISM USES THE INTERNET 2–11 (2004); Michael Whine, *Cyberspace—A New Medium for Communication, Command, and Control by Extremists*, 22 STUD. CONFLICT & TERRORISM 231, 231–41 (1999); Michele Zanini & Sean J.A. Edwards, *The Networking of Terror in the Information Age*, *in* NETWORKS AND NETWARS 29 (John Arquilla & David Ronfeldt eds., 2001); Mark Hosenball, *Al Qaeda's New Life*, NEWSWEEK, Dec. 30, 2002, at 47.

[13] Gabriel Weimann, *Virtual Training Camps: Terrorist Use of the Internet*, *in* TEACHING TERROR: STRATEGIC AND TACTICAL LEARNING IN THE TERRORIST WORLD 110, 111 (James J.F. Forest ed., 2006); WEIMANN, TERROR ON THE INTERNET, *supra* note 12, at 30; Lachow, *supra* note 12, at 100; WEIMANN, WWW.TERROR.NET, *supra* note 12, at 2–11; Whine, *supra* note 12, 233–41.

[14] *See generally* WEIMANN, TERROR ON THE INTERNET, *supra* note 12; Weimann, *Virtual Training Camps*, *supra* note 13; Whine, *supra* note 12; WEIMANN, WWW.TERROR.NET, *supra* note 12.

The anonymity offered by the Internet is very attractive for modern terrorists.[15] The Internet provides this anonymity, as well as easy access from everywhere, and gives terrorists the option to post messages, e-mail, upload or download information—and disappear into the dark. When American forces in Afghanistan shut down al Qaeda's camps, the terrorist group moved its base of operations to the Internet. The Internet has since become a valuable tool for al Qaeda, not just for coordination of operations and launching attacks, but also for virtual training camps, indoctrination, and recruitment. In reality, the Internet became for al Qaeda what experts call an "online terrorism university." More than 300 new pages of al Qaeda-related manuals, instructions, and rhetoric are published on the Internet every month. "It is not necessary . . . for you to join in a military training camp, or travel to another country . . . you can learn alone, or with other brothers, in [our online] preparation program," announced al Qaeda leader Abu Hadschir Al Muqrin.

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 modern Internet's roots are to be found in the early 1970s, during the days of the Cold War, when the U.S. Department of Defense was concerned with reducing the vulnerability of its communication networks to nuclear attack. The Defense Department decided to decentralize the entire 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

[15] Marc Rogers, *The Psychology of Cyber-Terrorism, in* TERRORISTS, VICTIMS AND SOCIETY 77 (Andrew Silke ed., 2003).

computers and perhaps as many as 60 million users spread across all seven continents. In 2005, the Net passed a dramatic milestone: the one-billionth user went online. According to Morgan Stanley estimates, 36% of Internet users are now in Asia and 24% are in Europe. Only 23% of users are in North America, where the Internet started. It took thirty-six years for the Internet to get its first billion users. However, Internet use has grown by 18% per year; thus, in January 2009, the estimated population of Internet users was 1.5 billion.

CMC is ideal for terrorists-as-communicators, and modern terrorist groups take full advantage of the Internet for inter-group and intra-group networking.[16] Al Qaeda, for example, has shown itself to be a remarkably nimble and adaptive entity, mainly due to its decentralized structure.[17] By its very nature, the Internet is in many ways an ideal arena for the activities of terrorist organizations. Most notably, it offers:

- 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;
- Interactivity;
- 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, etc.); and
- The ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source for stories.

[16] WEIMANN, TERROR ON THE INTERNET, *supra* note 12, at 25.

[17] Bruce Hoffman, *Al Qaeda, Trends in Terrorism, and Future Potentialities: An Assessment*, 26 STUD. CONFLICT & TERRORISM 427, 435 (2003).

These advantages have not gone unnoticed by terrorist organizations, no matter what their political orientation. Islamists and Marxists, nationalists and separatists, fundamentalists and extremists, racists and anarchists: all find the Internet alluring. Today, all active terrorist organizations maintain web sites, and many maintain more than one web site and use several different languages. As the following illustrative list shows, these organizations and groups come from all corners of the globe and they all are active on the Net:

- *From the Middle East*
  - Hamas (the Islamic Resistance Movement)
  - Lebanese Hezbollah (Party of God)
  - Al Aqsa Martyrs Brigades
  - Fatah Tanzim
  - Popular Front for the Liberation of Palestine (PFLP)
  - Palestinian Islamic Jihad
  - Kahane Lives movement
  - People's Mujahedin of Iran (PMOI—Mujahedin-e Khalq)
  - Kurdish Workers' Party (PKK)
  - Turkish-based Popular Democratic Liberation Front Party (DHKP/C)
  - Great East Islamic Raiders Front (IBDA-C) (which is also based in Turkey)
- *From Europe*
  - Basque ETA movement
  - Armata Corsa (the Corsican Army)
  - Real Irish Republican Army (RIRA)
  - Various groups associated wit al Qaeda
- *From Latin America*
  - Peru's Tupak-Amaru (MRTA) and Shining Path (Sendero Luminoso)

