Information Operations and Terrorism

Dorothy E. Denning

August 18, 2005

INTRODUCTION

The term "terrorism" generally refers to physical acts of violence intended to inculcate fear. It conjures up images of bombs exploding, bodies mutilated, and innocent lives lost. Behind the physical assaults, however, is another dimension of terrorism. It is the information dimension, and terrorists exploit it every bit as much as the physical. Their ultimate goal goes beyond the death and destruction they leave behind. It is power and influence. Terrorists seek a change, and their objective is to influence populations in ways that support that change. To do that, they engage in both physical and information operations, and they integrate those operations together.

The objective of this paper is to explore how terrorists use information operations (IO) to support their physical attacks and broader goals. The paper uses as a framework the components of IO promulgated in U.S. Department of Defense doctrine. While there is no reason to believe that terrorists follow U.S. military doctrine or even anything similar, the doctrine provides a conceptual basis for organizing the discussion.

Most of the discussion focuses on al-Qa'ida and the transnational jihadist movement comprising individuals and groups loosely bound by al-Qa'ida's radical Islamic ideology, but operating independently. The movement is said to consist of dozens of radical Islamic groups, who have been trained and financed by al-Qa'ida or who collaborate with al-Qa'ida. It includes thousands of Muslim militants who have trained together in Afghanistan and elsewhere (now Iraq), and an untold number who have been caught up by bin Laden's worldview.[1]

Two principle types of sources are used. The first is writings by terrorists and their supporters, including books, training manuals, online magazines, and information posted on websites. Where original sources are not in English, translations and summaries are used. The second is reports and analysis of terrorist actions that appear in news stories and scholarly publications. Most of the sources are available online. All are in the public domain. No classified sources were used in this study.

There is little scholarly literature on the topic of how terrorists use the full spectrum of IO capabilities, one exception being a recent article from former students and a colleague at my own institution, the Naval Postgraduate School.[2] While that paper also looks at terrorist IO in terms of the components of IO set forth in U.S. military doctrine, it offers a different perspective than the one offered here. In addition, there are publications that

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 AUG 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Operations and Terrorism	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) **Naval Postgraduate School,Center of Terrorism and Irregular Warfare,Monterey,CA,93943**	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
2005 pre-publication version to appear in Innovative Terrorism in the Information Age: Understanding the Threat of Cyber-Warfare (Lars Nicander and Magnus Ranstorp, eds.), Hurst

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)**	**23**	

address how terrorists use of specific methods of IO, for example, computer network attack.

In the course of this research, I did not encounter any terrorist writings that specifically mention either "information operations" or "information warfare." Many of the writings refer to specific elements of what the Department of Defense (DoD) calls information operations, however, they are not characterized as IO, and the terminology used differs from that used by the DoD. Thus, the view of terrorist IO presented here is based on an interpretation of terrorist writings and reports of their activities rather than any terrorist narrative about IO.

After giving a brief overview of military IO doctrine, the paper examines how terrorists employ the three types of capabilities outlined in that doctrine: core capabilities, supporting capabilities, and related capabilities. Emphasis is on how terrorists are using these capabilities today, not on how they might use them in the future. Emphasis is also on terrorist use of modern technologies, particularly the Internet, in support of these capabilities.

IO AND THE U.S. MILITARY

U.S. military doctrine defines IO as the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision making.[3] Computer network operations comprise computer network attack, defense, and exploit. Supporting capabilities include physical destruction, information assurance, physical security, counterintelligence, counterdeception, and counterpropaganda. Related capabilities consist of public affairs and civil military operations. The capabilities are not entirely disjoint. Information assurance, computer network defense, and operations security, for example, all involve protecting information from adversaries.

IO consists of both offensive and defensive operations. The Army defines offensive IO as the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision makers or to influence others to achieve or promote specific objectives.[4] Offensive IO seeks to create a disparity between the quality of information available to friendly forces and that available to adversaries. This is achieved through operations that destroy, disrupt, degrade, deny, deceive, exploit, or influence information, information systems, and decision making.

Defensive IO is defined as the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems.[5] Defensive IO ensures that friendly forces have access to timely, accurate, and relevant information while denying adversaries the opportunity to affect or exploit friendly information and information systems. This is achieved through operations that protect against, detect, restore after, and respond to adversary threats. All of the IO capabilities can support offensive and defense operations.

IO supports the informational instrument of national power, which along with the diplomatic, military, and economic instruments, serves to shape the security environment. It is employed across the full spectrum of conflict, from peace to crises to war. During peace, IO helps shape the strategic environment or prepare for crisis or war. During crisis, it supports contingency or crisis action plans. During war, it serves to synchronize the information element of combat power with the other elements of combat power.

IO CORE CAPABILITIES

The five IO core capabilities of U.S. military doctrine are psychological operations (PSYOP), military deception, electronic warfare (EW), computer network operations (CNO), and operations security (OPSEC).

Psychological Operations (PSYOP)

Psychological operations are planned operations that convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately to influence the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.[6]

U.S. policy stipulates that PSYOP is to be conducted exclusively by the Department of Defense. Because PSYOP targets foreign audiences, policy also requires that it be synchronized with the International Public Information Program (IPIP), which coordinates the dissemination of truthful information about U.S. foreign policy outside the U.S. Information distributed through IPIP must not be misleading. PSYOP cannot target U.S. audiences and must follow international law, treaties, and U.S. law, especially when conducted offensively.[7]

Although they do not refer to it as PSYOP, terrorists appear to understand and employ psychological operations. In particular, many of their public communications carry a strong psychological element. These messages target two principle groups: 1) supporters and potential supporters in their own geographic or global ethic/religious populations (e.g., Muslims), and 2) populations associated with enemy governments and their allies (e.g., Americans). Messages are distributed through a variety of media, including leaflets, magazines, newspapers, books, audio and video recordings, radio and television stations, and the Internet.

At first glance, it would appear that terrorist PSYOP differs from U.S. PSYOP by targeting local audiences as well as foreign ones. However, this conclusion is not justified for at least two reasons. First, my analysis of terrorist PSYOP is based on my interpretation of certain terrorist messages as containing a psychological component rather than on any categorization of the messages as PSYOP by the terrorists issuing them. If I apply the same lens to all U.S. government communications, I would find numerous messages from the White House and other non-defense agencies with a clear

psychological element that are not labeled as PSYOP. For example, a "100 Days" campaign ad for President Bush was said to be "fraught with a high-voltage emotional charge." Showing an anonymous terrorist in the background, the ad was said to be "designed to appeal to one primal, irreducible emotion: fear."[8]

Second, terrorists send very different messages to their supporters vs. enemy publics. Issue 8 of Al-Qa'ida's online training magazine, *Al-Battar Training Camp,* for example, distinguishes between messages that promote Islam and are positive to the organization from disinformation, which is designed to be detrimental to the enemies of Islam.[9]

Nevertheless, whereas it is difficult to conclude that terrorist PSYOP differs practically from U.S. PSYOP by targeting local audiences, there are substantive differences in the intent and content of their messages. Unlike U.S. messages, which are often designed to bring an end to violence and save lives, terrorist PSYOP is frequently directed toward promoting violence and threatening civilian populations with death and destruction. Suicide bombers are portrayed as martyrs rather than killers of innocent people.

