

CYBER EMBARGO: COUNTERING THE INTERNET JIHAD

Gregory S. McNeal*

If you are a young Muslim male, even a doctor, with a PC in Egypt, the Gulf states, Somalia, Morocco or Glasgow, as always with the Web you are marinating your mind in its content, and the content here is homicide on a mass scale. The answer—technical or political—is not obvious to me. But the one unacceptable answer is doing nothing.

Daniel Henninger¹

INTRODUCTION

As Daniel Henninger pointed out shortly after the attempted July 2007 Glasgow and London terrorist attacks, the solution to the problem of jihadist websites is not obvious. Nevertheless, doing nothing is no longer acceptable. Terrorists are engaged in an online jihad, characterized by the use of the internet to fundraise, distribute messages and directives, recruit, and proselytize. Although it is impossible to eliminate the presence of terrorists on the internet, this article details a proposal that would have a marked impact on the presence of terrorists on the internet. Using existing statutes, it is possible to regionalize terrorist websites, limiting them to a small number of countries from which they may receive internet services. Once the terrorist message is limited to a particular region, a modification of current laws can allow for a cyber embargo on jihadist websites and their supporters. These efforts, coupled with diplomatic cooperation, can further the attempt to curb the impact of jihadist websites, while simultaneously increasing the ability of governments to monitor these websites and, when necessary, shut them down.

This article is a thought piece, intended to create debate about my proposal. I have not exhaustively addressed all of the constitutional and policy issues associated with my proposal; instead, I hope this piece will serve as a platform for future scholarship. In this article, I outline my pro-

* Gregory S. McNeal is Visiting Assistant Professor of Law at The Pennsylvania State University, Dickinson School of Law. The author would like to convey his sincere appreciation to Audrey Buchring and Diane M. Donahue for their outstanding research assistance. As always his biggest debt of gratitude is owed to Stacy New for her unwavering support. This article was originally presented on March 30, 2007 at the Roe Green Foundation conference "Sacred Violence: Religion and Terrorism" organized by the Institute for Global Security Law and Policy at the Case Western Reserve University School of Law. A webcast of the conference may be accessed at <http://law.case.edu/centers/igslp/webcast.asp?dt=20070330>.

¹ Daniel Henninger, *The Blogosphere for Killers*, WALL ST. J., July 12, 2007, at A14.

posal for countering the internet jihad by using, as an example, the active and official website of Palestinian Islamic Jihad (PIJ), a designated terrorist organization. While I frequently reference PIJ, the principles I articulate have relevance to any other terrorist's website. In Part One I provide a brief overview of the status of Palestinian Islamic Jihad, and its brazen efforts to stay online despite government countermeasures. I outline a three-step process by which the PIJ web presence, and others like it, can be eliminated. Step one involves the use of the existing material support statute. Step two recommends the creation of a cyber embargo by modifying existing statutes to create a non-criminal "material supporter" designation that will prevent U.S. companies from conducting business with designated material supporters. Finally, step three involves diplomatic efforts to globalize the reach of the techniques detailed in steps one and two. Part One also explains the practical effect of each step of my proposed process on the official website of PIJ.

In Part Two of this article, I detail the threat posed by "cyber jihad." I explain how terrorists use the internet to recruit, train for attacks, and coordinate those attacks. I also describe the clear advantages terrorist organizations enjoy by using websites. This sets the stage for a discussion of the current statutory framework, which, to date, has only enjoyed moderate success.

In Part Three, I move beyond the threat and explore the legal and policy implications of using existing statutes to eliminate the web presence of terrorist organizations. I also detail the limitations of the current statute and prepare the reader for a discussion of how, with slight modifications, the existing statutory and policy framework can significantly diminish the advantages terrorist organizations enjoy through their web presence.

In Part Four, I present the critical next step in countering the cyber jihad. I explain the advantages of creating a cyber embargo on companies that provide "material support" to terrorist organizations, but that, for legal or policy reasons, may be beyond the reach of the material support statute. The creation of a cyber embargo rests upon a non-criminal "material supporter" designation that will prevent American companies from conducting business with designated "material supporters." In essence, this process involves the creation of virtual "persona non grata." I also detail the diplomatic efforts necessary to globalize the reach of this counter-terrorism strategy. Through cooperation with foreign governments, loopholes in the jihadist web presence can be closed and terrorist organizations can be forced to a limited number of potential host countries.

I conclude the article by discussing the implications of following my approach, and the new counterterrorism opportunities it presents.

I. THE PALESTINIAN ISLAMIC JIHAD EXAMPLE

PIJ is a designated terrorist organization,² responsible for the deaths of Americans and others.³ They brazenly boasted in 2006 that the FBI could not shut them down,⁴ and their boasts, thus far, have proven true. In January 2006, PIJ's official website was present on the web through the support of three U.S. companies. After a public shaming campaign led by Internet Haganah, a web based watchdog group,⁵ PIJ changed network providers. As of May 2006, however, PIJ maintained six active websites, five of which were based on servers in the United States, with six American companies involved in keeping those sites online.⁶ A further check conducted at the time of this article's publication showed that the official websites of PIJ were still operational, although they have now located all of their internet services outside the United States, obtaining network services from businesses in Malaysia.

Some see the above example as support for the argument that efforts to counter the presence of terrorists on the internet are a fruitless endeavor. At first blush, the example of PIJ seems to support this assertion—despite actions taken to shut PIJ down in January and May of 2006 the cyber jihadists almost immediately resurfaced to mock authorities.⁷ Nevertheless, critics should not be so quick to dismiss efforts to shut down jihadist websites. The web, like other battlefields in the struggle against terrorist organizations, is dynamic, and efforts that keep the terrorists moving impose costs on their operations. These costs include preventing the distribution of the terrorist message, disrupting the organization's regular activities, and damaging the morale of the organization.⁸ Moreover, as the PIJ example illustrates, efforts to counter the terrorist presence on the web can force such organizations to overseas internet service providers, thus limiting their

² U.S. Dept. of State, *Foreign Terrorist Organizations*, (Dec. 30, 2004), <http://www.state.gov/documents/organization/41055.pdf>.

³ Ali Waked, Ahiya Raved, & Efrat Weiss, *5 Killed in Hadera Bombing*, YNET NEWS, Oct. 6, 2005, <http://www.ynetnews.com/articles/0,7340,L-3159743,00.html>.

⁴ *New PIJ Site Unveiled, and a Review of All Active PIJ Sites*, INTERNET HAGANAH, May 11, 2006, <http://haganah.org.il/harchives/005604.html> [hereinafter *PIJ Site*] (“After issuing a communiqué promising that they would show the FBI that they could not be kept offline, US designated Terrorist group Palestinian Islamic Jihad has finally unveiled their saraya.ps site, representing their operational/terrorist unit—the Saraya al-Quds Brigade. Despite the Palestinian domain name, it is operating on a server in the USA.”)

⁵ See Internet Haganah, <http://haganah.org.il> (last visited Sept. 10, 2007) [hereinafter *Internet Haganah*].

⁶ *PIJ Site*, *supra* note 4.

⁷ See *supra* 4–6.

⁸ BOAZ GANOR, *THE COUNTERTERRORISM PUZZLE* 102 (2005).

host options and increasing the likelihood that authorities will be able to track them.

Step one in the process of shutting down a website such as PIJ is to use shaming techniques and the threat of criminal sanctions to stop U.S. companies from providing services to a designated terrorist organization. Websites such as Internet Haganah posted the details of U.S. companies who were providing services to PIJ as part of a shaming campaign.⁹ The website encouraged readers to contact those U.S. companies and demand that they stop supporting terrorists. The U.S. companies have more at stake than just their reputation. Current statutes make it a crime to provide material support to terrorist organizations, and the list of prohibited forms of support includes the provision of computer services. Shortly after the shaming campaign, with its attendant potential for criminal liability, the PIJ website shifted its operation to overseas service providers that are beyond the reach of U.S. laws and less susceptible to shaming techniques. As a result, the PIJ website is still operating today.

The second step to further isolate and eventually shut down the PIJ website is the most critical one. As the facts detailed in step one illustrate, current laws and techniques are limited, and terrorist organizations are quick to adapt and avoid the reach of shaming techniques and U.S. laws. Nevertheless, once terrorist organizations make their home outside the United States, they must still rely on the support of service providers in their new jurisdiction. While the terrorist organization itself may not be deterred by U.S. efforts, their service providers are vulnerable to commercial pressure and the desire to maintain their business—the majority of which likely comes from non-terrorist clientele. These service providers are the critical and weakest link in the terrorist's web presence. Accordingly, a cyber embargo is the quickest and most effective way to cease their support of terrorist organizations. Such an embargo focuses on those service providers who are providing material support to PIJ in the form of web services.

The example of PIJ demonstrates the necessity of this cyber embargo. After being forced off of U.S. network service providers, PIJ now receives an IP address and connection to the internet from a Malaysian network service provider, Time Net Central.¹⁰ They also receive registrar services from Time Telekom,¹¹ a major telecommunications company in Malaysia.¹² I propose a modification to existing statutes to create a new material

⁹ See *PIJ Site*, *supra* note 4.

¹⁰ See *generally* Asia Pacific Network Information Centre, <http://wq.apnic.net/apnic-bin/whois.pl> (last visited Jul. 17, 2007) (providing a searchable membership database of Asia Pacific Network Information Centre members).

¹¹ See *generally id.*

¹² See Time dotCom, <http://www.time.com.my/corporate/index.asp> (last visited Sept. 10, 2007).

supporter designation. U.S. companies and persons under this approach will be forbidden from doing business with a designated material supporter. The practical result of such a designation will be to create a cyber embargo, cutting off streams of income to overseas companies due to their affiliation with terrorist organizations.

With a cyber embargo in place, companies that support terrorists will be forced to choose between either losing all commercial services from the United States or continuing to provide services to the terrorist organization. The result in the case of PIJ is obvious. If Time Telekomm, a major international telecommunications company, were designated as a material supporter, then all U.S. commercial services would be cut off, including internet and financial services. In the face of this potential loss of income, Time Telekomm would likely cease providing services to PIJ immediately. Moreover, the network service provider Time Net Central, may also have ties to U.S. commercial activity, and would be reluctant to find itself designated a material supporter.

Nevertheless, it is still possible that Time Net Central is a much smaller organization and may not be deterred by a material supporter designation. As such, a further step is necessary to isolate these terrorist organizations and their overseas webhosts. The third step involves diplomatic efforts to standardize the creation of “designated material supporter” lists by urging nations to adopt the list and implement necessary domestic enforcement mechanisms. Such an adoption will expand the number of nations participating in a cyber embargo, and will foreclose overseas safe havens for terrorist websites. In the example above, Time Net Central, as a small, mostly domestic company, may not be concerned if commercial activity between it and the United States is disrupted. Time Net Central will likely be very concerned, however, if Malaysia has a similar designation process that cuts commercial ties between itself and a major Malaysian company such as Time Telekomm, for example. Thus, expanding the cyber embargo is key because as PIJ continues to shift its operations to countries it believes are safe havens the cyber embargo will continue to isolate them geographically.

II. RECRUITMENT, COORDINATION, TRAINING, AND CYBER JIHAD

Overview of Websites, Webhosts, and the Internet Jihad

Why should we be concerned with the presence of terrorists on the internet? Unlike cyberterrorism, which is the use of computers to attack networks and create chaos, the cyber jihad is information presented on behalf of terrorist organizations, and is seemingly less threatening than cyberterrorism. There is no evidence to indicate that cyberterrorist techniques

have been used for serious destructive activity.¹³ On the other hand, the cyber jihad can be used for many activities that directly support war.¹⁴ For example, Joseph Shahda, an expert in cyberterrorism, explains that “[t]errorist leaders including Bin Laden have stated that ‘media Jihad’ is as important as ‘battlefield Jihad’ and in this case the most common and powerful medium for the terrorists ‘media Jihad’ is the internet.”¹⁵ The internet is used on a daily basis to support the ongoing jihad. Via the internet, terrorist groups set up operation centers, raise money, recruit, spread propaganda, and communicate their ideologies. All of this is accomplished with minimal effort and resources, and without geographical limitation. Thus, the internet jihad is quite successful and has serious consequences. Officials would not allow PIJ or other terrorist organizations to operate a downtown recruiting center or headquarters; similarly, terrorists should not be allowed to engage in the same activity on the internet.

