Al Qaeda and the Internet: The Danger of "Cyberplanning"

TIMOTHY L. THOMAS

We can say with some certainty, al Qaeda loves the Internet. When the latter first appeared, it 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 "global village." Today the Internet still offers that promise, but it also has proven in some respects to be a digital menace. Its use by al Qaeda is only one example. It also has provided a virtual battlefield for peacetime hostilities between Taiwan and China, Israel and Palestine, Pakistan and India, and China and the United States (during both the war over Kosovo and in the aftermath of the collision between the Navy EP-3 aircraft and Chinese MiG). In times of actual conflict, the Internet was used as a virtual battleground between NATO's coalition forces and elements of the Serbian population. These real tensions from a virtual interface involved not only nation-states but also non-state individuals and groups either aligned with one side or the other, or acting independently.

Evidence strongly suggests that terrorists used the Internet to plan their operations for 9/11. Computers seized in Afghanistan reportedly revealed that al Qaeda was collecting intelligence on targets and sending encrypted messages via the Internet. As recently as 16 September 2002, al Qaeda cells operating in America reportedly were using Internet-based phone services to communicate with cells overseas. These incidents indicate that the Internet is being used as a "cyberplanning" tool for terrorists. It provides terrorists with anonymity, command and control resources, and a host of other measures to coordinate and integrate attack options.

Cyberplanning may be a more important terrorist Internet tool than the much touted and feared cyberterrorism option—attacks against information and systems resulting in violence against noncombatant targets. The Naval Postgrad-

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Al Qaeda and the Internet: The Danger of 'Cyberplanning'	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,122 Forbes Avenue,Carlisle,PA,17013-5244**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Parameters, US Army War College Quarterly, Spring 2003, Vol 33, No. 1

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**12**	

uate School (NPS) has defined cyberterrorism as the unlawful destruction or disruption of digital property to intimidate or coerce people.[1] Cyberplanning, not defined by NPS or any other source, refers to the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed. It can include cyberterrorism as part of the overall plan. Since 9/11, US sources have monitored several websites linked to al Qaeda that appear to contain elements of cyberplanning:

- alneda.com, which US officials said contained encrypted information to direct al Qaeda members to more secure sites, featured international news on al Qaeda, and published articles, fatwas (decisions on applying Muslim law), and books.
- assam.com, believed to be linked to al Qaeda (originally hosted by the Scranton company BurstNET Technologies, Inc.), served as a mouthpiece for jihad in Afghanistan, Chechnya, and Palestine.
- almuhrajiroun.com, an al Qaeda site which urged sympathizers to assassinate Pakistani President Musharraf.
- qassam.net, reportedly linked to Hamas.
- jihadunspun.net, which offered a 36-minute video of Osama bin Laden.[2]
- 7hj.7hj.com, which aimed to teach visitors how to conduct computer attacks.[3]
- aloswa.org, which featured quotes from bin Laden tapes, religious legal rulings that "justified" the terrorist attacks, and support for the al Qaeda cause.[4]
- drasat.com, run by the Islamic Studies and Research Center (which some allege is a fake center), and reported to be the most credible of dozens of Islamist sites posting al Qaeda news.
- jehad.net, alsaha.com, and islammemo.com, alleged to have posted al Qaeda statements on their websites.
- mwhoob.net and aljehad.online, alleged to have flashed political-religious songs, with pictures of persecuted Muslims, to denounce US policy and Arab leaders, notably Saudi.[5]

While it is prudent to tally the Internet cyberplanning applications that support terrorists, it must be underscored that few if any of these measures are really anything new. Any hacker or legitimate web user can employ many of these

---

Lieutenant Colonel Timothy L. Thomas, USA Ret., is an analyst at the Foreign Military Studies Office, Fort Leavenworth, Kansas. He has written extensively on information operations, combat in cities, and peacekeeping operations, among other issues, including four previous articles for *Parameters*. During his military career he served in the 82d Airborne Division and was the Department Head of Soviet Military-Political Affairs at the US Army's Russian Institute in Garmisch, Germany.

