ENDING THE CYBER JIHAD: COMBATING TERRORIST EXPLOITATION OF THE INTERNET WITH THE RULE OF LAW AND IMPROVED TOOLS FOR CYBER GOVERNANCE

Benjamin R. Davis[†]

I. INTRODUCTION

More than guns, bombs, or missiles, the Internet[1] is the most important tactical tool for terrorist groups today.[2] Just as millions of people use the Internet each day to catch up on the news, check the local weather, or order

[†] J.D. Candidate, December, 2006, The Catholic University of America, Columbus School of Law. The author works in the Office of Terrorism & Financial Intelligence, U.S. Department of The Treasury. He wishes to thank Evan Kohlmann, Marina Malenic, and Michael Froomkin for their comments and Caroline Swigert for the great laughs. The views expressed are those of the author only.

[1] The Internet is "an electronic communications network that connects computer networks and organizational computer facilities around the world." Merriam Webster's collegiate Dictionary 654 (11th ed. 2003). The word Internet describes the network itself—"an electronic communications network that connects computer networks and organizational computer facilities around the world. Id. The World Wide Web is "a part of the Internet accessed through a graphical user interface and containing documents often connected by hyperlinks." Merriam Webster's collegiate Dictionary 1444 (11th ed. 2003).

[2] Terrorism is "[t]he use or threat of violence to intimidate or cause panic, especially as a means of affecting political conduct." BLACK'S LAW DICTIONARY 1512-13 (8th ed. 2004). An alternative definition of terrorism is:

> [k]idnapping, murder, and other assaults against the life or physical integrity of those persons to whom the state has the duty according to international law to give special protection, as well as extortion in connection with those crimes. The use or threat of violence to intimidate or cause panic especially as a means of affecting political conduct.

Organization of American States Convention on Terrorism, Feb. 2, 1971, 27 U.S.T. 3949.

a book online, the technological leaders of Al Qaeda in Iraq[3] and its affiliated umbrella group, the Mujahideen Shura Council in Iraq, exploit the Internet to announce to the world their latest attacks against American and Iraqi civilians.[4] Averaging between ten and twenty online statements every day,[5] Al Qaeda in Iraq uses the Internet to broadcast the planning and implementation of suicide car bombings,[6] announce strategic alliances with

---

[3] Al Qaeda in Iraq is a loose network of autonomous terrorist cells and networks whose figurehead is now Abu Ayyub al-Masri after the assassination of Abu Musab al-Zarqawi in June 2006, http://www.timesonline.co.uk/article/0,,11069-2227490,00.html. Ellen Knickmeyer & Jonathan Finer, *Insurgent Leader Al-Zarqawi Killed in Iraq*, WASH. POST. (June 8, 2006); *U.S. Publish Picture of New al-Qaeda Leader*, TIMES ONLINE, June 15, 2006, http://www.timesonline.co.uk/article/0,,11069-2227490,00.html. Since Zarqawi swore allegiance to Osama bin Laden and Al Qaeda in late 2004, references to an Al Qaeda in Iraq group or network have become widespread by operatives and, in turn, by terrorism observers. Zarqawi was previously a senior leader of the Ansar al-Islam/Ansar al-Sunnah network. *See* KENNETH KATZMANN, CONG. RESEARCH SERVICE, AL QAEDA: PROFILE AND THREAT ASSESSMENT (2005). Al Qaeda, Al Qaeda in Iraq, and Ansar al-Islam/Ansar al-Sunnah are among the terrorist groups listed on the U.N. Security Council's 1267 Committee terrorist sanctions list. S.C. Res. 1267, U.N. Doc. S/RES/1267 (Oct. 15, 1999); *see also* THE NEW CONSOLIDATED LIST OF INDIVIDUALS AND ENTITIES BELONGING TO OR ASSOCIATED WITH THE TALIBAN AND AL-QAIDA ORGANISATION AS ESTABLISHED AND MAINTAINED BY THE 1267 COMMITTEE, http://www.un.org/Docs/sc/committees/1267/1267ListEng.htm.

> [T]he U.N. Security Council Committee [which] . . . oversees the implementation by States of the sanctions imposed by the Security Council on individuals and entities belonging or related to the Taliban, Usama Bin Laden and the Al-Qaida organization and maintains a list of individuals and entities for this purpose. In resolutions 1267 (1999), 1333 (2000), 1390 (2002) and 1455 (2003), the Security Council obliged all States to freeze the assets, prevent the entry into or the transit through their territories, and prevent the direct or indirect supply, sale and transfer of arms and military equipment with regard to the individuals/entities included on the list.

Id.