- Colombian National Liberation Army (ELN-Colombia)
- Armed Revolutionary Forces of Colombia (FARC)

- *From Asia*
  - Al Qaeda
  - Japanese Supreme Truth (Aum Shinrikyo)
  - Ansar al Islam (Supporters of Islam) in Iraq
  - Japanese Red Army (JRA)
  - Hizb-ul Mujehideen in Kashmir
  - Liberation Tigers of Tamil Eelam (LTTE)
  - Islamic Movement of Uzbekistan (IMU)
  - Moro Islamic Liberation Front (MILF) in the Philippines
  - Pakistan-based Lashkar-e-Toiba
  - Rebel movement in Chechnya

In July 2004, the independent National Commission on Terrorist Attacks upon the United States (the 9/11 Commission) released its findings in a 570-page report. The report points to the use of modern communication technologies for planning and execution of the 9/11 attacks: "Terrorists, in turn, have benefited from this same rapid development of communication technologies." The importance of the Internet, and its uses by al Qaeda for the attacks, is also noted:

> The emergence of the World Wide Web has given terrorists a much easier means of acquiring information and exercising command and control over their operations. The operational leader of the 9/11 conspiracy, Mohamed Atta, went online from Hamburg, Germany, to research U.S. flight schools. Targets of intelligence collection have become more sophisticated. These changes have made surveillance and threat warning more difficult.[18]

The report highlights uses of the Internet by al Qaeda operatives, which include searching the

[18] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 88 (2004).

Web for information on U.S. flight schools, using Internet communications, equipping the hijackers with e-mail accounts, coordinating the attackers' actions using e-mail, downloading anti-American Web pages, and gathering flight information.[19]

Many terrorists on the Internet belong to radical Islamist groups and organizations. Paradoxically, it is those who criticize and attack Western modernity, technology, and media who use the West's most advanced modern medium─the Internet. This should come as no surprise after the publication of several studies and especially Gary Bunt's books *Virtually Islamic, Islam in the Digital Age* and *iMuslims: Rewiring the House of Islam*. Bunt's research is a detailed description of the diverse manifestations of the Islamic presence online. He suggests that there has been a significant redirection of resources into the Net by Islamic organizations that adapted to the digital age, preferring the Net over traditional channels of communication. This trend is reflected in the volume of militant Islamic materials online and in the growing sophistication of Islamic web sites. For example, the presentation of video clips and audio broadcasts on Islamic sites applies some of the most recent developments in computer technology.

Bunt argues that "[t]he Islamic Internet landscape changes frequently, with new sites emerging on a daily basis. Some very proactive players change their content and format regularly, attempting to draw readers to their message(s) in order to establish links or a sense of community."[20] "Chat rooms are often unregulated and unmonitored by scholars and clerics, can provide a virtual hangout for teenage and young-adult Muslims, and are sometimes rife with anti-*kuffar* (nonbeliever) sentiment." Bunt concludes, "The Internet is clearly important in disseminating a broad range of Islamic political-religious opinions and

[19] *Id.* at 157, 529 n.140, 530 nn.152, 221–222.

[20] GARY R. BUNT, VIRTUALLY ISLAMIC: COMPUTER-MEDIATED COMMUNICATION AND CYBER ISLAMIC ENVIRONMENTS 10 (2000).

concerns to a global audience. Thus, many extremist Islamist activists and terrorists now see the Internet as a vital tool."[21] According to Bunt's latest book, the internet has profoundly shaped how Muslims perceive Islam and how Islamic societies and networks evolve and shift in the twenty-first century.[22] While these electronic interfaces appear new and innovative in terms of how media is applied, much of their content has a basis in classical Islamic concepts, with a historical resonance that can be traced back to the time of the Prophet Muhammad.

Monitoring terrorist presence on the Internet reveals thousands of terrorist web sites. While in the late 1990s there were merely a dozen terrorist web sites, by the year 2000 virtually all terrorist groups had established their presence on the Internet, and in 2003 there were over 2,600 terrorist web sites.[23] This number rose dramatically, and by 2006 there were over 5,600 web sites serving terrorists and their supporters; recent estimates show close to 8,000 web sites.[24]

How Terrorists Use the Internet

Today, all terrorist organizations, large and small, have their own web sites.[25] They use this medium to spread propaganda, to raise funds, to launder money, to recruit and train

[21] *Id.* at 14.

[22] *See generally* GARY R. BUNT, iMUSLIMS: REWIRING THE HOUSE OF ISLAM (2009).