A good example of the violent nature of some terrorist PSYOP is the video showing the beheading of the American civilian Nick Berg in Iraq in May 2004. Before the murder, a masked man reads a statement vowing more killings in revenge for the "Satanic degradation" of Iraqi prisoners at AbuGhraib. He tells scholars of Islam that the time has come to put aside conferences and sermons and "lift the sword," while warning mothers and wives of American soldiers that they "will see nothing from us except corpse after corpse and casket after casket of those slaughtered in this fashion." He ends his speech by calling upon Muslims to "kill the infidels wherever you see them, take them, sanction them, and await them in every place." The man then pushes Berg to the floor and shouts "God is greatest" above his screams as another man saws off his head and holds it up for the camera.[10] The video was subsequently posted on the Internet for anyone to see. Al-Qa'ida terrorists similarly used Paul Johnson's beheading in Saudi Arabia in June 2004 as a propaganda tool, posting a video of the captured aviation engineer on the Internet before the murder, and grisly photos of the brutal slaying after.[11]

The Internet has become particularly popular with al-Qa'ida and other terrorist groups as a means of PSYOP and propaganda. According to Bruce Hoffman, al-Qa'ida's website Alneda.com emphasized three themes: 1) the West is implacably hostile to Islam, 2) the only way to address this threat and the only language the West understands is the logic of violence, and 3) jihad is the only option.[12] The site contained audio and video clips of bin Laden and justification for the September 11 suicide attacks against Americans. Poetry was used to glorify the martyrs and the importance of the struggle against the enemies of Islam.

By some accounts, there are hundreds of jihad websites offering the latest news, images, and slogans of Islamic holy war.[13] Jihad is presented as a mandate for all Muslims. A book titled *The 39 Principles of Jihad* tells Muslims worldwide that they "must obey the Jihad against the infidels." The book was published in 2003 on a website displaying al-Qa'ida's donkey and automatic rifle insignia.[14] It includes elements of PSYOP, such as

the exhortation to take care of the families of the fighters or risk "misfortune and death by the hands of God."

Some of the jihadist PSYOP is specifically directed toward enrolling children in the jihad. A radical Islamic website in the U.K. posted a rap video designed to inspire young people to take up arms against the West. The Investigative Project, a counterterrorist research and investigative center, characterized the video as "undeniably entertaining, as professionally produced as any video you might see on MTV. Consider the irony: radical fundamentalism, sworn to destroy Western culture and beliefs, uses that culture to market its hate."[15]

Hamas and Hizballah use their websites to reach children through cartoons and comic-book style web pages, bedtime stories, and computer games. Children are being taught to hate Jews and Westerners, and to take up arms against them. "The children of stones are the heroes of today and tomorrow," reads the caption on a Hamas site that stresses the glory of death while fighting the Jews.[16] These Internet efforts are part of a much broader PSYOP campaign aimed at indoctrinating Palestinian youth in schools and communities. The educational system is said to inculcate students with Jew hatred through every possible medium.[17] In *The 39 Principles of Jihad*, Muslims are instructed to educate their children "to adore Jihad and the Mujahideen and to prepare themselves mentally for self-sacrifice for the sake of Allah."[18]

Terrorists use PSYOP to discourage their fellow Muslims from helping their enemies. After Saudi Arabia offered rewards up to $1.9 million for information leading to the arrests of suspects in the May and November 2003 suicide bombings, militants published a warning on a radical website: "We are warning anyone who cooperates with the authorities or gives the tyrants information leading to the arrest of one of the mujahideen. He will be liquidated."[19]

Jihadists direct numerous PSYOP messages to enemy populations. The messages attempt to portray the terrorists as powerful and on the side of Allah (God), threatening death and destruction unless the enemy follows the desired path. Following the September 11, 2001 attacks and U.S.-led military operations in Afghanistan, Al-Qa'ida issued a "Message to the American People" on their English-Language website calling on Americans to denounce their Administration and follow Islam, threatening more terror until Americans stop their transgression or "one of us dies."[20]

Al-Qa'ida has exploited the fear of nuclear attacks in their threats against the United States. According to Debka.com, the Milan daily *Il Giornal* ran a story about a video clip in which the terrorist group announced plans to destroy New York in a nuclear blast on or by February 2, 2004.[21] The clip, which was found on an al-Qa'ida affiliated website, was accompanied by the message: "If God wills it, the end of America is near." In support of this ominous threat, al-Qa'ida's No. 2 man, Ayman al-Zawahri, had claimed in a 2001 interview that the terrorist group had purchased suitcase nuclear bombs from former Soviet nuclear scientists in Moscow and Central Asia. Regardless of the veracity of the claims (Russian nuclear officials and experts adamantly denied that terrorists could have

bought Soviet-made nukes[22]), they serve to support al-Qa'ida's goals of portraying power and inciting fear.

A four-page "Message to the Spanish People" showed up on the Yahoo group Global Islamic Media (GIM) three months before the March 11, 2004 train bombings in Madrid. The PSYOP message aims to convince the Spanish to pull their troops out of Iraq and stop supporting the Americans. It attempts to play on humanitarian feelings and raise sympathy towards the Iraqi people, while at the same time threatening attacks if Spain did not comply: "If the Spanish people wishes to save the blood of its sons let them withdraw from Iraq alive before we send them as burned corps to their families, and before they are trodden under the feet of our children who witnessed the Americans treading their fathers."[23]

Although that particular warning had little apparent effect, the fallout from the bombings themselves was more significant. A few days after the horrific attacks, the Spanish people elected a Socialist Prime Minister who declared that Spain's troops would withdraw from Iraq by June. The terrorists rejoiced for bringing about a regime change – a change that was not expected based on earlier polls. However, the change in voter preference may have been motivated by more than just the violence. Despite evidence linking the bombings to jihadists and al-Qa'ida in particular, the former Prime Minister attempted to blame the bombings on the ETA.[24] As a result, he likely lost the public trust just before voters went to the polls.

Because acts of terrorism have profound psychological effects within the information space (namely on the minds of the target population), they could be considered PSYOP within the domain of IO. Emery, Earl, and Buettner take this approach in their analysis of terrorist use of IO.[25] I prefer to view kinetic terrorist attacks as operations that influence their targets psychologically through the use of physical violence rather than information, and hence not as IO. However, I do view the distribution of information, including text, images, audio, and video, that conveys threats of violence, such as the messages to Americans and Spaniards, or depicts acts of violence, such as the Berg video, as IO. Jihadists also make this distinction. In a 50-page report detailing their strategy to achieve a Western military withdrawal from Iraq, they wrote: "in order to force the Spanish government to withdraw from Iraq, the resistance should hit with painful attacks against its forces. This will be accompanied by an information campaign, which would present the reality of the situation inside Iraq. It is a must to exploit the coming general elections in Spain in March 2004." The Message to the Spanish People was part of the "information campaign," while acts of violence against Spanish troops in Iraq and later in Madrid constituted the "painful attacks."[26]

Terrorists are adept at integrating their physical acts of violence with IO. They make audio and video recordings of the incidents for distribution over the Internet and on television. Their violence becomes theater, staged for its psychological impact, and replayed played over and over again in the media as IO.