---

same measures for their own purposes, for business, or even for advertising endeavors. The difference, of course, is that most of the people on the net, even if they have the capabilities, do not harbor the intent to do harm as does a terrorist or al Qaeda member.

Highlighting several of the more important applications may help attract attention to terrorist methodologies and enable law enforcement agencies to recognize where and what to look for on the net. Sixteen measures are listed below for consideration. More could be added.

- *The Internet can be used to put together profiles*. Internet user demographics allow terrorists to target users with sympathy toward a cause or issue, and to solicit donations if the right "profile" is found. Usually a front group will perform the fundraising for the terrorist, often unwittingly. E-mail fundraising has the potential to significantly assist a terrorist's publicity objectives and finances simultaneously.[6]

Word searches of online newspapers and journals allow a terrorist to construct a profile of the means designed to counter his actions, or a profile of admitted vulnerabilities in our systems. For example, recent articles reported on attempts to slip contraband items through security checkpoints. One report noted that at Cincinnati's airport, contraband slipped through over 50 percent of the time. A simple Internet search by a terrorist would uncover this shortcoming, and offer the terrorist an embarkation point to consider for his or her next operation. A 16 September report noted that US law enforcement agencies were tracing calls made overseas to al Qaeda cells from phone cards, cell phones, phone booths, or Internet-based phone services. Exposing the targeting techniques of law enforcement agencies allows the terrorist to alter his or her operating procedures. The use of profiles by terrorists to uncover such material greatly assists their command and control of operations. The implication is that in a free society such as the United States, you can publish too much information, and while the information might not be sensitive to us, it might be very useful to a terrorist.

- *Internet access can be controlled or its use directed according to the server configuration, thus creating a true ideological weapon*. In the past, if some report was offensive to a government, the content of the report could be censored or filtered. Governments cannot control the Internet to the same degree they could control newspapers and TV. In fact, the Internet can serve as a terrorist's TV or radio station, or his international newspaper or journal. The web allows an uncensored and unfiltered version of events to be broadcast worldwide. Chat rooms, websites, and bulletin boards are largely uncontrolled, with few filters in place. This climate is perfect for an underfunded group to explain its actions or to offset both internal and international condemnation, especially when using specific servers. The Internet can target fence-sitters as well as true believers with different messages, oriented to the target audience.

In the aftermath of the 9/11 attacks, al Qaeda operatives used the Internet to fight for the hearts and minds of the Islamic faithful worldwide. Sev-

eral internationally recognized and respected Muslims who questioned the attacks were described as hypocrites by al Qaeda. Al Qaeda ran two websites, alneda.com and drasat.com, to discuss the legality of the attacks on 9/11. Al Qaeda stated that Islam shares no fundamental values with the West and that Muslims are committed to spread Islam by the sword. As a result of such commentary, several Muslim critics of al Qaeda's policies withdrew their prior condemnation.[7] Ideological warfare worked.

● *The Internet can be used anonymously, or as a shell game to hide identities*. Terrorists have access to Internet tools to create anonymity or disguise their identities. Online encryption services offer encryption keys for some services that are very difficult to break. The website spammimic.com offers tools that hide text in "spam," unsolicited bulk commercial e-mail. Speech compression technology allows users to convert a computer into a secure phone device. Network accounts can be deleted or changed as required. For example, Internet users can create Internet accounts with national firms such as America Online (AOL), or can even create an AOL Instant Messenger (AIM) account on a short-term basis. In addition, anonymous logins are possible for many of the thousands of chat rooms on the net. If desired, the user can access cyber cafes, university and library computers, or additional external resources to further hide the source of the messages.[8] An al Qaeda laptop found in Afghanistan had linked with the French Anonymous Society on several occasions. The site offers a two-volume Sabotage Handbook online.

