Exploring the Role of Virtual Camps

Jarret Brachman and James J.F. Forest

On August 8, 2005, a video entitled "Cubs of the Land of the Two Sanctuaries" was posted to militant radical Islamic web forum Tajdid.org.uk.[1] In the title of the video, the use of the word "cubs" suggests lion cubs, as militant radical Muslims commonly refer to themselves as lions, while the "Land of the Two Sanctuaries" is an Islamic term for Saudi Arabia, the two sanctuaries being Mecca and Medina. The video introduces a young girl, perhaps ten years old, with an AK-47 at her side. She is joined by a young boy, and together they begin speaking and gesturing in unison, waving pistols in the air as they recite the following speech: "We are terrorists, and terror is our way. Let the oppressors . . . and their masters know that we are terrorists and that we frighten. Prepare what force and equipment you can to terrorize the enemy of God. For terror is an obligation of the religion." While reciting lines such as, "We are terrorists, and terror is our way," the children place the pistols in front of their own chests. At other times they point the pistols up in the air, or towards the camera.[2]

Jihadi propagandists have been posting radical videos like this with increasingly regularity since the late 1990s. Some of these websites host photos and videos of *jihadi* summer camps for kids, displaying images of young Arab children dressed as suicide bombers and videos of children conducting mock beheadings. One recently hosted an animated cartoon featuring Iraqi *mujahidin* dragging American forces from their Humvee and executing them. The purpose of such web propaganda is obvious: appeal to a younger generation of future militants, while demonstrating to the enemies of Islam the threat posed by this generation. The existence of thousands of jihadi-styled websites also demonstrates one of the most important facets of the

global security environment—information technology is playing an increasingly central role in the evolution of modern terrorist networks.

Over the past decade, groups and movements of all persuasions have leveraged new information and communication technologies, the Internet and cellular phones in particular, in order to further their agendas. These technologies have facilitated:

- The coordination of activities, events and collective action
- The discussion of topics of interest and news with movement participants;
- The dissemination of propaganda, educational, and training materials;
- The ability to identify, recruit, and socialize new membership; and,
- Opportunities to find and exploit information about their opposition.

The very nature of the Internet—including easy access for virtually anyone to publish and retrieve information, the ability to maintain anonymity, a rich multimedia environment, and the ability to encrypt data transmissions—makes it an ideal arena for individuals and organizations of all ideological persuasions to mobilize resources, recruits and recognition of their political agendas. Radical *jihadi* propagandists have been particularly effective in harnessing the virtual world as a sanctuary for sharing their ideas, strategy, tactics, plans, and funds. By circumventing television, radio and newspapers, the Internet creates not just the tools, but an entirely new forum for fostering global awareness of issues unconstrained by government censorship or traditional cultural norms.

Despite the fact that *jihadi* websites have only recently received widespread public attention, pro-*jihad* webmasters have been hosting websites since before the attacks of September 11, 2001. The famed “al-Neda.com” run by Saudi al-Qa`ida propagandist, Yusuf al-

Ayiri, served as al-Qa`ida's first official website. Throughout the late 1990s, new sites emerged (like "Azzam.com") which provided important jihadi articles, communiqués, photos, testimonials and biographies of martyred *jihadi* fighters to its readers. As Internet penetration broadened and deepened around the world, jihadi use of the Internet has grown exponentially. It was not until the United States and its allies unseated the Taliban in Afghanistan, however, that senior al-Qa`ida leaders found themselves in a post-9/11 scramble to keep their movement motivated and coherent. As such, the Internet became not only a useful way to replace their dismantled training camps and reconnect their weakened organizational leadership, but one of the only ways to sustain the global jihadi movement.

Michael Innes observes in his introductory chapter to this volume that the virtual realm "is a key element of contemporary terrorist threats, facilitating both domestic and transnational terrorism through access to digital and internet-based channels for command, control, communications, and intelligence." Similarly, a recent report by the RAND Corporation suggests that terrorists "will move from hierarchical toward information-age network designs. More effort will go into building arrays of transnational internetted groups than into building stand alone groups."[3] During a recent visit to Europe, Ambassador Henry Crumpton, U.S. Coordinator for Counterterrorism, noted his current concern over "cyber-safe havens . . . Internet-based means for enemy communication, recruitment, training, planning, resource transfer and intelligence collection."[4]

Academics and analysts have begun exploring the ways in which jihadis look to the Internet for training. As Gabriel Weimann observed, "The Internet has become a valuable tool for the terrorist organization, not just to coordinate operations and launch attacks, but also as virtual training camps and a tool for indoctrination and recruitment. In reality, the Internet

became for al-Qa`ida what experts call an 'online terrorism university.'"[5] Terrorism analyst, Reuven Paz, notes calls it what the jihadis themselves call it: an "open university of jihadi."

As reflected in this chapter, our own analysis of how *jihadi* minded individuals and groups leverage the Internet reveals that while the Internet is playing an increasingly prominent role in the global spread of knowledge and know-how among its readers, it plays a more important role: it has become a virtual sanctuary within which *jihadis* can mobilize, educate and establish their version of Islamic governance. This chapter will examine the nature of these virtual terror training camps, as well as other ways in which terror organizations use the Internet, and then highlight the technical, legal and policy challenges that this phenomenon poses for the counterterrorism community.

The Use of the Internet for Recruitment, Mobilization, and Indoctrination

The Internet's primary benefit to those who advance terrorist ideologies is in facilitating the communication of information, knowledge and know-how to various audiences. With this information, jihadi propagandists seek to increase the number of people who are aware of the jihadi movement, the number and quality of those actually waging jihad as well as the number of those who fear the rise of the jihadis, predominantly Arab and Western governments and Western publics. This section will explore the various ways contemporary jihadi terrorists leverage the internet as a virtual sanctuary for identifying new jihadi candidates, providing them with the education and training they need to move forward and bolstering morale among them.