Recruiting and Communicating the Ideology

The internet provides an inexpensive recruiting tool for terrorists to win supporters and members from any part of the world.

Because the internet can be accessed easily by those at home or in public places, the number of potential recruits has gone up exponentially since the rise of the internet. Websites and chat rooms provide an instant connection between recruiters and interested sympathizers.

Technology has made instantaneous recruitment simple. With the internet capabilities of digital imaging and video, terrorists can broadcast powerful messages to a mass audience of sympathetic viewers.¹⁶ Bandwidth costs continue to decrease, thereby reducing streaming video costs.¹⁷ Furthermore, terrorists can use browsers to check language settings and direct the viewer to a site customized to his language and culture.¹⁸ Interested

¹³ See Joshua Green, *The Myth of Cyberterrorism*, WASH. MONTHLY, Nov. 2002, at 8, available at <http://www.washingtonmonthly.com/features/2001/0211.green.html>.

¹⁴ See Timothy L. Thomas, *Al Qaeda and the Internet: The Danger of “Cyberplanning,”* 33 PARAMETERS, Spring 2003 at 112, available at <http://www.carlisle.army.mil/usawc/Parameters/03spring/thomas.pdf> (“[The internet] provides terrorists with anonymity, command and control resources, and a host of other measures to coordinate and integrate attack options.”).

¹⁵ Jerry Gordon, *Fighting Internet Jihad: An Interview with Joseph Shahda*, NEW ENGLISH REVIEW (2007), http://www.newenglishreview.org/custpage.cfm/frm/11995/sec_id/11995.

¹⁶ See *id.* at 114.

¹⁷ See generally Scott Pelley, *Terrorists Take Recruitment Efforts Online*, CBS NEWS, Mar. 4, 2007, available at <http://www.cbsnews.com/stories/2007/03/02/60minutes/main2531546.shtml> (showing the presence of the growing practice of posting videos on the Internet).

¹⁸ Patrick S. Tibbetts, *Terrorist Use of the Internet and Related Information Technologies* 34 (Jun. 2002) (unpublished monograph, on file with the School of Advanced Military Studies).

viewers can then contact the terrorists by way of the contact information listed on the web. Once contact is established, terrorists can assess and recruit members for their cause.¹⁹ Through steganography, the process of embedding messages in graphic files, terrorists can use their websites to provide instructions to their recruits.²⁰

Again, anonymity plays a large role in the internet's efficacy as a terrorist tool. The anonymity of the internet has been found to foster higher levels of violence in people.²¹ This rise in violent feelings is understandable, when one considers that anonymity allows people to act freely, unfettered by a fear of consequences. Terrorists can encourage these feelings of violence, drawing people to their cause.

Additionally, terrorists are using the internet to target younger members of society. According to a congressional report, "web sites are often flashy and colorful, apparently designed to appeal to a computer savvy, media-saturated, video game-addicted generation."²² One such example was a website that presented the video game "Quest for Bush." The object of the game is to conquer Americans in the name of the jihad. Levels of the game include "Jihad Growing Up" and "American's Hell." Other sites play youth-oriented music like rap and hip-hop.²³

With the advent of internet recruitment, terrorists have been able to lower their costs while customizing their search for potential members on a global level. Furthermore, terrorists can stir web visitors into action by raising their feelings of violence and indignation. Thus, the internet has increased the pool of recruits for terrorist organizations.

Related to recruiting, one of the jihadists' main goals is to pass on their ideology and provide a sense of community and belonging.²⁴ Because the internet is capable of generating a virtual community, jihadists can reach supporters in any corner of the world. Ultimately, the community strengthens the bond of individuals to the group.²⁵

On the internet, communication is not unidirectional. Rather than issuing a statement that reaches group members, jihadist leaders can invite

¹⁹ *Id.* at 37.

²⁰ Thomas, *supra* note 15, at 119.

²¹ Beverley Lumpkin, *Islamic Extremists Say Web as Vital to Them as AK-47*, SEATTLE TIMES, May 3, 2007, available at http://seattletimes.nwsourc.com/html/nationworld/2003691528_webterrorists03.html.

²² *Id.*

²³ *Id.*

²⁴ See ANTI-DEFAMATION LEAGUE, JIHAD ONLINE: ISLAMIC TERRORISTS AND THE INTERNET 15 (2002), <http://www.adl.org/internet/jihad.asp> [hereinafter ADL].

²⁵ Hanna Rogan, JIHADISM ONLINE — A STUDY OF HOW AL-QAIDA AND RADICAL ISLAMIST GROUPS USE THE INTERNET FOR TERRORIST PURPOSES 25 (Mar. 20, 2006), available at <http://rapporter.ffi.no/rapporter/2006/00915.pdf>.

interactive participation.²⁶ By doing so, leaders can answer questions, address issues, and engage in discussions to create unity within the group. Once unity has been established, leaders can invite small groups of people to exchange strategies and work together toward the same goal. These strategies are often aimed at moving against the United States. One example is a jihadist Yahoo! message board that presented a strategy to compel United States-led coalition forces to leave Iraq.²⁷

In another, more recent example, six Muslim men living in the United States were charged with plotting to attack Fort Dix in New Jersey.²⁸ The men had planned to sneak onto the base as military personnel. The accused were united via the internet, where they all downloaded videos of Osama bin Laden preaching inspirational jihadist messages.²⁹ Their capture resulted from a tip by a store clerk who was hired by the men to dub video of their training and practice attacks onto a digital disk for internet use.³⁰

The internet has proven to be a simple, effective way for jihadists to communicate their ideology and create strong communities of supporters that strategize together. With its ability to eliminate geographical constraints, the internet allows jihadists from abroad to unite and work together with those on the homefront. The Fort Dix plot demonstrated that jihadists, with intent to contribute to the international cause, could join and construct a plot within U.S. borders.

Official websites of al Qaeda and other designated terrorist groups are not just hosted in the Arab world. In fact, many are registered or hosted in Europe, Asia, or the United States. These sites offer articles that condemn America, give biographies of Islamists killed in battle, and relate biased accounts of the current war in Afghanistan. They communicate an ideology with the intent to recruit members to the terrorist organization's cause.

Command and Control

Beyond recruiting, terrorist websites can also act as virtual command and control centers.³¹ The ease of accessibility and information exchange make websites ideal for serving some of the administrative functions

²⁶ *See id.*

²⁷ *Id.* at 24.

²⁸ *See* Posting of Fort Dix Plot: Complaint and Summary by Gregory McNeal to AIDP Blog, <http://aidpblog.org/2007/05/08/fort-dix-plot-complaint-and-summary> (May 8, 2007, 11:25a.m. EST) (citations omitted).

²⁹ *Six Men Arrested in Plot to Attack New Jersey's Fort Dix* (PBS television broadcast May 8, 2007), available at http://www.pbs.org/newshour/bb/government_programs/jan-june07/fortdix_05-08.html.

³⁰ *See id.*

³¹ Thomas, *supra* note 14, at 117.

of terrorist organizations. Terrorists are able to exert control over their missions through the internet with few geographic and communication limitations. A terrorist in Iran, for example, can coordinate attacks in the United States from afar. The convenience of the internet has made terrorist operations “cheaper, faster, and more secure.”³² Terrorist organizations are dynamic, and the internet has become the medium of choice for centralizing their operations. Communication and training is much easier to accomplish with the speed of the internet, and without the limitations of geography.

Prior to the age of the internet, terrorists were limited to communicating with each other by way of available electronics, such as telephones or radios. As a result, they were always at risk of being monitored by electronic surveillance tools, such as wiretaps.³³ The internet solved that problem by providing anonymity. For example, complex encryption keys, nearly impossible to break, mask terrorist messages. Terrorists can use spamming tools that hide messages in bulk commercial email. Network accounts can be easily set up under false names, and many internet access locations have anonymous logins. Often, hosting internet service providers are unaware of their clients’ site content.³⁴

Training Sites

Terrorists also use websites as training sites by posting training materials online.³⁵ For example, the training pamphlet, *How Can I Train Myself for Jihad*, was originally posted on Azzam.com, a website run by a British company and affiliated with Sheikh Abdullah Azzam, a mentor to Osama Bin Laden.³⁶ The document provided information on various aspects of battle, including martial arts, survival training, and firearm use.³⁷

The Azzam.com subscriber list included Said Bahaj, who is believed to be a key planner in the September 11, 2001 terrorist attacks, which peripherally demonstrates the use and effectiveness of internet training

³² THE GEORGE WASHINGTON UNIV. HOMELAND SEC. POLICY INST. & THE UNIV. OF VA. CRITICAL INCIDENT ANALYSIS GROUP, NETWORKED RADICALIZATION: A COUNTER-STRATEGY 1 (2000), available at <http://www.healthsystem.virginia.edu/internet/ciag/home.cfm>.

³³ See *id.*

³⁴ Thomas, *supra* note 14, at 115.

³⁵ See generally Gabriel Weimann, *www.terror.net: How Modern Terrorism Uses the Internet*, INST. OF PEACE SPECIAL REPORT 116 (2004), available at <http://www.usip.org/pubs/specialreports/sr116.pdf> (explaining many ways terrorist groups use the internet, including training purposes).

³⁶ See Stephanie Gruner & Gautam Naik, *Extremist Sites Under Heightened Security*, WALL ST. J. ONLINE, Oct. 7, 2001, http://news.zdnet.com/2100-9595_22-530855.html.

³⁷ Violence Policy Center, *Firearms Training for Jihad in America* (2001), <http://www.vpc.org/studies/jihad.htm>.

sites.³⁸ Another example of detailed online training comes from al Battar, al Qaeda's online journal. At one point, the constantly relocating al Battar was posted on www.alm2sda.net, a jihadist internet forum.³⁹ Topics included methods of intelligence gathering, discussions of bin Laden's political genius, and explanations of public kidnapping procedures.⁴⁰ One article provided a "how to" guide for dealing with hostages, instructing site visitors to "[s]eparate the young people from the old, the women and the children. The young people have more strength, hence their ability to resist is high. The security forces must be killed instantly. This prevents others from showing resistance."⁴¹

Dozens of sites feature information on how to build chemical and explosive weapons. The *Mujahadeen Poisons Handbook*, posted on the official Hamas website, included instructions for homemade poisons, poisonous gases, and other deadly materials for use in terrorist attacks.⁴² Other websites, like alned.com, offered motivational tidbits, religious support, and strategies for attack. Additionally, the media has speculated that such sites are written in Arabic to direct al Qaeda to other sites.⁴³ Some websites even trained readers to wage attacks through the computer system itself. For example, the site 7hj.com taught viewers how to damage computer systems with viruses.⁴⁴

Terrorists are able to run training websites more effectively by using video demonstrations. Videos train viewers to make explosive devices, gunpowder, mines, and suicide bomber vests. One website that featured links to such videos, Al Qalah, claimed responsibility for several terrorist attacks.⁴⁵ The website also featured Arabic voiceovers and written instruc-

³⁸ See *id.*

³⁹ Stephen Ulph, *Al-Battar Number 22 Released*, 1 TERRORISM FOCUS 8, Nov. 12, 2004, <http://jamestown.org/terrorism/news/article.php?articleid=2368849>.

⁴⁰ See *id.*; see also *Kidnapping the Focus of Al Battar Issue No. 10*, SITE Institute, May 24, 2004, <http://siteinstitute.org/bin/articles.cgi?ID=publications3804&Category=publications&Subcategory=0>.

⁴¹ Laura Mansfield, *Chechen Terrorists Follow al-Qaida Manual*, WORLDNETDAILY, Sept. 4, 2004, http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=40298.

⁴² Posting of Manual for Poisons and Chemical Gases Published on Hamas Website, Free Republic, <http://www.freerepublic.com/focus/news/816520/posts> (Jan. 3, 2003 16:30 PST).

⁴³ See, e.g., Paul Eedle, *Terrorism.com*, GUARDIAN, Jul. 17, 2002, at G2, available at www.guardian.co.uk/afghanistan/comment/story/0,11447,756638,00.html.