Not only are anonymous methods available for the people who use the Internet, but at times Internet service providers (ISPs) unwittingly participate in serving people or groups for purposes other than legitimate ones. The al Qaeda web site www.alneda.com was originally located in Malaysia until 13 May. It reappeared in Texas at http://66.34.191.223/ until 13 June, and then reappeared on 21 June at www.drasat.com in Michigan. It was shut down on 25 June 2002. The ISPs hosting it apparently knew nothing about the content of the site or even the fact that it was housed on their servers.[9] This shell game with their website enabled the al Qaeda web to remain functional in spite of repeated efforts to shut it down. Cyber deception campaigns will remain a problem for law enforcement personnel for years to come.

● *The Internet produces an atmosphere of virtual fear or virtual life*. People are afraid of things that are invisible and things they don't understand. The virtual threat of computer attacks appears to be one of those things. Cyberfear is generated by the fact that what a computer attack *could* do (bring down airliners, ruin critical infrastructure, destroy the stock market, reveal Pentagon planning secrets, etc.) is too often associated with what *will* happen. News reports would lead one to believe that hundreds or thousands of people are still active in the al Qaeda network on a daily basis just because al Qaeda says so. 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

"The Internet provides terrorists with anonymity, command and control resources, and a host of other measures to coordinate and integrate attack options."

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.

The Internet can be used to spread disinformation, frightening personal messages, or horrific images of recent activities (one is reminded of the use of the net to replay the murder of reporter Daniel Pearl by his Pakistani captors). Virtually, it appears as though attacks are well planned and controlled, and capabilities are genuine. Messages are usually one-sided, however, and reflect a particular political slant. There is often little chance to check the story and find out if it is mere bravado or fact. The Internet can thus spread rumors and false reports that many people, until further examination, regard as facts.

Recently, the Arab TV station al-Jazeera has played tape recordings of bin Laden's speeches and displayed a note purportedly signed by him praising attacks on an oil tanker near Yemen, and on US soldiers participating in a war game in Kuwait. These messages were picked up and spread around the Internet, offering virtual proof that bin Laden was alive. Most likely bin Laden was seriously injured (which is why we haven't seen him in over a year), but his image can be manipulated through radio or Internet broadcasts so that he appears confident, even healthy.

- *The Internet can help a poorly funded group to raise money.* Al Qaeda has used Islamic humanitarian "charities" to raise money for jihad against the perceived enemies of Islam. Analysts found al Qaeda and humanitarian relief agencies using the same bank account numbers on numerous occasions. As a result, several US-based Islamic charities were shut down.[10] The Sunni extremist group Hizb al-Tahrir uses an integrated web of Internet sites from Europe to Africa to call for the return of an Islamic caliphate. The website states that it desires to do so by peaceful means. Supporters are encouraged to assist the effort by monetary support, scholarly verdicts, and encouraging others to support jihad. Bank information, including account numbers, is provided on a German

site, www.explizit-islam.de.[11] Portals specializing in the anonymous transfer of money, or portals providing services popular with terrorists (such as the issue of new identities and official passports) are also available.[12]

The fighters in the Russian breakaway republic of Chechnya have used the Internet to publicize banks and bank account numbers to which sympathizers can contribute. One of these Chechen bank accounts is located in Sacramento, California, according to a Chechen website known as amina.com.

Of course, there are other ways to obtain money for a cause via the Internet. One of the most common ways is credit card fraud. Jean-Francois Ricard, one of France's top anti-terrorism investigators, noted that many Islamist terror plots in Europe and North America were financed through such criminal activity.[13]

● *The Internet is an outstanding command and control mechanism*. Command and control, from a US military point of view, involves the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Personnel, equipment, communications, facilities, and procedures accomplish command and control by assisting in planning, directing, coordinating, and controlling forces and operations in the accomplishment of a mission.

Command and control on the Internet is not hindered by geographical distance, or by lack of sophisticated communications equipment. Antigovernment groups present at the G8 conference in Cologne used the Internet to attack computers of financial centers and to coordinate protests from locations as distant as Indonesia and Canada. Terrorists can use their front organizations to coordinate such attacks, to flood a key institution's e-mail service (sometimes as a diversionary tactic for another attack), or to send hidden messages that coordinate and plan future operations.

