To appear in *Handbook on Internet Crime* (Y. Jewkes and M. Yar, eds.), Willan Publishing, 2009.

Terror's Web: How the Internet Is Transforming Terrorism

Dorothy E. Denning

Introduction

With over 1.4 billion persons on the Internet (Internet World Stats, 2008), or more than 21% of the world's population, it is not surprising to find terrorists among that population. Moreover, given the way the Internet has affected everything from booking a hotel to finding a partner, it is not surprising to see changes in the practice of terrorism. Indeed, the Internet is fundamentally transforming terrorism, including the way terrorists disseminate documents and propaganda, recruit and train new members, and inflict harm on their victims.

This chapter explores the relationship between the Internet and terrorism. It discusses how terrorists use the Internet and the impact of that use on terrorism and counterterrorism. Concepts are illustrated with examples drawn from a variety of terrorist groups, with particular emphasis on al-Qa'ida and the global jihadist movement associated with it. This movement, which subscribes to al-Qa'ida's ideology and violent tactics, is held together largely through the Internet.

Superficially, terrorists use the Internet in pretty much the same way that other individuals and groups use the Internet. They use it to communicate amongst themselves and to reach out to supporters, the media, governments, and the public. They use it to exchange messages and engage in online discussions. They use the net to distribute information, including text, images, audio, video, and software, and to find information. They use it to learn, transact business, and

generally facilitate their activities. And, like other bad actors on the Internet, they use the net to inflict harm. Yet from this seemingly normal usage, the very practice of terrorism is being transformed. This transformation takes the form more of an expansion of options and activities rather than a replacement of traditional ways of operating. The changes are perhaps most pronounced in the al-Qa'ida movement.

The following sections discuss six areas of terrorism practice that have been substantially altered by the Internet, especially the Web: media operations, attacks, recruitment, learning, finance, and security. The paper concludes with a section on counterterrorism strategies that exploit terrorists' use of the Internet.

Media Operations

After seizing the Japanese embassy in Lima, Peru on December 17, 1996, the Movimiento Revolucionario Tüpac Amaru (MRTA or Tüpac Amaru) launched a new era in terrorist media operations. By the following morning, the group had a website up and running out of Germany. The site had over 100 pages, which were updated using a laptop computer and satellite telephone uplink. Mainstream media, including the *New York Times*, received their information about the incident from the terrorist's website (Regan, 1999). During the initial hours of the conflict, the terrorists effectively owned the information environment relating to their operation.

MRTA's use of the Web represented a strategic innovation in terrorism. For the first time, terrorists could bring their message to a world audience without mediation by the established press or interference by the government. Further, they could offer news reports of world events that were favorable to their cause, thereby enhancing the propaganda value of their websites. In addition, they could use the Web to distribute information directly to their own members and supporters. The advantage the Web offered was immeasurable and recognized by terrorist groups worldwide.

By 1998, 12 of the 30 groups on the US State Department's list of terrorist organizations that year were said to have websites (Whitelaw, 1998), and by January 2002, researchers at Haifa University in Israel had found 29 sites from 18 organizations on the State Department's 2000 list (Tsfati and Weimann, 2002). Today, it would be surprising to find a terrorist group that did not have some presence on the Web.

Islamic terrorists have been particularly active on the Web. In October 2003, Internet Haganah, a project devoted to combating terrorism, 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 project claimed to have gotten approximately 300 additional terrorist-supporter websites shut down through their volunteer efforts.

Al-Qa'ida has been on the Web since the late 1990s, initially through the website alneda.com (Weimann, 2006: p. 67). Representing the Center for Islamic Studies and Research, the site was used to publish propaganda and send messages to al-Qa'ida members. According to Bruce Hoffman, the site 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 (Hoffman, 2003). 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. The English-language version of their site included a 'Message to the American People,' calling on Americans to denounce their Administration and follow Islam, threatening more terror until Americans stop their transgression or 'one of us dies.' By 2002, the site was on the run, moving to different domains and service providers, as it was taken down at the request of federal officials. At one point, the domain name itself was hijacked by a Maryland hacker, who posted copies of the original web pages and operated the site as a decoy. After five days, however, his cover was blown when a message appeared on an Islamic message board saying the site was a trap (Di

Justo, 2002). After that, al-Qa'ida supporters purportedly began using hackers to place their files in obscure directories of other websites (Delio, 2003).

Today, the al-Qa'ida movement makes extensive use of the Web, with an estimated 5,600 sites as of January 2008 and 900 more appearing each year (Weimann, 2008). These sites include static (non-interactive) websites and interactive forums, chat rooms, message boards, and blogs. Not all of these websites play a significant role, however. Internet Haganah identified a list of key sites in 2007, based on the extent to which members of the global movement link to the site and draw content from it. Their top twelve included muslm.net, alfirdaws.org, alhanein.com, tajdeed.or.uk, al-boraq.com, alhesbah.org, alnusra.net, ikhwan.net, ekhlaas.org, al-faloja.com, farouqomar.net, and al-ommh.net (Internet Haganah, 2007). Many of these were active in 2006 and have remained active in 2008, although exact domain names change.

Jihadist websites are used to distribute a wide variety of materials to members, supporters, potential recruits, adversaries, and the public at large. These include writings and audio and video recordings of Osama bin Laden, Ayman al-Zawahiri, and other al-Qa'ida leaders and operatives; horrific videos of bombings, beheadings, and other terrorist acts; fatwas (religious edicts); electronic magazines; training manuals and videos; news reports; calls to join the jihad; threats to 'infidels;' and software tools. To illustrate, before his death in 2006, Abu Musab al-Zarqawi, leader of the al-Qa'ida affiliated Islamic State of Iraq (ISI), posted gruesome videos of ISI's deadly terrorist operations on the Internet along with videos to immortalize ISI's suicide bombers (Glasser and Coll, 2005). He started a monthly Internet magazine, offering religious justifications for jihad and advice on how to conduct it, and posted films of his bomb making classes so that his expertise would not be lost. In summer 2005, ISI averaged nine online postings per day (Kimmage, 2008). By 2008, however, their postings had dramatically declined, most likely because of the stepped-up efforts against ISI, including the capture or killing of 39 ISI members responsible for producing and disseminating materials on the Internet (Reuters, 2008).

Al-Qa'ida's media operations are supported by a network of quasi-official production and distribution entities that 'brand' jihadist media and provide an authorized channel for distribution on approved websites (Kimmage, 2008). These entities serve the core leaders of al-Qa'ida and the armed groups associated with it. Posted materials bear the logos of the originating armed groups and the media centers they used. Focus is on conflict zones, to include Iraq, Afghanistan, and Somalia. Three of the most prominent media entities are the al-Fajr Media Center, the as-Sahab Institute for Media Production, and the Global Islamic Media Front. Most of the products are in the form of text, but videos and audio recordings are also distributed. In 2007, as-Sahab alone released 74 videos, about one every three days (IntelCenter, 2007). The high quality products are often posted in multiple languages, including Arabic and English, and in multiple formats such as Windows Media, MPEG4, flash, and a format for mobile devices. In addition, audio and video clips are often broadcast by major media such as CNN and al-Jazeera, so al-Qa'ida's audience is not limited to Internet users.