To enhance the emotional effects, terrorist sometimes fabricate information and images. In February 2004, *Talon News* reported that a Turkish-language website affiliated with Ansar al Islam had posted "shocking pictures of President George W. Bush and British Prime Minister Tony Blair lying in coffins after having apparently undergone autopsies." The pictures showed large stitches covering their chests.[27] Terrorists are likely to continue exploiting ever-improving technologies for creating false pictures.

To convey an image of power over their adversaries, terrorists have fabricated stories of successful attacks. For example, following the August 2003 power outage on the East Coast, Al-Hayat reported that they had downloaded a communiqué from the International Islamic Media Center's website, in which al-Qa'ida claimed credit for the outage. According to Al-Hayat, the message said the operation "was carried out on the orders of Osama bin Laden to hit the pillars of the U.S. economy" and that the brigades of Abu Fahes Al Masri had hit two main power plants.[28] In fact, the outage was attributed to other factors.

Military Deception

Military deception comprises actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. It is used to make an adversary more vulnerable to the effects of friendly force weapons, maneuver, and operations.[29]

Terrorists use deceptive means to protect their operations and intentions. For example, in order to hide intentions and weapons, a suicide bomber appears to be just another person boarding a bus or entering a crowded theater or street market. The September 11 suicide hijackers similarly blended into their communities, dressing and behaving much like average Americans.

During a search of an al-Qa'ida member's home, Police in the U.K. uncovered an al-Qa'ida training manual that instructs its members on various forms of deception, including the use of covers.[30] A section on forged documents, for example, deals with the use of false identity cards and passports. Members are instructed to use photographs without beards and to not carry documents for multiple identities at the same time.

There does not appear to be much evidence of terrorists staging elaborate ruses and feints, such as used by militaries. Their deceptions appear to be aimed more at concealing activities rather than leading their adversaries down a false path or into a trap.

Electronic Warfare (EW)

Electronic warfare is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. It has three major components: electronic protection, electronic warfare support, and electronic attack. Electronic attack refers to operations that use electromagnetic energy, directed

energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. It includes jamming. Electronic protection refers to operations that defend against adversary electronic attacks. Electronic warfare support refers to operations that search for, intercept, identify, and locate or localize sources of radiated electromagnetic energy for the purpose of threat recognition, targeting, planning, and conduct of future operations.[31]

I have not found much evidence of terrorists engaging in EW, although there have been some reports of terrorists using jamming. For example, the Revolutionary Armed Forces of Columbia (FARC) is said to have jammed all ground-to-air communications over a jungle area where government troops were deployed to capture the FARC leader. The jamming prevented the air force from mounting an effective defensive action in support of the ground troops.[32]

Computer Network Operations (CNO)

Computer network operations comprise computer network attack, computer network defense, and related computer network exploitation-enabling operations.

Computer Network Attack (CNA)

Computer network attack is operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[33] It includes cyber attacks that deface websites or tamper with other data stored on computers, computer viruses and worms, and denial-of-service attacks against Internet servers or particular e-mail accounts on those servers.

Numerous cyber attacks have been attributed to hackers affiliated with terrorist organizations or sympathetic to terrorist causes. The first reported incident of this nature took place in 1997 when an offshoot of the Liberation Tigers of Tamil Eelam (LTTE) claimed responsibility for "suicide email bombings" against Sri Lankan embassies over a two-week period. Calling themselves the Internet Black Tigers, the group swamped Sri Lankan embassies with about 800 emails a day. The messages read, "We are the Internet Black Tigers and we're doing this to disrupt your communications."[34]

About two years later, another terrorist group engaged in cyber attacks. During the Kosovo conflict, the Serb Black Hand (Crna Ruka) group reportedly crashed a Kosovo Albanian web site, justifying their actions with the statement "We shall continue to remove ethnic Albanian lies from the Internet." They also planned daily actions against NATO computers and deleted data on a Navy computer.[35]

The Israeli-Palestinian conflict has provoked numerous cyber attacks from hackers on both sides of the conflict. According to the security firm iDefense, at least two of the pro-Palestinian groups involved in a cyber intifada in late 2000 had terrorist connections.[36] One of these was UNITY, a Muslim extremist group with ties to Hizballah. After pro-Israeli hackers attacked Hizballah's website, the hackers launched a coordinated, multi-phased denial of service attack, first against official Israeli

government sites, second against Israeli financial sites, third against Israeli ISPs, and fourth, against "Zionist E-Commerce" sites. The other group, al-Muhajiroun, has ties to a number of Muslim terrorist organizations as well as bin Laden. The London-based group directed their members to a Web page, where at the click of a mouse members could join an automated flooding attack against Israeli sites that were attacking Moqawama (Islamic Resistance) sites. iDefense also noted that UNITY recruited and organized a third group, Iron Guard, which conducted more technically sophisticated attacks. According to a Canadian government report, the group's call for cyber jihad was supported and promoted by al-Muhajiroun.[37]

A more recent call for cyber attacks against Israeli computers appeared on a website affiliated with Al-Qassam Brigades, the military wing of Hamas, in 2003. Under the heading "the electronic jihad," someone opened a discussion about using computer viruses to inflict harm on Israel. The idea was to load a virus-infected page onto a website and then take steps to attract as many Israeli visitors as possible to the site.[38]

In early 2004, Internet Haganah, a website devoted to confronting Islamic terrorists on the Internet and stopping their use of the net as a communications and propagation tool, reported that the Al Aqsa Martyrs Brigade was planning a cyber attack against the El Al website.[39] Internet Haganah also reported that its own website was the target of jihadists. A message posted to a Yahoo! group attempted to recruit 600 Muslims for jihad cyber attacks against Internet Haganah. The motive was retaliation against Internet Haganah's efforts to close down terrorist-related websites. Muslim hackers were asked to register to a Yahoo! group called Jehad-Op.[40]

According to the Anti-Terrorism Coalition (ATC), the jihad was organized by a group named Osama Bin Laden (OBL) Crew, which also threatened attacks against the ATC website.[41] Founded in 2000 by an al-Qa'ida member living in Holland, since 2002 OBL Crew has been under the leadership of a San Diego man calling himself Ibn Shahbaz. Although the promised attacks against ATC either failed or never materialized, OBL Crew hackers did take over the Asian Hangout forum on June 26, 2004, which they used for recruiting.

The September 11, 2001 terrorist attack against the United States and follow-on U.S.-led war on terror provoked a cyberwar involving hackers all over the world. Although none of the hackers claimed to be terrorists, three groups of Muslim hackers formed the Al-Qaeda Alliance Online: GForce Pakistan, the Pakistan Hackerz Club, and Anti India Crew.[42] In one of their defacements, GForce Pakistan said they stood by bin Laden even as they condemned the September 11 attacks. "Osama bin Laden is a holy fighter, and whatever he says makes sense," they wrote on a U.S. website on October 17. The modified Web page warned that the group planned to hit major US military and British Web sites.[43] Subsequent defacement did in fact show up on ".mil" sites. However, the hackers were apparently concerned they would be regarded as terrorists, as a later defacement said, "GForce Pakistan is not a group of cyber terrorists." Calling themselves "cyber crusaders," they asked for "PEACE for everyone."[44]