The average citizen, the antigovernment protester, and the terrorist now have access to command and control means, limited though they may be, to coordinate and plan attacks. Further, there are "cracking" tools available to detect security flaws in systems and try to exploit them. Attaining access to a site allows the hacker or planner to command and control assets (forces or electrons) that are not his. The Internet's potential for command and control can vastly improve an organization's effectiveness if it does not have a dedicated command and control establishment, especially in the propaganda and internal coordination areas. Finally, command and control can be accomplished via the Internet's chat rooms. One website, alneda.com, has supported al Qaeda's effort to disperse its forces and enable them to operate independently, providing leadership via strategic guidance, theological arguments, and moral inspiration. The site also published a list of the names and home phone numbers of 84 al Qaeda fighters captured in Pakistan after escaping from Afghanistan. The aim presumably was to allow sympathizers to contact their families and let them know they were alive.[14]

● *The Internet is a recruiting tool*. The web allows the user complete control over content, and eliminates the need to rely on journalists for publicity.

Individuals with sympathy for a cause can be converted by the images and messages of terrorist organizations, and the addition of digital video has reinforced this ability. Images and video clips are tools of empowerment for terrorists. More important, net access to such products provides contact points for men and women to enroll in the cause, whatever it may be.[15] Additionally,

> Current versions of web browsers, including Netscape and Internet Explorer, support JavaScript functions allowing Internet servers to know which language is set as the default for a particular client's computer. Hence, a browser set to use English as the default language can be redirected to a site optimized for publicity aimed at Western audiences, while one set to use Arabic as the default can be redirected to a different site tailored toward Arab or Muslim sensibilities.[16]

This allows recruiting to be audience- and language-specific, enabling the web to serve as a recruiter of talent for a terrorist cause. Recently, the Chechen website qoqaz.net, which used to be aimed strictly against Russian forces operating in Chechnya, changed its address to assam.com, and now includes links to Jihad in Afghanistan, Jihad in Palestine, and Jihad in Chechnya. Such sites give the impression that the entire Islamic world is uniting against the West, when in fact the site may be the work of just a few individuals.

- *The Internet is used to gather information on potential targets*. The website operated by the Muslim Hackers Club reportedly featured links to US sites that purport to disclose sensitive information like code names and radio frequencies used by the US Secret Service. The same website offers tutorials in viruses, hacking stratagems, network "phreaking" and secret codes, as well as links to other militant Islamic and cyberprankster web addresses.[17] Recent targets that terrorists 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.[18] Attacks on critical infrastructure control systems would be particularly harmful, especially on a system such as the Supervisory Control and Data Acquisition (SCADA) system. Thus any information on insecure network architectures or non-enforceable security protocols is potentially very damaging.

Terrorists have access, like many Americans, to imaging data on potential targets, as well as maps, diagrams, and other crucial data on important facilities or networks. Imaging data can also allow terrorists to view counterterrorist activities at a target site. One captured al Qaeda computer contained engineering and structural architecture features of a dam, enabling al Qaeda engineers and planners to simulate catastrophic failures.[19]

With regard to gathering information through the Internet, on 15 January 2003 Defense Secretary Donald Rumsfeld observed that an al Qaeda training manual recovered in Afghanistan said, "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."[20]

● *The Internet puts distance between those planning the attack and their targets*. Terrorists planning attacks on the United States can do so abroad with limited risk, especially if their command and control sites are located in countries other than their own. Tracing the route of their activity is particularly difficult. The net provides terrorists a place to plan without the risks normally associated with cell or satellite phones.