Besides operating their own websites, jihadists have established groups in commercial networks such as Yahoo! and communities of interest on social networking sites. In 2006, Orkut reportedly had at least ten communities devoted to praising bin Laden, al-Qa'ida, or jihad against the United States, with one community drawing over 2,000 members (Hunt, 2006). In 2008, a posting on a jihadist forum advised 'all of the brothers' to create Yahoo! e-mail accounts and use e-mail groups to exchange messages. The author noted that authorities were striking jihadist websites, and the use of e-mail was intended to ensure jihadists were able to communicate (Internet Haganah, 2008).

Mass e-mailings have been used to reach broad audiences. The Jihadist Cyber-Attack Brigade, for example, announced in May 2008 they had successfully sent 26,000 e-mails to 'citizens of the Gulf and Arab countries explaining the words of our leader Usama Bin Ladin.' The announcement, which was posted to a jihadist website with links to a past bin Laden tape on 'Defending the Prophet,' claimed the operation was part of the 'Irhabi 007 Campaign.'

Irhabi (Terrorist) 007 was the codename for Younes Tsouli, a young man born in Morocco and living in West London. Tsouli assisted al-Qa'ida by operating websites for the terrorist group. He posted videos, statements, manuals, and other materials from Zarqawi and others on websites he set up and on anonymous File Transfer Protocol (FTP) servers he hijacked. For example, in July 2004 he uploaded about 60 files to an FTP server owned by the Arkansas State Highway and Transportation Department. He then posted a link to the files on al-Qa'ida's al-Ansar site (Labi, 2006).

Jihadists also recognize the value of using non-Jihadist websites to reach a larger audience, including the mainstream Arabic media. One outlet they have recommended is Wikinews. According to the Terrorism Research Center, a statement circulating on jihadist forums extols members to 'go to Wikinews and circulate the news of the Jihad and the Mujahideen.' TRC also noted that for a couple of days, the Arabic page of Wikinews (ar.wikinews.org) featured a statement from Omar al-Baghdadi, an Iraqi terrorist leader. However, the statement was removed and replaced with the message 'This is a terrorist article and has been deleted' (TRC, 2007). In addition to distributing news, jihadists see the potential of posting misinformation. For example, in response to a proposal on a jihadist forum to 'bankrupt American banks' by bombing them and causing 'a wave of withdrawals' by panicked customers, one respondent suggested that it might suffice to spread rumors through the Internet (OSC, 2008b).

Cyber Attacks

The term 'terrorism' generally refers to acts of violence, or threats thereof, against non-combatants. These acts, which are intended to coerce governments or institutions for social or political objectives, typically involve bombings, kidnappings, and other physical acts of murder or destruction. The Internet has transformed terrorism by adding another means of inflicting harm on non-combatants, namely through cyber attacks. While such attacks have so far resulted in neither death nor damage to physical property, the potential is there for producing these effects. A cyber

attack against the electric power grid, for example, could potentially destroy equipment and shut down power for an extended period of time, leading to loss of life and severe economic damage.

In the 1980s, Barry Collin, a former intelligence officer, coined the term ‘cyberterrorism’ to refer to the changing face of terrorism brought on by the convergence of the physical and virtual worlds. Collin later went on to outline scenarios in which terrorists could conduct cyber attacks with effects commensurate to physical acts of violence. In one, a cyberterrorist attack against the next generation of air traffic control system causes two large civilian aircraft to collide (Collin, 1997).

The term ‘cyberterrorism’ has been used to characterize everything from minor hacks to devastating attacks such as outlined by Collin. In 2001, the US National Infrastructure Protection Center defined it as ‘a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda.’ Although this definition allows for non-violent attacks, to include denial-of-service (DoS) attacks against Internet servers, government officials and scholars have been reluctant to label any cyber attack that has occurred so far as an act of cyberterrorism. This is because cyber attacks associated with terrorists have yet to produce damages or psychological effects comparable to those caused by bombings and other acts of violence. Indeed, they resemble those of other hackers who have nothing to do with terrorism. As a consequence, cyberterrorism is often dismissed as fear mongering.

The real issue, however, is not whether cyberterrorism is taking place today or whether it is a serious threat for the future. It is that the Internet has introduced a venue whereby hackers who align themselves with terrorist groups can inflict damage, particularly economic harm, without engaging in violence. They can do this at little cost and risk, and from anywhere in the world.

Individuals and groups who would never detonate a bomb or gun down another human being are thus able to support terrorist objectives. Moreover, not only can they launch attacks through the Internet, they can obtain hacking tools and information from the net as well. They do not need to worry about acquiring or manufacturing explosives, crossing borders, or funding their operations. The Internet has thus brought about an expansion of damaging acts in support of terrorist objectives, regardless of whether these acts are characterized as cyberterrorism or not.

The first reported incident of this nature took place in 1997 when a group aligning itself with 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' (CSI, 1998). Two years later, the Kosovo conflict inspired numerous hackers to join the conflict on one side or the other, or to protest the whole thing. Most of the cyber attacks took the form of web defacements and DoS attacks. Of particular interest here are the activities of the Serb Black Hand (Crna Ruka) group, because of the radical nature of Crna Ruka. According to reports, they crashed a Kosovo Albanian web site, planned daily actions against NATO computers, and deleted data on a Navy computer (Denning, 2001).

The first appearance of an al-Qa'ida associated hacker group appeared a few weeks after the September 11, 2001 terrorist attacks, when GForce Pakistan announced the formation of the 'Al-Qaeda Alliance Online' on a U.S. government website it had just defaced. Declaring that 'Osama bin Laden is a holy fighter, and whatever he says makes sense,' the group of Pakistani Muslim hackers posted a list of demands and warned that it planned to hit major U.S. military and British websites (McWilliams, 2001). Another GForce defacement contained similar messages along with heart-wrenching images of badly mutilated children said to have been killed by Israeli soldiers. A subsequent message from the group announced that two other Pakistani hacking groups had joined the alliance: the Pakistan Hackerz Club and Anti India Crew.

Collectively, the groups had already defaced hundreds of websites, often with political messages, in support of the objectives sought by Muslim terrorists fighting in Kashmir or against Israel. Although the group expressed support for bin Laden, they distanced themselves from terrorism. On October 27, GForce defaced a US military website with the message that it was 'not a group of cyber terrorists.' Condemning the attacks of September 11 and calling themselves 'cyber crusaders,' they wrote, 'ALL we ask for is PEACE for everyone.' This turned out to be one of their last recorded defacements. GForce Pakistan and all mention of the Al-Qaeda Alliance Online disappeared (Denning, 2006).