⁴⁴ See Yossi Melman, *Virtual Soldiers in a Holy War*, HA'ARETZ, Sep. 17, 2002, available at <http://www.freerepublic.com/focus/f-news/786923/posts>.

⁴⁵ Anti-Defamation League, *Terrorist Training Videos Appear Online*, http://www.adl.org/main_Terrorism/terrorist_training_video_82205.htm (last visited Aug. 22, 2005).

tions. In keeping with the anonymity of the internet, the videos did not show any faces.⁴⁶

The example of “Irahabi007,” also known as Younis Tsouli, supports these conclusions. Tsouli was an information technology student in London, and was one of al-Qaida’s most notorious cyber facilitators.⁴⁷ He distributed online weapons manuals and videotapes of bombings and beheadings.⁴⁸ He taught seminars on how to operate online anonymously, and how to hack into vulnerable websites and upload material onto them.⁴⁹

The internet serves as the ultimate center of operations for terrorist organizations. Not only does the internet provide terrorist organization websites with a safe location to train and communicate with their members, but it also provides global access. This kind of access facilitates fundraising, as well as recruiting, and allows propaganda to be spread all over the world in a very inexpensive and efficient manner.

Fundraising

Terrorist organizations use the internet to raise funds for their murderous activities. They rely on donations given through charities and non-governmental organizations that conduct business online. Terrorist groups often establish websites that front as charities, but serve as fundraising centers for their cause. For example, Al Qaeda employs charities under the guise of Islamic humanitarianism.⁵⁰ The Benevolence International Foundation (BIF), based in the United States, touts itself as an organization that provides relief to war-torn areas. BIF gave \$600,000 to Al-Qaeda trainees and funded activities for Osama bin Laden and other Islamists involved with the September 11, 2001 attack.⁵¹

Contributors are often unaware that the ultimate destinations of their donations are terrorist organizations. Moreover, terrorists have become adroit at soliciting donations. The webmaster can pull demographic information from online questionnaires that contributors fill out when donating to the charity. They then use this information to send out emails tailored to the contributor in the hope of gaining more sympathy and, ultimately, contributions.⁵²

⁴⁶ *Id.*

⁴⁷ See *A World Wide Web of Terror*, THE ECONOMIST, July 14, 2007, at 28 (“Irahabi007 was a central figure in enabling al-Qaeda.”).

⁴⁸ See *id.*

⁴⁹ *Id.*

⁵⁰ Thomas, *supra* note 14, at 116.

⁵¹ ADL, *supra* note 24, at 15.

⁵² Weimann, *supra* note 35, at 7–8 (2004).

The example of Irahbi007 supports these conclusions. Two days before his arrest, Irahbi007 had the following encrypted web chat with a colleague:

Abuthaabit: This media work, I am telling you, is very important. Very, very, very, very.

Irahbi007: I know, I know.

Abuthaabit: Because a lot of the funds brothers are getting is because they are seeing stuff like this coming out. Imagine how many people have gone [to Iraq] after seeing the situation because of the videos. Imagine how many of them could have been shaheed [martyrs] as well.⁵³

This admission confirms that the internet is one of the weapons terrorists use to raise funds and personnel to aid their cause.

Executions and Propaganda

Terrorist organizations have also begun to employ websites as a form of information warfare. Their websites can disperse inaccurate information that has far-reaching consequences. Because internet postings are not regulated sources of news, they can reflect any viewpoint, truthful or not. Thus, readers tend to consider internet items to be fact, and stories can go unchecked for some time.⁵⁴ Furthermore, streaming video and pictures of frightening scenes can support and magnify these news stories. As a result, the internet is a powerful and effective tool for spreading propaganda.

The usefulness of the internet for propaganda is similar to its usefulness for operation headquartering. Anonymity and global capability permit terrorists to spread their message quickly to all areas of the world with minimal risk of detection. Al Qaeda's use of the internet provides a good illustration. Rather than using official websites that are easier to pinpoint and shut down, al Qaeda uses semi-official sites to broadcast its propaganda. The people who maintain such sites are al Qaeda members or supporters, and they are almost impossible to identify.⁵⁵ Registering websites can be accomplished easily with fabricated information, and the ability of terrorists to remain anonymous lends to the allure of using the internet.

Azzam.com, an al Qaeda site, features more than four-dozen flattering biographies of foreign Mujahideen who were killed in the jihad. Many of these biographies are supplemented with images, audio, and video, and

⁵³ *A World Wide Web of Terror*, *supra* note 47.

⁵⁴ Thomas, *supra* note 14, at 116.

⁵⁵ ADL, *supra* note 24, at 12.

they aim to inspire readers to join the cause.⁵⁶ Other al Qaeda websites, such as *jehad.net*, give interested readers their perspective on the conflict in Afghanistan. Using such websites, Al Qaeda is able to broadcast a biased version of the news, while claiming to be a news source. One such example involves an insurgent “black propaganda” operation called “Lee’s Life for Lies”;

[t]his operation involved fabricating the false history of American soldier Lee Kendall, whose USB flash drive was found by insurgents. The insurgents utilized the information contained in the USB to write a fake letter that described the desperate situation of the foreign soldier in Iraq and the existence of abuses and unpunished war crimes.⁵⁷

Al Qaeda can, thus, downplay negative stories about unsuccessful attacks and highlight unfair treatment of Afghan (and other) civilians by Americans. These sites commonly use a tactic in which they report high death tolls for American troops to rally support.⁵⁸ In reality, however, death tolls are hundreds of times smaller than the sites claim. These tactics make readers and supporters believe that al Qaeda stands strong against the United States.⁵⁹

Many sites also feature statements made by Osama bin Laden or al Qaeda. Some post public executions, like that of kidnapped American Nick Berg.⁶⁰ In fact, an increasing number of websites have included graphic video testimonials of suicide bombers.⁶¹ These websites, which tap into visual imagery, are likely to have more power to connect with their audience. A recent report from The United States Military Academy at West Point’s Combating Terrorism Center reinforces this conclusion, stating “[v]isual imagery provides a key aspect of the terrorists’ message in that it

⁵⁶ See generally Azzam Publications, *Jihad Stories: Stories of Foreign Mujahideen Killed in Jihad*, <http://d.1asphost.com/TawheedJihad/Azzam/storieshome.htm> (last visited Sept. 24, 2007) (providing links to biographies of individuals killed in jihad).

⁵⁷ Manuel R. Torres Soriano, *Jihadist Propaganda and Its Audiences: A Change of Course?*, PERSPECTIVES ON TERRORISM, http://www.terrorismanalysts.com/pt/index.php?option=com_rokzine&view=article&id=8 (last visited Feb. 11, 2008).

⁵⁸ See generally, Jonathan Forman, *Defeat in the “Information Battle Space,”* NAT’L REVIEW ONLINE, May 17, 2007, <http://article.nationalreview.com/?q=MWI3MGFiN2EyODliODRiMGh1ZTJiYTMxYTM4OGRiYzA=&w=MA> (arguing that civilian death tolls are exaggerated by the Taliban and their allies to create the impression that coalition troops kill large numbers of civilians).

⁵⁹ ADL, *supra* note 24, at 13.

⁶⁰ Pepe Escobar, *The War of the Snuff Films*, ASIA TIMES, May 13, 2004, available at http://www.atimes.com/atimes/Front_Page/FE13A02.html.

⁶¹ See ADL, *supra* note 24, at 20.

allows these groups to paint a picture of their objectives, their enemies, and their strategy through graphics, photographs, and symbols.”⁶²

In light of the clear advantages terrorist organizations enjoy by using websites to recruit, coordinate, and enhance their operations, new and creative ways to diminish the terrorist web presence are necessary. To date, extant efforts have enjoyed only moderate success. Nevertheless, with slight modifications, the existing statutory and policy framework can markedly diminish the advantages terrorist organizations enjoy on the internet.

III. UNDERSTANDING THE EXISTING STATUTORY AND POLICY FRAMEWORK AND ISOLATING THE THREAT

Overview of Internet Architecture and Jihadist Techniques

The internet's ubiquity and resilience allows for seamless global communications thereby making it difficult to control its use by terrorists. The interconnected nature of the web means that for a website to operate effectively, it must rely on intermediaries to carry any individual message. These intermediaries are U.S. and foreign companies that support the internet jihad by providing domain names to, and hosting the websites of terrorist organizations. Some may be doing so unwittingly, while others may be turning a blind eye. The internet jihad, however, can be countered by enlisting corporate cooperation, and where cooperation fails, sanctioning companies that support terrorist organizations.

The first step is to identify terrorist websites; some claim to be “the official” website, while others merely post supportive information. While the task of identifying terrorist websites is difficult, small, private watchdog groups that police the internet for potential threats are emerging.⁶³ As previously mentioned, one particularly well-known watchdog website is Internet Haganah, run by Aaron Weisburd.⁶⁴ Keeping his costs low, Weisburd operates out of his home office and has a network of supporters who contribute time and money to the voluntary counterterrorism endeavor.⁶⁵ By going undercover as an interested party, Weisburd is able to discover jihadist sites that pose a high risk. Once Weisburd locates terrorist activity, he

⁶² U.S. Military Academy: Combating Terrorism Center at West Point, *The Islamic Imagery Project: Visual Motifs in Jihadi Internet Propaganda*, <http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=499&issueID=38> (last visited Feb. 12, 2008).

⁶³ See e.g., Globalterroralert.com, <http://www.globalterroralert.com/about.htm> (last visited Sept. 17, 2007); Homelandsecurity.com, <http://www.homelandsecurity.com> (last visited Sept. 17, 2007); Counterterrorism Blog, <http://www.counterterrorismblog.org>. (last visited Sept. 17, 2007).

⁶⁴ See *Internet Haganah*, *supra* note 5.

⁶⁵ Nadya Labi, *Jihad 2.0*, ATLANTIC MONTHLY, Jul./Aug. 2006, available at <http://www.theatlantic.com/doc/prem/200607/online-jihad>.

tracks down the host of the website and either shames the internet service provider (ISP) into shutting the site down, or provides the information to the appropriate authorities who can, in turn, notify the ISP.⁶⁶

While this solution is beneficial given its low cost, Weisburd's method has its weaknesses. The main problem is that when he shuts a website down, that same website will reappear somewhere else.⁶⁷ The terrorists who run these sites merely move to a new ISP. Because ISPs are numerous, the time-consuming tracking process must begin all over again. Unfortunately, jihadists are often able to jump from site to site much more quickly than the sites can be shut down.

Moreover, Jihadists have gone one step further. Not only do they switch ISPs, but they also take on new domains. Finding new domains is a fairly easy task. Al Qaeda, for example, uses mailing lists, chat rooms, and sympathizer websites that immediately broadcast the new domain name to al Qaeda members. Because these sources are password protected and fairly secure, jihadists ensure that only their group receives the information.⁶⁸

As in the example of PIJ, once a terrorist organization is shut down by its ISP the jihadists pack up and move to a new ISP. There are many ISPs in business, and thus relocating the website is akin to finding a needle in a haystack. Nevertheless, terrorist organizations are interested in recruiting, spreading their message, fundraising, and coordinating their efforts. Thus, a website that cannot be found does not benefit them, and therein lies the first of their weaknesses.

Moreover, all website or domain names (*.com, *.gov, *.org, etc.) are controlled by a domain name registrar, and the domain name servers maintain directory maps to each domain. Simply put, to create a website with a domain name, one must register and pay for it. Once the name is registered, the company that owns the name can keep track of which ISP is hosting their domain name.⁶⁹ When PIJ decided to operate their website, they selected the domain name saraya.ps. This domain name, like all domain names, is owned by a company called a domain name registrar (DNR). Different companies own the rights to a unique set of domain names, so PIJ had to approach the appropriate company to purchase the use of the name saraya.ps. Once they received their domain name, PIJ needed to find an ISP

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ Transcript of Discussion with Evan Kohlmann, International Terrorism Consultant, *Al Qaeda and the Internet* (Aug. 8, 2005), http://www.washingtonpost.com/wp-dyn/content/discussion/2005/08/05/DI2005080501262_pf.html [hereinafter *Washington Post*].