[4] SITE Institute, *The Mujahideen Shura Council Claims Responsibility for Several Suicide Bombings, IED Detonations, and Sniping of American, Iraq, and Kurdish Forces in al-Mosul, Baghdad, Heet, Beiji and al-Ramadi*, Aug. 2, 2006, http://siteinstitute.org (search "shura counsil"); SITE Institute, *The Mujahideen Shura Council in Iraq Issues a Video of the Mutilated Corpses of the Two Captured American Soldiers in al-Yusefiya*, July 10, 2006, http://siteinstitute.org (search "shura counsil video mutilated"). *See also* Mujahideen Shura Council in Iraq Web site, http://www.albayanat.blogspot.com (last visited Oct. 30, 2006); see also Scott Shane, *Zarqawi Built Global Jihadist Network on Internet*, N.Y. TIMES, June 9, 2006. See generally JEAN CHARLES BRISARD, ZARQAWI: THE NEW FACE OF AL-QAEDA (2005) (providing a ground-breaking look into the life and terrorist activities of Abu Musab al-Zarqawi).

[5] Susan B. Glasser & Steve Coll, *The Web as Weapon: Zarqawi Intertwines Acts on Ground in Iraq with Propaganda Campaign on the Internet*, WASH. POST, Aug. 9, 2005, at A1 [hereinafter *Web as Weapon*]; *see also* E-mail from Evan Kohlmann, International Terrorism Consultant, to Benjamin R. Davis (Mar. 22, 2006) (on file with author) (explaining that in 2006, Zarqawi and his associates have increased the number of online statements from approximately ten per day to twenty).

[6] *See* GLOBAL TERROR ALERT, AL-QAIDA'S DISTINGUISHED BATTLES OF MESOPOTAMIA (ABU MUSAB AL-ZARQAWI): THE BATTLE OF BADR AL-BAGHDAD (2005) [hereinafter BATTLES OF MESOPOTAMIA], http://www.globalterroralert.com (translating a December 2005

other terrorist groups, [7] and shock the world with the beheadings of kidnapped foreigners, such as American contractor Nicholas Berg.[8]

Unfortunately, Al Qaeda in Iraq is just one of many global and local terrorist networks exploiting the Internet to conduct terrorist operations. For example, the localized "home–grown" terrorist cell responsible for the July 7, 2005, suicide bomb attacks on the London tube and bus system that killed fifty-two people, was "carried out by four men who had scoured terror sites on the Internet" to obtain information on planning and carrying out terrorist attacks.[9] The September 11, 2001 planners and hijackers also exploited the Internet to achieve their goals. Senior Al Qaeda coordinators involved in the September 11th suicide hijacking plot, such as notorious Al Qaeda training camp manager, Abu Zubaydah, exchanged thousands of encrypted messages, posting their operational plans on a password-protected section of a Web site.[10] According to U.S. officials who examined the contents of Zubaydah's computer following his capture, the flow of e-mail messages regarding the attack began in May 2001 and continued through September 9, 2001.[11] However, "[t]he frequency of the messages was highest in August 2001, the month immediately preceding the attacks."[12] According to other reports, Mohammed Atta, the ringleader of the September 11th hijackers, transmitted a cryptic e-mail message to his co-conspirators over the Internet confirming that the final plan was in place just prior to the attacks.[13] The extensive use of the Internet by the September 11th hijackers and planners of attacks elsewhere illustrates how the Internet serves as a logistical tool for terrorist operatives.

Beneath the news headlines and TV images of bombings and beheadings posted on sites and chat groups across the Internet, something even more sinister and dangerous to the security of the United States and its allies is

---

video posted on an Islamic extremist Web site depicting the surveillance and planning phase of a suicide bombing attack in Iraq, complete with footage of the attack and airing of the attackers' "martyrdom" statements).

[7] *Web as Weapon*, *supra* note 5; *see also* David Bamford, *Zarqawi Shows Bin Laden Loyalty*, BBC, Oct. 18, 2004, http://news.bbc.co.uk/2/hi/middle_east/3752616.stm (announcing the alliance between Abu Musab al-Zarqawi and Osama bin Laden).

[8] *War on Terror Digest*, BBC MONITORING INT'L REP. May 11–13, 2004 (describing the online posting of the video-taped beheading of American contractor Nicholas Berg on the Al-Ansar bulletin board at www.al-ansar.biz).

[9] Mark Townsend, *Leak Reveals Official Story of London Bombings*, LONDON OBSERVER, Apr. 9, 2006, http://observer.guardian.co.uk/print/0,,329453825-102285,00.html.

[10] *See* ANTI-DEFAMATION LEAGUE, JIHAD ONLINE: ISLAMIC TERRORISTS AND THE INTERNET 9 (2002), *available at* http://www.adl.org/learn/internet/jihad_online.pdf [hereinafter ANTI-DEFAMATION LEAGUE].