Other hackers, however, have emerged in their place, engaging in what is sometimes called 'electronic jihad.' Jihadist forums are used to distribute manuals and tools for hacking, and to promote and coordinate cyber attacks, including a DoS attack against the Vatican website, which mainly fizzled, and an 'Electronic Battle of Guantanamo' attack against American stock exchanges and banks, which was canceled because the banks had been notified. The al-Jinan forum has played a particularly active role, distributing a software tool called Electronic Jihad, which hackers can use to participate in DoS attacks against target websites that are deemed harmful to Islam. The forum even gives awards to participants who are the most effective (Bakier, 2007). The objective is to 'inflict maximum human, financial and morale damage on the enemy by using the Internet.'

The al-Farouq forum has also promoted electronic jihad, offering a hacker library with information for disrupting and destroying enemy electronic resources. The library held key-logging software for capturing keystrokes and acquiring passwords on compromised computers, software tools for hiding or misrepresenting the hacker's Internet address, and disk and system utilities for erasing hard disks and incapacitating Windows-based systems. Postings on the forum in 2005 called for heightened electronic attacks against US and allied government websites (Pool, 2005a). On another jihadist forum, a posting in October 2008 invited youths to participate in an 'electronic jihadist campaign' against US military systems by joining the 'Tariq Bin-Ziyad

Brigades.' The recently formed group was looking to increase its ranks so it could be more effective (OSC, 2008a).

In a February 2006 report, the Jamestown Foundation reported that 'most radical jihadi forums devote an entire section to (hacker warfare).' The al-Ghorabaa site, for example contained information on penetrating computer devices and intranet servers, stealing passwords, and security. It also contained an encyclopedia on hacking websites and a 344-page book on hacking techniques, including a step-by-step guide for 'terminating pornographic sites and those intended for the Jews and their supporters' (Ulph, 2006). The forum Minbar ahl al-Sunna wal-Jama'a (The Pulpit of the People of the Sunna) offered a hacking manual that was said to be written in a pedagogical style and discussed motives and incentives for computer-based attacks, including political, strategic, economic, and individual. The manual discussed three types of attack: direct intrusions into corporate and government networks, infiltration of personal computers to steal personal information, and interception of sensitive information such as credit card numbers in transit (Pool, 2005b). Younis Tsoulis (Irhabi 007) also promoted hacking, publishing a 74-page manual 'The Encyclopedia of Hacking the Zionist and Crusader Websites' with hacking instructions and a list of vulnerable websites (Jamestown, 2008).

Electronic jihad often coincides with physical forms of terrorism and protest. Publication of the Danish cartoons satirizing the Prophet Mohammad, for example, sparked a rash of cyber attacks as violence erupted on the streets in early 2006. Zone-h, a website that records web defacements, recorded almost 3,000 attacks against Danish websites by late February. In addition, the al-Ghorabaa site coordinated a 24-hour cyber attack against *Jyllands-Posten*, the newspaper that first published the cartoons, and other newspapers sites (Ulph, 2006). A video purporting to document a DoS attack against the *Jyllands-Posten* website was later released on the jihadist site 3asfh.com. The video was in the style of jihadist videos coming out of Iraq, showing that the hackers were emulating the tactics of violent jihadists (Internet Haganah, 2006b).

Jihadists often target websites that are used to actively oppose them. For example, a message posted to a Yahoo! group attempted to recruit 600 Muslims for jihad cyber attacks against Internet Haganah's website. 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 (Reynalds, 2004). 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 (ATC, 2004).

The use of electronic jihad to support al-Qa'ida is explicitly promoted in a book by Mohammad Bin Ahmad As-Sālim titled *39 Ways to Serve and Participate in Jihâd*. Initially published on al-Qa'ida's al-Farouq website in 2003 (Leyden, 2003), principle 34 in the book discusses two forms of 'electronic *Jihâd*:' discussion boards (for media operations) and hacking methods, about which the book writes: 'this is truly deserving of the term "electronic *Jihâd*," since the term carries the meaning of force; to strike and to attack. So, whoever is given knowledge in this field, then he should not be stingy with it in regards to using it to serve the *Jihâd*. He should concentrate his efforts on destroying any American websites, as well as any sites that are anti-*Jihâd* and *Mujâhidîn*, Jewish websites, modernist and secular websites' (As-Sālim, 2003).

Al-Qa'ida has long recognized the value of inflicting economic harm on the U.S., and electronic jihad is seen as tool for doing so. After the Electronic Battle of Gauntanamo was canceled, a message posted on an Islamist website stated how 'disabling (stock market and bank websites) for a few days or even for a few hours … will cause millions of dollars worth of damage' (Alshech, 2007). A message on al-Jinan noted that hacking methods could 'inflict the greatest (possible) financial damage' on their enemies. According to Fouad Husseing, economically damaging cyber attacks are part of al-Qa'ida's long-term war against the U.S. In his book, *al-Zarqawi-al-Qaeda's Second Generation*, Husseing describes al-Qa'ida's seven-phase war as

revealed through interviews of the organization's top lieutenants. Phase 4, which is scheduled for the period 2010-2013, includes conducting cyberterrorism against the U.S. economy (Hall, 2005).

Although damages from cyber attacks attributed to al-Qa'ida and associated hackers so far has been minor compared to the damages from al-Qa'ida's violent acts of terror and even the cyber attacks of other actors such as the Russians who attacked Estonian websites in 2007, Husseing's book and other writings suggest that al-Qa'ida may be thinking bigger. A posting in a jihadist forum advocated attacking all computer networks around the world, including military and telecommunication networks, in order to 'bring about the total collapse of the West' (Alshech, 2007). Of course, the idea of shutting down every single network is utter fantasy, so vision by itself does not translate into a threat.

Recruitment

The Internet has transformed terrorist recruitment by providing a venue through which potential terrorists and supporters world-wide can learn about terrorist groups, join or provide assistance through Internet forums and groups, and engage in direct actions that serve terrorist objectives. They can contribute to Internet media operations, engage in cyber attacks, and donate money, software, and expertise through Internet channels. If desired, they can do all this without traveling or even formally joining. They simply sign up through their deeds. However, for those wishing to be part of the physical action, the Internet has facilitated the processes of joining and getting to a terrorist location as well.

The Internet has been particularly instrumental to the spread of al-Qa'ida. Indeed, it probably fair to say that the jihadist social movement associated with the terrorist organization would not exist without the Internet. The Internet has allowed self-selected individuals and groups of friends to formally or informally join the network, while operating independently from the central organization. And they can live anywhere in the world. The effect is a highly decentralized network of participants who operate in closely knit groups (cells) with little or no direction or even

recognition from al-Qa'ida's core leadership. This social network is held together largely through the Internet.