⁶⁹ See Marshall Brain, *How Domain Name Servers Work*, HOWSTUFFWORKS, <http://computer.howstuffworks.com/dns.htm> (last visited Sept. 19, 2007).

to host their actual site. Because the DNR can trace the location of its domain names,⁷⁰ it is always able to track saraya.ps to its ISP.

Knowing this, the jihadists have begun not only switching ISPs, but also changing domain names to avoid detection. This is because the DNR's directory details each new ISP of a given name, the sites are often shut down in quick succession by tracing the domain name to the next ISP. The mere act of changing names is enough to thwart the tracking process and begin the tedious hunting anew; however, it also results in a temporary loss of the terrorist organization's ability to communicate with their followers.

Shutting Down DNRs

One step toward immobilizing the internet jihad is to ignore the ISP and go straight to the DNR to shut down domain names themselves. Many jihadist sites purchase their names from U.S.-based companies, and hence would be easy to regulate. Once a site is identified as affiliated with a terrorist group, the DNR can be found without difficulty. Several sites, like whois.com and godaddy.com, maintain a listing of DNRs for domain names.⁷¹ For example, after entering alhanein.com, number three on Weisburd's current top twelve list of terrorist websites, the search turns up Fast Domain, Inc., a DNR based out of Utah.⁷²

Once a domain name is shut down, the site no longer appears in web searches. Web crawlers, such as Google and Yahoo! Search, limit their crawl space with rules. These rules forbid search returns of IP addresses, limiting returns to domain names only. Hence, jihadist networks without domain names would be crippled by an inability to recruit interested parties who use such web crawlers to search the internet.⁷³

Nevertheless, internet companies have proven that, due to the nature of the web business, they can neither be forced nor expected to police the hundreds of thousands of websites with which they are affiliated.⁷⁴ For ex-

⁷⁰ See Richard Keyt, *Who Owns Your Domain Name?*, KEYT LAW, May 1, 2001, <http://www.keytlaw.com/urls/whoowns.htm>.

⁷¹ See WHOIS, <http://www.whois.com> (last visited Sept. 17, 2007); See also GoDaddy, <http://www.godaddy.com> (last visited Sept. 17, 2007).

⁷² See generally, *The "Top Ten Twelve" List of Arabic Salafyist/Jihadist Forums*, INTERNET HAGANAH, http://internet-haganah.org/hmedia/27apr07/27apr07-salafy_forums.html (last visited Sept. 17, 2007).

⁷³ See generally *Rules to Limit the Web Crawl Space*, IBM, 2005, <http://publib.boulder.ibm.com/infocenter/wsihelp/v8r3/index.jsp?topic=/com.ibm.websphere.iisearch.ad.doc/administering/iisacweblim.htm> (explaining how crawl space can be limited).

⁷⁴ *Network Solutions Shuts Down Pedophile Website*, HOSTSEARCH, 2007, www.hostsearch.com/news/network_solutions_news_5782.asp (stating "[w]e host over 7.4 million domain names, and we sell packages where we host the content of a site, so we have hundreds of thousands of sites that we host.").

ample, in 2004 the American company, Network Solutions, hosted PIJ.⁷⁵ When a current customer complained about the company's support of a terrorist organization, the company's response was "Network Solutions has no responsibility or duty to police the rights of trademark owners concerning domain names."⁷⁶ Network Solutions further added, "If the domain owner in question is conducting criminal activity we would ask you to defer to either the police or the proper authorities."⁷⁷

Despite the difficulties associated with shutting down websites, and the impossibility of eliminating the entire terrorist web presence, there are good reasons to make efforts. While some companies may be unwilling to cut off their clients, others may simply be unaware that they are hosting terrorist websites. In 2005, Weisburd alerted the U.S. government that forty-eight Iranian government websites, including the official website of Iran's Supreme Leader, were hosted by the American company CI Host.⁷⁸ Because of a trade embargo enacted in 1980, U.S. companies are not permitted to be in business with Iran, which has been denoted by President Bush as being a member of the "Axis of Evil."⁷⁹ CI Host was unaware that they were hosting such clients, and immediately shut down all forty-eight sites once they were informed of the issue.⁸⁰

The Problem and the Lack of a Coherent Strategy

Shutting down websites hosted within the United States is possible, but companies are sometimes reluctant to do so. Consider again the example of PIJ and one of their websites, qudsway.net. This site is hosted in Iran and has a domain name registered with a U.S. company, Network Solutions.

The most direct and effective option for shutting the site down would be to enlist the cooperation of Iran as the law enforcement arm in the country where the site is hosted. Since Iranians are the main backers of the PIJ, however, any attempt to work with them would be unsuccessful. The only other option would require Network Solutions to sever PIJ's registration with the domain name qudsway.net. Weisburd tried to shut the website down by contacting Network Solutions, but he met with serious resistance. A representative of Network Solutions sent him the following message:

⁷⁵ Rachel Ehrenfeld, *Shutting Down Cyber-Terror*, FRONTPAGE MAG., Oct. 21, 2004, available at <http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=15605>.

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ See Todd Bensman & Robert Riggs, *Top Iranian Government Websites Discovered on N. Texas Internet Company*, CBS-11 NEWS (Dallas), Jun. 13, 2005, http://cbs11tv.com/localnews/local_story_164173338.html (last visited Sept. 19, 2007).

⁷⁹ Exec. Order No. 12,205, 3 C.F.R. 248 (Apr. 7, 1980).

⁸⁰ See Bensman, *supra* note 78.

In reviewing your site located at <http://haganah.org.il/haganah/> I noted that my company is called out as being a company that is keeping qudsway.net online. Honestly, do you really think that there is not a good reason that the site is still up. Use your brain, I know that you must be more intelligent than your posts would have people believe. I find blogs like yours loathsome because you are criticizing the actions of a company when you have no idea what is actually happening.⁸¹

As one can infer from the Network Solutions message, there may be “good reasons” that the website was still up. Perhaps the government chose to monitor the site and requested Network Solutions keep the site in operation, or it may just represent the lack of a clear policy.⁸² Either way, qudsway.net continues to flourish.

While it would certainly consume substantial government resources to attempt to shut down individual websites, service providers can shut down sites and domain names with relative ease.⁸³ Many of these service providers do not even physically house the servers. Rather, they provide an IP address and network access.⁸⁴ As Professor Orin Kerr points out, however, there are serious flaws in assuming that ISPs can monitor and control their property like a physical property owner, who can monitor and control their property.⁸⁵ Kerr states that “[t]he common theme is that computer owners can know and control what is happening within their networks; civil liability can lead to less crime because computer owners have the power (and, with civil liability, the incentive) to minimize criminal activity.”⁸⁶ He states that the problem with this reasoning is that

[C]omprehensive ISP monitoring appears to be extremely difficult, even putting aside the very important privacy questions it raises. ISPs can have hundreds of thousands or even millions of customers; it is very difficult and time consuming for an ISP to watch just one or two customers in a comprehensive way; and it is easy for any customer to circumvent or defeat ISP monitoring.⁸⁷

⁸¹ *Qudsway.net: Proof that the United States and Iran *Can* Act Cooperatively*, INTERNET HAGANAH, May 14, 2006, available at <http://haganah.org.il/harchives/005605.html>.

⁸² *See id.*

⁸³ *See Send Your Complaints to 71 Hayarkon Street*, INTERNET HAGANAH, May 22, 2006, <http://haganah.org.il/harchives/005614.html>.

⁸⁴ *See PIJ Site*, *supra* note 4.

⁸⁵ Orin Kerr, *Virtual Crime, Virtual Deterrence: A Skeptical View of Self Help, Architecture, and Civil Liability*, 1 J.L. ECON. & POL'Y 197, 211 (2005).

⁸⁶ *Id.*

⁸⁷ *Id.* at 212.

Kerr has accurately stated the common theme—a theme related to my proposal. Nevertheless, my proposal is distinguishable from his suggesting civil liability, as mine adds both a notification requirement and watch dog monitoring. Thus, while sifting through websites for terrorist activities is beyond the reasonable capability of service providers, they would have no difficulty shutting down websites or domain names upon notification by government officials or third party monitors. Notwithstanding this, without some threat of penalty, be it criminal sanction, civil penalty, or shaming, there is little incentive for the service providers to act after notification.

Material Support Statute as a Tool to Stop the Internet Jihad

Following September 11, 2001, Congress and the justice system responded to the threat of terrorism through a dramatic increase in prosecutions under the material support statutes.⁸⁸ The material support statutes have been two of the most frequently charged terrorism related offenses since 9/11, culminating in ninety-two individuals facing allegations that they violated either Section 2339A or Section 2339B.⁸⁹ One of the key aspects of the material support statutes is their independence from any specific event, creating a separate offense for those attempting to support terrorism. Furthermore, they allow the charges to be made early in the terrorist plot.⁹⁰ Section 2339A provides the government with tools to prosecute individuals and organizations that are actively supporting terrorist activities, either financially or otherwise. Expanding this concept of material support, Congress enacted Section 2339B, which focused on “providing material support or resources to designated foreign terrorist organizations.” The two statutes share the definition of “material support” found in Section 2339A and incorporated by reference into Section 2339B.

Section 2339A was originally passed in the early 1990s after the first bombing of the World Trade Center while Congress was actively seeking a way to cut off funds given for the support of terrorist actions.⁹¹ The purpose of Section 2339A is to stop the furnishing of resources to any individual or group with the knowledge or intention that it be used to lend support to any of more than two dozen different terrorist activities.⁹² Within

⁸⁸ Robert M. Chesney, *The Sleeper Scenario: Terrorism—Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1, 20 (2005).

⁸⁹ *See id.*

⁹⁰ *See* 18 U.S.C. § 2339B(c) (2000) (“Whenever it appears to the Secretary of the Attorney General that any person is engaged in, or is about to engage in, any act that constitutes, or would constitute, a violation of this section, the attorney General may initial civil action in a district court of the United States to enjoin such violation.”).

⁹¹ *See* Chesney, *supra* note 88, at 12–13.

⁹² Listed offenses include: knowing or intending that they are to be used in preparation for, or in carrying out, a violation of: 18 U.S.C.S. § 32 (LexisNexis 1993 & Supp. 2007) (destruc-

Section 2339A, material support is defined as any property, tangible or intangible, or service, including expert advice or assistance and communications equipment.

The scope of Section 2339A is often considered to be very narrow and unattainable by practical standards.⁹³ Thus, only a short period after Section 2339A was passed, Congress added Section 2339B, making it a