[11] *Id.*

[12] *Id.*

[13] Tom Zeller Jr., *On The Open Internet, a Web of Dark Alleys*, N.Y. Times, Dec. 20, 2004; GABRIEL WEIMANN, UNITED STATES INSTITUTE OF PEACE, WWW.TERROR.NET: HOW MODERN TERRORISM USES THE INTERNET, 116 SPECIAL REPORT 10 (2004), *available at* http://www.usip.org/pubs/specialreports/sr116.pdf.

taking place. Terrorist webmasters and militant extremists from dozens of countries are exploiting the anonymous, inexpensive, and easily accessible global reach of the Internet. Violent extremists are using the Internet to recruit potential terrorist operatives, solicit funding for operations, train current terrorists with the latest in bomb-making know-how, and plan operations against civilian targets worldwide.[14] The success Al Qaeda and affiliated movements have had in exploiting the Internet as an operational center illustrates that "al Qaeda has become the first guerilla movement in history to migrate from physical space to cyberspace. With laptops and DVDs . . . jihadists have sought to replicate the training, communication, planning, and preaching facilities they lost in Afghanistan with countless new locations on the Internet."[15] As one Islamic extremist described in a message he posted on the Al Qaeda-affiliated Global Islamic Media Front Web site, "[t]he technology of the Internet facilitated everything. Today's Web sites are the way for everybody in the whole world to listen to the *mujaheddin* [sic]."[16]

Today's *mujahideen* have launched a cyber *jihad*,[17] signaling a new and terrifying era in the war against Islamic-extremist terrorism. In this first global conflict of the twenty-first century, religious extremists are equipped with more than guns, bombs, and a populist message against the *infidel*;[18] terrorists are also armed with a technical and strategic mastery of

---

[14] GABRIEL WEIMANN, TERROR ON THE INTERNET 123–29 (2006) [hereinafter TERROR ON INTERNET] (providing a number of examples of online manuals that explain how to construct explosive devices).

[15] Steve Coll & Susan B. Glasser, *Terrorists Turn to the Web as Base of Operations*, WASH. POST, Aug. 7, 2005, at A1 [hereinafter *Terrorists Turn*].

[16] *Web as Weapon*, *supra* note 5, at A1. *Mujahideen* is a group or individual (*mujahid)* that wages *jihad* or religious war. *See* MERRIAM WEBSTER'S COLLEGIATE DICTIONARY 814 (11th ed. 2003). *Mujahideen* are also known as Islamic guerilla fighters who wage battle in conflict zones where they believe Muslim peoples are facing persecution or repression. *See id. See generally* STEVE COLL, GHOST WARS: THE SECRET HISTORY OF THE CIA, AFGHANISTAN, AND BIN LADEN, FROM THE SOVIET INVASION TO SEPTEMBER 10, 2001 (2004) (providing a substantive description of the Arab–Afghan *mujahideen* in Afghanistan during the 1980s and the global spread of *mujahideen* to predominately Muslim conflict zones worldwide during the 1990s).

[17] Cyber jihad is a term coined to loosely describe Islamic extremist terrorists' use of the Internet as a communications, fundraising, recruitment, training, and planning tool in their battle against the enemy. Other authors who have referred to a cyber jihad in a similar context include, *U.S. Govt. Vulnerable to Cyber-Jihad, Security Summit Hears*, WASH. INTERNET DAILY (Mar. 21, 2006); Marc Lynch, *Al-Qaeda's Media Strategies,* 83 NAT'L INT. 50 (2006). While not a complete list, some of the most commonly named enemies of Islamic terrorist groups include the Unites States, Western European countries, secular Arab governments, and Israel; *see World Islamic Front Statement Urging Jihad Against Jews And Crusaders,* Feb. 23, 1998, http://www.fas.org/irp/world/para/docs/980223-fatwa.htm (naming the United States, Israel, Zionists, and Christian Crusaders as enemies of Islam).

[18] An infidel is "an unbeliever with respect to a particular religion." MERRIAM WEBSTER'S COLLEGIATE DICTIONARY 40 (11th ed. 2003). The term is used derisively by many Islamic extremists to condemn non-Muslims and Muslims who do not share extremists'

the Internet. This knowledge enables terrorists to indoctrinate, recruit, and train new members for attacks with little or no threat of discovery or capture.[19]

Al Qaeda and other terrorist groups are effectively using the Internet and an estimated 4,500 terrorist-related Web sites[20] to advertise a global brand of terror to millions of sympathetic Web users. According to Gabriel Weimann, a professor at the University of Haifa in Israel who tracks more than 4,000 terrorist-related Web sites, "[t]he Internet is the network that connects them all. . . . You can see the virtual community come alive."[21] The value of the Internet to terrorist groups is now so significant that it makes no difference whether terrorist leaders "are on a mountain in the Hindu Kush or living with their beards shaved off in a suburb of Karachi . . . . They can inspire and guide a worldwide movement without physically meeting their followers–without knowing who they are."[22]

Despite growing evidence of the pervasive threat of online terrorist operations, many U.S. policymakers continue to focus their Internet security concerns on the threats posed by offensive cyber attacks on the country's information technology infrastructure.[23] As Internet security expert Bruce

---

militant beliefs. In an October 2001 video-taped speech, Osama bin Laden denounced all Americans as infidels. *See U.S. 'Infidels' are not safe: bin Laden,* CBC NEWS, Oct. 8, 2001.