Jihadist forums have played a prominent role in al-Qa'ida's recruitment strategy. In one forum, a participant nicknamed Wali al-Haq posted the steps a candidate should take to join al-Qa'ida: 1) understand and adhere to the identity, ideology, and objectives of al-Qa'ida; 2) prepare physically, scientifically and spiritually; and 3) either directly join a jihadist faction or pursue a solitary path in taking up the jihadist cause. According to al-Haq, any Muslim who supports al-Qaeda in any way, be it financially, physically or by simply showing desire of intent to join, is considered to be a jihadist in al-Qaeda (Bakier, 2008a). On another forum, would-be jihadists were invited to sign an oath of loyalty to bin Laden, al-Zawahiri, Zarqawi, and Taliban chief Mullah Muhammad Omar. The announcement said 'This is the Internet that Allah operates in the service of jihad and of the mujahedoun … such that half the mujahedoun's battle is waged on the pages of the Internet, which is the only outlet for passing announcements to the mujahedoun' (MEMRI, 2005).

As-Sālim's book, *The 39 Principles of Jihad*, calls upon every Muslim to 'obey the Jihad against the infidels.' In addition to engaging in electronic jihad (principal 34), the book suggests participating in martyrdom and other operations, supplying money and equipment to fighters, fund raising, assisting families of fighters, preaching, prayer, educating children, and so forth (As-Sālim, 2003). In effect, there is something for everyone.

Marc Sageman, author of *Leaderless Jihad*, has observed that while websites have been instrumental for distributing documents and other materials, it is through the interactive forums that relationships are built, bonding takes place, and beliefs are hardened. He writes, 'It is the forums, not the images of the passive websites, which are crucial in the process of radicalization. People change their minds through discussion with friends, not by simply reading impersonal stories' (Sageman, 2008: 116). Sageman believes that the forums are to the current generation of

jihadists what the mosques were to the previous generation. They play a much larger role in al-Qa'ida's efforts to recruit jihadists than the passive websites, where the visitors are already predisposed to the views that are promulgated. Moreover, it is in conversation that commitments are made, plans are hatched, and actions are put into motion. In today's networked world, these conversations can as easily be online as in person. However, William McCants, a fellow at the Combatting Terrorism Center at West Point, notes that face-to-face contact with committed militants usually precedes online activity and is essential for continued radicalization. He also says that the mainstream Muslim forums play a bigger role in Jihadist missionary activity than the jihadist forums (McCants, 2008).

Jihadi Web forums have helped bring would-be jihadists to Iraq. Citing Rita Katz, director of the SITE Institute, the *New York Post* reported in September 2003 that a 'maze of secret chat rooms' was used to direct potential recruits into Iraq (Lathem, 2003). After expressing interest in one of these rooms, a candidate received a propaganda video from someone calling himself Merciless Terrorist. The video instructed him to download software called Pay Talk, which would allow him to communicate by voice in an 'impossible to monitor "talking chat room."' There, the would-be-terrorist is given more detailed instructions and directed to a sympathetic Islamic center or mosque for screening.

According to Evan Kohlmann, Al-Qa'ida's al-Ansar forum was 'a virtual matchmaking service for budding Islamic militants searching for a path to jihad, and particularly for the emerging mujahidin frontline in Iraq. In one case, a Moroccan user asked for help contacting Zarqawi's network in Iraq, whereupon his travel arrangements were brokered on his behalf over e-mail (Kohlmann, 2008). For jihadists transiting Syria on their way to Iraq, the forum www.nnuu.org offered instructions about what to do (Ulph, 2005). Another forum held a live interview with a militant in Iraq, who answered questions about the progress of the conflict in Iraq and how to emigrate and join the fighting (Drennan and Black, 2007).

Terrorists use the Internet to recruit children as well as adults, offering slick videos, comic-book style readings, and computer games. For example, a radical Islamic website in the U.K. posted a rap video designed to inspire young people to take up jihad 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.' On one of Hizballah's websites, kids can download a computer game called 'Special Force.' The game, which is based on the Israeli invasion of Lebanon in 1978 and 1982 and their forced withdrawal in 2000, involves liberating the military posts occupied by the Israelis. It was designed to introduce young people to the resistance and help win the international media war with Israel (WorldNetDaily, 2003).

In addition to recruiting supporters of terrorism, the Internet has been used in at least one case to entrap an unsuspecting victim for a terrorist act. In January 2001, a Palestinian woman in Yassir Arafat's Fatah organization went to an Internet chat room, where she presented herself as an Israeli woman of Moroccan background to a young Israeli man. After he agreed to meet her in Jerusalem, she drove him into Palestinian territory, where a gunman was waiting to end the man's life (Nacos, 2002: 103-104).

Learning

The Internet in transforming terrorist learning by giving terrorists a fast and easy way to learn about terrorist ideology, methods, and targets. They can educate themselves, alone or in small groups, without the need to visit a library, travel to a terrorist training camp, or enroll in a university.

Al-Qa'ida clearly recognizes the value of the Internet for education and training. One prominent leader, Aub Musab al-Suri (now in US custody), contended that by taking advantage of information technology, Muslims can access military and ideological training in any language, at any time, anywhere (CTC, 2006: p. 54).

In November 2003, the Saudi-owned London daily *Al-Shrq al-Awsat* reported that al-Qa'ida had opened Al-Qa'ida University for Jihad Sciences on the Internet. The virtual university was said to comprise several 'colleges,' including colleges for the technology of explosive devices, booby-trapped cars and vehicles, electronic jihad, and media jihad.

Al-Qa'ida's online 'university' is realized by a collection of web forums with instructional materials in the form of manuals, magazines, and videos, as well as on-line discussions and coaching. In addition to the hacking manuals described earlier, jihadist sites provide documents and videos on how to build and use various types of physical weapons such as explosives, poisons, AK-47s, and surface-to-air missiles. Information about explosives has included chemical formulas and diagrams for the large-scale production of explosives such as TNT, C4, and PETN; a blueprint for a nitrate-producing machine for making improvised explosives; instructions for evading airport scanning machines (Nathan, 2003); a do-it-yourself plan for making dirty bombs (Al-Matrafi, 2005); and a video for constructing a suicide bomb vest (Myers, 2004). In one forum, a terrorist who had trouble building a bomb received coaching that allowed him to succeed. Besides weapons, Jihadist manuals provide instructions on such topics as intelligence, interrogations, kidnapping, assassinations, operations security, and terrorist cells. There is even a 51-page manual on recruiting, explaining how to select candidates and a three-phase process for winning them over (Bakier, 2008b).

At least some of the instructional materials are rather archaic. For example, the 'Al Qaeda Training Manual,' found by British police and released by the Department of Justice in 2001, says nothing about computers, software, the Internet, cell phones, satellite phones, or other modern information technologies known to be used by al-Qa'ida. The section on secret writing and ciphers (lesson 13) makes no mention of modern cryptographic systems and is based entirely on manual methods that appear to be at least 50 to 100 years old. More recent training

documents, however, cover computers, e-mail, the Internet and Web, encryption, and other modern information technologies.