As Harvard University professor Joseph Nye has observed, "This generation of terrorists is adept at using technology to increase its 'soft power.' The current global struggle against terrorism is not only about whose army wins, but also whose story wins."[6] In addition to the gigabytes of weapons manuals, explosives videos and graphic images housed on their websites, jihadi propagandists have been particularly effective in constructing and advancing a coherent narrative.

For example, Adam Gadahn—a U.S. citizen who now calls himself "Azzam the American"—has produced several documentary styled videos, in conjunction with an al-Qa`ida media outlet, As-Sahab media, that have received significant coverage in the mainstream press as well. These products walk their audience through a list of travesties committed by Western civilization and the local Arab regimes they prop up. Other jihadi online propaganda products highlight the methods needed in order to resist this advance of Western culture into the Islamic world. And still others focus on the jihadi end-state: the establishment of the global Islamic caliphate.

Literally thousands of pro-terrorist websites exist throughout the world, hosted in multiple languages, and all of which seek to establish a rationale for their use of violence in pursuit of particular goals and objectives. In addition to written appeals for action, images, music, speeches and videos are also used to persuade—or at least connect with—a website visitor on an emotional and intellectual level. Estimates suggest that in 2006, over a billion humans have at least some access to the Internet (an actual figure is impossible to determine), offering an enormous opportunity for terror groups to reach new audiences. According to RAND researchers Michelle Zanini and Sean Edwards:

> Using some of the same marketing techniques employed by commercial enterprises, terrorist servers could capture information about the users who browse their websites, and then later contact those who seem most interested. Recruiters may also use more interactive Internet technology to roam online chat rooms and cyber cafes, looking for receptive members of the public—particularly young people. Electronic bulletin boards and Usenet discussion forums can also serve as vehicles for reaching out to potential recruits. Interested computer users around the world can be engaged in long-term 'cyber relationships' that could lead to friendship and eventual membership.[7]

However, as Weimann notes, "modern terrorists do not recruit directly online; they use the Net only to identify, profile and select potential candidates for recruitment. Afraid of having their groups infiltrated by security agencies and counterterrorism forces, they will use the Internet only for the early stages of the recruitment process." [8] Once radicalized, individuals seeking to do more than read or discuss the problem will seek out like-minded individuals in the physical world, often at mosques, school, work or other local environments.

Examples of the Internet's use for recruitment and mobilization range from right-wing extremists in the U.S. to Islamic militants in Saudi Arabia, Chechnya and Indonesia. However, while most terrorist groups are local in scope and objectives, many terrorism researchers have described a globalized jihadist terror movement as the most important security threat of the current decade. The Web's growing centrality in al-Qa`ida-related radicalization and mobilization has led analysts, such as former CIA deputy director John E. McLaughlin, to describe the movement as primarily driven today by "ideology and the Internet."[9] Terrorism

researchers Scott Atran and Jessica Stern note that the Internet provides a way to connect with individuals and provide them direction as they surf jihadi websites.[10] In fact, no matter at what level one is willing to serve and participate in jihad, training and educational materials exist to help move an interested browser down a specific trajectory.

Those who monitor *jihadi* websites, for instance, have found detailed instructional documents and videos that explain how to use specific software packages or access certain types of files online. These tutorials are accompanied with a "*jihadi*-approved" version of the software to download, which often includes computer programs for video editing or webpage design. To this end, *jihadi* computer programmers have actually launched new stand-alone web browsing software, similar to Internet Explorer, which searches only particular sites. By structurally constraining web traffic, the software seems to be discouraging the freedom to navigate to other online destinations, thus facilitating the intellectual separation of *jihadi* visitors from the chaos of cyberspace. These efforts to define and bound *jihadi* ideological space, critical for *jihadi* success in light of the multiplicity of alternative viewpoints that can accessed online, should be expected to accelerate as ideologues seek dominance over this technology.

More thoughtful jihadi candidates can read about *jihadi* ideology and strategy from the al-Qa`ida library site (http://tawhed.ws), which hosts over 3,000 books and monographs from respected *jihadi* thinkers. One recent posting in a radical Islamic discussion forum, Tajdid al-Islami, demonstrated for participants how *jihadi*-themed books can even be downloaded on to cell phones.[11] In addition to books, anyone can download propaganda and recruitment videos directly on to their mobile devices.[12] Anyone anywhere can access a wealth of material at any intellectual level related to waging violent jihad. In short, the Internet provides individuals with

the resources and social networks they need to move from being angry to being able to act on that anger.

Norwegian terrorism researcher, Thomas Hegghammer, identifies three basic categories of websites within the jihadi Internet community.[13] First, there are the message boards where one finds the political and religious discussions among the sympathizers and potential recruits. These provide links to the second type, the "information hubs," where new radical-Islamist texts, declarations, and recordings are posted. These are often find among popular online "communities" hosted by Yahoo!, Geocities and others, where members can discuss a certain topic, post relevant articles and multimedia files, and share a meeting place for those with similar interests. Creating your own website within these forums is free, quick, and extremely easy.[14] Finally, there is the third type of sites, the "mother sites," which are run by people who get their material directly from the ideologues or operatives.[15]

In March 2005, a statement on the jihadi forum *Minbar Ahl al-Sunna wal-Jama'a* noted that an Information Jihad Brigade had been formed, with the stated objective of launching a full-scale propaganda war to "influence the morale of our enemies." This is now one of several jihadi media brigades that have emerged in recent years, their primary goal being to conduct psychological operations convincing Western forces, their families, their governments, Western publics that they are losing the Global War on Terror while simultaneously proving to their own constituencies that the jihadis are winning the global war on Jews, Crusaders and apostates.