The examples involving Muslim hackers reflect ways in which the global jihad movement has incorporated the concept of cyber attacks as a form of electronic jihad into its strategic objectives. Sheikh Omar Bakri Muhammad, the London-based Islamic cleric who heads al-Muhajiroun and has ties to bin Laden, told *Computer World* in November 2002 that al-Qa'ida and other radical Muslim groups were actively planning to use the Internet as a weapon in their holy war against the West. He noted that the military wings of al-Qa'ida and other radical Islamic groups were using and studying the Internet for their own operations. He said that "in a matter of time, you will see attacks on the stock market," and that he "would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies."[45]

The use of cyber attacks is also appearing in al-Qa'ida publications and training programs. Principle 34 of *The 39 Principles of Jihad* directs computer experts to "use their skills and experience in destroying American, Jewish and secular websites as well as morally corrupt web sites."[46]

In late 2003, an affiliate of al-Qa'ida announced the opening of Al-Qa'ida University for Jihad Sciences on the Internet, with a college on electronic jihad. The announcement was circulated by the Islamic Information Center, which in the past had disseminated statements by bin Laden on the Internet. The other colleges include the technology of explosive devices, booby-trapped cars and vehicles, and media jihad. The announcement noted that there were already specialists in electronic Jihad, one of the colleges of the university.[47]

Terrorists or their sympathizers have reportedly hijacked Internet servers in order to share documents. While this might not be considered an "attack," it nonetheless represents unauthorized use of computers. In one such case, 70 files were uploaded to an unprotected FTP (file transfer protocol) site run by the Arkansas government for its contractors. A person calling himself Irhabi 007, or Terrorist 007, put links to the files on a message board belonging to al Ansar.[48] The motivations for using hijacked sites could include access to free storage and avoidance of detection by authorities.

Imam Samudra, one of the terrorists convicted in the October 12, 2002 Bali bombings, advocates the use of computer attacks to raise funds for terrorist activities in his autobiography *Me Against the Terrorist!* In a chapter titled "Hacking: why not?" Sumadra offers some rudimentary information on hacking, particularly as it applies to credit card fraud ("carding"). Evidence found on his seized computer showed he at least had made an attempt at carding.[49]

These developments show that terrorists have begun to integrate cyber attacks into their thinking, strategies, and operations. Further developments are likely as computers and the Internet achieve higher penetration rates throughout the world, and young hackers and computer enthusiasts join the ranks of terrorists.

In examining terrorist use of CNA, I have intentionally avoided calling any of it "cyberterror."[50] The main reason is that the attacks have not been terrorizing. Unless

and until they become so, it seems more appropriate to label them simply as cyber attacks rather than as some peculiar form of terror.

Computer Network Exploit (CNE)

Computer network exploitation consists of enabling operations and intelligence collection to gather data from target or adversary computers and networks in support of CNA.[51] It includes the use of scanners to identify network access points and vulnerabilities.

It is reasonable to assume that the same terrorist-affiliated hackers who conduct CNA use CNE to map their targets before attack. However, hackers do not distinguish CNE as a separate activity from CNA; it is considered to be part of the attack process.

Computer Network Defense (CND)

Computer network defense consists of defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.[52] In short, CND refers to operations that protect against adversary CNA. It includes the use access controls, encryption, authentication, firewalls, intrusion detection, anti-viral tools, audit, security management, and security awareness and training.

Because terrorist organizations use the Internet and maintain websites, they cannot ignore CND. Hamas and Hizballah, for example, have had to defend their websites against Israeli hackers who in the past have defaced them. In addition, all computers hooked up to the Internet are constantly under siege by hackers and script kiddies who indiscriminately attack any machine that is vulnerable. Computers operated by terrorists would be no exception. Thus, we can conclude that terrorists must employ CND or their presence on the Internet would not survive.

Operations Security (OPSEC)

Operations security is the process of identifying essential elements of friendly information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems, determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive essential elements of friendly information time to be useful to adversaries, and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.[53]

OPSEC includes camouflage, concealment, and decoy employment. It is offensive when it is used to protect information about friendly force actions, intentions, and future operations from adversaries. It is defensive when it is used to protect information that could be used by adversaries to target or attack friendly forces.

Terrorists make extensive use of offensive and defensive OPSEC. Their operations and organizational survival depends on secrecy. Underground groups must hide not only their plans and operations, but also the places they live and meet.

To avoid drawing attention to themselves, terrorists may attempt to dress, act, and talk like those around them. In April 2004, the FBI issued a warning that al-Qa'ida had prioritized the recruitment and use of operatives whose background or appearance allows them to blend easily into Western society. The report said al-Qa'ida seeks individuals who speak English or are of European ancestry, people who have U.S. or West European passports, and naturalized U.S. citizens of Middle Eastern or South Asian descent. These groups are perceived to have greater freedom of access in the West.[54]

The al-Qa'ida training manual emphasizes security and integrates it into such topic areas as housing, communications, transportation, training, meetings, and operations. Under telephone communications, for example, members are instructed to use phones in public places and to use codes or speak in general terms in case their conversations are being monitored. Under apartments, they are told that nobody should know the location except those who use it, and that it is preferable to rent apartments using false names, appropriate cover, and non-Muslim appearance. Members are also told to prepare secret locations in their apartments for hiding documents, records, arms, and other important items.

An entire lesson is devoted to the security plan, which is defined as "a set of coordinated, cohesive, and integrated measures that are related to a certain activity and designed to confuse and surprise the enemy, and if uncovered, to minimize the work loss as much as possible." In a section on stationary meetings, members are given a list of precautions to follow. These include wearing clothing suitable for the meeting place, traveling to the meeting through secondary places, and using a meeting location in the middle of a group of houses, not at the beginning.

In January 2004, al-Qa'ida launched the Internet magazine *Al-Battar Training Camp* for the purpose of giving Muslim youth jihad training without the need to travel to a terrorist training camp.[55] The sixth issue, published in March, includes a detailed description of the organization structure of project cells.[56] The issue emphasizes the importance of security, including the use of compartmentalization within project cells and dead drops (including websites) for communications up and down the chain of command. Members of the project management team are to be trained in secret communications, among other things. Other issues of the magazine also contain articles that discuss security.

Methods for secure communications are covered in a lesson on secret writing and codes and ciphers in the al-Qa'ida training manual. This lesson is particularly archaic, however, describing manual methods of encipherment that appear to be at least 50 to 100 years old. The manual does not mention modern computer and communication technologies and the varieties of secrecy technologies that have been developed for them. Yet al-Qa'ida and other terrorists use these technologies, including anonymous e-mail accounts, encryption, and possibly steganography.

The September 11 hijackers, for example, accessed anonymous Hotmail and Yahoo! accounts from computers at Kinko's and at a public library.[57] They also used secret code

words and phrases. Three weeks before the attacks, Mohammad Atta reportedly received a coded email message that read: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts and the faculty of engineering."[58] The faculties referred to the four targets (twin towers, Pentagon, and Capitol); the faculty for urban planning may have represented the World Trade Center tower hit by Atta's plane since he had studied urban planning in Hamburg, Germany.