In January 2004, jihadists launched two educational magazines on the Internet. The first, called the *Al-Battar Training Camp*, was introduced to give Muslim youth jihad training without the need to travel to a terrorist training camp. Published by the Military Committee of the Mujahideen in the Arabian Peninsula, the electronic publication offered instruction and exercises in the use of arms (WorldNetDaily, 2004). The sixth issue, published in March 2004, gave a detailed description of the organization structure of a project cell, described desired skill sets, and emphasized 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 (Mansfield, 2004). The magazine appeared to have been discontinued by the end of the year. The second magazine, called the *Base of the Vanguard*, was directed at new recruits who could not break cover to undergo formal training. Spearheaded by Saif al-Adel, the manual contains quotes and articles by al-Qa'ida leaders, including bin Laden and al-Zawhiri. It gave technical advice on physical training, operations security, and light weapons; encouraged the use of weapons of mass destruction, and warned operatives to resist counter-terrorist psychological operations: 'They will try and wear down your morale by publishing false reports about the arrest of other cells' (Burke, 2004). In late 2006, jihadists launched a third educational magazine that focused on technical issues. Called *The Technical Mujahid*, the first two issues covered information security technologies, including software tools for encryption (discussed later in this paper). The magazine was released by the Al-Fajr Media Center (CIIR, 2007).

Al-Qa'ida's online training materials have been instrumental to jihadists planning attacks. According to *The Daily Telegraph*, Nick Reilly, the 22-year old suicide bomber in the UK who tried unsuccessfully to detonate a series of nail bombs, learned how to make the bombs from videos posted on YouTube. The Telegraph also reported that Reilly had been 'groomed by two men on

the YouTube website who claimed to be living on the Afghan-Pakistan border and to be in touch with al-Qaeda' (Gardham, 2008).

Jihadists have expressed an interest in virtual reality tools, in particular flight simulation software (Internet Haganah, 2006a). Virtual reality might also be used for instruction in particular weapons such as surface-to-air missiles or to lead would-be suicide bombers through the process of detonating their bombs and receiving their promised virgins and other heavenly rewards.

Despite the benefits of online training, it comes at a price, as potential terrorists do not have the opportunity to meet established terrorists and develop personal bonds of trust. Further, online training in the use of physical weapons is not likely to be as effective as getting hands-on experience in a camp with experienced instructors. However, these limitations can be overcome if terrorists work in small groups that meet physically, and use on-line coaching to help them through difficulties. Al-Suri envisioned Muslim homes serving as training camps as well as staging grounds for waging jihad (CTC, 2006: 54).

In addition to learning from materials posted on jihadist websites, jihadists use the Internet for research. For example, in January 2002, the National Infrastructure Protection System (NIPC) reported that al-Qa'ida members had 'sought information on Supervisory Control and Data Acquisition (SCADA) systems available on multiple SCADA-related websites. They specifically sought information on water supply and wastewater management practices in the U.S. and abroad' (NIPC, 2002). Such information could be useful in planning either physical or cyber attacks against SCADA-controlled critical infrastructures.

Although most jihadist research may be conducted on public websites, there has been at least one reported incident of jihadists breaking into accounts to collect intelligence. According to Magnus Ranstorp, al-Qa'ida hackers used simple password cracking tools, freely available on the Internet, to gain access to the e-mail account of a US diplomat in the Arab world. They had

retrieved his bank statements, which revealed information about his location and movement (Ranstorp, 2004).

Finance

The Internet has given terrorists new ways of raising, spending, and hiding money. Funds are raised through on-line solicitations and various cyber crimes such as identity theft and credit card fraud. The Tamil Tigers pioneered both in a single operation. After compromising a computer system at Sheffield University in England in 1997 and capturing the user IDs and passwords of faculty, they used the email accounts to send out messages asking donors to send money to a charity in Sri Lanka (Vatis, 2001).

Al-Qa'ida has used the Internet to solicit and move funds. In addition, they have funded purchases through online credit card fraud. Younes Tsouli (Irhabi 007), for example, used stolen identities and credit card numbers to pay for web hosting services. To acquire card numbers, he and his two cohorts planted keystroke loggers on their websites and sent out e-mails with links to fake websites requesting financial information (Krebs, 2007; Mansfield, 2006). The trio ran up $3.5 million in fraudulent charges, registered more than 180 website domains with 96 different Web hosting companies, purchased hundreds of prepaid cell phones and more than 250 airline tickets, and laundered money through online gaming sites (Lormel, 2008).

In his autobiography *Me Against the Terrorist!*, 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. A chapter titled "Hacking: why not?" offers rudimentary information on hacking, particularly as it applies to credit card fraud. Evidence found on his seized computer showed he at least had made an attempt at carding (Sipress, 2004).

Even if terrorists do not use stolen card numbers to make purchases, online transactions can lower procurement costs and speed transaction times. They also can provide some level of

secrecy. On one jihadist forum, a participant suggested establishing phony online retail stores for receiving contributions to the jihad. Another suggested using the CashU online service, which was said to allow money payments and transfers without risk of theft, fraud, or exposure of personal information (MEMRI, 2007).

Security

Operations security has always been a concern for terrorists. Because of their violent acts, they must hide from police and military forces. Traditionally, this has entailed using safe houses, code words, encryption, dead drops, false identities, and other methods of concealment.

In using the Internet, terrorists expose themselves to a new set of risks. If they take no security precautions at all, authorities can monitor their online activities, collect evidence, and determine their physical locations. Terrorists are generally aware of these vulnerabilities, and so have learned and adopted new security practices. Some of the tools they use include the use of cyber cafés, anonymous e-mail accounts, virtual dead drops, coded and encrypted e-mail, encrypted files and disks, hidden files and directories, password-protected websites and forums, and anonymous web browsing via proxies.

The September 11 hijackers, for example, accessed anonymous Hotmail and Yahoo! accounts from computers at Kinko's and at a public library (Ross, 2001). 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' (Ha'aretz, 2002). The faculties referred to the four targets (World Trade Center twin towers, Pentagon, and Capitol); the faculty for urban planning may have represented the tower hit by Atta's plane since he had studied urban planning in Hamburg, Germany.

According to reports, the principal architect of the 9/11 attacks, Khalid Shaikh Mohammed, trained high-level al-Qa'ida operatives in the use of encryption (AFP, 2005). One of his pupils might have been his nephew, Ramzi Yousef, a key operative in the 1993 World Trade Center bombing. Yousef stored information about his Bojinka plot to destroy eleven airliners on his laptop in encrypted files. The encryption was sufficiently robust that it took cryptanalysts more than a year to break the code (Freeh, 1997). However, some of the encryption used by al-Qa'ida has been much easier to crack. Files on al-Qa'ida computers acquired by the *Wall Street Journal* in Afghanistan in November 2001, for example, were encrypted with Microsoft's 40-bit version of the Data Encryption Standard (DES), a weak version of DES that had been approved for export (stronger codes are now exportable) (Hooper, 2001).