Focused on turning their enemy's strengths against them, *jihadis* actively use the latest Western software—including Windows Movie Maker, Adobe Acrobat, and others—to create anti-Western products intended to inspire their followers and humiliate their enemies. These al-Qa`ida affiliated or inspired media outlets have found a wealth of imagery from Western media

sources, which they manipulate to craft their own propaganda products. Over the past year, this imagery has increasingly focused on profiling wounded and dead American soldiers in disturbingly graphic ways. Perhaps even more shocking to Western audiences is the black humor that often accompanies this imagery.[16]

These types of propaganda products are typically burned to CD-ROM and distributed by hand not only to *jihadi* activists but also to anyone who may be curious about the movement. Available in markets and under the counters of some shops, these videos can be purchased throughout the Middle East and Southeast Asia. The sniper has become a folk hero for some Iraqis, who may not necessarily subscribe to the *jihadi* ideology, but do feel a connection with the active resistance waged by the sniper against what they perceive to be imperialistic U.S. forces.

In addition to using technology for education and indoctrination purposes, jihadi groups have also exploited these technologies to revolutionize the way in which their supporters participate in the struggle. For example, in November 2005, the information bureau of "The Army of the Victorious Group," a Sunni insurgent group operating in Iraq, used several radical Islamic websites to announce a contest for designing the organization's website. The winner would not only have his design implemented, but he would receive a prize in the form of the opportunity to fire missiles via computer at a U.S. army base in Iraq.[17] The announcement emphasized that:

> The winner will fire three long-range missiles from any location in the world at an American army base in Iraq, by pressing a button [on his computer] with his own blessed hand, using technology developed by the *jihad* fighters, Allah willing.[18]

By stressing the "opportunity for our brothers outside Iraq to join their brothers on the front line[s] in Iraq, the land of the frontier and of *jihad*, and to [participate in] destroying the strongholds of polytheism and heresy," the contest sponsors demonstrate their view that the very *use* of technology is an integral part of the education and indoctrination process. Such novel applications of technology allow those interested in supporting fighting in Iraq to do so from the comfort of their homes.

In sum, it is widely recognized today that websites, chat forums and other forms of online communications play an important role in the terrorist world, particularly in terms of spreading ideology and mobilizing support for a particular cause. Indeed, security agencies of many countries are seeking ways to address this issue—but perhaps there is not much that can be done. In fact, *Jihadi* web users have become increasingly aware of attempts by governments to monitor their online behavior. In order to enhance operational security in the use of technology, *jihadis* have recently posted protocol about safe ways to use technology. For example, a guide for using the Internet safely and anonymously recently emerged on a *jihadi* forum site.[19] The guide explains how governments identify users, penetrate their usage of software chat programs including Microsoft Messenger and PalTalk as well as advising readers to not use Saudi Arabian based email addresses (those that end with a ".sa" extension) because they are not secure. Rather, the author of this guide suggests, *jihadis* should register for anonymous accounts from commercial providers, like Hotmail and Yahoo. This is but one small example of a more worrisome aspect of the Internet's role in worldwide terrorism: providing strategic and tactical guidance for groups and individuals.

Training and Organizational Development

> "The Internet has become the new Afghanistan for terrorist training, recruitment, and fundraising . . . Terrorist groups are exploiting the accessibility, vast audience, and anonymity of the Internet to raise money and recruit new members."[20]

— PC World, July 7, 2004

In April 1999, while visiting an Internet cafe in the Victoria district of London, a young man downloaded two books—*The Terrorists' Handbook* and *How to Make Bombs, Book Two*—from a seemingly ordinary website.[21] Following the instructions provided in these texts, he packed a plastic pipe with flash powder he had removed from various fireworks, and sealed the pipe with glue. This was put into a box surrounded by around 1,500 nails of differing sizes, which would act as shrapnel when the pipe was detonated. He added a modified timer and two battery-powered electrical igniters (which would serve as detonators), placed the device inside a sports bag, took a taxi to Brixton, South London, and left the bag on the corner of busy Electric Avenue. The explosion occurred at 5:25 p.m., injuring 50 people. The following Saturday, a second explosion took place, this time in Brick Lane, an East London neighborhood. The same type of device was used, this time injuring thirteen. Less than a week later, an explosion ripped apart the Admiral Duncan pub in Soho, London at approximately 6:10 p.m. The pub had been full of Friday evening patrons: three were killed, four needed amputations, 26 suffered serious burns, and another 53 were injured in other ways.[22]

Thanks to a series of tips to Scotland Yard, David Copeland's terrifying nail bombing campaign ended while the dead and maimed were still being counted from the wreckage of the Admiral Duncan pub. At his trial, Copeland told police that he was a Nazi, and that he hoped the explosions would "set fire to the country and stir up a racial war." The media focus on the trial of this young engineer from Farnborough, Hampshire, brought considerable public attention to the widespread availability of online resources like *The Terrorists' Handbook* and *How to Make Bombs, Book Two.* Both titles are still easily accessible; a search for the keyword phrase "terrorist handbook" on the popular Google search engine found over 423,000 matches. One site gives instructions on how to acquire ammonium nitrate, Copeland's "first choice" of explosive material.