tion of aircraft or aircraft facilities); 18 U.S.C.S. § 37 (LexisNexis 1993 & Supp. 2007) (violence at international airports); 18 U.S.C.S. § 81 (LexisNexis 1993 & Supp. 2007) (arson within special maritime and territorial jurisdiction); 18 U.S.C.S. § 175 (LexisNexis 1993 & Supp. 2007) (biological weapons offenses); 18 U.S.C.S. § 229 (LexisNexis 1993 & Supp. 2007) (chemical weapons offenses); 18 U.S.C.S. § 351 (LexisNexis 1993 & Supp. 2007) (congressional, cabinet, and Supreme Court assassination and kidnapping); 18 U.S.C.S. § 831 (LexisNexis 1993 & Supp. 2007) (nuclear material offenses); 18 U.S.C.S. § 842(m) (LexisNexis 2005 & Supp. 2007) (plastic explosives offenses); 18 U.S.C.S. § 844(f)(i) (LexisNexis 2005 & Supp. 2007) (burning or bombing federal property or property used in interstate or foreign commerce); 18 U.S.C.S. § 903(c) (LexisNexis 2005 & Supp. 2007) (killing or attempted killing of another during an attack on a federal facility with a dangerous weapon); 18 U.S.C.S. § 956 (LexisNexis 2005 & Supp. 2007) (conspiracy to murder, kidnap, or maim overseas); 18 U.S.C.S. § 1114 (LexisNexis 1994 & Supp. 2007) (killing of attempted killing of federal officers and employees); 18 U.S.C.S. § 1116 (LexisNexis 1994 & Supp. 2007) (murder or manslaughter of foreign officials, official guests, or internationally protected persons); 18 U.S.C.S. § 1203 (LexisNexis 1994 & Supp. 2007) (hostage taking); 18 U.S.C.S. § 1361 (LexisNexis 1994 & Supp. 2007) (destruction of federal property); 18 U.S.C.S. § 1362 (LexisNexis 1994 & Supp. 2007) (destruction of communication lines, stations, or systems); 18 U.S.C.S. § 1363 (LexisNexis 1994 & Supp. 2007) (destruction of property within special maritime and territorial jurisdiction of the United States); 18 U.S.C.S. § 1366 (LexisNexis 1994 & Supp. 2007) (destruction of an energy facility); 18 U.S.C.S. § 1751 (LexisNexis 1991 & Supp. 2007) (presidential assassination or kidnapping); 18 U.S.C.S. § 1992 (LexisNexis 1991 & Supp. 2007) (wrecking trains); 18 U.S.C.S. § 1993 (LexisNexis 1991 & Supp. 2007) (terrorist attacks and other acts of violence against mass transportation systems); 18 U.S.C.S. § 2155 (LexisNexis 1991 & Supp. 2007) (destruction of national defense material); 18 U.S.C.S. § 2156 (LexisNexis 1991 & Supp. 2007) (production of defective national defense material); 18 U.S.C.S. § 1280 (LexisNexis 1991 & Supp. 2007) (violence against maritime navigation); 18 U.S.C.S. § 2281 (LexisNexis 1991 & Supp. 2007) (violence against maritime fixed platforms); 18 U.S.C.S. § 2332 (LexisNexis 1991 & Supp. 2007) (violence against Americans overseas); 18 U.S.C.S. § 2332(a) (LexisNexis 1991 & Supp. 2007) (weapons of mass destruction); 18 U.S.C.S. § 2332b (LexisNexis 1991 & Supp. 2007) (multinational terrorism); 18 U.S.C.S. § 2332f (LexisNexis 1991 & Supp. 2007) (bombing public places or facilities); 18 U.S.C.S. § 2340A (LexisNexis 1991 & Supp. 2007) (torture); 42 U.S.C.S. § 2284 (LexisNexis 1996 & Supp. 2007) (sabotage of nuclear facilities or fuel); 49 U.S.C.S. § 46502 (LexisNexis 2004 & Supp. 2007) (aircraft piracy); 49 U.S.C.S. § 60123(b) (LexisNexis 2004 & Supp. 2007) (destruction of gas pipeline facilities); or any offense listed in 18 U.S.C.S. § 2332(b)(g)(5)(B) (LexisNexis 1991 & Supp. 2007) (except for sections 2339A and 2339B), or in preparation for, or in carrying out the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act, shall be fined under this title, imprisoned not more than fifteen years, or both, and if the death of any person results, shall be imprisoned for any term of years or for life.

⁹³ See JOHN ROTH ET AL., NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., MONOGRAPH ON TERRORIST FINANCING, 31–32 (2004); available at http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf.

crime to knowingly provide material support or resources to a specifically “designated foreign terrorist organization.”⁹⁴ Because Section 2339B does not require that support be tied to a specific terrorist act as in Section 2339A, the material support statute’s applicable use is significantly broadened by providing a way to prosecute *indirect* terrorist conduct. Furthermore, Section 2339B only requires that the “defendant knowingly provide material support or resources to a foreign terrorist organization.”⁹⁵ If a donor gives a designated foreign terrorist organization material support of the kind listed in the statute, even if it is meant to be used for peaceful non-violent means, the donor is still in violation of Section 2339B. The policy position is that all support, regardless of its intended use when given to a designated terrorist organization, will ultimately free funds that can be used to further violent terrorist activities.⁹⁶

Section 2339B is the most used of the two material support statutes, as well as the most debated. Defendants often challenge section 2339B on the constitutional basis of freedom of association and the due process clause. Challengers claim that the right of association includes the right to support that idea or group through the donation of money and goods. In *Humanitarian Law Project v. Gonzales (HLP)* the defendants claimed that without a specific intent requirement written into Section 2339B, the statute violates the Fifth Amendment.⁹⁷ The plaintiffs relied upon precedent set by *Scales v. United States*.⁹⁸ *Scales* was a conviction based on the Smith Act, which specifically criminalized being a member in an organization whose goal was to overthrow the government.⁹⁹ The court in *HLP* disagreed with *Scales*, stating Section 2339B is fundamentally different by not criminalizing the membership, but instead the actions which would “materially support” the group’s intentions.¹⁰⁰ The effect of this distinction is that the court found that the specific intent requirement does not defeat the purpose and constitutionality of Section 2339B.

Although the validity of the statute itself has been upheld, courts have found portions of the statute to be impermissibly vague. In *US v. Sattar*, a terrorist organization called the Islamic Group (IG) operated within the United States as a radical Islamic group opposing any “infidels” who did

⁹⁴ 18 U.S.C. § 2339(a)(1) (2000).

⁹⁵ *Weiss v. National Westminster Bank PLC*, 453 F.Supp.2d 609, 625 (E.D.N.Y., 2006) (quoting 18 U.S.C. §2339B (1995)) (internal quotations omitted).

⁹⁶ S. 390, 104th Cong. § 301 at 65 (1995), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_bills&docid=f:s390is.txt.pdf.

⁹⁷ *Humanitarian Law Project v. Gonzales*, 380 F.Supp. 2d 1134, 1140 (C.D.Cal. 2005).

⁹⁸ *See id.* at 1143.

⁹⁹ *See id.* at 1144.

¹⁰⁰ *See id.* at 1145.

not agree with either the IG's interpretation of Islamic law or the sentence and detention of the Islamic leader of the IG, Sheikh Abdel Rahman.¹⁰¹ The indictment against the defendants included a charge of facilitating correspondence between Rahman and third parties, namely other IG leaders.¹⁰² The court found that the "provision of communications equipment" was unconstitutional because "a criminal defendant simply could not be expected to know that the conduct alleged was prohibited by the statute."¹⁰³ In addition, the court in *Sattar* stated the "provision" of "personnel" was also interpreted as impermissibly vague due to the lack of notice or standards for its application.¹⁰⁴ Nevertheless, the court denied the defendant's claim that the statute was also overbroad and thus unconstitutional in light of its sweeping purpose and applicability.¹⁰⁵ Section 2339B is content-neutral, and Congress has the ability to prohibit the "supply of tangible support."¹⁰⁶

Designation as a Foreign Terrorist Organization

A variety of lists compiled by U.S. government agencies designate groups or individuals as terrorists.¹⁰⁷ The Secretary of State has the power to declare a group a "foreign terrorist organization" (FTO) pursuant to 8 U.S.C. § 1189. The Secretary is authorized to make such a designation if three conditions are met: (1) the organization is foreign, (2) the organization engages in terrorist activity, and (3) the terrorist activity threatens the security of U.S. citizens or the national security of the United States.¹⁰⁸ If the Secretary finds that the organization meets these requirements, the Secretary can add the organization to the FTO list by informing Congress seven days before the designation, and then publishing a notice in the Federal Register.¹⁰⁹ As of October 2005, there have been forty-two listed foreign terrorist organizations identified.¹¹⁰

Section 2339B(g)(6) defines the term "terrorist organization" as "an organization designated as a terrorist organization under section 219 of the

¹⁰¹ U.S. v. *Sattar*, 272 F. Supp. 2d 348, 353 (S.D.N.Y. 2003).

¹⁰² *Id.* at 355.

¹⁰³ *Id.* at 358 (citing U.S. v. *Handakas*, 286 F.3d 92, 104 (2d. Cir. 2002)).

¹⁰⁴ *Id.*

¹⁰⁵ *Id.* at 361–62.

¹⁰⁶ *Id.* at 362.

¹⁰⁷ See AUDREY KURTH CRONIN, THE "FTO LIST" AND CONGRESS: SANCTIONING DESIGNATED FOREIGN TERRORIST ORGANIZATIONS, CRS REPORT FOR CONGRESS RL 32120 3–5 (October 21, 2003), available at <http://www.fas.org/irp/crs/RL32120.pdf>.

¹⁰⁸ 8 U.S.C. § 1189(a)(1) (Supp. 2004).

¹⁰⁹ *Id.* § 1189(a)(2)(A).

¹¹⁰ See OFFICE OF COUNTERTERRORISM, U.S. DEP'T OF STATE, FOREIGN TERRORIST ORGANIZATION (FTO) (Oct. 11, 2005) <http://www.state.gov/s/ct/rls/fs/37191.htm>.

Immigration and Nationality Act” which is codified at 18 U.S.C. 1189. Once an organization has been designated an FTO, the effects of that designation are in two important areas: finance and immigration.¹¹¹ Under the Antiterrorism and Effective Death Penalty Act of 1996, it is a crime to donate money, assets, or any other “material support” to a designated FTO.¹¹² Members of an FTO are also forbidden from entering the country and, if already present, are often subject to removal.¹¹³ Furthermore, if any bank or financial institution finds that it controls an FTO’s money or has interests in the FTO’s assets, they must retain possession of, or control over, the funds and report them to the Office of Foreign Assets Control of the U.S. Department of the Treasury.¹¹⁴ Most importantly, Section 2339B applies specifically to any donation of “material support” to a designated FTO on the State Department’s list.¹¹⁵

The U.S. Department of the Treasury compiles its own list of terrorist organizations, but the list also includes individuals designated as terrorists.¹¹⁶ Pursuant to Executive Order 13224, all property, and interests in property, within the United States owned by certain persons are blocked. According to the U.S. Department of Treasury website,¹¹⁷ these persons/organizations include: (1) foreign individuals or entities listed in the Annex to E.O. 13224;¹¹⁸ (2) foreign individuals or entities that “have committed or . . . pose a significant risk of committing acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy” of the United States;¹¹⁹ (3) individuals or entities that either are “owned or controlled by” or “act for or on behalf of” those parties already designated under sub-sections 1(a), 1(b), 1(c), or 1(d)(i) of E.O. 13224;¹²⁰ (4) individuals or entities that “assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of such acts of terrorism or those” parties already designated under E.O. 13224;¹²¹ and (5) individuals or entities that are “otherwise associated” with those parties already designated under sub-sections 1(a), 1(b),

¹¹¹ CRONIN, *supra* note 107, at CRS-2–3.

¹¹² 18 U.S.C. 2339B(a)(1) (2000).

¹¹³ CRONIN, *supra* note 107, at CRS-3.

¹¹⁴ *See* 8 U.S.C. § 1189.

¹¹⁵ 18 U.S.C. § 2339B.

¹¹⁶ *See* CRONIN, *supra* note 107, at CRS-4.

¹¹⁷ Treas. Dep’t Designations, <http://www.ustreas.gov/officesenforcement/designations.shtml> (last visited Sept. 21, 2007).

¹¹⁸ Exec. Order No. 13,224, 3 C.F.R. 786 (2001), *reprinted in* 50 U.S.C. § 1701 (Supp. III 2000).

¹¹⁹ *Id.*

¹²⁰ *Id.*

¹²¹ *Id.*

1(c), or 1(d)(i), of E.O. 13224.¹²² This list includes the criteria the Department of State uses to determine whether or not to block financial assets of terrorists and their affiliated members. There are currently over three hundred persons identified as “Specially Designated Global Terrorists” (SDGT) including the original “specially designated terrorists” list.¹²³

The main distinction between the Department of State’s FTO list and the Department of Treasury’s SDGT list is the lack of an immigration element.¹²⁴ Another distinguishing feature of the SDGT list is that the designation has no time limit, while the designation of an FTO contains a provision for re-evaluation after five years (if one has not been petitioned for before that time).¹²⁵ Furthermore, the lists are founded in separate legislation, and each department takes the lead on adding new organizations or individuals to their respective lists.¹²⁶ Currently, the SDGT list contains more than two hundred organizations and individuals who have had their assets frozen under E.O. 13224.¹²⁷

The FTO list has been challenged as facially unconstitutional for denying groups their right to due process. In *U.S. v. Rahmani*, the court decided that the legislation’s restriction on a court’s ability to review the constitutionality of 8 U.S.C. 1189 was impermissible.¹²⁸ The court went on to declare that a group’s exclusion from and inability to challenge their designation as an FTO denied them due process.¹²⁹ On appeal, the circuit court overruled the first finding because “[m]any administrative determinations are reviewable only by petition to the correct circuit court.”¹³⁰ The circuit court also held that a third party does not have the power to challenge the designation on a constitutional due process basis.¹³¹ Therefore, while the systems have been challenged and critiqued, the court has generally held that the designation of organizations as terrorist organizations is facially constitutional.