● *The Internet can be used to steal information or manipulate data*. Ronald Dick, Director of the FBI's National Infrastructure Protection Center, considers the theft or manipulation of data by terrorist groups as his worst nightmare, especially if the attacks are integrated with a physical attack such as on a US power grid.[21] Richard Clark, Chairman of the President's Critical Infrastructure Protection Board, said the problem of cybersecurity and data protection had its own 9/11 on 18 September 2001 when the Nimda virus spread through Internet-connected computers around the world, causing billions of dollars of damage. Nimda's creator has never been identified. This virus, hardly noticed in the wake of the airliner attacks and anthrax scares, set off a chain reaction among software companies (including Microsoft) to get very serious about plugging vulnerabilities.[22] In the fall of 2001 a number of unexplained intrusions began occurring against Silicon Valley computers. An FBI investigation traced the intrusions to telecommunication switches in Saudi Arabia, Indonesia, and Pakistan. While none was directly linked to al Qaeda, there remain strong suspicions that the group was somehow involved.[23]

● *The Internet can be used to send hidden messages*. The practice of steganography, which involves hiding messages inside graphic files, is a widespread art among criminal and terrorist elements. Hidden pages or nonsensical phrases can be coded instructions for al Qaeda operatives and supporters. One recent report noted,

> Al Qaeda uses prearranged phrases and symbols to direct its agents. An icon of an AK-47 can appear next to a photo of Osama bin Laden facing one direction one day, and another direction the next. The color of icons can change as well. Messages can be hidden on pages inside sites with no links to them, or placed openly in chat rooms.[24]

In addition, it is possible to buy encryption software for less than $15. Cyberplanners gain an advantage in hiding their messages via encryption. Sometimes the messages are not even hidden in a sophisticated manner. Al-Jazeera television reported that Mohammed Atta's final message (another advantage of the Internet—the impossibility of checking sources) to direct the attacks on the Twin Towers was simple and open. The message purportedly said, "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."[25] The reference to the various faculties was apparently the code for the buildings targeted in the attacks.

● *The Internet allows groups with few resources to offset even some huge propaganda machines in advanced countries*. The web is an attractive device to those looking for a way to attack major powers via the mass media. The "always on" status of the web allows these individuals not only to access sites day and night but also to scold major powers and treat them with disdain in a public forum. The web can be used to counter facts and logic with the logic of the terrorist. There is no need for the terrorist organization to worry about "the truth," because ignoring facts is a standard operating procedure.

Al Qaeda uses polemics on the net not only to offset Western reporting, but also to counter Muslims who don't toe the party line. It defends the conduct of its war against the West and encourages violence. The web is important to al Qaeda because it can be used to enrage people and neutralize moderate opinion. The website of the Center for Islamic Studies and Research (according to one source, a made-up name), for example, has 11 sections, including reports on fighting in Afghanistan, world media coverage of the conflict, books on jihad theology, videos of hijackers' testaments, information about prisoners held in Pakistan and Guantanamo Bay, and jihad poetry.[26]

It does not pay for any major power to lie, as facts can be easily used against them. Even in the war in Chechnya, there were times when the Chechens would report a successful ambush of a Russian convoy, and the Russians would deny the event ever happened. To prove their point, the Chechens would show video footage of the ambush on the Internet, thus offsetting the credibility of the Russian official media and undercutting the power of their massive propaganda machine. Al Qaeda officials are waiting to do the same to Western media reporting if the opportunity presents itself.

● *The Internet can be used to disrupt business*. This tactic requires precise timing and intimate knowledge of the business climate in the target country. It attempts to harm businesses by accusing them of guilt by association.

Hizbullah, for example, has outlined a strategy to cripple Israeli government, military, and business sites with the aim of disrupting normal economic and societal operations. Phase one might be to disable official Israeli government sites; phase two might focus on crashing financial sites such as those on the Israeli stock exchange; phase three might involve knocking out the main Israeli internet servers; and phase four might blitz Israeli e-commerce sites to ensure the loss of hundreds of transactions.[27] A final phase could be to accuse companies that do business with a target government as guilty by association and call for a boycott of the firm's products. Arab terrorists attacked Lucent Technologies in a round of Israeli-Arab cyber skirmishes, for example.[28] All of these plans require insider knowledge in order to carry out the operation in a timely and accurate manner.