The globalization of access to the Internet has had a dramatic impact on the dissemination of this type of knowledge. As Bruce Hoffman aptly observed, "using commercially published or otherwise readily accessible bomb-making manuals and operational guides to poisons, assassinations and chemical and biological weapons fabrication . . . the 'amateur' terrorist can be just as deadly and destructive as his more 'professional' counterpart."[23] Throughout the Middle East, Southeast Asia and Europe, cells affiliated with al-Qa`ida that have recently carried out or seriously planned bombings have relied heavily on the Internet.[24]

Although these virtual combat classrooms do not render physical training camps obsolete, information technologies do change the nature of education, indoctrination, and participation. Terrorist training manuals available online provide guidance for a broad range of activities, from acquiring explosives and rocket propelled grenade launchers to falsifying documents and target vulnerability assessment. Over the past several years, al-Qa`ida and its affiliates have been building a massive and dynamic online library of training materials—some supported by experts

who answer questions on message boards or in chat rooms—covering such varied subjects as how to mix ricin poison, how to make a bomb from commercial chemicals, how to pose as a fisherman and sneak through Syria into Iraq, how to shoot at a U.S. soldier, and how to navigate by the stars while running through a night-shrouded desert.[25] According to Weimann, "More than 300 new pages of al-Qa`ida-related manuals, instructions and rhetoric are published on the Internet every month."[26]

For example, an individual known as "al-Mohager al-Islami" ("The Islamic Immigrant") recently published online a nearly 40-page pamphlet on "The Art of Kidnapping—The Best and Quickest Way of Kidnapping Americans." The manual includes information for planning raids, the composition of support crews, general rules for these crews to follow, observation points, kidnapping suggestions, and methods of capturing Americans."[27] He has also posted messages to dozens of jihadist e-group forums, both public and password-protected, about the locations and equipment of U.S. and British sites in Kuwait, Qatar and other areas, including photos of embassies and living areas, and has provides logistic information about several bases in Iraq, calling upon the mujahideen to target these sites.[28] As Iraqi insurgents perfect their combat techniques, they communicate them to a larger audience through a variety of channels, including the Internet. Increasingly, military commanders have reported a growing trend of Iraqi insurgent tactics being replicated in Afghanistan.[29] The Taliban's use of remote triggered improvised explosive devices (IEDs), for example, demonstrates a notable evolution from the hard-wired detonators they had previously used.[30] In recent months, government officials in Thailand have reported a similar upsurge in the technical sophistication of tactics used by their own radical Islamic insurgents in the south of the country.[31] Thai security forces attribute these seemingly overnight advancements, particularly in terms of how guerrillas are wiring and deploying

improvised explosive devices, to a combination of the availability of *jihadi* training manuals, which they have found in safe houses in CD-ROM and hardcopy form, and direct instruction from Thai *jihadis* with al-Qa`ida training camp experience.

In another example, the online training magazine *Muaskar al-Battar,* or Camp of the Sword, has become required reading in the jihadis' online terrorist training curriculum.[32] Even military websites in Europe and North America—many of which offer publicly available field manuals on everything from conducting psychological operations to sniper training and how to install Claymore anti-personnel mines—have become resources for developing particular kinds of knowledge useful for terrorists and insurgents in other parts of the world. Other prominent sources of operational knowledge include *The Anarchist Cookbook* and *The Mujahideen Poisons Handbook.* The latter was written by Abdel Aziz in 1996 and "published" on the official Hamas website, detailing in 23 pages how to prepare various homemade poisons, poisonous gases, and other deadly materials for use in terrorist attacks.[33] The *Terrorist's Handbook*, published by "Chaos Industries and Gunzenbombz Pyro Technologies," offers 98 pages of step-by-step operational knowledge.[34] But the multi-volume *Encyclopedia of the Afghan Jihad,* written in Arabic and distributed on paper and on CD-ROM, is perhaps one of the most oft-cited terrorist training manuals in existence today. It contains a wealth of operational knowledge for new terrorists, covering topics such as recruitment of new members, discharging weapons, constructing bombs and conducting attacks. Specific examples are included, such as how to put small explosive charges in a cigarette, a pipe or lighter in order to maim a person; drawings of simple land mines that could be used to blow up a car (not unlike the improvised explosive devices seen most recently in Iraq); and radio-controlled devices that could be used to set off a

whole truckload of explosives, like those used to destroy the U.S. embassies in Kenya and Tanzania in August 1998.

Tom Metzger—the guru of the "lone wolf" or "leaderless resistance" model of activism—has provided right-wing extremist groups with strategic guidance for several decades, through his *White Aryan Resistance* (WAR) monthly newspaper, books, a telephone hotline, a website, and a weekly e-mail newsletter (*Aryan Update).* His primary contribution to the field of terrorist knowledge has been in advocating individual or small-cell underground activity, as opposed to above-ground membership organizations. He argues that individual and cellular resistance leaves behind the fewest clues for law enforcement authorities, decreasing the chances that activists will end up getting caught. Specific guidelines for this strategy include: act alone and leave no evidence; do not commit robbery to obtain operating funds; act silently and anonymously; do not deface your body with identifiable tattoos; understand that you are expendable; and whatever happens, do not grovel.[35] While Metzger intended his operational knowledge to improve the capabilities of like-minded racists, some observers have noted its salience for (and adoption by) other terrorist-minded groups as well.

Elaborate video games are also available on the Internet to help training new would-be terrorists. The first computer game developed by a political Islamist group is called *Special Force,* and was launched in February 2003 by the Lebanese terrorist group Hizballah.[36] A "first-person shooter" game, *Special Force* gives players a simulated experience of conducting Hizballah operations against Israeli soldiers in battles re-created from actual encounters in the south of Lebanon, and features a training mode where players can practice their shooting skills on targets such as Israeli Prime Minister Sharon and other Israeli political and military figures. The game can be played in Arabic, English, French, and Farsi, and is available on one of the

Hizballah websites.[37] Mahmoud Rayya, a member of Hizballah, noted in an interview for the *Daily Star* that the decision to produce the game was made by leaders of Hizballah, and that "in a way, *Special Force* offers a mental and personal training for those who play it, allowing them to feel that they are in the shoes of the resistance fighters."[38]

According to terrorism analyst Madeleine Gruen, Hizballah's Central Internet Bureau developed the game in order to train children physically and mentally for military confrontation with their Israeli enemies.[39] By the end of May 2003, more than 10,000 copies of *Special Force* been sold in the United States, Australia, Lebanon, Syria, Iran, Bahrain, and United Arab Emirates. Games such as these, as Gruen notes, "are intended to dehumanize the victim and to diminish the act of killing." In essence, through simulating acts of violence, these games develop the player's skill to kill other human beings without having to leave the comfort of their own home.