¹²² *Id.*

¹²³ CRONIN, *supra* note 107, at CRS-4.

¹²⁴ *See id.*

¹²⁵ 8 U.S.C. § 1189(4)(C) (Supp. 2004).

¹²⁶ *See* CRONIN, *supra* note 107, at CRS-4.

¹²⁷ Office of Foreign Asset Control, Specially Designated Nationals and Block Persons, Dep’t. of Treasury (Feb. 12, 2008), *available at* <http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf>.

¹²⁸ *See* *U.S. v. Rahmani*, 209 F.Supp.2d 1045, 1054 (C.D. Cal. 2002).

¹²⁹ *See id.* at 1058.

¹³⁰ *U.S. v. Afshari*, 446 F3d 1150, 1154 (9th Cir. 2005).

¹³¹ *Id.* at 1155.

Treasury Regulations and IEEPA as Tools

The Treasury's authority to confront and counter terrorists in cyberspace stems largely from the powers provided to the President by IEEPA. The IEEPA allows the President to declare a national emergency in response to a threat to national security, foreign policy, or economy of the United States. With such a declaration the President can exercise a broad set of powers including blocking property, investigating, and regulating and prohibiting transactions.¹³² On September 23, 2001, President Bush invoked this power, declaring a national emergency with respect to the threat posed by al-Qaida, and issued E.O. 13224, "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism."¹³³

The Order included an initial list of twenty-seven targets, including Osama bin Laden and al-Qaida.¹³⁴ In addition, it provided that the Secretaries of State and Treasury could add specified categories of persons (individuals and entities) to the list.¹³⁵ The categories of individuals and entities "designatable" by the Secretary of the Treasury are:

- (a) persons determined to be owned or controlled by, or to act for, or on behalf of, those persons either listed in the Annex to the EO [Executive Order] or determined to be subject to the EO;
- (b) persons determined to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, those persons listed in the Annex to this order or determined to be subject to this order;
- (c) persons determined to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, acts of terrorism as defined by the EO, or
- (d) persons determined to be otherwise associated with those persons listed in the Annex to the EO order or those persons determined to be subject to the EO.¹³⁶

Placement on the list requires U.S. persons, which for purposes of this article would also include ISPs and DNRs, to block property and interests in property—including "services of any nature whatsoever,"¹³⁷ belonging to the designated sanctions targets.¹³⁸ In addition, U.S. persons are also

¹³² *Id.* §§ 1701–02 at 232, 253, 262.

¹³³ Exec. Order No. 13,224, *supra* note 118.

¹³⁴ *Id.* at Annex.

¹³⁵ *See id.* at §1.

¹³⁶ *See id.* §§ 1(c), (d)(i).

¹³⁷ 31 C.F.R. § 594.309 (2006).

¹³⁸ *Id.* at § 594.301.

prohibited under E.O. 13224 (and its implementing regulations) from engaging in “any transaction or dealing . . . in [blocked] property or interests in property,” including the provision of services to or for the benefit of persons designated pursuant to the E.O.¹³⁹

This means that Treasury Regulations may be an extremely effective tool in countering the internet jihad. Those companies organized under the laws of the United States, or any ISPs physically located in the United States, are thus prohibited by law from providing internet service to or for the benefit of al-Qaeda, Hezbollah, Hamas, PIJ, and any other entities or individuals designated pursuant to the Order.

Furthermore, treasury regulations found in 31 C.F.R. § 594, as well as those available on Office of Foreign Assets Control’s (OFAC) internet homepage,¹⁴⁰ also apply to potential sanctions for internet providers supporting jihadist websites.¹⁴¹ According to OFAC guidance, those who wish

¹³⁹ *Id.* at § 594.406.

¹⁴⁰ U.S. Dep’t of the Treasury, Office of Foreign Assets Control: Mission, <http://www.treas.gov/offices/enforcement/ofac/> (last visited Feb. 15, 2008).

¹⁴¹ § 594.201 Prohibited transactions involving blocked property.

(a) . . . *property and interests in property of . . . persons [designated pursuant to E.O. 13224] that are in the United States, that hereafter come within the United States, or that hereafter come within the possession or control of U.S. persons, including their overseas branches, are blocked and may not be transferred, paid, exported, withdrawn or otherwise dealt in . . .*”

§ 594.204 Prohibited transaction or dealing in property; contributions of funds, goods, or services.

Except as otherwise authorized, *no U.S. person may engage in any transaction or dealing in property or interests in property of persons whose property or interests in property are blocked pursuant to § 594.201(a), including but not limited to the making or receiving of any contribution of funds, goods, or services to or for the benefit of persons whose property or interests in property are blocked pursuant to § 594.201(a).*

§ 594.309 Property; property interest.

The terms property and property interest include, but are not limited to . . . services of any nature whatsoever . . .”

§ 594.406 Provision of services.

(a) . . . *the prohibitions on transactions or dealings involving blocked property contained in §§ 594.201 and 594.204 apply to services performed in the United States or by U.S. persons, wherever located, including by an overseas branch of an entity located in the United States:*

(1) *On behalf of or for the benefit of a person whose property or interests in property are blocked pursuant to § 594.201(a); or*

(2) *With respect to property interests subject to §§ 594.201 and 594.204.*

(b) *Example: U.S. persons may not . . . provide legal, accounting, financial, brokering, freight forwarding, transportation, public relations, educational, or other services to a person whose property or interests in property are blocked pursuant to § 594.201(a).*

§ 594.409 Charitable contributions.

to provide services to targets of Treasury sanctions may not do so without *ex ante* case by case authorization by Treasury.¹⁴² The potential civil penalties for violations of IEEPA regulations is \$250,000.¹⁴³

Acting pursuant to these authorities, the Treasury may issue Cease and Desist orders (C&Ds) to U.S.-based internet companies providing services in violation of existing sanctions programs.¹⁴⁴ The C&Ds would be issued pursuant to IEEPA, E.O. 13224 (or possibly E.O. 13438),¹⁴⁵ and 31 C.F.R. § 594. If systematically employed as part of a long-term program targeting terrorist websites, jihadists will be forced to seek domain names and ISPs from overseas hosts.

Under the same laws and regulations, OFAC can also demand information from internet service providers' client lists, such as those clients

Unless otherwise specifically authorized by the Office of Foreign Assets Control by or pursuant to this part, *no* charitable contribution or *donation of* funds, goods, *services, or technology*, including those to relieve human suffering, such as food, clothing, or medicine, *may be made to or for the benefit of a person whose property or interests in property are blocked* pursuant to § 594.201(a). (emphasis added).

¹⁴² See O.F.A.C. Guidance Ltr., 030606-FACRL-IA-07 (June 3, 2003) (providing interpretative guidance on Iranian Transaction Regulation 31 C.F.R. § 560, on the provision of Internet Connectivity Services and is persuasive with regard to the interpretation of Global Terrorism Sanctions Regulations).

¹⁴³ Press Release, Dep't of the Treasury, Office of Foreign Assets Control, Civil Penalties—Interim Policy (Nov. 27, 2007) *available at* www.treas.gov/offices/enforcement/ofac/civpen/penalties/interim_pol_11272007.pdf. (“On October 16, 2007, the President signed into law the International Emergency Economic Powers Enhancement Act (‘IEEPA Enhancement Act’ or ‘Act’), Pub. L. No. 110-96, which, *inter alia*, increased the maximum civil penalty applicable to violations of orders or regulations issued under IEEPA. The new maximum civil penalty is the greater of \$250,000 or an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed.”).

¹⁴⁴ See Statement by Assistant Sec’y Juan Zarate Before the United Nations Sec. Council 1267 Sanctions Comm., JS-2189 (Jan. 10, 2005) *available at* <http://treas.gov/press/releases/js2189.htm>.

¹⁴⁵ See Exec. Order No. 13,438, 27 Fed. Reg. 39,719 (Jul. 19, 2007) *available at* <http://www.treas.gov/offices/enforcement/ofac/legal/eo/13438.pdf>. The E.O. provides that “the Secretary of the Treasury, in consultation with the Secretary of State and the Secretary of Defense,” may designate persons determined: “(i) to have committed, or to pose a significant risk of committing, an act or acts of violence that have the purpose or effect of: (A) threatening the peace or stability of Iraq or the Government of Iraq; or (B) undermining efforts to promote economic reconstruction and political reform in Iraq or to provide humanitarian assistance to the Iraqi people; (ii) to have materially assisted, sponsored, or provided financial, material, logistical, or technical support for, or goods or services in support of, such an act or acts of violence or any person whose property and interests in property are blocked pursuant to this order; or (iii) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order.” *Id.*

receiving domain names or web-hosting.¹⁴⁶ Signing up for an account with an ISP generally involves providing your name, address, telephone number, and billing information, which invariably includes a credit card number.¹⁴⁷ The example of Irhabi007 supports this; investigators there found stolen credit card information and confirmed that the cards were used to pay American internet providers, on whose servers Irhabi007 had posted jihadi propaganda.¹⁴⁸ According to the *Washington Post*, that lead demonstrated to authorities that “they had netted the infamous hacker.”¹⁴⁹

Shaming and Watch-Dog Groups: Steps Short of Using the Statute

Despite the fact that designated foreign terrorist organizations are publicly listed on the Department of State and Department of Treasury websites, internet companies are either undeterred by the threat of prosecution, or are unaware of their client’s terrorist status. As such, and as the PIJ example illustrates, these companies continue to do business with them. The material support statute may be a means for government officials to shut down the phenomenon of cyber jihad, although doing so would be an extreme step.

While the government has a legitimate interest in keeping terrorists from recruiting, they do not want to be seen as attempting to censor the internet. A wiser interim policy is to persuade internet service providers and domain name registrars to voluntarily take down or suspend services when those services are assisting terrorist organizations. Network Solutions, which I wrote critically about earlier in the article, often avoids acknowledging the fact that it has retained through their User Policy Agreement, the ability to regulate and take down a site that it deems “unlawful,” “threaten-

¹⁴⁶ 31 C.F.R. § 501.602 (“Every person is required to furnish under oath, in the form of reports or otherwise, from time to time and at any time as may be required by the Director, Office of Foreign Assets Control, complete information relative to any transaction, regardless of whether such transaction is effected pursuant to license or otherwise, subject to the provisions of this chapter or relative to any property in which any foreign country or any national thereof has any interest of any nature whatsoever, direct or indirect. The Director may require that such reports include the production of any books of account, contracts, letters or other papers connected with any such transaction or property, in the custody or control of the persons required to make such reports. Reports with respect to transactions may be required either before or after such transactions are completed . . . the Director may, through any person or agency, conduct investigations, hold hearings, administer oaths, examine witnesses, receive evidence, take depositions, and require by subpoena the attendance and testimony of witnesses and the production of all books, papers, and documents relating to any matter under investigation, regardless of whether any report has been required or filed in connection therewith.”).

¹⁴⁷ JOHN R. LEVINE, ET AL., *THE INTERNET FOR DUMMIES* 60 (7th ed. 2000).

¹⁴⁸ Rita Katz & Michael Kern, *Terrorist 007, Exposed*, WASH. POST, Mar. 26, 2006, at B1.

