
"U.S. Strategy for Countering Jihadist Websites"

Testimony by Gregory S. McNeal
Associate Professor of Law
Pepperdine University School of Law

Before the

United States House of Representatives
Committee on Foreign Affairs
Subcommittee on Terrorism, Nonproliferation and Trade
September 29, 2010

PEPPERDINE UNIVERSITY
School of Law

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, and in some instances imprudent, my testimony details a series of proposals that can have an impact on the presence of terrorists on the Internet. Using existing statutes and watchdog groups, it is possible to regionalize terrorist Web sites, 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 a cyber embargo on jihadist Web sites and their supporters. These efforts, coupled with diplomatic cooperation, can further the attempt to curb the impact of jihadist Web sites, while simultaneously increasing the ability of governments to monitor these Web sites and, when necessary, shut them down.

As others have noted in testimony and policy articles, terrorist Web sites may move their operations and continually pop up at new hosts, especially given the dynamic nature of the Web. However, like other battlefields in the struggle against terrorist organizations, 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.[1] Efforts to counter the terrorist presence on the Web can force such organizations to overseas Internet service providers (ISPs), thus limiting their host options and increasing the likelihood that authorities will be able to track them and monitor them.

Step one in the process of shutting down a terrorist Web site is to use shaming techniques and the threat of criminal sanctions to stop US companies from providing services to designated terrorist organizations.[2] As an example, Web sites such as Internet Haganah posted the details of US companies that were providing services to Palestinian Islamic Jihad (PIJ) as part of a shaming campaign. The Web site encouraged readers to contact those US companies and demand that they stop supporting terrorists. The US companies have more at stake than just their reputations. 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 Web site shifted its operation to overseas Internet service providers (ISPs) that are beyond the reach of US laws and less susceptible to shaming techniques. As a result, while temporarily troubled by their exposure, the PIJ Web site is still operating today.

Thus, the second step to further isolate and eventually shut down terrorist Web sites is the most critical one. Current laws and techniques are limited, and terrorist organizations are quick to adapt and avoid the reach of shaming techniques and US laws. Nevertheless, once terrorist organizations make their home outside the United States, they must still rely on the support of ISPs in their new jurisdictions. While the terrorist organization itself may not be deterred by US efforts, their ISPs are vulnerable to commercial pressure and the desire to maintain their business, the majority of which likely comes from non-terrorist clientele. These ISPs 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 ISPs that are providing material support to terrorist Web sites in the form of Web services.

---

[1] Boaz Ganor, The Counterterrorism Puzzle 102 (2005).

[2] The U.S. State Department and Department of Treasury both maintain lists of designated terrorist organizations. Those lists are available at http://www.state.gov/s/ct/list/index.htm and http://www.treas.gov/offices/enforcement/ofac/sdn/ respectively.

This is true because, after being forced off of US network service providers, a terrorist Web site will need to receive an IP address and connection to the Internet from overseas providers. I propose a modification to existing statutes to create a new cyber supporter designation that will sweep these ISPs within the sanction of US laws. Under this approach, US companies and persons will be forbidden from doing business with a designated cyber 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 losing all commercial services from the United States and continuing to provide services to the terrorist organization. The result is obvious; if the terrorist's ISP was a major international telecommunications company and it was designated as a cyber supporter, then all US commercial services would be cut off, including Internet and financial services. In the face of such potential loss of income, that company would likely cease providing services to the designated terrorist group. Nevertheless, it is still possible that the overseas company may not be deterred by a cyber-supporter designation. As such, a further step is necessary to isolate these terrorist organizations and their overseas Web hosts. The third step involves diplomatic efforts to standardize the creation of "designated cyber 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 Web sites. Expanding the cyber embargo is key because, as an overseas terrorist Web site continues to shift its operations to countries that it believes are safe havens, the cyber embargo will continue to isolate them geographically. This type of cooperative diplomatic approach is one which has been particularly successful in Europe through the "Check the Web" initiative an open-source monitoring and database creation project handled by the European Law Enforcement Organization (Europol), for the purposes of monitoring the Internet for terrorist use, especially recruitment, training, and propaganda.