Overall, the global spread of Internet connectivity provides an increasingly useful mechanism for the terrorists to engage in distance learning activities. The invention and increasing availability of online language translation tools offers a particularly unique and important dimension to the transfer of knowledge in the terrorism world. With these tools, websites in English can be translated online and used to educate non-English speaking terrorist-minded individuals. Meanwhile, the ability to rapidly transfer new information in electronic form to a global audience, simultaneously and in multiple languages, presents additional challenges to those seeking to curb the ability of terrorist organizations to train new members. Further, individual "seekers of jihad" throughout the world now have access to information that can develop their knowledge and abilities in the deadly terrorist tradecraft.

It is thus most important to recognize that a large proportion of the terrorist-related material available on the Internet is meant to produce individual action. Among many religious extremists, action in service to one's god (even murder) is itself the endstate. Thus, the primary goal of the videos and manuals described in this chapter are intended to provide a global audience with the knowledge of how and why to conduct a terrorist attack. One al-Qa`ida training manual describes the importance of conducting terrorist attacks for:[40]

- boosting Islamic morale and lowering that of the enemy
- preparing and training new members for future tasks
- a form of necessary punishment
- mocking the regime's admiration among the population
- removing the personalities that stand in the way of the [Islamic] Da'wa [Call]
- agitating [the population] regarding publicized matters
- rejecting compliance with and submission to the regime's practices
- giving legitimacy to the Jama'a [Islamic Group]
- spreading fear and terror through the regime's ranks
- bringing new members to the organization's ranks

Without action, it can be argued, the terrorist group or movement risks stagnation and atrophy. As Bruce Hoffman observed, terrorists are like sharks—they must continue moving and attacking in order to ensure their survival. Thus, terrorist groups rely on the Internet for mobilization (developing an individual's will to kill) and training (developing their skill to kill). Combined, these aspects of online terrorism resources generate considerable alarm among most

government security agencies. However, there are other important uses of the Internet worth consideration as well, such as soliciting and managing a group's financial support and logistics.

Financial and Operational Support

In addition to mobilization and training, terrorist groups are increasingly turning to the Internet to support their operational needs, particularly in the areas of financial transactions, attack planning, target surveillance, and exploring the potential for computer-based attacks (referred to by some observers as "cyberterrorism"). While the most valuable terrorist-oriented uses of the Internet involve the exchange of information, the growing dominance of online commerce has not gone unnoticed. Several terrorist group websites now solicit donations or try to raise funds through the sale of videos, audios, or other items—in some cases, even accepting credit cards or other forms of electronic payment. The Internet also provides an easy mechanism to move organizational funds from one part of the world to another, and often in a manner that is difficult (if not impossible) for government authorities to trace. The existence of Internet-accessible unregulated "offshore" financial institutions (e.g., the Cayman Islands) offers a particularly attractive haven for terrorist finances. The global spread of online commercial transactions has also enabled new forms of criminal activity, such as fraud and identity theft, which can generate funds to support terrorist organizations.

In addition to raising funds and transferring money, the Internet allows members of terror cells to coordinate their planning for a terrorist attack, as well as gather intelligence on the target of their attack. Through the use of free, disposable e-mail accounts (Hotmail, Yahoo!, etc.),

individual members can communicate “below the radar screen,” creating significant difficulties for counterterrorism agencies. Meanwhile, there are many types of freely available information that available for terrorists attack planning. Satellite imagery, street maps, photos of buildings and the surrounding area, news reports and other forms of information can be found online using any number of website search engines. In many cases, a potential target may have unknowingly posted information online that would be useful to terrorists. The public websites of many government organizations and private businesses provide driving directions, hours of operation, key personnel, hours of operation, typical periods of peak activity, and so forth. However, an amateur computer hacker who gains access to their internal network would no doubt find a variety of operational manuals, guidelines, security procedures, official memorandum, personnel information, and perhaps even building schematics. While the protection of these and other kinds of information is a primary concern of information technology professionals, there is growing concern that the tools and techniques developed by mainstream computer hackers (most often, used for monetary gain or curiosity than anything else) are being studied and adapted for more nefarious means by terrorist organizations.

These online tools also offer terrorists the capability to conduct new kinds of attacks—the so-called cyberterror threat. The Internet offers a rich source of information for self-styled hackers or crackers to learn how to conduct a wide variety of cyber-attacks against any private or public entity with an online presence. These resources are becoming increasingly sophisticated, and can enable a would-be terrorist to potentially bring down a power grid or an airport control tower, among other types of targets. A host of websites provide detailed step-by-step instructions for conducting denial of service attacks, packet sniffing, password cracking, buffer overflow attacks, network vulnerability testing, and so forth. Web surfers can download free software (like

the SuperScan vulnerability scanning tool or the Ethereal packet sniffing program) for use in exploiting virtually any type of computer or network system. An entire world of hacker communities is supported online through chat rooms and other communication forums, where members share ideas and experiences, sometimes even boasting of their exploits in a perverse form of one-upmanship. Criminal hackers (an increasing concern of the FBI, Interpol, and many other agencies) most often use their technical knowledge in an effort to gain financial rewards. Terrorists may use the same knowledge and tools to gain financial rewards, but may also seek to cause real harm to economies, infrastructure, and people.[41]

Some observers have proposed scenarios in which terrorists attack dams, chemical plants, water systems, and other sensitive systems, causing massive damage and casualties. While such scenarios typically involve some form of physical attack, usually with conventional explosives, security professionals also acknowledge an increasing threat from cyber-savvy terrorists. Over 85% of the critical infrastructure in the U.S. is owned and operated by the private sector, and its management functions are handled by various industrial control systems including Supervisory Control and Data Acquisition (SCADA) systems which are frequently connected directly or indirectly to the Internet in order to allow remote monitoring of their functions (and thus reduce the company's labor costs).[42] While numerous cases have been reported in recent years of computer hacker attacks against prominent government agencies and businesses, technology experts agree that many such attacks go unreported. In the case of the private sector, companies have historically proved reluctant to acknowledge such intrusions for fear that doing so would alarm shareholders and other stakeholders, and possibly affect revenues.