[23] WEIMANN, TERROR ON THE INTERNET, *supra* note 12, at 105.

[24] WEIMANN, TERROR ON THE INTERNET, *supra* note 12; Weimann, *Virtual Training Camps*, *supra* note 13, at 110. The following are monitoring organizations' web sites: Site Intelligence Group, http://www.siteintelgroup.org/ (last visited Mar. 21, 2010); Intel Center, http://intelcenter.com/ (last visited Mar. 21, 2010); Mansfield Report, Global Strategic Translations & Analysis, http://www.lauramansfield.com/subscribers/ (last visited Mar. 21, 2010); The Middle East Media Research Institute, http://www.memri.org/; http://www.ctc.usma.edu/ (last visited Mar. 21, 2010).

[25] *See generally* WEIMANN, TERROR ON THE INTERNET, *supra* note 12; *see also* Hoffman, *supra* note 12, at 4; WEIMANN, WWW.TERROR.NET, *supra* note 12, at 2.

members, to communicate and conspire, and to launch attacks. Nevertheless, governments try to counter and catch modern terrorists using traditional means.[26]

Terrorism and the Internet are related in several ways.[27] At this point, terrorists use the Internet for propaganda and communication more than they attack the Internet. Yet, Frank Cilluffo of the Office of Homeland Security remarks, "While bin Laden may have his finger on the trigger, his grandchildren may have their fingers on the computer mouse." Future terrorists may indeed see greater potential for cyberterrorism than do the terrorists of today. Cyberterrorism may also become more attractive as the real and virtual worlds become more closely coupled. For instance, a terrorist group might simultaneously explode a bomb at a train station and launch a cyberattack on the communications infrastructure, thus magnifying the impact of the event. Unless these systems are carefully secured, conducting an online

[26] HANNA ROGAN, JIHADISM ONLINE: A STUDY OF HOW AL-QAIDA AND RADICAL ISLAMIST GROUPS USE THE INTERNET FOR TERRORIST PURPOSES 13, 20, 24, 26–27, 29, 31 (Norwegian Def. Research Establishment ed., 2006), *available at* http://rapporter.ffi.no/rapporter/2006/00915.pdf; MICHAEL A. VATIS, CYBER ATTACKS DURING THE WAR ON TERRORISM: A PREDICTIVE ANALYSIS (Dartmouth Coll. Inst. for Security Tech. Stud. ed., 2001), *available at* http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf; Nadya Labi, *Jihad 2.0*, 298 ATLANTIC MONTHLY 102, 105 (2006); Marc Lynch, *Al-Qaeda's Media Strategies*, 83 NAT'L INTEREST 50, 53–54 (2006); David Talbot, *Terror's Server*, 108 TECH. REV. 46, 48 (2005); Steve Coll & Susan B. Glasser, *Terrorists Turn to the Web as Base of Operations*, WASH. POST, Aug. 7, 2005, at A1; Susan B. Glasser & Steve Coll, *The Web as a Weapon*, WASH. POST, Aug. 9, 2005 at A1; Jon Swartz, *Terrorists' Use of Internet Spreads*, USA TODAY, Feb. 21, 2005, at 3B ; Maura Conway, *Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet*, FIRST MONDAY, Nov. 4, 2002, at 12–13, http://131.193.153.231/www/issues/issue7_11/conway/index.html; WEIMANN, TERROR ON THE INTERNET, *supra* note 12, at 111–45; Conway, *Terrorism and the Internet*, *supra* note 12, at 283–92; Conway, *Terrorist Use of the Internet and Fighting Back*, *supra* note 12, at 11–20; Thomas, *Al Qaeda and the Internet*, *supra* note 12; WEIMANN, WWW.TERROR.NET, *supra* note 12, at 5–10.

[27] *See generally* WEIMANN, TERROR ON THE INTERNET, *supra* note 12.

operation that physically harms someone may be as easy tomorrow as penetrating a web site is today.

Web sites are only one of the Internet's services used by modern terrorism.[28] For example, according to Katz and Devon:

> Yahoo! has become one of al Qaeda's most significant ideological bases of operation. Utilizing several facets of Yahoo!'s service, including chat functions, e-mail, and most importantly, Yahoo! Groups, al Qaeda and its supporters have inserted themselves like a cancer into a company that screams, "American pop culture," and made it as much their own as a training camp in Khost. . . . Creating a Yahoo! Group is free, quick, and extremely easy, and al Qaeda and its supporters have wasted no time in starting up several Yahoo! Groups with topics related to the terrorist group and the downfall of Western civilization. Very often, the groups contain the latest links to jihadist web sites, serving as a jihadist directory, and are sometimes the first to post al Qaeda communiqués to the public.[29]