TREASURY REGULATIONS AND IEEPA AS A POTENTIAL TOOL

The Treasury Department has an underused tool allowing for broad sanctioning authority that also can be used against terrorist Web sites. This authority was created by the International Emergency Economic Powers Act (IEEPA).[3] 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 the 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.[4] On September 23, 2001, President Bush invoked this power, declaring a national emergency with respect to the threat posed by al-Qaida, and issued Executive Order 13,224, "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism."[5]

[3] 50 U.S.C. §§ 1701-1707 (2000).
[4] *Id.* §§ 1701-1702 at 232, 253, & 262.
[5] Exec. Order No. 13,224, 3 C.F.R. § 786 (2001), *reprinted in* 50 U.S.C. § 1701 (Supp. III 2000).

The order included an initial list of 27 targets, including Osama bin Laden and al-Qaida.[6] In addition, it provided that the Secretaries of State and Treasury could add specified categories of persons (individuals and entities) to the list.[7] The categories of individuals and entities eligible for designation 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.[8]

Placement on the list requires US persons, which for purposes of this testimony would include ISPs and domain name registrars, to block property and interests in property, including "services of any nature whatsoever,"[9] belonging to the designated sanctions targets.[10] In addition, US persons are prohibited under EO 13,224 (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 EO.[11]

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-Qaida, Hezbollah, Hamas, PIJ, and any other entities or individuals designated pursuant to the EO.

Furthermore, treasury regulations found in 31 C.F.R. § 594[12] area source of potential sanctions for ISP's supporting jihadist Web sites. According to OFAC guidance, those who wish to provide services to targets of Treasury sanctions may not do so without *ex ante* case-by-case

---

6 *Id.* at 790.
7 *See id.* at §1.
8 *See id.* §§ 1(c), (d)(i).
9 31 C.F.R. § 594.309 (2006).
10 31 C.F.R. § 594.301.
11 31 C.F. R. § 594.406.
12 US Dep't of the Treasury, Office of Foreign Assets Control: Mission, *http://www.treas.gov/offices/enforcement/ofac/*.

authorization by Treasury.[13] The potential civil penalty for violations of IEEPA regulations is $250,000.[14]

Acting pursuant to these authorities, the Treasury may issue cease-and-desist orders (C&Ds) to US-based ISPs providing services in violation of existing sanctions programs. OFAC investigators often serve C&Ds on US persons involved with a designated target.[15] The C&Ds would be issued pursuant to IEEPA, EO 13,224 (or possibly EO 13,438),[16] and 31 C.F.R. § 594. If systematically employed as part of a long-term program targeting terrorist Web sites, 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 ISPs' client lists, such as those clients receiving domain names or Web-hosting. These administrative subpoenas—known as 602s after the relevant section of the regulations—are another traditional OFAC function.[17] 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, placing terrorist Web sites squarely within the sights of 602s.[18]

While terrorists using the Internet are unlikely to provide accurate information and will likely employ stolen credits cards to make online purchases for their Internet services, existing Treasury regulations using 602s and C&Ds require little additional effort and may produce valuable leads. The example of Irhabi007 supports this; investigators there found stolen credit card information and confirmed that the cards were used to pay US Internet providers on whose servers Irhabi007 had posted jihadi propaganda.[19] According to the *Washington Post*, that lead demonstrated to authorities that "they had netted the infamous hacker."[20]

SHAMING AND WATCHDOG GROUPS

Despite the fact that designated foreign terrorist organizations (FTOs) are publicly listed on the Department of State and Department of Treasury Web sites, Internet companies are oftentimes either undeterred by the threat of prosecution or are unaware of their client's terrorist status. As such, these companies frequently continue to do business with designated FTOs.