[19] The rise of the cyber jihad was by no means unforeseen. As early as 1996, experts on warfare and the Internet described terrorists' emerging use of the Internet as 'netwar' or 'cyberwar.' *See* JOHN ARQUILLA & DAVID RONFELDT, THE ADVENT OF NETWAR, 3–16, 19–24, 81–82 (1996) (defining 'netwar' as a conflict of societal-level ideas waged on the Internet via process of disrupting, damaging, or modifying what a population knows or thinks it knows about itself and the world around it). The authors also defined the 'cyberwar' as the "conducting of, and preparation for, military operations according to information-related principles." *Id.*

[20] *Terrorists Turn*, *supra* note 15, at A1; Jon Swartz, *Terrorists' Use of Internet Spreads*, USA TODAY, Feb. 21, 2005, at 3B (reporting that the number of terrorist-affiliated Web sites has increased from approximately a dozen in 1997 to an estimated 4,350 in 2005).

[21] Terrorists Turn, supra note 15.

[22] Paul Eedle, *Terrorism.com*, THE GUARDIAN, Jul. 17, 2002.

[23] *See* Jimmy Lee Shreeve, *The New Breed of Cyber-Terrorist*, THE INDEP., April 9, 2006. The article reports that Scott Borg, the director and chief economist of the U.S. Department of Homeland Security's Cyber Consequences Unit, argues that "attacks on computer networks are poised to escalate to full-scale disasters that could bring down companies and kill people." *Id.* It is important to note that this Comment does not examine what has traditionally been defined as offensive cyber-terrorism. Although the threat of a crippling cyber attack on the nation's information technology infrastructure by a terrorist group remains a national security priority for the United States and its allies, it is not the focus of this Comment. This matter has previously been dealt with at length by a number of legal scholars and policymakers. *See*, *e.g.*, Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber Attacks,* 2002 U. ILL. J.L. TECH. & POL'Y 1 (2002); Richard W. Walker, *Gilmore Warns of Threat to Information Systems,* GOV'T COMP. NEWS, Mar. 27, 2002 (quoting James Gilmore, Chairman of the National Advisory Panel to Assess Domestic Response Capabilities for Terrorism of Weapons of Mass Destruction as saying that cyber attacks "are the most likely next [terrorist] attacks").

Schneier argues, "[t]he [cyberterrorism] hype is coming from the U.S. Government and I don't know why. . . . If [terrorists] want to attack they will do it with bombs like they always have. . . . Breaking pager networks and stopping e-mail is not an act of terror."[24] Meanwhile, other national security experts believe "that the threat of cyberplanning may be graver than the threat of terrorist attacks on the world's [infrastructure] networks."[25] The concern is that that the virtual free rein terrorists currently have over the Internet is allowing them to plan large-scale attacks against civilian targets, while policymakers continue to worry primarily about a cyber attack on the nation's information infrastructure. While a cyber attack on America's information systems resulting in significant economic losses or the deaths of Americans may or may not occur,[26] there is substantial evidence of a cancerous expansion of the cyber jihad, which can be

---

According to Georgetown University law professor, Dorothy E. Denning:

> [c]yberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Cyberterrorism: *Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services*, 105th Cong. (2000) (testimony of Dorothy E. Denning, Professor, Georgetown University), *available at* http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html. Terrorist planning activities that have been publicized suggest that a number of terrorist groups have indicated an interest in carrying out a cyber attack on the information systems of American economic and critical infrastructure hubs. For instance, a Web site operated by the Muslim Hackers Club offers tutorials in spreading viruses, hacking stratagems, network 'phreaking;' and links to secret sites which purport to disclose sensitive information like 'code names' and radio frequencies used by the Secret Service. *See Computer Lessons for Terrorists*, NEWSWEEK, May 20, 2002, at 4 (Atlantic ed.) ("FBI and Defense Intelligence Agency ('DIA') officials issued a warning that the Club included computer experts who had conducted classes on how to mount terror attacks on computer networks.").

[24] Mark Ward, *Cyber Terrorism 'Overhyped,'* BBC NEWS, March 14, 2003, http://news.bbc.co.uk/1/hi/technology/2850541.stm.

[25] Zeller, *supra* note 13, *citing* Timothy L. Thomas, *Al Qaeda and the Threat of Cyber Planning,* PARAMETERS 11–20 (2003).

[26] *See* Kevin Coleman, *Cyber Terrorism*, DIRECTIONS MAG., Oct. 10, 2003 (analyzing the significant rise in the number of cyber security attacks on American business networks and the resulting economic losses). *B*ut see Robert Lemos, *What are the Real Risks of Cyberterrorism?*, ZDNET, Aug. 26, 2002 (providing an in-depth examination of threats posed to the United States' transportation and security systems, generally down-playing the threat, and concluding that the greatest threat posed by cyber terrorism is to the Internet itself).

directly linked to terrorist attacks that killed thousands of innocent civilians.[27]

Limiting the ability of terrorist networks to use the Internet as an operational platform is one of the most significant challenges that lawmakers and national security experts face.[28] The problem could not be more central to winning the war on terrorism. The growing devastation and technological sophistication of terrorist attacks since September 11th, 2001,[29] require that sovereign states and international organizations responsible for regulating the Internet, such as the Internet Corporation for Assigned Names and Numbers ("ICANN"),[30] eliminate, or at least diminish, opportunities for terrorists to communicate, plan operations, and raise funds online.[31]

---

[27] *See* Zeller, *supra* note 13.