More recently, uploading, downloading, and viewing video has become very popular. YouTube was established in February 2005 as an online repository, facilitating the sharing of video content. YouTube claims to be the "the world's most popular online video community." A 2007 report from the Pew Internet and American Life Project puts the percentage of U.S. online video viewers using YouTube at 27%, ahead of all other video sharing sites.[30] In the 18-to-29-year-old age groups, this leadership is even more pronounced with 49% of U.S. online video viewers using YouTube.[31] In fact, *CNNMoney* reported that in January 2008 alone, nearly 79 million users worldwide viewed more than 3 billion YouTube

---

[28] *Id.*

[29] Rita Katz & Josh Devon, *WWW.JIHAD.COM: E-Groups Abused by Jihadists*, NAT'L REV. ONLINE, July 14, 2003, http://www.nationalreview.com/comment/comment-katz-devon071403.asp.

[30] MARY MADDEN, ONLINE VIDEO 14 (Pew Internet & American Life Proj. 2007), *available at* http://www.pewinternet.org/Reports/2007/Online-Video/03-The-Audience-for-Online-Video/06-Half-of-young-adult-video-viewers-say-they-watch-video-on-YouTube.aspx?r=1.

[31] *Id.*

videos.[32] Terrorist groups realize the potential of this easily-accessed platform for the dissemination of their propaganda and radicalization videos. Convicted terrorist Younis Tsouli ("Irhabi007") praised the usefulness of this new online apparatus: "A lot of the funding that the brothers are getting is coming because of the videos. Imagine how many have gone after seeing the videos. Imagine how many have become shahid [martyrs]."

Hezbollah, Hamas, al Qaeda and its numerous affiliates, the LTTE, and the Shining Path of Peru all have propaganda videos on YouTube. In 2008, Hamas allegedly launched its own video-sharing web site, although the group denied ownership of the site. AqsaTube, in addition to having a similar name, was designed to look just like YouTube and even copied its logo. Once certain Internet providers refused to host the web site, Hamas launched a PaluTube and TubeZik, while the Tamil Tigers launched TamilTube. These videos are not just aimed at Middle Eastern Muslim youth. More recent videos posted on these video-sharing web sites are dubbed in English or have English subtitles.

A recent study conducted by Conway and McInerney analyzed the online supporters of jihad-promoting video content on YouTube, focusing on postings and comments on martyr-promoting material from Iraq.[33] The findings suggest that a majority of comments were posted by users under thirty-five years of age, residing outside the Middle East and North Africa; the largest percentage of supporters were located in the United States. The researchers concluded,

> What is clearly evident however is that jihadist content is spreading far beyond traditional jihadist web sites or even dedicated forums to embrace, in particular, video sharing and social networking—both hallmarks of Web

[32] Yi-Wyn Yen, YouTube Looks for the Money Clip, CNNMoney.com (Mar. 25, 2008), http://techland.blogs.fortune.cnn.com/2008/03/25/youtube-looks-for-the-money-clip/.

[33] *See generally* Maura Conway & Lisa McInerney, *Jihadi Video & Auto-Radicalisation: Evidence from an Exploratory YouTube Study*, *in* INTELLIGENCE AND SECURITY INFORMATICS, LNCS 5376, at 108, 108–18 (Daniel Ortiz-Arroyo et al. eds., 2008).

> 2.0—and thus extending their reach far beyond what may be conceived as their core support base in the Middle East and North Africa region to diaspora populations, converts, and political sympathizers.[34]

Recent studies have identified numerous, albeit sometimes overlapping, ways in which contemporary terrorists use the Internet. Some of these ways 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. Other ways, however, are much more unusual and distinctive, for instance, hiding instructions, manuals, and directions in coded messages or encrypted files. The various uses of the Net by modern terrorists may be grouped into two broad categories: communicative uses and instrumental uses.

The Communicative Uses of the Internet by Terrorists

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 the television, radio, or print media. The fact that terrorists themselves have direct control over the content of their web sites offers further opportunity to shape how they are perceived by different target audiences and to manipulate their image and the images of their enemies. Most terrorist sites do not celebrate their violent activities. Instead—regardless of their nature, motives, or location—most terrorist sites emphasize two issues: the restrictions placed on freedom of expression and the plight of their comrades who are political prisoners. These issues resonate powerfully with their own supporters and are calculated to elicit sympathy from Western audiences who cherish freedom of expression and who frown on measures taken to silence political opposition.

[34] *Id.* at 117.

Common elements of terror sites include the organization's communiqués and the speeches and writings of its leaders, founders, and ideologists. The sites often present a word-for-word series of the organizations' official statements, which the visitor can browse along with selected announcements arranged by date. The sites tend to recycle materials previously distributed through the mass media and other communication means. Some terrorist sites house a veritable online "gift shop" through which visitors can order and purchase books, video and audiocassettes, stickers, printed shirts, and pins with the organization's badges.