Jihadists have developed encryption software that at least superficially rivals strong products like Pretty Good Privacy (PGP). Al-Qa'ida's Mujahideen Secrets, for example, offers 2048-bit asymmetric (public-key) and 256-bit symmetric (single-key) encryption using the latest US standards, including the Advanced Encryption Standard. The tool, initially released in 2007 by the Global Islamic Media Front, is described in the second issue of *The Technical Mujahid*. According to the magazine, the GIMF developed their own software because they did not trust 'foreign' programs such as PGP. The software can be run from a memory stick, allowing easy portability. While encrypting files with the tool is fairly straightforward, sending encrypted messages is more complicated, as users must first acquire the public keys of their correspondents and then copy-paste encrypted text into message windows (CIIR, 2007).

The second issue of *The Technical Mujahid* also discusses steganography, or methods of hiding messages in cover media such as image and audio files (CIIR, 2007). A steganographic technique was introduced in the first issue as well, as part of a general discussion about how to conceal files on computer. The method, called Alternate Data Streams (ADS), allows hidden data to be associated with a file (TRC, 2006b).

Despite al-Qa'ida's interest in steganography, there have been no confirmed reports of jihadists actually using it. There have been indicators of possible use, including jihadist files that tested positive with steganographic detection tools. However, the codes could not be cracked, so the test results may have been false positives. In one case, reported by *ABC News* in October 2001, 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' (Ross, 2001).

In addition to having expertise in encryption, Khalid Shaikh Mohammed is said to have communicated through an e-mail 'virtual dead drop,' where messages are composed but never sent. Instead, they are saved as drafts and then read by the intended recipient from the draft message folder of a shared e-mail account (AFP, 2005). Other jihadists have also used this technique, including one of the convicted terrorists behind the Madrid train bombings in 2004 (Johnson, 2005).

Jihadists make extensive use of password-protected web forums for private meetings and discussions. They are like virtual safe houses, but more vulnerable to monitoring and infiltration than their physical counterparts. Jihadists are aware of these risks and urge caution on the private forums, as well as on public ones. They tell members to access the sites from Internet cafés, but not the same one repeatedly, and to use proxies to conceal their IP addresses; to be suspicious of other participants and wary about what they read and post; to use different usernames and passwords on different forums, and to guard their passwords; to be careful about giving out personal information; and to watch out for spyware and other forms of malicious software. To mitigate the risks, some jihadist forums have implemented 'cloaking' technology, which blocks forum access from IP addresses in the US in order to keep US intelligence services from monitoring the forums. However, if the IP check is only performed for accesses via the

website's home page, spies may still be able to gain access by going to an inner page on the site (TRC, 2006a).

Implications for Counterterrorism

Just as the Internet is transforming terrorism, it is also transforming counterterrorism by providing another channel whereby terrorists can be monitored and potentially subverted. Further, such counterterrorism activities can be performed remotely and from a safe location, avoiding the difficulties and risks associated with infiltrating terrorists' physical space. One effect is that individuals and groups from all over the world can participate in counterterrorism as independent agents. In effect, al-Qa'ida's own network of jihadists is matched by a global network of counter-jihadists. The following briefly describes four counterterrorism strategies that explicitly take advantage of al-Qa'ida's Internet presence: intelligence collection, denial, subversion, and engagement.

The first strategy, intelligence collection, involves monitoring al-Qa'ida's Internet forums and message exchanges in order to develop actionable intelligence regarding their members and social networks; safe houses and other facilities where members gather and weapons are produced; proposals and plans for terrorist acts; financial sources and transactions; and other relevant information. Information gleaned from such surveillance can be used to thwart plots and facilitate arrests and convictions. Law enforcement and intelligence agencies engage in such monitoring, and it has been valuable in the fight against al-Qa'ida. Individuals working alone and with groups such as Internet Haganah and SITE also contribute to the effort. Posing as a jihadist from the safety of her home, retired Montana judge Shannen Rossmiller has infiltrated al-Qa'ida websites and passed along information to the FBI. Her findings have led to numerous terrorist arrests and convictions (Rossmiller, 2007).

The second strategy, denial, involves taking actions that deny al-Qa'ida access to the Internet, for example, by shutting down their e-mail accounts, websites, and forums, and by

removing jihadist content from other sites. The premise is that by getting al-Qa'ida off the net, they will be unable to post materials and engage with potential recruits. Further, communications among jihadists will be severely hampered, making it more difficult for them to plan and organize actions. Internet Service Providers already practice some denial by shutting down websites that directly advocate violence or provide support to known terrorist organizations in violation of laws. In addition, sites such as YouTube help by removing videos that train terrorists or incite violence. However, the sites and content often reappear elsewhere, so the effects may not last. Another problem with denial is that much of the content posted by jihadists is permissible under principles of free speech. Denial also has adverse effects on intelligence collection, potentially taking away valuable sources of information as sites move and jihadists move further underground on the Internet or off the net entirely. Further, denial requires international cooperation to be fully successful, as jihadist accounts and websites can be hosted all over the world. Such cooperation can be difficult to achieve.

Still, denial can impair al-Qa'ida's efficiency and undermine trust in their online sites. To illustrate, in September 2008, al-Qa'ida's media arm was severely hampered when several of its key websites went down. A month later, only one forum, al-Hesbah, was back online. The effect was to curtail the dissemination of videos and other materials from al-Qa'ida's leadership and to raise suspicions about infiltrators and the authenticity of look-alike sites (Knickmeyer, 2008). On one jihadist forum, a participant posted a message expressing alarm over the attacks and urging the recruitment of computer specialists to address the problem. He asked what would happen if they had no jihadist forums or websites, and then answered that it 'would bring all communication between the mujahidin and the children of the Islamic nation to an end.' He said it would 'delay the carrying out of operations and the transmission of jihadist news' (OSC, 2008c).

The third strategy, subversion, involves infiltrating al-Qa'ida forums, disrupting their operations, and undermining al-Qa'ida objectives, for example, by injecting misinformation into a forum discussion in order to erode trust in a leader or sow seeds of discord. One drawback of

subversion strategies is that they are risky – operations can have unintended consequences and backfire. Also, if not coordinated with intelligence operations, they can undermine collection efforts and lead to false conclusions. However, the strategy should not be dismissed outright, as subversive techniques can be effective. Already, participants in some jihadist forums have warned that intelligence services and other opponents may have infiltrated the forums in order to fuel discord and distort the forum, suggesting that the forums were not operating as smoothly and effectively as they would like (OSC, 2008d, 2008e).

The fourth strategy, engagement, involves conversing with jihadists and potential recruits in online forums, challenging basic premises and beliefs through dialog and writings. The goal is to draw people out of the movement and deter potential recruits from joining. If indeed it is through conversations that potential recruits are radicalized and become committed to the jihad, then alternative conversations may be employed to lead them in the opposite direction. Saudi Arabia's online Al-Sakinah ('Tranquility') campaign illustrates this. Muslim scholars and sheikhs with expertise on Islam, aided by experts in sociology and psychology, enter extremist web forums and engage with participants, encouraging them to renounce their extremist ideas. According to reports, the campaign has been successful. About 700 individuals recanted their beliefs, including high-ranking members of al-Qa'ida (Cilluffo, 2007; Yehoshua, 2006).