[28] *Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11*, WEEKLY COMP. PRES. DOC. 1347–1351 (2001). President Bush stated in his speech to a Joint Session of Congress in the days immediately following September 11th that "[o]ur war on terror begins with Al Qaida, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped, and defeated." *Id.*

[29] *See* OFFICE OF THE COORDINATOR FOR COUNTERTERRORISM, U.S. DEP'T OF STATE, COUNTRY REPORTS ON TERRORISM 2004 1 (2005), *available at* http://www.state.gov/documents/organization/45313.pdf (providing an annual evaluation of terrorist attacks worldwide; the assessment includes the various types, locations, responsible groups, and number of deaths and casualties resulting from terrorist acts).

[30] ICANN is the principal organization responsible for the governance of the Internet. ICANN "[i]s an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions." Internet Corporation for Assigned Names and Numbers, ICANN Information, http://icann.org/general/ (last visited Oct. 30, 2006). ICANN shares administrative, research and development, and policy-making roles with a number of other organizations. These entities include: (1) The Internet Engineering Task Force ("IETF"), http://www.ietf.org/overview.html (last visited Oct. 30, 2006) ("[IETF is]a large open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet"); (2) the Domain Name Systems Security Extensions ("DNSSEC"), http://www.dnssec.net/ (last visited Oct. 30, 2006) ("[An organization] designed to protect the Internet from certain attacks, such as DNS cache poisoning. It is a set of extensions to DNS, which provide: (a) origin authentication of DNS data, (b) data integrity, and (c) authenticated denial of existence."); and (3) the International Telecommunications Union (ITU), http://www.itu.int/aboutitu/overview/history.html (last visited Oct. 30, 2006). The ITU is a United Nations specialized agency partially responsible for developing and coordinating Internet-related global policies. *Id*.

[31] The National Commission on Terrorist Attacks Upon the United States emphasized the importance of limiting the ability of terrorists and their associates to communicate, travel and transfer funds across borders. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, MONOGRAPH ON TERRORIST FINANCING 2–12 (2004) [hereinafter 9/11 COMMISSION REPORT]; 9/11 COMMISSION REPORT, STAFF REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, 9/11 AND TERRORIST TRAVEL 2 (2004) [hereinafter 9/11 STAFF REPORT ON TERRORIST TRAVEL].

Despite recognizing that the Internet has become a primary weapon in the arsenal of the enemy, the U.S. government and its international allies have done a poor job of restricting terrorists' continued use of this powerful tool.[32] Some policymakers and intelligence officials argue, however, that terrorists' online activities provide a valuable trove of intelligence regarding the ideological foundations and tactical operations of terrorist movements.[33] For example, Michael Vatis, former director of the National Infrastructure Protection Center ("NIPC"), argues that the U.S. and its allies exploit terrorist Web sites as a source of information useful in preventing attacks and shutting off key nodes of communication and fundraising.[34] In the summer of 2006, British intelligence and law enforcement illustrated the potential value of this surveillance strategy by using the Internet to monitor the activities of a network of terrorist operatives planning to blow up a number of U.S.–bound commercial airliners with liquid explosives.[35] Through the monitoring of the operatives' Internet communications, authorities discovered strategic details of the plan to blow the planes up in mid-air and learned that the plot was reaching an operational phase when the plotters began reviewing U.S.–bound airline schedules and ticket prices.[36]

However, while monitoring the activities of known and suspected terrorist operatives will allow authorities to win a few online battles and disrupt some terrorist plots, there are significant signs that governments and international organizations are losing the long–term war against the cyber jihad. Proponents of this intelligence-gathering counterterrorism strategy fail to acknowledge that the passive surveillance approach to combating the cyber jihad in recent years has allowed terrorists to expand their presence online

---

[32] *See* WEIMANN, *supra* note 13, at 14. Gabriel Weimann argues that the Internet is difficult to regulate due, in part, to the borderless and decentralized nature of its design, which make it an "ideal arena for activity by terrorist organizations." These systemic characteristics include easy access, little or no regulation, censorship, or other forms of government control, potentially huge audiences spread throughout the world, anonymity of communication, fast flow of information, inexpensive development and maintenance of a web presence, a multimedia environment, and the ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source for stories. *Id.*

[33] Bill Gertz, *CIA Mines 'Rich' Content from Blogs*, WASH. TIMES, April 19, 2006.

[34] ONLINE NEWSHOUR: ONLINE TERRORISM, (PBS Internet broadcast, Aug. 2, 2005), http://www.pbs.org/newshour/bb/terrorism/july-dec05/online_8-02.html [hereinafter Vatis interview]. The NIPC is a U.S. government interagency office responsible for detecting, warning, and responding to cyber attacks.