While the government has a legitimate interest in keeping terrorists from recruiting, it does not want to be seen as attempting to censor the internet. Thus, 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, a Virginia based company, for example, often avoids acknowledging the fact that it has retained, through its user policy agreement, the ability to regulate and take down a site that it deems "unlawful," "threatening," or which "constitutes an illegal threat, hate propaganda, profane, indecent or otherwise

---

[13] *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).

[14] 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*.

[15] *See* Statement by Assistant Sec'y Juan Zarate Before the UN Sec. Council 1267 Sanctions Comm., JS-2189 (Jan. 10, 2005), available at *http://treas.gov/press/releases/js2189.htm*.

[16] *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*.

[17] 31 C.F.R. § 501.602.

[18] John R. Levine, *et al*., The Internet for Dummies 60 (7th ed. 2000).

[19] Rita Katz & Michael Kern, "Terrorist 007, Exposed," *Wash. Post*, Mar. 26, 2006, at B1.

[20] *Id.*

objectionable material of any kind or nature."[21] Of course, Network Solutions is not the only Web service provider that hosts extremist Web sites. For example, another site based in Dallas, *thePlanet.com*, was accused of hosting three different terrorist Web sites and a Hamas monthly news magazine, each run by designated FTOs.[22]

Because it is difficult for companies and the government to monitor to whom Internet services are being provided, independent watchdog sites stand in the best position to fill the gap. A number of watchdog 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.[23] After finding a terrorist Web site, 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."[24] These interested parties include both government and private entities.[25] Internet Haganah encourages individuals to take action by learning about both the terrorist Web site and the group, understanding the terms of service of the host company, and finally making a calm, informed, complaint to the company.[26] Often these complaints go unanswered, at which point Internet Haganah recommends that an individual go to the local media for publicity.[27] No company wants to see its name smeared across the morning news as a supporter of terrorism, especially in their key market.[28]

Tactics such as these have successfully encouraged sites to take down other questionable material, such as Web sites that cater to pedophiles. For example, in April 2007, Network Solutions shut down a Web site after receiving complaints from customers.[29] The site had been publicly broadcast in The Bellingham Herald newspaper, prompting the complaints.[30] Company spokeswoman Susan Wade responded by saying that, although there is no way that Network Solutions could possibly "police the content of everything that's going up because hosting providers can sell thousands of sites a day," it appreciates when third parties get involved or "when we get served legal papers that say, 'Hey, take a look at this.'"[31]

OTHER LEGAL ACTION AND ASSOCIATED CHALLENGES

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 US 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

---

[21] Network Solutions Acceptable Use Policy, *http://www.networksolutions.com/legal/aup.jsp*.
[22] "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*.
[23] Nadya Labi, "Jihad 2.0," *The Atlantic Monthly*, Jul./Aug. 2006, available at *http://www.theatlantic.com/doc/prem/200607/online-jihad*.
[24] *Id.*
[25] *Id.*
[26] *See* "Confronting the Global Jihad Online: What Can You Do," *Internet Haganah*, Nov. 18, 2004, *http://internet-haganah.com/harchives/003133.html*.
[27] *Id*.
[28] *See id*.
[29] *See* "Network Solutions Shuts Down Pedophile Website," *HostSearch*, Apr. 7, 2007, *www.hostsearch.com/news/network_solutions_news_5782.asp*.
[30] *Id.*
[31] *Id.*

recruitment and propaganda dissemination.[32] 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."[33] The House of Representatives took notice of the presence of terrorism on the Internet and called on all corporate owners of Web sites that share user-posted videos to take down terrorist and jihadist propaganda.[34] Yet, even without this express resolution, the government already has a powerful legal tool available in the form of § 2339, the material support statute.

Prosecutors can use § 2339 to stop US Internet service providers (ISPs) 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 and its subsections holds that, if a person is found to have materially supported a designated FTO, that person "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."[35] While to date no case has been brought against an ISP, a plain reading of the statute suggests that those who continue to provide services to terrorist Web sites after being notified of the sites support of terrorism have arguably satisfied the definition of providing "material support."[36] This is especially the case in light of the Supreme Court's recent opinion in *Holder v. Humanitarian Law Project*, which held that, providing a service to a terrorist organization is distinguishable from independent advocacy which is protected by the First Amendment.