Overall, the Internet offers an array of mobilization, training, and operational support capabilities to terrorist groups—capabilities which were not available to groups and movements

before the modern information age. As such, it has been argued that the global security environment of the 21st century is facing a "new terrorism"—a globally-networked, highly sophisticated and adaptable adversary which will be much more difficult to defeat than any previous types of violent non-state actors.

Challenges for Countering Terrorist Use of Virtual Sanctuaries

Among the many challenges faced by security organizations in the information age, three areas of concern seem most salient for addressing the role of virtual training camps in the terrorist world. First, the technical challenges of mapping and disrupting globally decentralized networks are perhaps the daunting. Second, there are a host of legal challenges to consider, particularly when it comes to the role of the Internet in a liberal democracy. Third, the policy decisions over what can or should be done are naturally driven by a variety of political necessities, social norms, and procedural constraints. Further, while each of these categories present many specific challenges, the globalized nature of the Internet demands a response that is internationally coordinated. The current lack of global cooperation in addressing virtual training camps is one of the most pressing vulnerabilities that contemporary terrorist groups are able to exploit in the global security environment.

Technical Challenges

The most obvious hurdle to combating jihadi use of the Internet is its open access design. Anyone, anywhere can access the Internet. Technologies discussed above, including IP proxy

software, allow for people to access the Internet anonymously, making law enforcement's job all the more complicated. Making matters more difficult, the number of jihadis using the Internet and the number of jihadi websites are both increasing on a daily basis.

Jihadi web propagandists have developed new protocols for posting internet videos. They post upwards of 20 copies of a video in high resolution, 20 copies in medium resolution, 20 copies in low resolution and 20 copies in cell phone format to a variety of free file hosting services. In fact, some websites have long lists of the various services that detail the length of time that files can be hosted for free and the megabyte limitations on those files. Pulling down all of these redundant copies of one video would be an incredibly time-consuming task, particularly given that there are thousands of these types of videos that have been released to date in such a manner. Further, removing videos from a website—or taking an entire website offline—most often has only a temporary impact, as the same materials tend to appear on some other web server shortly thereafter. Because electronic forms of information can be duplicated and distributed without limits, the technical challenges posed by virtual sanctuaries are particularly daunting.

Legal Challenges

The primary transit hub of Internet financial and information transactions – the United States – has only recently indicated a serious commitment to tackling the challenges discussed in this chapter, as reflected in its first national strategy for securing cyberspace.[43] To its credit, this document highlights the importance of multinational cooperation, particularly since many of the most active websites are hosted in countries beyond those that are committed to the global war on terrorism. By allowing terrorist training websites to exist on Internet servers within their

jurisdiction, these countries are in essence playing host to online centers of knowledge transfer in the terrorist world. As a result, governments are facilitating a vast "ungoverned space" which terrorist organizations are able and willing to take advantage of. Yet, despite a critical need for international cooperation, there are no global or even regional legal standards for addressing online activity by violent non-state actors. Some countries (like Brazil) have no laws against computer crime, while others which do have some form of legal framework for dealing with virtual sanctuaries encounter significant difficulties when confronted with the need to protect civil liberties of free speech.

Jihadis themselves have grown increasingly familiar with cyber monitoring laws and widely discuss changes to those laws in their own Internet forums. These posts are usually accompanied by updates to their own standard operating procedure manuals for online activity, which often includes details about using web-proxy software, IP masking software and illegal copies of other computer software. Thus, while countries grapple with increasingly complex legal challenges, terrorists are finding new ways to exploit critical vulnerabilities that allow them to sustain and expand their virtual sanctuaries.

Procedural and Policy Challenges

To date, there is no widespread consensus on a national strategy for dealing with these jihadi websites. Some have suggested launching an aggressive campaign to remove them from existence. However, because of free speech protections in this country, much of what is posted in the jihadi Internet world cannot be used as justification for removal. Some private citizens have engaged in their own attempts to bring the sites down, either by hacking them, or by identifying

the Internet Service Provider that hosts the site, contacting them with detailed information about the type of website they are hosting on their server, and requesting that they be removed.

Other analysts contend that removing such sites is actually detrimental to longer-term efforts to monitor and track the jihadi movement. Because the Internet is the only way that the jihadis have to mobilize, recruit and communicate on a global basis, and given the limitless ability to change Internet addresses and find new servers very rapidly, this side argues that terrorists will find a way to adapt to any government effort to remove their web presence. Additionally, rapid changes in web addresses make it more difficult, they argue, for analysts to effectively monitor the conversation and files being transferred – a key window into the jihadi mindset.

Conclusion

This chapter has identified a variety of difficult challenges for counterterrorism, challenges which demand a globally coordinated response. The Internet provides one of the most popular "ungoverned spaces" for terrorists to exploit for a variety of purposes. These purposes include more well known uses, including fundraising; communicating their strategic vision for the future of the jihadi movement; and providing detailed instructions about tactics including bomb construction, assassination techniques, covert cell communication and hacking. Jihadis also use the internet for less tangible activities, including the establishment of a flourishing radical Islamic thought community online, what can be called "Internet as emirate."[44] This pervasive and ever-expanding jihadi web activity facilitates knowledge of, and a culture grounded in, the

salafi jihadi ideology. Whether a jihadi candidate wants to learn more about tactics, strategy, ideology or simply be entertained, they can thanks to the help of the Internet.