[35] Philip Webster, *A Plan 'To Commit Unimaginable Mass Murder*,' TIMES ONLINE, Aug. 11, 2006, http://www.timesonline.co.uk/article/0,,2-2308087,00.html; *Bank of England Names 19 Terror Suspects*, USA TODAY, Aug. 11, 2006.

[36] Webster, *supra* note 35; *Bank of England Names 19 Terror Suspects*, *supra* note 35.

and develop increasingly sophisticated web infrastructures for indoctrination, fundraising, recruitment, and the planning of terrorist operations.[37]

While the Internet's laissez faire legal environment has encouraged dramatic technological innovation and commercial growth in the last decade,[38] the lack of effective U.S. or international cyber regulation or governance mechanisms[39] permits terrorist activity to operate in a relatively lawless

---

[37] For one example of the challenges and limited utility of e–mail and telecommunications surveillance. *S*ee Barton Gellman et al., *Surveillance Net Yields Few Suspects,* WASH. POST, Feb. 5, 2006 (describing how the Bush administration's previously secret warrantless surveillance of approximately 5,000 American-based individuals' telephone and e-mail communications has resulted in fewer than 10 individuals each year arousing enough suspicion to have their domestic communications surveilled); *s*ee also Terrorists Turn, *supra* note 15; Evan Kohlmann, *The Real Online Terrorist Threat*, 85 FOREIGN AFFAIRS 5 (2006); Swartz, *supra* note 20. Some experts argue that there is no distinction between online cyber jihad activities and terrorists in the field. *Se*e Howard Altman, *Web Warriors Track Down, Close Jihadist Internet Sites,* TAMPA TRIB., Nov. 17, 2005. The article quotes Evan Kohlmann as stating: "A lot of people [differentiate] between Internet terrorism and regular terrorism. There is no difference. Anything they do, they do on the Internet, including recruitment, training, financing, and propaganda." *Id.*; *s*ee also Yuki Noguchi & Sara Kehaulani Goo, *Terrorists' Web Chatter Shows Concern About Internet Privacy*, WASH. POST, Apr. 13, 2006, at A14, (describing a noticeable increase in discussions in Islamic extremist chat rooms regarding the need to observe enhanced online security procedures by using a proxy software program that removes digital tracks and to avoid using the Google video toolbar, which records keyword searches and the user's IP address).

[38] Pub. F. Inst., *Embracing Entrepreneurship and Am. Econ. Growth* (Nat'l Comm'n on Entrepreneurship White Paper) http://www.publicforuminstitute.org/nde/sources/reports/whitepap.pdf (describing the nexus of innovation and entrepreneurship on the Internet which drives economic growth).

[39] An entire body of legal scholarship has emerged in the last decade which identifies and describes the characteristics of the Internet that make it a uniquely challenging institution to govern and regulate. In a particularly influential early analysis regarding the legal dimensions of Internet regulation, David Johnson and David Post argue that attempts to regulate the flow of electronic information across geographical boundaries are futile:

> The notion that the effects of an activity taking place on that Web site radiate from a physical location over a geographic map in concentric circles of decreasing intensity, however sensible that may be in the non virtual world, is incoherent when applied to Cyberspace. A Web site physically located in Brazil . . . has no more of an effect on individuals in Brazil than does a Web site physically located in Belgium or Belize that is accessible in Brazil. Usernet discussion groups, to take another example, consist of continuously changing collections of messages that are routed from one network to another, with no centralized location at all. They exist, in effect, everywhere, nowhere in particular, and only on the Net.

See David Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996) [hereinafter Johnson & Post]. Johnson and Post emphasize that cyberspace can and should be conceived "as a distinct 'place' for purpose of legal analysis by recognizing a legally significant border between Cyberspace and the 'real world.'" *Id.* at 1378. Johnson and Post conclude, however, that once rules governing behavior on the Internet can be expected to eventually emerge naturally, as online users and service providers bring order to anarchy and find meaningful ways to accomplish their ends and govern themselves. *Id.* at 1387–91; *see also* David Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155, 166–67 (1996).

zone. Currently, most states and international organizations have established very limited legal regimes to identify, investigate, and track terrorist-related Web sites.[40] As former Central Intelligence Agency ("CIA") Director George Tenet urges, now is the time for the international community to implement a "wholesale taming of cyberspace."[41] Tenet told a conference at the end of 2004, "I know that these actions would be controversial in this age where we still think the Internet is a free and open society with no control or accountability. But, ultimately, the Wild West must give way to governance and control."[42]

In an effort to address the cyber jihad threat and tame the "Wild West" of the Internet, this Comment provides a comprehensive examination of domestic and international initiatives which address this situation. This Comment demonstrates that existing domestic and international regulatory regimes are insufficient to meet the growing threat that terrorists' use of the Internet poses to U.S. and European security interests. In response to these ineffective initiatives, this Comment proposes several new regulatory measures to combat terrorists' exploitation of the Internet for planning and operational purposes. Specifically, this Comment argues for a prevention and enforcement-oriented international governance regime developed and implemented by the ICANN and its stakeholders.[43]