Who are the targeted audiences of these sites? Do they appeal to current and potential supporters, to the international community, or to their enemies (namely, the public who is part of the opposing socio-political community in the conflict)? An analysis of the sites' contents indicates an attempt to approach all three audiences.[35] The slogans and text on these sites appeal strongly to the supporter-public. Of course, the sites in local languages (especially Arabic) target these audiences more directly than do the English and other-language versions. These pages include detailed information about recent activities of the organizations and elaborate in detail about internal politics and relationships between local groups. Reaching out to supporters is also evinced from the fact that the sites offer appropriate items for sale, including printed shirts, badges, flags, and video- and audiocassettes.

But an important target audience, in addition to supporters of the organizations, is the international "bystander" public—surfers who are not involved in the conflict. This is evident from the presentation of basic information about the group, its leaders, and extensive historical background material (with which the supporter-public is presumably familiar).

[35] Conway, *supra* note 26. Conway, *Terrorist 'Use' of the Internet*, *supra* note 12, at 19–30; Conway, *Terrorism and the Internet*, *supra* note 12, at 283–98; Yariv Tsfati& Gabriel Weimann, *www.terrorism.com: Terror on the Internet*, 25 STUD. CONFLICT & TERRORISM 317, 322 (2002).

Most of the sites offer versions in several languages in order to enlarge their international audience. The sites use English in addition to the local language of the organization's supporters. Judging from the content of many of the sites, journalists might also constitute another "bystander" target audience. The organizations often place press releases on the web sites. The detailed background information might also be useful for international reporters.

Approaches to reaching enemy audiences are not as clearly apparent from the content of many sites. However, on some sites the desire to reach this audience is evidenced by efforts to demoralize the enemy or to create feelings of guilt. The Jihadists try to utilize their web sites to change public opinion in their enemies' states, to weaken public support for the governing regime, to stimulate public debate, and, of course, to demoralize the enemy. They use the Internet to deliver threats and messages to enemy governments and to enemy populations. They can also use the Internet to harm the credibility of enemy media, enemy officials, and the establishment. In this case, the target audience is the enemy population, but the attack is on its official media credibility.

The Internet also grants terrorists a cheap and efficient means of networking. Many terrorist groups, among them Hamas and al Qaeda, have transformed from strictly hierarchical organizations with designated leaders to affiliations of semi-independent cells that have no single commanding hierarchy. Through the Internet, these loosely interconnected groups are able to maintain contact with one another and with members of other terrorist groups. For instance, dozens of sites supporting terrorism in the name of jihad permit terrorists, in places as far-removed from one another as Chechnya and Malaysia, to exchange ideas and practical information about how to build bombs, establish terror cells, and carry out attacks.

Modern terrorists' use of the Internet is also a key ingredient in the concept of terrorism as psychological warfare. "Cyber-fear," argues Thomas,

> is generated by the fact that what a computer attack *could* do (i.e., bring down airliners, ruin critical infrastructure, destroy the stock market, reveal state secrets, etc.) is too often associated with what *will* happen . . . It is clear that the Internet empowers small groups and makes them appear much more capable than they might actually be, even turning bluster into a type of virtual fear. The net allows terrorists to amplify the consequences of their activities with follow-on messages and threats directly to the population at large, even though the terrorist group may be totally impotent. In effect, the Internet allows a person or group to appear to be larger or more important or threatening than they really are.[36]

A terrifying example is the way in which Pakistani captors used the Internet to entrap Jewish-American reporter Daniel Pearl through false e-mail communications, kidnapped and murdered him, and then posted the gruesome video on the Internet. This pattern was later repeated by Abu Mussab al Zarqawi and the insurgents in Iraq who beheaded numerous hostages and posted the videotaped executions online.

Practical Uses of the Internet by Terrorists

In addition to communicative uses of the Internet, terrorists use the medium for instrumental purposes. The Internet may serve terrorists as an excellent source of useful information. 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 the schedules and locations of targets such as transportation facilities, nuclear power plants, public buildings, and airports and ports. They can even learn of counterterrorism measures taken in these places. Dan Verton, in his book *Black Ice: The Invisible Threat of Cyberterrorism*, 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.[37]

Numerous tools are available to facilitate such data collection, often called

[36] Thomas, *Al Qaeda and the Internet*, *supra* note 12, at 112–23.

[37] DAN VERTON, BLACK ICE: THE INVISIBLE THREAT OF CYBER-TERRORISM 109 (2003).

datamining, including search engines, e-mail distribution lists, chat rooms, and discussion groups. Many web sites offer their own search tools for extracting information from databases on their sites. Word searches of online newspapers and journals can likewise generate useful information for 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. According to former Secretary of Defense Donald Rumsfeld, 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."