¹⁴⁹ *Id.*

ing,” or which “constitutes an illegal threat, hate propaganda, profane, indecent or otherwise objectionable material of any kind or nature.”¹⁵⁰ Of course, Network Solutions is not the only web service provider that hosts extremist websites, another site based in Dallas, thePlanet.com has also been accused of hosting three different PIJ websites, as well as a Hamas monthly news magazine, each run by designated FTOs.¹⁵¹

Because it is difficult for companies and the government to monitor whom internet services are being provided to, independent watch-dog sites stand in the best position to fill the gap. A number of watch-dog sites already monitor the internet for terrorist activity and information. This brings me back to the example of Internet Haganah. While Internet Haganah is primarily run by Weisburd out of his home, it enjoys the help of groups from around the world.¹⁵² After finding a terrorist website, Weisburd determines which internet companies are providing the site support and either “shames service providers into shutting down the sites that host them or gathers what he terms ‘intel’ for interested parties.”¹⁵³ These interested parties include both government and private entities.¹⁵⁴ Internet Haganah encourages individuals to take action by learning about both the terrorist website and the group, understanding the terms of service of the host company, and finally making a calm, informed complaint to the company.¹⁵⁵ Often these complaints go unanswered, at which point Internet Haganah recommends that an individual go to the local media for publicity.¹⁵⁶ No company wants to see its name smeared across the morning news as a supporter of terrorism, especially in their key market.¹⁵⁷

Tactics such as these have successfully encouraged sites to take down other questionable material, such as websites that cater to pedophiles. For example, in April 2007, Network Solutions shut down a website after receiving complaints from customers.¹⁵⁸ The site had been publicly broad-

¹⁵⁰ Network Solutions Acceptable Use Policy, <http://www.networksolutions.com/legal/aup.jsp> (last visited Sept. 26, 2007).

¹⁵¹ *Dallas Server Company Carries Zarqawi Death Videos, Terrorist Websites* (CBS-11 television broadcast Nov. 14, 2004), available at <http://haganah.org.il/hmedia/press-15nov04-cbs11-dallas.pdf>.

¹⁵² Labi, *supra* note 65, at 104.

¹⁵³ *Id.*

¹⁵⁴ *Id.*

¹⁵⁵ *See Confronting the Global Jihad Online: What Can You Do*, INTERNET HAGANAH, Nov. 18, 2004, <http://internet-haganah.com/harchives/003133.html>.

¹⁵⁶ *Id.*

¹⁵⁷ *See id.*

¹⁵⁸ *See Network Solutions Shuts Down Pedophile Website*, HOSTSEARCH, Apr. 7, 2007, www.hostsearch.com/news/network_solutions_news_5782.asp.

casted in the *Bellingham Herald* newspaper, prompting the complaints.¹⁵⁹ Company spokeswoman, Susan Wade, responded by saying that although there is no way they could possibly “police the content of everything that’s going up because hosting providers can sell thousands of sites a day,” they appreciate when third parties get involved or “when we get served legal papers that say, ‘Hey, take a look at this.’”¹⁶⁰

What Impact Will Using the Statute Have on the Internet Jihad?

When shaming, complaints, and bad publicity fail, government officials may need to bring legal action against companies that are providing support to terrorist organizations. The U.S. Senate Committee on Homeland Security and Governmental Affairs has conducted hearings on violent Islamic extremism, covering various aspects of the problems including how the internet fosters recruitment and propaganda dissemination.¹⁶¹ At the hearings, the George Washington University Homeland Security Policy Institute endorsed the use of “[l]egal means for disrupting extremist use of the Internet[, which] may be useful against websites that directly advocate violence or provide material support to known terrorist organizations, crossing the line from protected speech to illegal acts of violence.”¹⁶² The House of Representatives has also begun to take notice of the presence of terrorism on the internet. House Resolution 224 has been referred to committee, calling on all corporate owners of websites that share user-posted videos to take down terrorist and jihadist propaganda.¹⁶³ Yet, even without this express resolution, the government already has a powerful legal tool available in the form of Section 2339.

Prosecutors can use Section 2339 to stop U.S. internet providers from providing their services as “material support” to FTOs. Ignoring the threat of prosecution exposes companies to prison, fines, and significant public outcry. Section 2339 holds that if a person is found to have materially supported a designated foreign terrorist organization, they “shall be fined under this title or imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life.”¹⁶⁴ While to date no case has been brought against an ISP, a plain read-

¹⁵⁹ *Id.*

¹⁶⁰ *Id.*

¹⁶¹ *The Internet: A Portal to Violent Islamic Fundamentalism Before the S. Comm. On Homeland Security and Governmental Affairs*, 110th Cong. (2007) available at <http://www.senate.gov/~govt-aff/index.cfm?Fuseaction=Hearings.Detail&HearingID=441>.

¹⁶² THE GEORGE WASHINGTON UNIV. HOMELAND SEC. POLICY INST. ET AL., NETWORKED RADICALIZATION: A COUNTER-STRATEGY 20 (2007) available at http://www.gwumc.edu/hspi/reports/NETworked%20Radicalization_A%20Counter%20Strategy.pdf.

¹⁶³ H.R. Res. 224, 110th Cong. (2007).

¹⁶⁴ 18 U.S.C. § 2339B(a)(1) (Supp.).

ing of the statute suggests that those who provide services to terrorist websites have satisfied the definition of providing “material support.”¹⁶⁵

While most prosecutions under the Section 2339 have centered upon individuals who have physically provided material support, either through the provision of objects such as weaponry or funding, the statute has only recently been used to prosecute individuals who use computers and the internet as a means of providing material support.¹⁶⁶ In 2004, The District Court of Connecticut indicted Babar Ahmad on terrorism charges including a violation of Section 2339A, providing material support.¹⁶⁷ The charges allege that Ahmad created websites in order to “recruit mujahideen, raise funds for violent jihad, recruit personnel . . . solicit military items,” and to give instructions on how to travel to Pakistan to fight for the Taliban, and for the “surreptitious transfer of funds” to terrorist groups.¹⁶⁸ Some of the websites opened and maintained by Ahmad were serviced through a U.S. company, OLM, which was headquartered in Connecticut at the time.¹⁶⁹

The Ahmad case proves that a material support prosecution for providing internet services is at least conceivable; yet, no such actions have been brought against internet service providers. This is likely due to the fact that most companies want to cooperate, and when they are reluctant to do so, their reluctance is short-lived when faced with the threat of prosecution.

Despite the utility of threatening prosecution, there are legal challenges to successfully using the material support statute. Some may argue that targeting internet service providers amounts to censorship by proxy.¹⁷⁰ According to Professor Kreimer of the University of Pennsylvania:

¹⁶⁵ *See id.*

¹⁶⁶ *See, e.g.*, Criminal Complaint at 3–4, *U.S. v. Lindh*, No. 02–51–M (E.D.Va. 2002) (claiming John Walker Lindh admitted to traveling to Pakistan to receive paramilitary training and traveling to Afghanistan to join the Taliban); Indictment at 86–94, *U.S. v. Al-Arian*, No. 8:03–CR (M.D.Fla. 2003) (charging Sami Amin Al-Arian with conspiracy to provide material support to Palestinian Islamic Jihad–Shiqaqi by raising funds for the organization); Indictment at 10–20, *U.S. v. Sattar*, No. 02–Crim.–395 (S.D.N.Y. 2002) (charging Ahmed Abdel Sattar with conspiracy to provide material support to Islamic Gama’at by providing telephone equipment, financing, and transportation); Indictment at 7–9, *U.S. v. Babar Ahmed*, (D.Conn. 2004) (charging Babar Ahmed with conspiracy to provide material support to Al-Qaida by maintaining internet accounts used to recruit members, solicit donations, and communicate to a U.S. Naval enlistee encouraging “the enlistee to ‘keep up the psychological warfare [sic].’”).

¹⁶⁷ Indictment at para. 18, *U.S. v. Babar Ahmed* (D. Conn. 2004).

¹⁶⁸ *Id.* at para. 12.

¹⁶⁹ *Id.* at para. 21A.

¹⁷⁰ *See, e.g.*, Seth F. Kreimer, *Censorship by Proxy: the First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 11 (2006).

If unrestrained by First Amendment doctrine, the “material support” statutes, or other similar criminal prohibitions that might be adopted, will threaten to recruit a federally conscripted corps of censors. Webmasters, site owners, or technicians could find themselves the subjects of criminal prosecution for facilitating the transmission of any message originating with federally proscribed organizations. A risk-averse Internet intermediary would not need to descend into paranoia to conclude that the most prudent course would be to proactively censor messages or links that might prove problematic, and to respond to official “requests” with alacrity.¹⁷¹

Professor Kreimer goes on to argue that First Amendment protection should be read “at a minimum . . . [to] provide similar protection to those who innocently associate with illicit actors or provide links in the chain of communications over the Internet.”¹⁷² I do not disagree with Professor Kreimer’s assertion; in fact, this is why I argued above that the first step should be, as some watchdog groups advocate, to first contact the internet company, then conduct a public shaming and media campaign. Only when those methods fail should the government consider prosecuting those companies who support terrorist websites. It is only then that the government can argue that the company was aware of its support of terrorist organizations. It is critical to bear in mind that the government in such a prosecution is not targeting the company’s speech; it is instead targeting the company’s provision of services to a designated terrorist organization.

Similarly, Treasury regulations have undergone First Amendment scrutiny and survived. For example, an examination of case law involving the constitutionality of OFAC actions involving First Amendment claims by U.S. persons indicates that courts overwhelmingly rule in favor of the agency, especially when the cases involve counterterrorism-related enforcement actions. As stated in a D.C. Circuit Court of Appeals decision, “there is no First Amendment right nor any other constitutional right to support terrorists.”¹⁷³ Despite this fact, the Treasury has not aggressively attempted to cut off cyber-services to terrorism supporters—not even to key al-Qaida facilitators.

One example of Treasury action was the December 2006 designation of Kuwaiti Hamid al-Ali, a cleric who supported al-Qaeda in Iraq and funded terrorist cells in Kuwait.¹⁷⁴ At the time of Hamid al-Ali’s designa-

¹⁷¹ *Id.* at 93–94.

¹⁷² *Id.* at 94.

¹⁷³ *Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156, 166 (D.C. Cir. 2003); *see also* *Humanitarian Law Project v. Reno*, 205 F.3d 1130, 1133 (“[T]here is no constitutional right to facilitate terrorism [with materials or funding.]”).

¹⁷⁴ Press Release HP-191, U.S. Dep’t of the Treasury, Treasury Designations Target Terrorist Facilitators (Dec. 7, 2006), *available at* <http://www.treas.gov/press/releases/hp191.htm>.

tion, the Treasury, under Secretary Stuart Levey, declared that these “individuals support every stage of the terrorist life-cycle, from financing terrorist groups and activity, to facilitating deadly attacks, and inciting others to join campaigns of violence and hate. The civilized world must stand united in isolating these terrorists”¹⁷⁵ Rather than isolating these terrorists, however, Hamid al-Ali has continued to operate his website outside of Washington state.¹⁷⁶ His operations have included the religious sanctioning of suicide bombings and the incitement of individuals to “join the armed resistance of the jihadi movement[.]”¹⁷⁷

Two barriers to Treasury action may be found, not in the First Amendment, but instead in decades old pieces of legislation. In 1988, Representative Howard Berman (D-CA) proposed The Berman Amendment, which limited the President’s powers under IEEPA by creating an exemption for “informational materials.”¹⁷⁸ Also, in 1994 Congress passed the Free Trade in Ideas Amendment which expanded the Berman Amendment to non-tangible forms of information.¹⁷⁹ The Conference Report on the bill stated that the language of the Berman Amendment was explicitly intended to have broad scope.¹⁸⁰

Given the age of these pieces of legislation, a case can be made that their silence regarding terrorism and internet services supporting terrorism may provide for an exception to their broad scope. Even in the absence of an exception, one may argue that terrorist websites provide more than information, that is by allowing fundraising, training, recruiting, and operational details these websites provide “instrumental uses” that are distinguishable from “communicative uses.”¹⁸¹

Moreover, in *U.S. v. O’Brien*,¹⁸² the Supreme Court declared that government actions which advance “sufficiently important governmental

¹⁷⁵ *Id.*

¹⁷⁶ Chris Heffelfinger, *Kuwaiti Cleric Hamid al-Ali: The Bridge Between Ideology and Action*, 5 *TERRORISM MONITOR* 4, available at <http://www.jamestown.org/terrorism/news/article.php?articleid=2373349>.

¹⁷⁷ *Id.*

¹⁷⁸ See The Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100–418, 102 Stat. 1107 (1988) (“The authority granted to the President in this subsection does not include the authority to regulate or prohibit, directly or indirectly, the importation from any country, whether commercial or otherwise, of publications, films . . . or other informational materials . . .”) (codified at 50 U.S.C.A. App. § 5(b)(4)) [hereinafter Berman Amendment].