This Comment includes eight parts. Part II of this Comment provides background analysis regarding the technologies and techniques that terrorists use in pursuing their cyber jihad. Part III examines the rise of the cyber jihad from the mid-1990s to the present, and the ways in which terrorists use the Internet to further their lethal agenda. Part IV evaluates the U.S. government's domestic responses to the cyber jihad threat since September 11th through law enforcement and judicial actions. This section asserts that the U.S. is failing to combat the cyber terror threat by implementing legislation that incorrectly focuses on deterrence and voluntary compliance by Internet providers. Part V analyzes the international community's responses to this challenge, noting that although some progress has been made recently in combating online terror, efforts to date have been insuffi-

---

[40] For a compilation of the substantive computer crime laws in 44 different countries see The Legal Framework–Unauthorized Access to Computer Systems, Moss District Court, Norway, *available at* http://www.mosstingrett.no/info/legal.html (last visited Nov. 20, 2006) [hereinafter Legal Framework–Unauthorized Access to Computer Systems].

[41] Zeller, *supra* note 13.

[42] *Id.*

[43] ICANN stakeholders are constituent members of ICANN committees and governing bodies that maintain an active voice in Internet regulatory issues. Stakeholders include sovereign governments, private companies, individual Internet users, non-governmental organizations, and Internet policy experts. ICANN, Advisory Committees, Committees of the Board of Directors, Task Forces, and Other Committees, http://icann.org/committees/ (last visited Oct. 30, 2006).

cient to seriously address the problem. Part VI presents five core principles of governance that ICANN should apply in attempting to address the cyber jihad problem. Part VII recommends several regulatory and enforcement tools for ICANN to implement in order to eliminate, or greatly restrict, the cyber jihadist threat. Part VIII concludes that ICANN and its major supportive stakeholders should implement an explicit timetable for Internet security reform, as terrorists' ongoing exploitation of the Internet poses an increasingly ominous national security threat to the United States and its allies.

II. A TERRORIST'S PLAYGROUND: BACKGROUND & CONTEXT OF THE PROBLEM

One of the great ironies of the Internet era is that the very characteristics of the Internet that appeal to government, industry, and private users are some of the same dynamics that make it an ideal operational headquarters for contemporary global terrorist movements.[44] Cyber jihadists' masterful manipulation of the Internet[45] illustrates that Al Qaeda and affiliated organizations "have understood that both time and space have in many ways been conquered by the Internet."[46]

A. Gateways to the Cyber Jihad

Like any Internet user, a terrorist operative will find setting up a Web site or e-mail account to be a very simple and inexpensive process. With minimal disclosure requirements (which are difficult, if not impossible, for providers to verify for accuracy), a cyber jihadist can set up any number of free e-mail accounts within a matter of minutes.[47]

A cyber jihadist who wishes to set up a Web site must typically visit the site of an Internet Service Provider[48] ("ISP"), which, as the name suggests, "provide[s] Internet access services to customers in exchange for a fee."[49] When registering with an ISP, the cyber jihadist faces little scrutiny regard-

---

[44] *See* WEIMANN, *supra* note 13, at 3; Brenner & Goodman, *supra* note 23, at 5; ANTI-DEFAMATION LEAGUE, *supra* note 10, at 3.

[45] *Web as Weapon*, *supra* note 5, at A1.

[46] *Id.*

[47] *See* Lawrence V. Molnar, *Who Owns 'Invisible.com,' and 'WhoIs' Disappearing? A Practitioner Looks for Answers*, 48 RES GESTAE 26, 26-27 (2005) (comparing the ease with which a person can set up a Web site or e-mail with acquiring a library card).

[48] Worldwide, it is estimated that there are now more than 10,000 Internet Service Providers in operation, including dozens in states known to harbor or be sympathetic to terrorist elements. *S*ee CIA WORLD FACTBOOK (2005), http://www.cia.gov/cia/publications/factbook/index.html.

[49] Brad Boline & Daniel A. Tysver, ISP Liability, BITLAW, http://www.bitlaw.com/internet/isp.html (last visited Oct. 30, 2006).

ing the information provided. While technically illegal, it is exceedingly easy for ISP registrants to provide false or misleading information on their ISP registration form,[50] which is then posted on the WhoIs registrar site.[51] An examination of an ISP registrant profile on file with WhoIs illustrates this point. Among the site registrants listed by a single U.S. ISP were presumably fictitious account holders such as "Bill Clinton," "God," and "Mickey Mouse."[52] ISPs in most countries operate under very limited guidelines for regulation and oversight, and face limited fiduciary duties to verify account information or monitor content posted on a site.[53]

ICANN has minimal accreditation disclosure requirements for users who wish to establish a domain name.[54] These regulations are to be implemented and enforced by the ISP on the individual user level.[55] However, ISPs have little incentive to enforce those requirements. In fact, because of poor enforcement efforts by individual governments and ICANN, "most registrars do not conduct any background checks, nor assume any responsibility or liability due to a customer's registration containing false or improper contact information."[56] As a result of these lax policies, "individuals or entities with misguided, improper or outright illegal motives can own a domain name and enjoy worldwide attention while hiding behind improper or false identities."[57]

Each Web site or e-mail account holder exhibits a unique identifier address called an Internet Protocol ("IP") address[58] which address attaches to all electronic communication sent over the Internet from a particular computer.[59] One purpose of the IP address and ISP registration information is to identify Web users and providers, and to assist investigative authorities

---

[50] Molnar, *supra* note 47.