While most prosecutions under § 2339 have centered on individuals who have physically provided material support, either through the provision of objects such as weaponry or funding, the statute has recently been used to prosecute individuals who use computers and the Internet as a means of providing material support.[37] In 2004, The District Court in Connecticut indicted Babar Ahmad on terrorism charges, including a violation of § 2339A, providing material support.[38] The charges allege that Ahmad created Web sites 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.[39] Some of the Web sites opened and maintained by Ahmad were serviced through a US company, OLM, which was headquartered in Connecticut at the time.[40]

---

[32] 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*.

[33] 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*.

[34] H.R. Res. 224. 110th Cong. (2007).

[35] 18 U.S.C. § 2339B(a)(1) (Supp.).

[36] *See id.*

[37] *See*, *e.g.*, Criminal Complaint at 3-4, United States v. Lindh, No. 02-51-M (E.D. Va. 2002) (claiming that John Walker Lindh admitted to traveling to Pakistan to receive paramilitary training and traveling to Afghanistan to join the Taliban); Indictment at 86-94, United States 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, United States 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, United States 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 US Naval enlistee encouraging "the enlistee to 'keep up the psychological warefare.[sic]'").

[38] Indictment at ¶ 18, United States v. Babar Ahmed (D. Conn. 2004)

[39] *Id.* at ¶ 12.

[40] *Id.* at ¶ 21A.

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 ISPs. 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 constitutional challenges to successfully using the material support statute. Some may argue that targeting ISPs amounts to censorship by proxy.[41] It is true that the "material support" statutes, or other similar criminal prohibitions that might be adopted, may "threaten to recruit a federally conscripted corps of censors...[and that] 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.[42] However, protecting individuals from innocent mistakes is why I argued that the first step in any enforcement strategy should be, as some watchdog groups advocate, to contact the ISP then to conduct a public shaming and media campaign. Only when those methods fail should the government consider prosecuting those companies who support terrorist Web sites. It is only then that the government can argue that the company was aware or "on notice" 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. As the Supreme Court held this summer in *Holder v. Humanitarian Law Project*, providing a service especially when one is on notice that they are coordinating that provision of a service to a terrorist organization is a crime that is unprotected by the First Amendment.

BARRIERS TO USE OF TREASURY REGULATIONS

It is important to note that, Treasury regulations have faced First Amendment scrutiny and survived. For example, an examination of case law involving the constitutionality of OFAC actions involving First Amendment claims by US 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 decision, "there is no First Amendment right nor any other constitutional right to support terrorists."[43] Despite this fact, Treasury has not aggressively attempted to cut off cyber-services to terrorism supporters, not even to key al-Qaida facilitators.

Granted, there are some examples of attempted action, such as the December 2006 designation of Kuwaiti Hamid al-Ali, a cleric who supported al-Qaeda in Iraq and funded terrorist cells in Kuwait.[44] At the time of Hamid al-Ali's designation, 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"[45] Rather than isolating these terrorists, however, Hamid al-Ali continued to operate his Web site outside of Washington state.[46] His operations included the religious sanctioning of suicide bombings and the

---

[41] *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).

[42] *Id.* at 93-94.

[43] 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.]").

[44] Press Release HP-191, US Dep't of the Treasury, Treasury Designations Target Terrorist Facilitators (Dec. 7, 2006), available at *http://www.treas.gov/press/releases/hp191.htm*.