These four strategies can be used together and in combination with other strategies that are not Internet specific, for example, capturing al-Qa'ida terrorists, countering al-Qa'ida's ideology, and winning 'hearts and minds.' They have the advantage of directly targeting the media that is holding the global movement together. Without the Internet, al-Qa'ida would not likely have its global reach, either as a terrorist network or as an inspiration.

Further Reading

Despite the large number of books on terrorism, only one is devoted to terrorist use of the Internet, namely Garbriel Weimann's *Terror on the Internet* (2006, United States Institute of

Peace). Fortunately, it is very good. For new developments, Internet Haganah (internet-haganah.com/haganah/) is an excellent resource.

References

AFP (2005) 'Cyber-jihadists weave a dangerous web,' Agence France-Presse, October 27.

Al-Matrafi, S. (2005) 'Terrorist Website Drops Dirty Bomb,' *Arab News*, March 11.

Alshech, E. (2007) 'Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad,' *MEMRI Inquiry and Analysis Series*, No. 329 (The Middle East Media Research Institute), February 7.

As-Sālim, M. (2003) *39 Ways to Serve and Participate in Jihâd* (At-Tibyân Publications), http://tibyan.wordpress.com/2007/08/24/39-ways-to-serve-and-participate-in-jihad/ (accessed June 30, 2008).

ATC (2004) 'ATC's OBL Crew Investigation,' Anti-Terrorism Coalition, July 1.

Bakier, A. H. (2007) 'Forum Users Improve Electronic Jihad Technology,' *Terrorism Focus*, 4:20, June 26.

Bakier, A. H. (2008a) 'Jihadi Website Advises Recruits on How to Join al-Qaeda,' *Terrorism Focus*, 5:18, May 6.

Bakier, A. H. (2008b) 'Jihadis Publish Online Recruitment Manual,' *Terrorism Focus*, 5:34, September 24.

Burke, J. (2004) 'Al-Qaeda Launches Online Terrorist Manual,' *Observer*, January 19.

CIIR (2007) 'Al-Qaida Media Arm Releases the Second Issue of Its Tech Magazine,' Global Issues Report, Center for International Issues Research, March 19.

Cilluffo, F. et al. (2007) 'NETworked Radicalization: A Counter Strategy,' The George Washington University Homeland Security Policy Institute and the University of Virginia Critical Incident Analysis Group.

Collin, B. (1997) 'The Future of Cyberterrorism: The Physical and Virtual Worlds Converge,' *Crime & Justice International*, March.

CSI (1998) 'Email Attack on Sri Lanka Computers,' *Computer Security Alert*, No. 183, Computer Security Institute, June, p. 8.

CTC (2006) 'Harmony and Disharmony: Exploiting al-Qa'ida's Organizational Vulnerabilities,' Combating Terrorism Center, United States Military Academy, West Point, February 14.

Delio, M. (2003) 'Al-Qa'ida Website Refuses to Die,' *Wired News*, April 7.

Denning, D. E. (2001) 'Activism, Hacktivism, and Cyberterrorism,' in J. Arquilla and D. Ronfelt (eds) *Networks and Netwars* (Santa Monica: RAND), p. 273.

Denning, D. E. (2006) 'A View of Cyberterrorism Five Years Later,' in K. Himma (ed) *Readings in Internet Security: Hacking, Counterhacking, and Society* (Boston: Jones and Bartlett).

Di Justo, P. (2002) 'How Al-Qaida Site Was Hijacked,' *Wired News*, August 10, 2002.

Drennan, S. and Black, A. (2007) 'Jihad Online – The Changing Role of the Internet,' *Janes*.

Freeh, L. J. (1997) Statement before the Senate Committee on Commerce, Science, and Transportation, regarding the Impact of Encryption on Law Enforcement and Public Safety, March 19.

Gardham, D. (2008) 'Al-Qaeda Terrorists Who Brainwashed Exeter Suicide Bomber Still on the Run,' *The Daily Telegraph*, October 16, 2008.

Glasser, S. B. and Coll, S. (2005) 'The Web as Weapon: Zarqawi Intertwines Acts on Ground with Propaganda Campaign on the Internet,' *The Washington Post*, August 9.

Ha'aretz (2002) 'Virtual Soldiers in a Holy War,' *Ha'aretz Daily*, September 16.

Hall, A. (2005) 'Al-Qaeda Chiefs Reveal World Domination Design,' *The Age*, August 24.

Rossmiller, S. (2007) 'My Cyber Counter-Jihad,' *Middle East Quarterly,* Summer.

Hoffman, B. (2003) 'Al Qaeda, Trends in Terrorism, and Future Potentialities: An Assessment, *Studies in Conflict & Terrorism,* 26:429-442.

Hoffman, B. (2006) 'The Use of the Internet By Islamic Extremists,' Testimony presented to the House Permanent Select Committee on Intelligence, May 4.

Hooper, I. (2001) 'Kabul Computer Reveals Files of Top Al Qaeda Officials,' Associated Press, December 21.

Hunt, K. (2006) 'Osama Bin Laden Fan Clubs Build Online Communities,' *USA Today*, March 9.

IntelCenter (2007) 'al-Qaeda Messaging Statistics (QMS),' v3.3, September 9.

Internet Haganah (2006a) 'Don't You Just Love It When ...,' January 28, http://internet-haganah.com/harchives/005435.html (accessed October 21, 2008).

Internet Haganah (2006b) 'How the Brothers Attacked the Website of Jyllands-Posten,' February 7, http://internet-haganah.com/harchives/005456.html (accessed October 21, 2008).

Internet Haganah (2007) 'Top…Nineteen List of Arabic Salafist/Jihadist Sites,' April 22, http://internet-haganah.com/harchives/006013.html (accessed April 24, 2007).

Internet Haganah (2008) 'Portrait of Rats, Preparing to Drown,' October 10, http://internet-haganah.com/harchives/006420.html (accessed October 10, 2008).

Internet World Stats (2008) 'Internet Usage Statistics,' http://www.internetworldstats.com/stats.htm (accessed October 8, 2008).

Jamestown (2008) 'Hacking Manual by Jailed Jihadi Appears on Web," *Terrorism Focus*, 5:9, Jamestown Foundation, March 4.

Johnson, K. (2005) 'Terrorist Threat Shifts as Groups Mutate and Merge,' *The Wall Street Journal*, February 14.

Kimmage, D. (2008) 'The Al-Qaeda Media Nexus,' RFE/RFL (RadioFreeEurope/RadioLiberty) Special Report, March.