Al-Qa'ida has used encryption to protect information stored in computer files. Ramzi Yousef, a key operative in the first World Trade Center bombing in 1993, stored the information about his Bojinka plot to destroy 11 airliners on his laptop in encrypted files. The encryption was sufficiently robust that it took cryptanalysts more than a year to break the code.[59] Yousef's uncle, Khalid Shaikh Mohammed, is said to have trained high-level al-Qa'ida operatives in the use of encryption.[60]

After the *Wall Street Journal* bought two computers from looters in Afghanistan in November 2001, they found a treasure trove of encrypted files belonging to al-Qa'ida. The files had been encrypted with Microsoft's 40-bit version of the Data Encryption Standard (DES), which had been approved for export (now codes with unlimited and unbreakable key sizes can be exported). Although 40-bit keys are usually regarded as extremely weak, it took the Journal five days to crack one of the keys using several computers. The files contained memos of the terrorist group's chemical and biological weapons program, justifications for killing civilians, and a propaganda video showing people fleeing from the World Trade Center.[61]

Al-Qa'ida also reportedly acquired customized ciphers on the international black market around 1996. The terrorist group encrypted their satellite data communications and used hard-to-tap spread-spectrum radios.[62]

There have been reports of al-Qa'ida members using steganography, that is, methods of hiding messages in cover media.[63] In October 2001, *ABC News* reported that French investigators believed that suspects arrested in an alleged plot to blow up the U.S. Embassy in Paris planned to transmit the go-ahead for the attack hidden inside a picture posted on the Internet. Investigators found a notebook full of secret codes on one of the men, who was characterized as a "computer nerd well versed in the messaging technique."[64]

Italian investigators also found indications of al-Qa'ida terrorists hiding messages in image files on the Internet. In November 2001, they confiscated eleven computers from the Via Quaranta mosque during an investigation into an Islamic terrorist cell that provided logistical support to al-Qa'ida. The computers held images of the World Trade Center (downloaded before September 11), political leaders such as President Bush, and pornographic material, all taken from the Internet. The images had been modified before being sent back onto the Web, suggesting that they contained hidden messages.[65]

The Glasgow communications firm Iomart said they had passed hundreds of files with hidden Arabic text and date references to U.S. authorities after the September 11 attacks. They had found the hidden messages in image and music files on the Internet.[66] In July 2004, the Northeast Intelligence Network reported that their analysis of a re-released video of bin Laden uncovered what appeared to be secret codes. They found alpha-numeric sequences in some of the frames that were not present in the original video.[67]

Terrorist-related information has been found hidden on compact disks. Saudi authorities, for example, found hidden files with bomb-making instructions on CDs they had confiscated from local computer shops.[68] The raids were conducted following a crackdown on Muslim militants after the bombings in Riyadh attributed to al-Qa'ida. The shops were selling the CDs.

IO SUPPORTING CAPABILITIES

IO supporting capabilities include physical destruction, information assurance (IA), physical security, counterintelligence, counterdeception, and counterpropaganda.

Physical Destruction

Physical destruction is the application of combat power to destroy or degrade adversary forces, sources of information, command and control systems, and installations.[69] Although physical destruction primarily serves conventional (non-IO) warfare objectives, it becomes an IO element when used to disrupt, deny, degrade, or destroy information, information systems, the decision making process, or the decision maker.

Terrorism is generally defined by acts of physical violence and the threat of such acts, particularly against civilians. While these acts are intended to influence decision makers, in general they do not involve denying, degrading, or destroying information resources or the decision makers. Rather, the typical terrorist act destroys civilians, in the process injecting additional information into the decision making process, namely images that portray the terrorists' power and generate fear. Terrorists seek to bring their cause and capabilities to the attention of decision makers and their populations, and they leverage the media for this purpose. Thus, I do not consider most acts of terrorist violence as IO, although I readily acknowledge their psychological elements and influence objectives, and their integration with IO, typically through media distribution of pictures taken of the violent acts. The Madrid bombings on the eve of elections clearly influenced the outcome, but not by degrading or destroying the election process itself or the information and systems used to run it. Rather, voters went to the polls with images of the carnage, memories of lost friends and loved ones, and fear of further attacks, as well as a sense that the current government had lied to them by attributing the attacks to the ETA.

Terrorists do, however, engage in certain destructive acts that more clearly fit the criteria for IO, for example, assassinations of government leaders, which destroy decision makers.

Information Assurance (IA)

Information assurance comprises information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[70] IA incorporates CND. It supports OPSEC by ensuring the confidentiality of information.

The section on OPSEC describes how terrorists use various security technologies for confidentiality purposes, including encryption. Encryption can also provide data integrity and data and sender authentication, thereby serving a broader IA objective.

Terrorists are also known to use password-protected areas on websites, the passwords serving as a means of authenticating those seeking access to the areas and confidentiality for the information exchanged within them.

The section on CND notes that terrorists must employ CND to ensure the survivability of their networks and presence on the Internet. Through CND, terrorists are also providing IA, including confidentiality, integrity, authentication, and availability.

Physical Security

Physical security is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.[71] Physical security supports the core IO areas, including OPSEC, as well as other supporting areas, including IA.

Many of the security measures presented in the al-Qa'ida training manual relate to physical security. As previously noted, the security precautions for apartments include preparing secret locations for hiding documents, records, arms, and other important items. Other physical security measures for apartments include replacing locks and keys with new ones, making sure that apartments used for undercover work are not visible from higher apartments, and using signs such as opening a curtain or hanging out a towel to note that the place is safe to enter.

Counterintelligence (CI)

Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.[72] The CI mission is to detect, identify, assess, counter, neutralize, or exploit hostile intelligence collection.

The al-Qa'ida training manual instructs members on CI.[73] When going to a meeting location, members are advised to make sure there are no enemy security personnel behind them or at the meeting place. When taking public transportation to a meeting, members should board and embark at a secondary station, as "main stations undergo more careful surveillance." CI security precautions for apartments include ensuring that there has been no surveillance prior to the members entering the apartment.

Members of al-Qa'ida are also instructed on particular methods of intelligence and counterintelligence. For example, a section on surveillance offers six clues for detecting surveillance conducted by car. These include the surveillance car entering a dead-end street, and entering and immediately exiting a parking lot.

Counterdeception

Counterdeception consists of efforts to negate, neutralize, diminish the effects of, or gain the advantage from a foreign deception operation. It does not include the intelligence function of identifying foreign deception operations.[74]

The al-Qa'ida training manual includes a few provisions that relate to counterdeception. For example, a section on recruiting agents from enemy camps explains that new recruits must be tested to weed out those who may try to mislead. One way of testing involves asking a recruit to provide information that is already known. If the provided information fails to match that which is known, this may be an indication that the person is deceptive. Another way of testing involves giving the recruit an opportunity to tamper with work documents. In dealing with agents, members are advised to not receive packages from the agents, because they could be booby trapped.

Counterpropaganda

Propaganda is considered to be any form of communication designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor. It can be a mix of truths and lies, including misinformation, disinformation, and opposing information. Counterpropaganda consists of programs of products and actions designed to nullify propaganda or mitigate its effects. It is directed toward the target of adversary propaganda and serves to degrade the harmful influence of adversary PSYOP on friendly forces and other audiences.[75] Counterpropaganda is the responsibility of PSYOP units when the target of propaganda is a foreign audience.

Terrorists engage in counterpropaganda to offset what they consider to be propaganda from enemy governments. Al-Qa'ida, for example, turns what the U.S. and West calls a "war on terrorism" into a "crusade against Islam" and its own "terrorism." In so doing, al-Qa'ida attempts to turn Muslims against the West, projecting an image of Muslims as victims of Western aggression. Al-Qa'ida justifies its own killing as a response to that aggression.