[45] *Id.*

[46] Chris Heffelfinger, "Kuwaiti Cleric Hamid al-Ali: The Bridge Between Ideology and Action," 5 *Terrorism Monitor* 4 (Jamestown Found., Apr. 2007), available at *http://www.jamestown.org/terrorism/news/article.php?articleid=2373349*.

incitement of individuals to "join the armed resistance of the jihadi movement[.]"[47] While Hamid al-Ali has reportedly renounced jihad, as recently as Monday, September 27, 2010 I was able to find this passage on his website, automatically translated from the original Arabic by Google:

> Simmer to the Islamic nation, to produce a comprehensive jihad to defeat the final this attack on our nation Alziosaliip, and purify the land of Islam from Rjsha, and expelled the Zionist entity from our country, and abort all plans, and restore the Islamic caliphate. Thank God that our nation great list to confront this challenge, the intention is stronger than the determination of black, and steadily like the stability of ancestors, and here made martyrs in every moment, across the front line that extends from the occupied Kashmir to Palestine beloved, through Afghanistan, the proud, and Iraq tall, to draw blood through the Glory , the path of sacrifice and send a brilliant victory, God willing.[48]

Ali's website receives registration services from Whois Manager out of Portland, OR; registrar services from Active Registrar, Inc., and servers from EuroVPS a UK based internet company. Ali is still preaching jihad, and he's doing so with the support of U.S. and allied companies.

In light of this, it's possible that the barriers Treasury action may be found, not in the First Amendment but in decades-old pieces of legislation. In 1988, Representative Howard Berman (D-Cal.) proposed the Berman Amendment, which limited the President's powers under IEEPA by creating an exemption for "informational materials."[49] Also, in 1994 Congress passed the Free Trade in Ideas Amendment, which expanded the Berman Amendment to non-tangible forms of information.[50] The Conference Report on the bill stated that the language of the Berman Amendment was explicitly intended to have broad scope.[51]

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 Web sites provide more than information, that is, by allowing fundraising, training, recruiting, and operational details, these Web sites provide "instrumental uses" that are distinguishable from "communicative uses."[52]

Moreover, in *United States v. O'Brien,*[53] the Supreme Court declared that government actions that advance "sufficiently important governmental interests" may allow incidental limitations on the First Amendment for speech and non-speech. 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

---

47 *Id.*
48 Webpage of Hamid al-Ali, http://h-alali.net/
49 *See* The Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, 102 Stat. 1107 (1988) (codified at 50 U.S.C. § 5(b)(4)) [hereinafter Berman Amendment].
50 Foreign Relations Authorization Act of 1994, Pub. L. No. 103-236, § 525; *see also* Berman Amendment.
51 *Id.* (citing H.R. Rep. No. 103-482, at 483 (1994) (Conf. Rep.).
52 *See generally* Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," 116 2004 *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).
53 United States v. O'Brien, 391 U.S. 367 (1968).

> Amendment freedoms is no greater than is essential to the furtherance of that interest.[54]

Federal courts applying this test to OFAC activity have allowed the Treasury to restrict the import of books from sanctioned nations.[55] Courts have also upheld presidential action on the ground 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."[56]

Finally, Supreme Court precedent buttresses the view that not all speech in these contexts is protected. For example, speech that is likely to incite violence[57] or that creates a clear-and-present danger of a substantive evil[58] 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 Web sites 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 government concern.

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 Web sites from US-based ISPs, the jihadist Web presence will still remain. As discussed already, a terrorist organization may maintain its Web presence by using 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. Thus, merely forcing jihadist Web sites overseas is not a sufficient counterterrorism strategy given the ubiquity of the Internet and the fact that sites hosted outside the United States appear as seamlessly as those hosted within the United States. Therefore, new legal tools are necessary to further counter the threat of jihadist websites.

An aggressive application of current statutes may suffice to counter these websites by targeting material supporters. Treasury's designation process, if liberally and aggressively applied, may also provide an adequate remedy. As detailed earlier, subparagraph three of Executive Order 13224 allows Treasury to block both property and interests in property that "act for or on behalf of" those parties already designated as terrorist organizations. Furthermore, subparagraph 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.'"[59] A broad interpretation of these rules would result in the blocking of both property and interests in property for jihadist website supporters.