● *The Internet can mobilize a group or diaspora, or other hackers to action*. Websites are not only used to disseminate information and propaganda. They also are used to create solidarity and brotherhood among groups. In the case

"The Internet allows a person or group to appear to be larger or more important or threatening than they really are."

of Islamist terrorist organizations, the Internet substitutes for the loss of bases and territory. In this respect the most important sites are alneda.com, jehad.net, drasat.com, and aloswa.org, which feature quotes from bin Laden tapes, religious legal rulings that justify the terrorist attacks, and support for the al Qaeda cause.[29] In addition, website operators have established a site that is "a kind of database or encyclopedia for the dissemination of computer viruses."[30] The site is 7hj.7hj.com, and it aims to teach Internet users how to conduct computer attacks, purportedly in the service of Islam.[31]

- *The Internet takes advantage of legal norms*. Non-state actors or terrorists using the Internet can ignore Western notions of law and focus instead on cultural or religious norms. At a minimum, they ignore legal protocols on the Internet. In addition, they use the net to break the law (when they hack websites or send out viruses) while at the same time the law protects them (from unlawful surveillance, etc.).

International investigations into such behavior are difficult to conclude due to the slow pace of other nations' investigative mechanisms, and the limited time that data is stored.[32] However, in the aftermath of the events of 9/11 in the United States, the terrorists' actions actually initiated several changes in the US legal system that were not to the terrorists' advantage. For example, in the past, the privacy concerns of Internet users were a paramount consideration by the US government. After 9/11, new legislation was enacted.

The controversial USA Patriot Act of 2001 included new field guidance relating to computer crime and electronic evidence. The Patriot Act is designed to unite and strengthen the United States by providing the appropriate tools required to intercept and obstruct terrorism. It establishes a counterterrorism fund in the Treasury Department, amends federal criminal code that authorizes enhanced surveillance procedures, provides guidelines for investigating money-laundering concerns, removes obstacles to investigating terrorism (granting the FBI authority to investigate fraud and computer-related activity for specific cases), and strengthens criminal laws against terrorism.[33]

The "Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001" provides the authority to do several things. Authorizations include: intercepting voice commu-

nications in computer hacking investigations; allowing law enforcement to trace communications on the Internet and other computer networks within the pen register and trap and trace statute ("pen/trap" statute); intercepting communications of computer trespassers; writing nationwide search warrants for e-mail; and deterring and preventing cyberterrorism. The latter provision raises the maximum penalty for hackers that damage protected computers (and eliminates minimums); states that hackers need only show intent to cause damage, not a particular consequence or degree of damage; provides for the aggregation of damage caused by a hacker's entire course of conduct; creates a new offense for damaging computers used for national security and criminal justice; expands the definition of a "protected computer" to include computers in foreign countries; counts prior state convictions of computer crime as prior offenses; and defines computer "loss." In addition, the guidance develops and supports cyber-security forensic capabilities.[34]

- *The Internet can be used to divert attention from a real attack scenario.* Al Qaeda can plant threats on the Internet or via cell phones to mislead law enforcement officials. Terrorists study how the United States collects and analyzes information, and thus how we respond to information.

Terrorists know when their Internet "chatter" or use of telecommunications increases, US officials issue warnings. Terrorists can thus introduce false information into a net via routine means, measure the response it garners from the US intelligence community, and then try to figure out where the leaks are in their systems or what type of technology the United States is using to uncover their plans. For example, if terrorists use encrypted messages over cell phones to discuss a fake operation against, say, the Golden Gate Bridge, they can then sit back and watch to see if law enforcement agencies issue warnings regarding that particular landmark. If they do, then the terrorists know their communications are being listened to by US officials.[35]

In conclusion, it should be reiterated that cyberplanning is as important a concept as cyberterrorism, and perhaps even more so. Terrorists won't have an easy time shutting down the Internet. Vulnerabilities are continuously reported and fixed while computers function without serious interference (at least in the United States). One hopes that law enforcement and government officials will focus more efforts on the cyberplanning capabilities of terrorists in order to thwart computer attacks and other terrorist activities. At a minimum, America can use such measures to make terrorist activities much harder to coordinate and control. Paul Eedle, writing in *The Guardian*, summed up the value of the Internet to al Qaeda:

> Whether bin Ladin or al Qaeda's Egyptian theorist Ayman al-Zawahiri and their colleagues are on a mountain in the Hindu Kush or living with their beards shaved off in a suburb of Karachi no longer matters to the organization. They can inspire

and guide a worldwide movement without physically meeting their followers—without knowing who they are.[36]

Such is the power and the danger of cyberplanning.