There is a growing consensus across the U.S. government that information must be countered with information, not simply bullets and bombs. As Nye observes, "repeated polls show that Osama bin Laden in his cave has communicated more effectively than America or Britain have despite their massive budgets for public diplomacy. Jordan and Pakistan are front line states in George W. Bush's war on terror, but polls show far more people saying they trust bin Laden than the U.S. president."[45] One question that policymakers and Internet analysts are now beginning to ask is whether they can take advantage of the Internet in the same ways that the jihadis do? Are there vulnerabilities of virtual sanctuaries (beyond so-called honey-pots) that we can exploit? If so, how?

The generation of policymakers not raised with the internet or cell phones to become more aware of the changing nature of the threat and increase investment in monitoring and surveillance. One nation acting alone will not be enough. Democratic leaders must use soft or attractive power to disseminate a positive narrative about globalization and the prospects for a better future that attracts moderates and counters the poisonous jihadist narratives on the web. Fortunately, we have a credible story to tell. [46]

NOTES

The views expressed are those of the authors and not of the Department of the Army, the U.S. Military Academy, or any other agency of the U.S. Government.

[1] "حصريا على منتدى التجديد ولأول مرة .. (فديو) .. أشبال من بلاد الحرمين" (Exclusively on Tajdid Forum for the First Time, Video: Cubs from the Land of the Two Sanctuaries)," 9 August 2005. Online at: http://www.tajdeed.org.uk/forums/showthread.php?s=8454388d52907025a6fa6157feb51bde&threadid=37270.

[2] Portions of this chapter have previously appeared in James J.F. Forest, "Training Camps and Other Centers of Learning," in *Teaching Terror: Strategic and Tactical Learning in the Terrorist World,* edited by James J.F. Forest (Lanham, MD: Rowman & Littlefield, 2006); and James J.F. Forest, "Teaching Terrorism: Dimensions of

Information and Technology," in *The Making of a Terrorist: Recruitment, Training and Root Causes,* edited by James J.F. Forest (Westport, CT: Praeger Security International, 2005).

[3] John Arquilla, David F. Ronfeldt, and Michele Zanini, "Networks, Netwar and Information-Age Terrorism," in *Countering the New Terrorism,* edited by Ian O. Lesser, Bruce Hoffman, John Arquilla, David F. Ronfeldt, Michele Zanini and Brian Michael Jenkins (Santa Monica: RAND Corporation, 1999), 41.

[4] Henry Crumpton, "Remarks at RUSI Conference on Transnational Terrorism," January 16, 2006. Online at the website of the U.S. Embassy in London, U.K.

[5] Gabriel Weimann, "Virtual Training Camps: Terrorists' Use of the Internet" in *Teaching Terror: Strategic and Tactical Learning in the Terrorist World* (Lanham, MD: Rowman & Littlefield, 2006).

[6] Joseph Nye, "How to Counter Terrorism's Online Generation," *Financial Times*, October 13, 2005.

[7] Michelle Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age," in *Networks and Netwars,* edited by Jon Arquilla and David Ronfeldt, (Santa Monica: RAND Corporation, 2001) 43-4.

[8] Gabriel Weimann, "Terrorist Dot Com: Using the Internet for Terrorist Recruitment and Mobilization," in *The Making of a Terrorist, Volume 1: Recruitment,* edited by James J.F. Forest (Westport, CT: Praeger, 2005)

[9] Steve Coll and Susan B. Glasser "E-Qaeda From Afghanistan to the Internet: Terrorists Turn To The Web As Base Of Operations," *The Washington Post,* August 7, 2005.

[10] Scott Atran and Jessica Stern, "Small groups find fatal purpose through the web," *Nature* 437, 29 September 2005, downloaded from http://www.nature.com/nature/journal/v437/n7059/full/437620a.html

[11] *Tajdid Al-Islami*, "Here Are Books That Can be Read on a Cell Phone," February 16, 2006, <www.tajdeed.org.uk/forums/showthread.php?s=8bf3d9789390e5e7dad7d22476adeb3b&threadid=38954>.

[12] The *jihadi* website, Mohajroon, has featured links to video clips that can be viewed on cell phones. See Mohajroon, "Visuals Section," <http://www.mohajroon.com/modules.php?name=Islamic_Gawal&operation=subsection&subsection=1> (accessed March 8, 2006)..

[13] Cited by Lawrence Wright, "The Terror Web," *The New Yorker*, 2 August 2004.

[14] See Rita Katz and Josh Devon, "WWW.JIHAD.COM: E-Groups abused by jihadists," *National Review Online* (14 July 2003) at: http://www.nationalreview.com/comment/comment-katz-devon071403.asp

[15] Portions of this paragraph are from Gabriel Weimann, "Terrorist Dot Com: Using the Internet for Terrorist Recruitment and Mobilization," in *The Making of a Terrorist, Volume 1: Recruitment,* edited by James J.F. Forest (Westport, CT: Praeger, 2005)

[16] Goafalaldyn.com, "The Sarcastic Bloody Comedy Video Tape Hidden Camera of the Mujahideen in Iraq," September 6, 2005 <www.goafalaladyn.com/vb/showthread.php?t=5324> (currently unaccessible).

[17] The *Al-Hesbah Forum* is currently inaccessible but had been found at <www.alhesbah.org>. The Flash document had been posted at: <http://heretic.maid.to/cgi-bin/stored/serio0835.swf>.