"Without recruitment terrorism cannot prevail, survive, and develop. Recruitment provides the killers, the suicide bombers, the kidnappers, the executioners, the engineers, and the soldiers—the armies of future terrorism. The Internet has become a useful instrument for modern terrorists' recruitment."[38] The Internet combines several advantages for the recruiters: it makes information gathering easier for potential recruits by offering more information, more quickly, and in multimedia format. The global reach of the Internet allows groups to publicize events to more people; and, by increasing the possibilities for interactive communication, the Internet offers new opportunities for assisting groups, along with more chances for contacting the group directly. Online recruitment by terrorist organizations is said to be widespread, though the Internet is used more for initial attraction, ideological recruitment, and social support than for direct recruitment. Moreover, the online process is more often activated to reward recruits and suicide terrorists, thus serving as an additional indirect recruitment initiative. Finally, terrorist recruiters may use interactive Internet technology to roam online chat rooms to look for receptive members of the public

[38] Gabriel Weimann, *Terrorist Dot Com: Using the Internet for Terrorist Recruitment and Mobilization*, *in* THE MAKING OF A TERRORIST 53–65 (James J.F. Forest ed., 2006).

(particularly young people) using sophisticated profiling procedures.

Terrorists use the Internet to set up and activate virtual training camps; they use online communications to provide information to fellow terrorists, including maps, photographs, directions, codes, and technical details of how to use explosives.[39] The Net 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 of how to construct a wide range of bombs. Another manual, *The Mujahadeen Poisons Handbook*, written by Abdel-Aziz and published on the official Hamas web site, details in twenty-three pages how to prepare various homemade poisons, poisonous gases, and other deadly materials for use in terrorist attacks.

Terrorists use the Internet not only to learn how to build bombs and use arms, but also to plan and coordinate specific attacks. Al Qaeda operatives relied heavily on the Internet in planning and coordinating the September 11 attacks. Federal officials found thousands of encrypted messages that had been posted in a password-protected area of a web site on the computer of arrested al Qaeda terrorist Abu Zubaydah, who reportedly masterminded the 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. It is often simple to use the Internet in public facilities without being traced or identified; for example, at many public libraries, "hawalas" (storefront money exchanges), or Internet cafes terrorists and their followers can access the Internet without presenting identification.

Finally, 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

[39] Weimann, *Virtual Training Camps*, *supra* note 13, at 119.

fundraising network is built upon a foundation of charities, nongovernmental organizations, and other financial institutions that use web sites and Internet-based chat rooms and forums to solicit and gather funds. 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. According to Thomas, the Internet is also used "to put together profiles"; Internet user demographics (culled, for instance, from personal information entered on online questionnaires and order forms) allow terrorists to identify users who have sympathy for a particular cause or issue.[40] 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).

Cyberterrorism

The threat posed by cyberterrorism has grabbed the attention of the mass media, the security community, and the information technology industry. Journalists, politicians, and experts in a variety of fields have popularized a scenario in which sophisticated cyberterrorists electronically break into computers that control dams or air traffic control systems, thus wreaking havoc and endangering not only millions of lives, but national security itself. Because most critical infrastructure in Western societies is networked through computers, the potential threat from cyberterrorism is, to be sure, very alarming. Hackers, although not motivated by the same goals that inspire terrorists, have demonstrated that individuals can gain access to sensitive information and to the operation of crucial services. At least in theory, terrorists could thus follow the hackers' lead and then, having broken into government and private computer systems, cripple or disable the military, financial, and service sectors of advanced economies. The growing dependence of our societies on

[40] Thomas, *Al Qaeda and the Internet*, *supra* note 12, at 112–123.

information technology has created a new form of vulnerability by giving terrorists the chance to approach targets that would otherwise be utterly unassailable, such as national defense systems and air traffic control systems. The more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructure.

What should be considered as cyberterrorism? Dorothy Denning has put forward an unambiguous definition in numerous articles:

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against crucial infrastructures could count as acts of cyberterrorism, depending on their impact. Attacks that disrupt non-essential services or that are mainly a costly nuisance would not.[41]

It is important to distinguish between cyberterrorism, hacking, and "hacktivism"—a term coined by scholars to describe the marriage of hacking and political activism. Hacktivism, although politically motivated, does not constitute cyberterrorism. Hacktivists want to protest and disrupt; they do not want to kill, maim, or terrorize. However, hacktivism does highlight the threat of cyberterrorism: individuals with no moral restraint may potentially use methods similar to those developed by hackers to wreak havoc. Moreover, the line between cyberterrorism and hacking or hacktivism may sometimes blur, especially if terrorist groups are able to recruit or hire computer-savvy hacktivists or if hacktivists decide to escalate their actions by attacking the systems that operate critical elements of the national

[41] Dorothy E. Denning, *Cyberterrorism: The Logic Bomb Versus the Truck Bomb*, GLOBAL DIALOGUE (Autumn 2000), http://www.worlddialogue.org/content.php?id=111; Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, *in* NETWORKS AND NETWARS 239, 281 (John Arquilla & David Ronfeldt eds., 2001); Dorothy E. Denning, *Is Cyber Terror Next?*, *in* UNDERSTANDING SEPTEMBER 11 (Craig Calhoun et al. eds., 2002).

infrastructure, such as electric power networks and emergency services.