This strategy is underscored in an April 2004 audio message purportedly from bin Laden. Addressing "our neighbors north of the Mediterranean", the speaker says: "*…* we would like to inform you that labeling us and our acts as terrorism is also a description of you and of your acts. … Our acts are reaction to your own acts, which are represented by the destruction and killing of our kinfolk in Afghanistan, Iraq and Palestine. … The act that horrified the world; that is, the killing of the old, handicapped [Hamas spiritual leader] Sheikh Ahmed Yassin, may God have mercy on him, is sufficient evidence."[76]

Bin Laden appeals to "honest people" to form a committee and use the media to "enlighten European peoples of the justice of our causes, above all Palestine." He says that contrary to the lies "that we hate freedom and kill for the sake of killing," their killing followed acts of invasion.

IO RELATED CAPABILITIES

Related capabilities consist of public affairs (PA) and civil military operations (CMO).

Public Affairs (PA)

Public affairs are those public information, command information, and community relations' activities directed toward both the external and internal publics with interest in the Department of Defense.[77] It makes available timely and accurate information so that the public, Congress, and the news media may assess and understand the facts about national security and defense strategy. PA information is intended to be credible.

Terrorists integrate their PA activity with their PSYOP and counterpropaganda, addressing both external and internal publics. While their PSYOP is aimed mainly at their supporters and potential supporters plus enemy populations, their PA messages are aimed at a broad international audience as well. As noted earlier, terrorists use a variety of media for their messages, including leaflets, magazines, newspapers, books, audio and video recordings, radio and television stations, and the Internet. In addition to distributing their own materials directly, terrorists also leverage mainstream mass media. They send stories and video clips to newspapers and television stations, and have granted interviews to reporters.

Terrorists began using the web for PA in December 1996 when the Tupac Amaru seized the Japanese embassy in Lima, Peru. By the following morning, the group had a public website up and running out of Germany. The site had over 100 pages, which were updated using a laptop computer and satellite telephone uplink.[78]

Tupac Amaru's website represented a strategic innovation in terrorism, particularly as it relates to propaganda and public affairs. For the first time, terrorists could write their own stories and bring their message to a world audience without mediation by the established press or interference by the government. They were not dependent on the major newspapers and TV stations to report on their attacks. The advantage this gave the terrorists was immeasurable.

By January 1998, there were at least 16 English-language sites representing 14 terrorist organizations on the State Department's 1996 list, according to researchers at Haifa University in Israel who scanned the web. Their January 2002 scan found 29 English or Arabic sites from 18 organizations on the State Department's 2000 list.[79] The researchers reported that the sites usually included background information on the organization and its leaders, founders, and heroes; information on the political and ideological aims of the organization; and up-to-date news. The terrorists justified their violence, saying they had no choice owing to their own weakness against an oppressive enemy, and that the enemy (e.g., state) was the real terrorist. When the researchers scanned the web in 2003-2004, they found hundreds of websites serving terrorists and their supporters.[80]

As of October 27, 2003, Internet Haganah listed 65 active websites with affiliations to six Islamic terrorist organizations. These included Al Aqsa Martyrs Brigades (10 websites), al-Qa'ida (24), Hamas (19), Hizballah (5), Hizb ut-Tahrir (4), and Palestinian Islamic Jihad (2). The organization claimed to have gotten approximately 300 additional terrorist-supporter websites shut down through their volunteer efforts.[81] The Anti-Terrorism Coalition listed 162 websites and 286 e-mail groups in their database as of July 12, 2004, although many were no longer active.[82]

Hamas's primary website, represented by the Palestine Information Center, is offered in seven languages, each hosted on a different server and with its own content. The versions include Arabic, English, Farsi, French, Malay, Russian, and Urdu.[83] Their English site includes news stories, political analysis, Palestinian history, web pages devoted to "Zionist terrorism" and human rights violations against Palestinians, photos of Palestinians killed in Israeli strikes, and videos (including one that "exposes Zionist practices"). There is also a link to "If Americans Knew," a website with a claimed counterpropaganda mission "to inform and educate the American public on issues of major significance that are unreported, underreported, or misreported in the American media."[84]

Al-Qa'ida has been especially active on the web. What was reported to be their official website, Alneda.com, appeared after the September 11 attacks. Representing the Center for Islamic Studies and Research, the site was used to publish propaganda and send messages to al-Qa'ida members. The site has repeatedly disappeared and then reappeared in different locations. Additional al-Qa'ida sites have also appeared.

In October 2003, al-Qa'ida supporters in Saudi Arabia launched a website with a bimonthly online magazine called *Sawt al-Jihad* (The *Voice of Jihad*).[85] The magazine deals with jihad and the mujahideen in the Arabian Peninsula, and mixes PSYOP into its propaganda and news. The first issue contains an interview with one of the men responsible for the May 12, 2003 suicide attack in Riyadh and essays implicitly calling for the killing of all Americans. Later, the website published an audio recording of the suicide attack as transmitted through a cell phone, videos showing two of the bombers reading their wills less than two weeks before the attacks, and speeches by bin Laden and Sheikh Abu Omar Muhammad Al-Seif.[86]

The ninth issue, issued in January 2004, reported on a new film relating to the attack on the Al-Muhayya Crusader settlements during Ramadan of 2003. The "Badr al-Riyadh film," which was posted on the web site for the Islamic Center for Studies and Research, shows the attack from its initial planning and training stages through execution. It includes ideological discussions regarding the religious legitimacy of the attacks; footage of the suicide bombers training for the mission, making statements, and assembling the truck bomb; scenes showing a white truck being spray painted to look like a Saudi police vehicle; and footage showing the truck rolling out with the bombers on board, followed by sounds of gunfire and the beginning of the explosion. The tape then goes black.[87]

The eleventh issue, issued a month later in February, further extols the Badr al-Riyadh video and emphasizes the importance of propaganda, according to the SITE Institute.[88] SITE reports that the issue claims the film has set the stage for a new phase, where people will move from passively sympathizing with the mujahideen to "giving all possible support to the mujahideen, standing by them with heart and soul, with prayers and by urging sons to become time bombs and heroic commandos against the crusaders and their allies…"

Jihad doctrine directs all Muslims to use the media to engage in activities that fall within the scope of PA, PSYOP, and counterpropaganda. Principle 21 of the book *The 39 Principles of Jihad*, for example, calls for "publishing the Mujahideens' activities in order to arouse the notion of solidarity and strengthen pride and hope among the believers, to praise the ideal of self sacrifice for the sake of Allah and to break the media siege imposed by the enemy." It suggests several distribution media, including Internet websites and forums, distribution lists, and text messaging on cell phones. Principle 34, which calls for "performing electronic Jihad," also has a PSYOP and public relations aspect, advocating "participating in Internet forums to defend the Islam and Mujahideen, to preach Jihad and to encourage Muslims to learn more about this sacred duty."[89]

Civil Military Operations (CMO)

Civil military operations are activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, and to consolidate and achieve operational United States objectives.[90] It may include activities and functions, conducted by the military, that are normally the responsibility of the local, regional, or national government. CMO supports both military operations and civil authorities.

Some terrorist organizations engage in CMO to assist their local populations. Hamas, for example, is more than just a militant organization. It also helps fund schools and hospitals, and provide welfare checks to the needy. In the Gaza refugee camps, the organization is said to run every school, hospital, and charity.[91] Hamas also uses donations to provide financial support to the families of suicide bombers. The result of

Hamas's CMO is that the organization receives reciprocal support. The local communities become a source of new recruits, money, and protection.