[18] *Islamist Website Design Contest: Winner Fires Missiles U.S. Army Base in Iraq*, The Middle East Media Research Institute Special Dispatch 1038, December 1, 2005, <http://memri.org/bin/articles.cgi?Page=archives&Area=sd&ID=SP103805> (accessed March 26, 2006).

[19] See: "A Guide for Internet Safety and Anonymity Posted to Jihadist Forum, SITE Institute, 24 March 2006, < http://siteinstitute.org/bin/articles.cgi?ID=publications160206&Category=publications&Subcategory=0>

20 "Terrorists Rely on Tech Tools," *PCWorld,* July 7, 2004, at: http://www.pcworld.com/news/article/0,aid,116822,tk,dn070804X,00.asp

[21] The following story is explored in great detail in several articles of the *Guardian Unlimited* website (http://www.guardian.co.uk/bombs), including Jeevan Vasagar, "Deadly Net Terror Websites Easy to Access" (Saturday July 1, 2000); Nick Hopkins and Sarah Hall, "David Copeland: a quiet introvert, obsessed with Hitler and bombs" (Friday June 30, 2000); and "Nailbomber 'Used Net to Build Bombs'" (Monday June 5, 2000).

[22] See James J.F. Forest, "Training Camps and Other Centers of Learning" (2006) and James J.F. Forest, "Teaching Terrorism" (2005).

[23] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), p. 203.

[24] For example, see Steve Coll and Susan B. Glasser "E-Qaeda From Afghanistan to the Internet" (2005).

[25] Steve Coll and Susan B. Glasser "E-Qaeda From Afghanistan to the Internet" (2005).

[26] Gabriel Weimann, "Virtual Training Camps: Terrorists' Use of the Internet" in *Teaching Terror: Strategic and Tactical Learning in the Terrorist World* (Lanham, MD: Rowman & Littlefield, 2006).

[27] SITE Institute, 22 December 2005, located at www.siteinstitute.org. Some examples of other jihadi manuals on a variety of issues are at:
http://www.geocities.com/tadrebatfialjihad10/COLT-45.zip
http://www.geocities.com/tadrebatfialjihad10/katem00721.zip
http://www.geocities.com/algazairiyat_00768/dawrat.zip

[28] Timothy L. Thomas, "Cyber Mobilization: The Neglected Aspect of Information Operations and Counterinsurgency Doctrine," in *Countering Terrorism and Insurgency in the 21st Century*, edited by James J.F. Forest (Westport, CT: Praeger, 2007)

[29] Sami Yousafzai and Ron Moreau, "Unholy Allies," *Newsweek*, September 26, 2005, <www.msnbc.msn.com/id/9379240/site/newsweek> (accessed March 26, 2006); David S. Cloud, "Insurgents Are Continually Getting More Sophisticated with Their Devices," *The New York Times*, August 3, 2005.

[30] Vicky O'Hara, "Troop Protections from Homemade Bombs Sought," broadcast on " National Public Radio," March 4, 2005, < www.npr.org/templates/story/story.php?storyId=4522369> (accessed March 26, 2006).

[31] Shaun Waterman, "Thai Militants Learn from Iraq Insurgency," *United Press International*, February 15, 2006, <www.upi.com/SecurityTerrorism/view.php?StoryID=20060215-020216-8561r> (accessed March 26, 2006).

[32] Steve Coll and Susan B. Glasser "E-Qaeda From Afghanistan to the Internet" (2005).

[33] Gabriel Weimann, *WWW.Terror.Net - How Modern Terrorism Uses the Internet.* Special Report 116 (United States Institute of Peace, 2004), p. 9. Available online at http://www.usip.org.

[34] Bruce Hoffman, *Inside Terrorism* (1999) p. 203.

[35] See "Leaderless Resistance Strategy Gains Momentum Among Militant White Supremacists," and "Aryan National Congress Focuses on Revolutionary Tactics," *Klanwatch Intelligence Report,* No. 74, August 1994, pp. 6-9; Also, see "Tom Metzger/White Aryan Resistance," on the "Extremism in America" Anti-Defamation League website at http://www.adl.org.

[36] Madeleine Gruen, "Innovative Recruitment and Indoctrination Tactics by Extremists: Video Games, Hip Hop, and the World Wide Web," in *The Making of a Terrorist: Recruitment, Training and Root Causes* (vol. 1), edited by James JF Forest (Westport, CT: Praeger, 2005); Also, see Gabriel Weimann, "Virtual Training Camps."

[37] See www.specialforce.net, last accessed 11/13/04

[38] At http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=31323.

[39] Madeleine Gruen, 2005.

[40] Ben Venzke and Aimee Ibrahim, "Al Qaeda Tactic/Target Brief, v. 1.5" *IntelCenter* (14 June 2002), 6

[41] However, it is doubtful that al Qaeda or any other group would actually want to "bring down the Internet." Indeed, according to Louise Richardson, the Executive Dean of the Radcliffe Institute, for all the concern about "cyberterrorism," the Internet is "far too valuable to al Qaeda" and other groups: "Al Qaeda could not function without the Internet." See Ruth Walker, "Terror online, and how to counteract it," *Harvard Gazette,* 3 March 2005. Online at: http://www.news.harvard.edu/gazette/2005/03.03/01-cyberterror.html

[42] For more on this, please see Aaron Mannes, "The Terrorist Threat to the Internet," in *Homeland Security: Protecting America's Targets* (Volume 3: Critical Infrastructure), edited by James J.F. Forest (Westport, CT: Praeger, 2006).

[43] *National Strategy for Security Cyberspace* (Washington, DC: The White House, 2002).

[44] Jarret Brachman. "High Tech Terror: Al-Qaeda's Use of New Media Technologies." *Fletcher Forum of World Affairs.* February, 2006.

[45] Joseph Nye, "How to Counter Terrorism's Online Generation" 2005.

[46] Ibid.