Why are hackers seen as threatening, and why are they often associated with terrorism? Because hackers themselves like to exaggerate their abilities. Douglas Thomas, a professor at the University of Southern California, spent seven years studying computer hackers in an effort to understand better who they are and what motivates them. According to Thomas,

> Hacking stories make good copy, but they are very rarely accurate, tending to exaggerate threats and downplay the realities of the event. There is a big difference between hacking into NASA's central control system (which has *not* happened) and hacking into the server that hosts their web page (which has happened repeatedly). Most media reports fail to distinguish between the two (or to explain that hacking a web page is essentially the same as spray painting a billboard, posing very little actual risk).[42]

How real is the threat of cyberterrorism? Cyberterrorism conjures up images of vicious terrorists unleashing catastrophic attacks against computer networks, wreaking havoc, and paralyzing nations. This is a frightening scenario—but how likely is it to occur? Could terrorists cripple critical military, financial, and service computer systems? The vulnerability of the energy industry is at the heart of *Black Ice: The Invisible Threat of Cyber-Terror*, in which Verton, a former intelligence officer, argues that America's energy sector would be the first domino to fall in a strategic cyberterrorist attack against the United States.[43] Verton explores in frightening detail how the impact of such an attack could rival, or even exceed, the consequences of a more traditional physical attack. He claims that during any given year, the average, large, utility company experiences about one million cyberintrusions that require investigation to ensure that critical system components have not been compromised.

---

[42] *Cyberterrorism: Is the Nation's Critical Infrastructure Adequately Protected?: Hearing Before the Subcomm. on Gov't Efficiency, Fin. Mgmt. and Intergovernmental Relations of the H. Comm. on Gov't Reform*, 107th Cong. 14 (2002) (statement of Douglas Thomas, Associate Professor, Annenberg School for Communication).

[43] VERTON, *supra* note 37, at 38.

Amid all the dire warnings and alarming statistics that the cyberterrorism generates, it is important to remember one simple statistic: so far, there have been no recorded instance of a terrorist cyberattack on U.S. public facilities, transportation systems, nuclear power plants, power grids, or other key components of the national infrastructure. Cyberattacks are common, but they have not been conducted by terrorists, and they have not sought to inflict the kind of damage that would qualify them as cyberterrorism. As Joshua Green reports in *The Myth of Cyberterrorism*, "When U.S. troops recovered al Qaeda laptops in Afghanistan, officials were surprised to find its members more technologically adept than previously believed."[44] Officials discovered structural and engineering software, electronic models of a dam, and information on computerized water systems, nuclear power plants, and U.S. and European stadiums. But the evidence uncovered did *not* suggest that al Qaeda operatives were planning cyberattacks, only that they were using the Internet to communicate and coordinate physical attacks. Neither al Qaeda nor any other terrorist organization has tried to stage a serious cyberattack.

As Denning concludes, "At least for now, hijacked vehicles, truck bombs, and biological weapons seem to pose a greater threat than cyber terrorism. However, just as the events of September 11 caught us by surprise, so could a major cyber assault. We cannot afford to shrug off the threat."[45] There is growing evidence that modern terrorists seriously consider adding cyberterrorism to their arsenal. Verton, for example, argues that "al Qaeda has shown itself to have an incessant appetite for modern technology," and provides numerous quotes from bin Laden and other al Qaeda leaders that show their recognition of this new cyberweapon.[46] Paradoxically, success in the war on terror is likely to make

[44] Joshua Green, *The Myth of Cyberterrorism*, WASH. MONTHLY, Nov. 2002, at 8.

[45] Denning, *Is Cyber Terror Next?*, *supra* note 41.

[46] VERTON, *supra* note 37, at 93.

terrorists turn increasingly to unconventional weapons such as cyberterrorism.

Future terrorists may indeed find more possibilities for cyberterrorism than do the terrorists of today. Furthermore, the next generation of terrorists are now growing up in a digital world, one in which hacking tools are sure to become more powerful, simpler to use, and easier to access.[47] The notion of "coupled" attacks, or of the use of "magnifiers" (combining conventional strikes and cyberattacks) is most alarming For instance, a terrorist group might simultaneously explode a bomb at a train station and launch a cyberattack on the communications infrastructure, thus compounding the destructive impact of the event. The challenge before us is to assess what needs to be done to address this ambiguous but potential threat of cyberterrorism, but to do so without inflating its real significance and without manipulating the fear it inspires.