¹⁷⁹ Foreign Relations Authorization Act of 1994, Pub. L. No. 103–236, § 525; see also, Berman Amendment, *supra*, note 178.

¹⁸⁰ *Id.* (citing H.R. REP. NO. 103–482, at 483 (1994) (Conf. Rep.)).

¹⁸¹ See generally Weimann, *supra* note 35 (explaining many ways terrorist groups use the internet, including training purposes).

¹⁸² *U.S. v. O’Brien*, 391 U.S. 367 (1968).

interests” may allow for incidental limitations on the First Amendment for speech and nonspeech. The *O’Brien* Court held that

a government regulation is sufficiently justified if it is within the Constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on the alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.¹⁸³

Federal Courts applying this test to OFAC activity have allowed the Treasury to restrict the import of books from sanctioned nations.¹⁸⁴ Courts have also upheld Presidential action on the grounds that barring provision of financial support to terrorists was unrelated to suppression of free expression, and that any incidental restrictions on First Amendment freedoms were “no greater than necessary.”¹⁸⁵

Finally, Supreme Court precedent buttresses the view that not all speech is protected. For example, speech which is likely to incite violence,¹⁸⁶ or which creates a clear and present danger of a substantive evil,¹⁸⁷ is unprotected. The content neutral nature of statutes, regulations and other government activity that can counter the cyber jihad makes a successful First Amendment challenge less likely. Accordingly, more government action against terrorist websites and their supporters is necessary to counter the cyber jihad and to fully define the limits of the First Amendment in this critical area of governmental concern.

IV. A CYBER EMBARGO OF DESIGNATED MATERIAL SUPPORTERS

Even if the use of shaming and the threat of the material support statute or Treasury regulations can be successful in driving jihadist websites from U.S.-based service providers, the jihadist web presence will still remain. As the PIJ example demonstrates, a terrorist organization may maintain its web presence by utilizing the services of foreign companies. These companies are, in essence, providing material support, although they have not yet been charged or convicted of the specific offense. Merely forcing jihadist websites overseas is not a sufficient counterterrorism strategy given the ubiquity of the internet, and the fact that sites hosted outside the United

¹⁸³ *Id.* at 377.

¹⁸⁴ *See Teague v. Reg’l Comm’r of Customs, Region II*, 404 F.2d 441, 445 (2d Cir. 1968).

¹⁸⁵ *Global Relief Foundation, Inc. v. O’Neill*, 207 F.Supp.2d 779, 806 (N.D.Ill. 2002), (citing *Humanitarian Law Project v. Reno*, 205 F.3d 1130, 1135 (9th Cir. 2000); *Palestine Info. Office*, 853 F.2d at 939–40; *cf. Walsh v. Brady*, 927 F.2d 1229, 1234–35 (D.C.Cir. 1991)).

¹⁸⁶ *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969).

¹⁸⁷ *Schenck v. U.S.*, 249 U.S. 47 (1919).

States appear as seamlessly as those hosted within the United States. Therefore, new policy and legal proscriptions are necessary to further counter the cyber jihad.

An aggressive application of current statutes may suffice to counter the cyber jihad by targeting “material supporters.” The Department of the Treasury’s designation process, if liberally and aggressively applied, may provide an adequate remedy. As detailed above, sub paragraph three of E.O. allows the Department of the Treasury to block both property and interests in property, which “act for or on behalf of” those parties already designated as terrorist organizations. Furthermore, sub paragraph four allows similar techniques to be applied to “individuals or entities that ‘assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of ‘such acts of terrorism or those parties already designated.’”¹⁸⁸ A broad interpretation of these rules would result in the blocking of both property and interests in property for “material supporters.” In the PIJ example, the practical effect of this designation would be to block the assets of Time Telekom and the Malaysian network service provider supporting the PIJ website.

Nevertheless, this process is limited because these entities may not have assets worth blocking. Thus, a true cyber embargo would entail creating a new process whereby those foreign communications companies that provide material support to terrorist organizations may be designated as “material supporters.” Such a designation would prevent U.S. companies from conducting business with designated entities. This process would create virtual “persona non grata.” The interconnected nature of the world wide web necessitates that even those overseas companies that provide web services to terrorist organizations (the material supporters) must still rely on other web service providers, many of which are in the United States, to communicate. This reliance is the weak link in the cyber jihadist’s web presence. Designating overseas web providers as “material supporters” forces those companies to choose between either losing all commercial services from the United States or continuing to provide services to the terrorist organization.

How would such a designation work? I propose amending the U.S. Code to create a category of “designated material supporter.” U.S. companies would be forbidden from engaging in commercial services with entities bearing such a designation. The designation would include elements of the material support statute, but would limit itself to internet companies. Moreover, the designation could include a provision that allows companies to sever ties to terrorist organizations to avoid being designated a “material supporter.”

¹⁸⁸ Exec. Order No. 13,224, *supra* note 118.

Diplomatic efforts could further expand the cyber embargo. Initially this diplomatic effort need not be expansive. Rather, it could focus on the nine countries that control 95.58% of all registrars.¹⁸⁹ Preventing these registrars from engaging in commercial activity with “material supporters” would have a dramatic impact on the “designated material supporter,” likely forcing them out of business if they do not cease their ties to jihadists. Diplomatic efforts have worked in the past, albeit on a small scale. For example, the U.S. Department of Defense reportedly used its leverage to shut down Palestinian resistance sites hosted by the Ukraine in 2004.¹⁹⁰ In another instance “the British government, responding to the U.S. request under the Mutual Legal Assistance Treaty between the two countries, ordered the closure of twenty media websites in seventeen countries that advocated terrorism.”¹⁹¹ Working through diplomatic channels to shut down foreign companies that serve as material supporters is the critical next step in countering the cyber jihad.

As each country cuts off internet support within their jurisdiction, terrorist websites will be forced to find support in new jurisdictions. Continued monitoring and diplomatic efforts would thus remain critical. Additionally, because 95.8% of all domain registrars are located in nine countries with which the United States has strong diplomatic ties, the internationalization of these efforts is achievable.¹⁹² Furthermore, internationalizing an agreement that will ensure that other countries shut down “designated material supporters” is the next step in countering the internet jihad.

Continuing diplomatic efforts to prohibit dealing with “designated material supporters” will create a system whereby terrorist organizations will have extremely limited choice of locations where they can register and operate their websites. In most cases, the internet jihadists will be forced to register in small, already ostracized countries such as Iran or Libya, which maintain control over their respective .IR and .LY domain names. By limiting internet jihadists to these countries, diplomatic measures, such as trade

¹⁸⁹ Thirty-six countries have ICANN Accredited Registrars. Within those thirty-six countries there are 522 Accredited Domain Name Registrars: 281 of which are located in the United States (54%); 124 of which are located in Canada (28%); 16 of which are located in Germany (3.07%); 12 of which are located in the UK (2.3%); 11 of which are located in the ROK (2.11%); 10 of which are located in Australia (1.9%); 8 of which are located in France (1.53%); 8 of which are located in Japan (1.53%); 6 of which are located in Spain (1.14%). ICANN-Accredited Registrars, <http://www.icann.org/registrars/accredited-list.html> (last visited Sept. 16, 2007).

¹⁹⁰ Al Click, *The Pentagon Closes Jihad Websites*, GUERRILLA NEWS NETWORK, Dec. 29, 2004, available at http://alpinestar.gnn.tv/headlines/547/The_Pentagon_Closes_Jihad_Websites (last visited Oct. 19, 2007 (original on file with author)).

¹⁹¹ Rachel Ehrenfeld, *Shutting Down Cyberterrorism*, Oct. 21, 2004, <http://www.frontpage-magazine.com/Articles/Printable.asp?ID=15605>.

¹⁹² See *supra* note 189.

restrictions or even the dramatic step of blocking internet traffic to those countries, can be brought to bear. Those countries that host jihadist websites will then have to decide if they are willing to protect the internet jihadists at the cost of losing their legitimate commercial internet traffic.

CONCLUSIONS AND IMPLICATIONS

Given the ubiquity of the internet, and the challenges of tracking down constantly moving websites, domain name registrars, and internet service providers, one may be left to conclude that efforts to counter the internet jihad are pointless. Nevertheless, the only truly effective way to counter the internet jihad is to continually make efforts to shut them down. Doing so can dramatically impact the terrorist web presence. For example, Aaron Weisburd claims to have been responsible for shutting down 80% of jihadist websites.¹⁹³

The limited efforts of watchdog groups prove that the fight against cyber jihadists is not a fruitless one. Through increased support of watchdog groups, expanded shaming techniques, and the use of existing statutes, terrorist websites can be forced to overseas service providers. This first step is not enough, however, as the world wide web is dynamic, and the move to overseas service providers will allow cyber jihadists to seamlessly maintain their web presence. Thus, more aggressive use of existing designation techniques, and the creation of a new “material supporter” designation are necessary to create a cyber embargo of jihadist websites and those companies that provide them services. Diplomatic efforts are necessary to fully realize the potential of the cyber embargo, as cyber jihadists can continually move and find new “material supporters” in other jurisdictions. Through continued diplomatic efforts, terrorist websites can be forced to exist in a geographically limited number of jurisdictions.

Furthermore, even if only some jihadist sites are closed down, the jihadists will still be restricted to a few overseas hosts. These few hosts would no longer be needles in a haystack; with fewer places to go, the major jihadist sites with direct links to terrorism could be quickly identified and monitored by investigators.¹⁹⁴ The end result of this process will not eliminate the cyber jihadist presence, but geographically limiting terrorists allows

¹⁹³ See *Myth, Reality, and Jihadist Use of the Internet*, INTERNET HAGANAH, Mar. 01, 2007, <http://internet-haganah.com/harchives/005928.html>. (Weisburd claims an “80% mortality rate” regarding those sites which his website archived. Those sites were shut down by asking the service provider to discontinue the site; he refers to this as “active web site interdiction efforts.”); See also Ariana Eunjung Cha, *Watchdogs Seek Out the Web's Bad Side*, WASH. POST, Apr. 25, 2005, at A1 (“Weisburd said he and his supporters are responsible for dismantling at least 650 and as many as 1,000 sites he regards as threatening, especially Islamic radical sites.”).

¹⁹⁴ See *id.*

for government and civilian orchestrated monitoring, as well as for offensive actions to shut down these sites. Some websites may, for intelligence reasons, be identified as sites that the government will not want to shut down. Instead, the government may choose to monitor or compromise these sites as they may contain valuable intelligence information, such as user names, locations, and messages that users believe to be encrypted but are in fact being monitored. This technique is not universally accepted though, as some contend “getting real actionable intelligence from a terrorist website or forum is extremely difficult and requires a lot of time and a lot of luck[,] and in many cases the small amounts of available actionable intelligence would only be noticed after the act is done.”¹⁹⁵ Thus, geographically limiting these sites will corral the cyber jihadists onto a limited number of web servers, effectuating monitoring and other counterterrorism techniques.

While some may argue that the anonymity of the internet makes locating and shutting down jihadist websites too challenging, one must bear in mind that jihadists use websites for the specific purpose of dispersing information and connecting with each other. To a large extent, jihadists are forced to relinquish anonymity in order to reach their own audience.¹⁹⁶ In addition, anonymity is a two-way street. Trackers and investigators can infiltrate the jihadist ranks by acting as interested jihadists, avoiding detection through anonymity.¹⁹⁷

The key to countering cyber jihad is to relentlessly target jihadist websites by keeping them continually on the move, cutting off their resources by targeting “material supporters,” and finally limiting their potential areas of operation so that increased monitoring and other counterterrorism techniques can be applied to them. Following these steps will go a long way toward addressing the technical and political issues inherent in the internet jihad, that have plagued lawmakers and policy experts.

¹⁹⁵ Gordon, *supra* note 15.

¹⁹⁶ See A. Aaron Weisburd, *Global Jihad, the Internet and Opportunities or Counterterrorism Operation*, INTERNET HAGANAH, Aug. 23, 2005. <http://internet-haganah.com/harchives/004824.html>.

¹⁹⁷ See *id.*