Terrorists cannot engage in substantial CMO, however, in places where they must operate covertly to avoid capture. An al-Qa'ida cell in Miami or London, for example, is not likely to help the broad community, although it may help a local Mosque that provides financial support, cover, or recruits for the organization.

CONCLUSIONS

Terrorists employ all the IO capabilities of U.S. military doctrine, including the five core capabilities of PSYOP, military deception, EW, CNO, and OPSEC, and the supporting and related capabilities. They use IO to support both offensive operations (acts of terrorism) and defensive operations (e.g., protecting their hiding places). They use IO strategically in support of broad objectives. While terrorists do not speak and write of "IO," they demonstrate an understanding of the value and methods of IO capabilities.

Terrorists appear to be particularly adept at PSYOP, PA, counterpropaganda, and certain forms of OPSEC and deception, driven by their desire to simultaneously reach desired audiences and hide from their enemies. They recognize the value of various media, including the Internet, and exploit it to support their cause. Terrorists and their supporters have a CNO capability, with CNA manifesting itself as "electronic jihad" rather than as acts of terror.

Unlike the U.S. military, terrorists are not constrained by laws that prohibit certain activities or activities against certain populations. Terrorists are free to use violence against civilian populations as their principle psychological and kinetic tool. Also, civilians who support the global jihad can effectively join and take actions on behalf of terrorist groups, for example, engaging in CNA or PSYOP.

Effective counterterrorism requires a thorough understanding of how terrorists operate across all dimensions, including the information dimension. This overview of terrorist IO is given in the spirit of aiding counterterrorism efforts against al-Qa'ida and other terrorists.

Endnotes

[1] "The Changing Threat of Al-Qaeda," *The Independent*, All Africa Global Media, January 12, 2004; "Al-Qaeda No Longer a Group," *PakTribune*, January 3, 2004; Walter Pincus, "Spread of Bin Laden Ideology Cited," *Washington Post*, April 4, 2004.
[2] Norman E. Emery, Robert S. Earl, and Raymond Buettner, "Terrorist Use of Information Operations," *Journal of Information Warfare*, 2004 (to appear).
[3] This definition is based on that given in Field Manual (FM) 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures, U.S. Army, November 2003. It is consistent with joint initiatives.
[4] FM 3-13.
[5] FM 3-13.
[6] FM 3-13; Joint Doctrine for Information Operations, Joint Pub (JP) 3-13, Joint Chiefs of Staff, October 9, 1998.

[7] FM 3-13.
[8] Mark Follman, "Be Very Afraid," *Salon*, April 9, 2004.
[9] Laura Mansfield, "Al Qaeda Maps Plans for Assassinations from Camp al Battar, Issue 8," Northeast Intelligence Network, April 15, 2004; http://www.homelandsecurityus.com/ .
[10] The translation is by the National Virtual Translation Center and made possible by DARPA's enhanced TIDES Iraq Reconstruction Report (eTIRR) research effort, May 14, 2004.
[11] "Al Qaeda militants kill American hostage," *CNN.com*, June 19, 2001.
[12] Bruce Hoffman, "Al Qaeda, Trends in Terrorism, and Future Potentialities: An Assessment," *Studies in Conflict & Terrorism*, 26:429-442, 2003.
[13] Cam McGrath, "Activists Crusade Against E-Jihad," *IPSNews*, April 12, 2004.
[14] Jonathan D. Halevi, "39 Principles of Jihad," Center for Special Studies, Intelligence and Terrorism Information Center, September 2003, TUhtm.e_p39/var/eng/il.org.intelligence.www//:httpUT . Quotes are from Halevi's summary of the text.
[15] http://www.ipnews.planetgac.com , accessed February 3, 2004. The video can be viewed at the site.
[16] Cam McGrath, "Activists Crusade Against E-Jihad," *IPSNews*, April 12, 2004.
[17] Alyssa A. Lappen and Jerry Gordon, "Former Terrorist Speaks," *FrontPageMagazine.com*, April 2, 2004.
[18] Jonathan D. Halevi, "39 Principles of Jihad," Center for Special Studies, Intelligence and Terrorism Information Center, September 2003, TUhtm.e_p39/var/eng/il.org.intelligence.www//:httpUT .
[19] "Rising Internet Use in the Globalization of Terror," SO/LIC Global Issues Report, prepared by SAIC, March 23, 2004.
[20] "A Message to the American People," accessed on al-Qa'ida's site at www.cambuur.net in early December 2002. The site is no longer available.
[21] Al Qaeda Threatens To Nuke New York By February 2nd," Debka.com, January 1, 2004.
[22] Anna Badkhen, "Al Qaeda Bluffing About Having Suitcase Nukes, Experts Say," *San Francisco Chronicle*, March 23, 2004.
[23] Reuven Paz, "A Message to the Spanish People: The Neglected Threat of Qa`idat al-Jihad," PRISM Special Dispatches, Vol. 2, No. 2, March 18, 2004.
[24] Michael Morris, "The Biggest Bomb in Spain Exploded Sunday," *The American Thinker*, March 15, 2004.
[25] Norman E. Emery, Robert S. Earl, and Raymond Buettner, "Terrorist Use of Information Operations," *Journal of Information Warfare*, 2004 (to appear).
[26] "Al Qaida Web Site Outlined Spain Strategy Last December," Geostrategy-Direct, Week of April 27, 2004.
[27] Jeremy Reynalds, "Terrorist Group Parades Pictures of Bush, Blair in Coffins," *Talon News*, February 2, 2004.
[28] Mohamad Saleh, "Al Qaeda Claims Responsibility for Power Blackout in U.S.!," Dar Al-Hayat, August 18, 2003, http://english.daralhayat.com/arab_news/08-2003/Article-20030818-14bdd659-c0a8-01ed-0079-6e1c903b7552/story.html .
[29] FM 3-13.
[30] According to the Department of Justice, the manual was found in a computer file described as the "the military series" related to the "Declaration of Jihad." A translation is available at http://cryptome.quintessenz.org/mirror/alq-terr-man.htm . Other authors have referred to this manual as the "Military Studies."
[31] FM 3-13.
[32] Jamie Dettmar, "Columbian Government Losing Its War on Drugs, *Insight*, May 18, 1998, http://www.insightmag.com/news/1998/05/18/NewsAlert/Se-213883.shtml .
[33] FM 3-13, JP 3-13.
[34] "Email Attack on Sri Lanka Computers," *Computer Security Alert*, No. 183, Computer Security Institute, June 1998, p. 8.
[35] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism," in *Networks and Netwars* (J. Arquilla and D. Ronfelt, eds.), RAND, 2001, p. 273.
[36] Israeli-Palestinian Cyber Conflict, iDefense Intelligence Services Report, January 3, 2000.
[37] "Al-Qaida Cyber Capability," Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada,