The Challenge: Online Counterterrorism

Counterterrorism on the Internet certainly lingers behind the terrorists' manipulative use of this medium. Given the growth of Internet research in recent years, it is rather surprising that research of online countermeasures has been overlooked or at least has not provided efficient strategy, fruitful devices, or tactics. Several factors combine to explain this gap: "(a) difficulties in tracking and tracing cyber communications, (b) the lack of globally-accepted processes and procedures for the investigation and prevention of cyber[terrorism], and (c) inadequate or ineffective information sharing systems between the public and private sectors," between governments, and between counterterrorism agencies.[48]

But the technological reasons for the lack of online countermeasures are marginal when compared with the legal problems. Responding to terrorist web sites is an extremely sensitive and delicate issue, because most of the rhetoric disseminated on the Internet is

[47] ROGAN, *supra* note 26, at 32.

[48] Jody R. Westby, *Countering Terrorism with Cyber Security*, 47 JURIMETRICS 297, 297–300 (2007).

considered protected speech under the First Amendment. The case of “Carnivore” may illustrate the problematic state of online countermeasures. In February 1998, Attorney General Janet Reno unveiled plans to establish a new FBI command center to fight cyberattacks on the nation’s critical computer networks. In October 2001, the U.S. House of Representatives approved an antiterrorism bill that gave law enforcement officials expanded surveillance powers to monitor Internet behavior and email. After the September 11 attacks, FBI agents were already visiting the offices of Internet service providers (ISPs), network providers, and email vendors around the country in search of those who perpetrated the attacks. The FBI used the controversial e-mail surveillance system “Carnivore” to conduct those investigations. The system forces ISPs to attach a black box, essentially a powerful computer running specialized software, to their networks, through which all of the ISPs’ subscribers’ communications flow. In traditional wiretaps, the government is required to minimize its interception of non-incriminating or innocent communications, but “Carnivore” does just the opposite, by scanning through tens of millions of e-mails and other communications from innocent Internet users as well as those targeted suspects. ISP networks being subjected to Carnivore is like telephone companies being forced to give the FBI access to all calls on its network when the FBI has permission only to seek calls for one subscriber. “Carnivore” can be configured to do one of several things. It can record all of the e-mail messages sent to and from a specific e-mail account. It can record all of the network traffic to and from a specific IP address. It can record all of the email headers (i.e., TO and FROM addresses) sent to and from a specific email account. It can record all of the servers, webpages, or FTP files visited by a particular IP address. Finally, it can track all users who access a particular webpage or FTP file. When the FBI’s use of “Carnivore” was revealed in July 2000, members of Congress expressed concern, and stated their intent to examine the issues and draft appropriate legislation. Because “Carnivore” provides the FBI with access to

communications of all monitored ISP subscribers, not just those of the court-designated target, it raises substantial privacy issues for millions of Internet users.

The virtual war between terrorists and counterterrorism forces and agencies is certainly vital, dynamic, and ferocious. The National Security Agency, the CIA, the FBI, the Defense Intelligence Agency, other U.S. and foreign intelligence agencies, and some private contractors, are fighting back by cracking terrorist passwords, monitoring suspicious web sites, cyberattacking other sites, and planting bogus information. However, there could be better ways to counter the threat: "The government efforts are inadequate. The private sector is doing a better job than the government. Our enemies have embraced the Internet. We have to ask how closely the government is monitoring it."[49]

This is not the place to discuss a definitive answer to terrorist exploitation of the Internet, but two conclusions are to be stated. First, we must become better informed about the uses to which terrorists put the Internet, and we must become better able to monitor their activities. "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."[50] 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 to monitor terrorist activities on the Internet, and to explore measures to limit the usability of this medium by modern terrorists.

Second, while clearly we must better defend our societies against terrorism, in the process, we must not 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

[49] Les Blumenthal, *U.S. Seeks to Counter Terrorists' Use of the Internet*, KANSAS CITY STAR, Sept. 23, 2007, at A23.

[50] WEIMANN, WWW.TERROR.NET, *supra* note 12, at 11.

ideals of free speech and open communication; it is a marketplace of ideas unlike any marketplace that has existed before. Unfortunately, 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 hand the terrorists a victory, and deal democracy a blow. The use of advanced techniques to monitor, search, track, and analyze communications carries inherent dangers. Although such technologies might prove very helpful in the fight against cyberterrorism and against Internet-savvy terrorists, they might also hand governments—especially authoritarian governments and agencies with little public accountability—tools with which to violate civil liberties domestically and abroad. It does not take much imagination to recognize that the long-term implications of giving governments these tools could be profound and damaging for democracies and their values and could add a heavy price in terms of diminished civil liberties to the high toll exacted by terrorism itself.