Knickmeyer, E. (2008) 'Al-Qaeda Web Forums Abruptly Taken Offline,' *Washington Post*, October 18.

Kohlmann, E. F. (2008) 'Al-Qa'ida's "MySpace": Terrorist Recruitment on the Internet,' *CTC Sentinel*, 1:2, January.

Krebs, B. (2007) 'Terrorism's Hook Into Your Inbox,' *The Washington Post*, July 5.

Labi, N. (2006) 'Jihad 2.0,' *The Atlantic Monthly*, July/August.

Lathem, N. (2003) 'Al-Qa'ida Trolls Net,' *New York Post*, September 15.

Leyden, J. (2003) 'Al-Qaeda: The 39 Principles of Holy War,' *Virtual Jerusalem*.

Lormel, D. (2008) 'Credit Cards and Terrorists,' Counterterrorism Blog, January 16.

Mansfield, L. (2004) 'Everything You Always Wanted to Know About Becoming a Terrorist, but Were Afraid to Ask,' Northeast Intelligence Network, March.

Mansfield, L. (2006) 'Me and Terrorist 007,' March 1, 2006, http://www.lauramansfield.com/j/007.asp (accessed March 27, 2008)

McLeod, J. (2007) 'Exposing On-Line Jihadists,' *Canada Free Press*, August 10.

McCants, W. (2008) 'How Online Recruitment Works,' September 18, http://www.jihadica.com/how-online-recruitment-works/ (accessed October 10, 2008)

McWilliams, B (2001) 'Pakistani Hackers Deface U.S. Site With Ultimatum,' *Newsbytes*, October 17.

MEMRI (2005) 'Now Online: Swear Loyalty to al-Qa'ida Leaders,' *MEMRI Special Dispatch Series*, No. 1027 (The Middle East Media Research Institute), November 18.

MEMRI (2007) 'Islamists Propose Ways to Transfer Funds to Islamic State of Iraq,' Islamic Websites Monitor No. 84, *MEMRI Special Dispatch*, No. 1543 (The Middle East Media Research Institute), April 13.

Myers, L (2004) 'Web Video Teaches Terrorists to Make Bomb Vest,' *MSNBC News*, December 22, http://www.msnbc.msn.com/id/6746756/ (accessed October 9, 2008).

Nacos, B. L. (2002) *Mass-Mediated Terrorism* (Oxford: Rowman & Littlefield Publishers, Inc.).

Nathan, A. (2003) 'Bomb Designed to Evade Airport Scanning Machines,' *Times Online*, October 26.

NIPC (2002) 'Terrorist Interest in Water Supply and SCADA Systems,' Information Bulletin 01-001, National Infrastructure Protection Center, January 30.

OSC (2008a) 'Jihadist Forum Invites Youths to Join "Electronic Jihadist Campaign",' Open Source Center, October 6, 2008.

OSC (2008b) 'Jihadist Forum Member Proposes Attacking US Banks, Elicits Discussion,' Open Source Center, October 6, 2008.

OSC (2008c) 'Forum Member Discusses Importance of Jihadist Websites; Suggests Asking for Help,' Open Source Center, October 8.

OSC (2008d) 'Jihadist Forum Member Warns of "Intellectual Discord" in Forums,' Open Source Center, October 9.

OSC (2008e) 'Website Posts Article Expressing Concern That Members May Belong to Intelligence Services,' Opens Source Center, November 10.

Pool, J. (2005a) 'New Web Forum Postings Call for Intensified Electronic Jihad Against Government Websites,' Jamestown Foundation, August 23.

Pool, J. (2005b) 'Technology and Security Discussions on the Jihadist Forums,' Jamestown Foundation, October 11.

Ranstorp, M. (2004) 'Al-Qaida in Cyberspace: Future Challenges of Terrorism in an Information Age,' in L. Nicander and M. Ranstorp (eds) *Terrorism in the Information Age – New Frontiers?* (Stockholm: Swedish National Defence College).

Regan, T. (1999) 'How Terrorists Use the Internet to Spread Their Messages,' *Christian Science Monitor*, July 1.

Reuters (2008) 'US Military Says Hits Al Qaeda Propaganda Units,' Reuters, March 22.

Reynalds, J. (2004) 'Internet "Terrorist" Using Yahoo to Recruit 600 Muslims for Hack Attack,' *Mensnewsdaily.com*, February 28, http://www.mensnewsdaily.com/archive/r/reynalds/04/reynalds022804.htm (accessed October 21, 2008).

Ross, B. (2001) ‘A Secret Language,’ *ABCNEWS.com*, October 4.

Sageman, M. (2008) *Leaderless Jihad* (Philadephia: University of Pennsylvania Press).

Salomon, A (2003) ‘Terrorists Twin Tower Images, Secret Porn Messages,’ *ABCNEWS.com*, May 8, 2003.

Sipress, A. (2004) ‘An Indonesian’s Prison Memoir Takes Holy War Into Cyberspace,’ *The Washington Post*, December 14, p. A19.

TRC (2006a) ‘Al Qaeda Has No Cloak,’ Terrorism Research Center, July 21.

TRC (2006b) ‘The Technical Mujahid Takes on Covert Communication,’ Terrorism Research Center, December 11.

TRC (2007) ‘Jihadists See Wiki News Service as Potential Propaganda Tool,’ Terrorism Research Center, January 26.

Tsfati, Y. and Weimann, G. (2002) ‘www.terrorism.com: Terror on the Internet,’ *Studies in Conflict & Terrorism*, 25, pp. 317-332.

Ulph, S. (2005) ‘Islamist Website Issues Travel Warning for Syrian Mujahideen Crossing Into Iraq,’ *Terrorism Focus*, 2:7, Jamestown Foundation, March 31.

Ulph, S. (2006) ‘Internet Mujahideen Refine Electronic Warfare Tactics,’ *Terrorism Focus*, 3:5, Jamestown Foundation, February 7.

Vatis, M. (2001) 'Cyber Terrorism and Information Warfare: Government Perspectives,' in Y. Alexander and M. S. Swetnam (eds.) *Cyber Terrorism and Information Warfare*, (Transnational Publishers, Inc.).

Weimann, G. (2006) *Terror on the Internet* (Washington, DC: United States Institute of Peace).

Weimann, G. (2008) 'Al-Qa'ida's Extensive Use of the Internet,' *CTC Centenial*, 1:2, pp. 607.

Whitelaw, K. (1998) 'Terrorists on the Web: Electronic "Safe Haven,"' *U.S. News & World Report*, June 22, p. 46.

WorldNetDaily (2003) 'Trouble in Holy Land: Hezbollah's New Computer Game,' March 3.

WorldNetDaily (2004) 'Al-Qaida Offers Do-It-Yourself Terror Training, January 5.

Yehoshua, Y. (2006) 'Reeducation of Extremists in Saudi Arabia,' *MEMRI Inquiry and Analysis Series*, No. 260 (The Middle East Media Research Institute), January 18.