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

---

[54] *Id.* at 377.
[55] *See* Teague v. Reg'l Comm'r of Customs, Region II, 404 F.2d 441, 445 (2d Cir. 1968).
[56] 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, 1234-1235 (D.C. Cir. 1991)).
[57] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).
[58] Schenck v. United States, 249 U.S. 47 (1919).
[59] Exec. Order No. 13,224.

communications companies that provide material support to terrorist organizations may be designated as "cyber supporters." Such a designation would prevent US companies from conducting business with designated entities. This process would create a virtual *persona non grata*. The interconnected nature of the World Wide Web requires 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 "cyber 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 US Code to create a category of "designated cyber supporter." US 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 provides notice and a safe harbor provision that allows companies to sever ties to terrorist organizations to avoid being designated a "cyber supporter."

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 percent of all domain registrars.[60] Preventing these registrars from engaging in commercial activity with "material supporters" would have a dramatic impact on the designated entity, likely forcing it out of business if it did not sever its ties to jihadists. Diplomatic efforts have worked in the past, albeit on a small scale. For example, the US Department of Defense reportedly used its leverage to shut down Palestinian resistance sites hosted by the Ukraine in 2004.[61] 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."[62] 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 Web sites will be forced to find support in new jurisdictions. Continued monitoring and diplomatic efforts would thus remain critical. Additionally, because 95.8 percent 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. Furthermore, internationalizing an agreement that will ensure that other countries shut down "designated cyber supporters" is the next step in countering jihadist websites.

Continuing diplomatic efforts to prohibit dealing with designated cyber supporters will create a system whereby terrorist organizations will have extremely limited choice of locations where they can register and operate their Web sites. 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,

---

[60] Within those nine countries, there are 522 Accredited Domain Name Registrars, 281 of which are located in the United States (54 percent); 124 of which are located in Canada (28 percent); 16 of which are located in Germany (3.07 percent); 12 of which are located in the United Kingdom (2.3 percent); 11 of which are located in the Republic of Korea (2.11 percent); 10 of which are located in Australia (1.9 percent); 8 of which are located in France (1.53 percent); 8 of which are located in Japan (1.53 percent); and 6 of which are located in Spain (1.14 percent).

[61] 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).

[62] Rachel Ehrenfeld, "Shutting Down Cyberterror," Oct. 21, 2004, *http://www.frontpagemagazine.com/Articles/Printable.asp?ID=15605*.

diplomatic measures, such as trade restrictions can be brought to bear. Those countries that host jihadist Web sites will then have to decide if they are willing to protect the Internet jihadists at the cost of jeopardizing trade relations.

CONCLUSION AND IMPLICATIONS

Given the ubiquity of the Internet and the challenges of tracking constantly moving Web sites, domain name registrars, and ISPs, 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.

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 Web sites 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 "cyber supporter" designation are necessary to create a cyber embargo of jihadist Web sites 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 "cyber supporters" in other jurisdictions. Through continued diplomatic efforts, terrorist Web sites 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---instead with fewer places to go, the major jihadist sites with direct links to terrorism could be quickly identified and monitored by investigators---effectively corralled into places where they could be more closely monitored.[63] The end result of this process will not eliminate the cyber jihadist presence, but geographically limiting terrorists allows for government and civilian orchestrated monitoring, as well as for offensive actions to shut down these sites.

Some Web sites might, 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. While some advocate for this technique, it is important to note that it is not universally accepted, 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."[64] 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 Web sites too challenging, one must bear in mind that jihadists use Web sites for the specific purpose of dispersing information and connecting with each other. To a large extent, jihadists are

---

63 *See id.*

64 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*.

forced to relinquish anonymity in order to reach their own audience.[65] 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.[66]

The key to countering jihadist websites is to relentlessly target them, keeping them continually on the move, cutting off their resources by targeting "cyber 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.

[65] *See* A. Aaron Weisburd. "Global Jihad, the Internet and Opportunities or Counter-terrorism Operation," *Internet Haganah*, Aug. 23, 2005. *http://internet-haganah.com/harchives/004824.html*.
[66] *See id.*