NOTES

1. Patricia Daukantas, "Government Computer News via Infowar.com," 14 December 2001, http://www.infowar.com.

2. Jack Kelley, "Militants Wire Web with Links to Jihad," *USA Today*, 10 July 2002, from *CNO/IO Newsletter*, 8-14 July 2002.

3. Ibid.

4. Yossi Melman, "Virtual Soldiers in a Holy War," *Ha'aretz*, http://www.haaretz.com, 17 September 2002.

5. Habib Trabelsi, "Al-Qaeda Wages Cyber War against US," *Middle East Times*, Dubai, 27 June 2002, rpt. in CNO/IO Newsletter, 1-7 July 2002.

6. Patrick S. Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," unpublished paper, School of Advanced Military Studies, Fort Leavenworth, Kansas, June 2002, p. 20.

7. Paul Eedle, "Al-Qaeda Takes Fight for 'Hearts and Minds' to the Web," *Jane's Intelligence Review*, August 2002, rpt. in CNO/IO Newsletter, 5-11 August 2002.

8. Tibbetts, pp 7, 9.

9. Eedle, "Al-Qaeda Takes Fight."

10. Colin Soloway, Rod Nordland, and Barbie Nadeau, "Hiding (and Seeking) Messages on the Web," *Newsweek*, 17 June 2002, p. 8.

11. "Sunni Extremist Group Hizb al-Tahrir Promotes Ideology on the Internet," FBIS, http://199.221.15.211, 5 February 2002.

12. C. E. Manin, "Terrorism and Information Communication Technology," *La Tribune*, College Interarmees de Defense, April 2002, p. 112.

13. Michael Elliot, "Reeling Them In," *Time*, 23 September 2002, p. 33.

14. Paul Eedle, "Terrorism.com," *The Guardian*, 17 July 2002, downloaded from the FBIS website on 17 July 2002.

15. Tibbetts, p. 37.

16. Ibid., p. 34.

17. Mark Hosenball, "Islamic Cyberterror," *Newsweek*, 20 May 2002

18. Tom Squitieri, "Cyberspace Full of Terror Targets," *USA Today*, 5 June 2002.

19. Barton Gellman, "FBI Fears Al-Qaeda Cyber Attacks," *San Francisco Chronicle*, 28 June 2002, pp. 1, 10.

20. "Citing Al Qaeda Manual, Rumsfeld Re-Emphasizes Web Security," *InsideDefense.com*, http://www.insidedefense.com/, 15 January 2003.

21. Gellman, pp. 1, 10.

22. John Schwartz, "Despite 9/11 Warnings, Cyberspace Still at Risk," *The Post Standard* (Syracuse, N.Y.), 11 September 2002, pp. D-10, 11.

23. Maria T. Welch, "Accumulating Digital Evidence is Difficult," *The Post Standard*, 11 September 2002, pp. D-9, 11.

24. Ibid.; also Soloway, Nordland, and Nadeau.

25. Melman.

26. Eedle, "Terrorism.com."

27. Giles Trendle, "Cyberwars: The Coming Arab E-Jihad," *The Middle East*, No. 322 (April 2002), p. 6.

28. Tim McDonald, "Fanatics with Laptops: The Coming Cyber War," *NewsFactor.com* via *Yahoo! News*, 16 May 2002.

29. Melman.

30. Ibid.

31. Ibid.

32. Manin, p. 112.

33. See "Bill Summary & Status for the 107th Congress," http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:@@@L&summ2=m&.

34. See "Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001," http://www.cybercrime.gov/PatriotAct.htm.

35. John Diamond, "Al-Qaeda Steers Clear of NSA's Ears," *USA Today*, 17 October 2002, *CNO/IO Newsletter*, 23-30 October 2002, pp. 17-18.

36. Eedle, "Terrorism.com."