http://www.epc-pcc.gc.ca/emergencies/other/TA01-001_E.html.
[38] "Hamas Sympathizers Have a Plan for Computers – Maybe Yours!" Internet Haganah, accessed April 8, 2003.
[39] Internet Haganah website at http://66.98.144.142/haganah/index.html , accessed March 24, 2004.
[40] Jeremy Reynalds, "Internet 'Terrorist' Using Yahoo to Recruit 600 Muslims for Hack Attack," *Mensnewsdaily.com*, February 28, 2004.
[41] "ATC's OBL Crew Investigation," July 1, 2004, http://atdatabase.r8.org/ . The ATC's Intelligence Department became an independent organization, called Anti-Terrorism Intelligence (ATI), in March 2005.
[42] Brian McWilliams, "Anti-India Hackers Turn Attacks on US Systems," *Newsbytes*, December 10, 2001.
[43] This defacement is mirrored at http://defaced.alldas.de/mirror/2001/10/20/www.dtepi.mil/ .
[44] GForce defacement on October 27, 2001 of a .mil website.
[45] Dan Verton, "Bin Laden Cohort Warns of Cyberattacks," *Computerworld*, November 18, 2002; Dan Verton, "Al-Qaeda Poses Threat to Net," *Computerworld*, November 25, 2002.
[46] Jonathan D. Halevi, "39 Principles of Jihad," Center for Special Studies, Intelligence and Terrorism Information Center, September 2003, TUhtm.e_p39/var/eng/il.org.intelligence.www//:httpUT .
[47] "Al-Qa'ida Reportedly Establishing Open 'Internet University' to Recruit Terrorists," OSAC Foreign Press Report of article by Muhammad al-Shafi in London *Al-Sharq al-Awsat* in Arabic, November 20, 2003.
[48] David McGuire, "Al Qaeda Messages Posted on U.S. Server," *The Washington Post*, July 13, 2004.
[49] Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War Into Cyberspace," *The Washington Post*, December 14, 2004, p. A19.
[50] I have written several articles on the prospects of cyberterrorism. For example, see Dorothy E. Denning, "Is Cyber Terror Next?" in *Understanding September 11* (Craig Calhoun, Paul Price, and Ashley Timmer eds.), *The New Press*, 2002; also at http://www.ssrc.org/sept11/essays/denning.htm .
[51] FM 31-3.
[52] FM 31-3.
[53] FM 3-13. The definition in JP 3-13 is the same except for the word "critical" instead of "essential" in the first sentence.
[54] "Al-Qaeda Recruitment Of Non-Traditional Operatives," FBI Intelligence Bulletin No. 21, April 7, 2004.
[55] "Al-Qaida Offers Do-It-Yourself Terror Training," *WorldNetDaily*, January 5, 2004.
[56] Laura Mansfield, "Everything You Always Wanted to Know About Becoming a Terrorist, but Were Afraid to Ask," Northeast Intelligence Network, March 2004.
[57] Brian Ross, "A Secret Language," ABCNEWS.com, October 4, 2001.
[58] "Virtual Soldiers in a Holy War," *Ha'aretz Daily*, September 16, 2002.
[59] Louis J. Freeh, Director FBI, Statement before the Senate Committee on Commerce, Science, and Transportation, regarding the Impact of Encryption on Law Enforcement and Public Safety, March 19, 1997.
[60] Examining the cyber Capabilities of Islamic Terrorist Groups, Technical Analysis Group, Institute for Security Technology Studies, Dartmouth College, March 2004, slide 22.
[61] D. Ian Hopper, "Kabul Computer Reveals Files of Top Al Qaeda Officials," *Associated Press*, December 21, 2001.
[62] Lou Dolinar, "Bin Laden's Electronics Arsenal," *NY Newsday*, September 23, 2001.
[63] One of the earliest reports predated the September 11 attacks: Jack Kelley, "Terror Groups Hide Behind Web Encryption," *USA Today*, February 6, 2001. However, the newspaper has subsequently discredited the author, saying he fabricated stories and plagiarized material.
[64] Brian Ross, "A Secret Language," *ABCNEWS.com*, October 4, 2001.
[65] Alexandra Salomon, "Terrorists' Twin Tower Images, Secret Porn Messages," *ABCNEWS.com*, May 8, 2003.
[66] "Internet Link in Terror Probe," *BBC News*, October 10, 2001.
[67] "The Re-released 'Encoded' Osama bin Laden Footage," Northeast Intelligence Network, July 26, 2004, http://www.homelandsecurityus.com .
[68] "Saudi Arrests Five After Seizing Bomb-Making CDs," *Reuters*, Riyadh, December 25, 2003.
[69] FM 3-13.
[70] FM 3-13, JP 3-13.
[71] FM 3-13, JP 3-13.

[72] FM 3-13, JP 3-13.
[73] For a more thorough analysis of the manual's instructions in denial, deception, and other CI practices, see Richard H. Shultz, Jr. and Ruth Margolies Beitler, "Tactical Deception and Strategic Surprise in Al-Qa'ida's Operations," *Middle East Review of International Affairs*, Vol. 8, No. 2, June 2004, pp. 56-79. The article also gives case studies of Al Qa'ida's use of denial and deception.
[74] FM 3-13, JP 3-13.
[75] FM 3-13.
[76] "Osama Bin Laden Audio Tape Translation," Northeast Intelligence Network, April 15, 2004, http://www.homelandsecurityus.com/ .
[77] FM 3-13, JP 3-13.
[78] Tom Regan, "How Terrorists Use the Internet to Spread Their Messages," *Christian Science Monitor*, July 1, 1999.
[79] Yariv Tsfati and Gabriel Weimann, "www.terrorism.com: Terror on the Internet," *Studies in Conflict & Terrorism*, 25: 317-332, 2002.
[80] Gabriel Weimann, "www.terror.net, How Modern Terrorism Uses the Internet," United States Institute of Peace, Special Report 116, March 2004.
[81] http://www.geocities.com/internet_haganah , October 27, 2003.
[82] http://atcterrorlist.showsit.info/ .
[83] http://www.palestine-info.info/ .
[84] http://www.ifamericansknew.org/ .
[85] Special Dispatch Series No. 591, MEMRI, October 17, 2003, http://www.memri.org/bin/latestnews.cgi?ID=SD59103. The article cited the al-Qa'ida online magazine at http://www.cybcity.com/suondmag/index.htm .
[86] Special Alert No. 11, MEMRI, October 21, 2003, http://www.memri.org/bin/latestnews.cgi?ID=SA1103. Reuven Paz, "Sawt al-Jihad: New Indoctrination of Qa'idat al-Jihad," PRISM Series of Global Jihad, No. 8, Global Research in International Affairs (GLORIA) Center, www.e-prism.org .
[87] "Al-Qa'ida's 'Voice of Jihad' Magazine – Issue No. 9," Special Dispatch Series No. 650, MEMRI, January 27, 2004; Brian Ross and David Scott, "Caught on Tape, Video Purports t o Show Al Qaeda Planning for Terror Attack," ABCNEWS.com, February 5, 2004. An analysis of the film by IntelCenter can be found at http://www.intelcenter.com .
[88] "Eleventh Issue of Sawt Al-Jihad Released," SITE Institute, February 24, 2004.
[89] Jonathan D. Halevi, "39 Principles of Jihad," Center for Special Studies, Intelligence and Terrorism Information Center, September 2003, TUhtm.e_p39/var/eng/il.org.intelligence.www//:httpUT .
[90] FM 3-13.
[91] Campbell Brown, "New Hamas Leader: No U.S. Attacks," MSNBC News, March 24, 2004.