[51] *See* WhoIs.com, http://whois.com/nonssl/cus_faq.htm (last visited Oct 30, 2006). The 'WhoIs' Web site provides provides a search function for users to find domain name registration information by domain names and IP addresses. *Id.*

[52] *See Accuracy and Integrity of the WhoIs Database: Hearing Before the Subcom. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 107th Cong. 15 (2002).

[53] Molnar, *supra* note 47, at 26–28.

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] Each computer on the Internet has a unique address called its Internet Protocol (IP) address that permits each individual computer user to send and receive messages and visit Web sites. *See* ICANN Information, http://icann.org/general/ (last visited Oct. 30, 2006).

[59] *Id.* The legitimacy of the IP system is challenged by new services which effectively hide a user's IP address. For example, some Internet Service Providers are now offering Internet users and owners of Web sites the opportunity to establish "dynamic IPs" that do not have fixed Internet Protocol addresses. *See, e.g.,* No-IP Free–Free Dynamic DNS, http://www.noip.com/services/managed_dns/free_dynamic_dns.html (last visited Oct. 30, 2006) (offering Internet user free no IP URLs.).

in tracing the origins or user identity of a particular message or Web site.[60] In reality, however, the lack of substantial and reliable ISP and IP identifier information typically leaves investigators with few leads or tips with which to begin an investigation.[61] Further complicating investigator's efforts are cyber jihadists' practice of frequently alternating the location of their Internet usage.[62] This cat-and-mouse activity often greatly limits the value of tracking down the location of a particular IP address.[63]

Even when authorities are successful in closing down an extremist Web site or capturing a cyber jihadist responsible for disseminating operational material, their associates are easily able to reconstitute the site or e-mail addresses at another ISP or e-mail provider by once again providing false registrant information.[64]

B. A Global Game of Cat and Mouse

Despite an ever-growing number of Islamic extremist Web sites used to incite or plan violent attacks, the efforts of the United States and other governments around the world have proven to be ineffective at disrupting terrorist-affiliated sites and preventing cyber jihadists' initial access to the Internet.[65] Cyber jihadists build strength online in numbers, redundancy,

---

[60] Hans Klein, *ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy*, 18 THE INFO. SOC'Y 193, 195 (2002).

[61] *See Internet Domain Name Fraud—The U.S. Government's Role in Ensuring Public Access to Accurate WhoIs Information: Hearing before the H. Subcomm. on Courts, the Internet and Intellectual Property of the Committee on the Judiciary*, 108th Cong. 2 (2003) [hereinafter *Internet Domain Name Fraud Hearing*] (examining the complications which false and deceptive ISP registration information pose to investigators).

[62] *See* Marketing of Terrorism Through the Internet, Intelligence and Terrorism Information Center at the Center for Special Studies (2004), www.intelligence.org.il/eng/sib/12_04/int_m.htm (last visited Oct. 30, 2006) [hereinafter ITIC Marketing of Terrorism Study] (providing a troubling study of how terrorists exploit anonymity and lack of regulation on the Internet and describing how the terrorist group Hamas was able to re-launch its main Web site from a Malaysia-based provider within days after its U.S.-hosted site was shut down). According to the organization's Web site, The Intelligence & Terrorism Information Center ("ITIC") "is part of the Center for Special Studies (CSS), an NGO [non-governmental organization] dedicated to the memory of the fallen of the Israeli Intelligence Community and it is located near Gelilot, north of Tel Aviv. It is headed by (Col. Ret.) Dr. Reuven Erlich." It focuses its investigative efforts on the activities of Hamas and Hizballah, terrorist financing, as well as "anti Israeli incitement and hate propaganda." *See* ITIC, http://www.terrorism-info.org.il/engsite/content/T1.asp?Sid=18&pid=121 (last visited Oct. 18, 2006).

[63] Molnar, *supra* note 47, at 26–30.

[64] *See Internet Domain Name Fraud Hearing, supra* note 61.

[65] WEIMANN, *supra* note 13, at 15 (describing the dramatic growth of terrorist groups that exploit the Internet for tactical gain) Weimann's research concluded that there are currently more than 4,300 terrorist related Web sites. *Id*.

and decentralization of their communications, thereby limiting the impact of enforcement actions against a Web site or email account.[66] The global Web site infrastructure of the designated Palestinian terrorist group Hamas[67] illustrates this point. A 2004 study by the Israel-based Intelligence and Terrorism Information Center ("ITIC") found that Hamas utilizes twenty active Web sites in seven languages that are hosted by ISPs in Rus-

---

[66] *Id.*

[67] In October 1997, the United States Department of State designated Hamas (a.k.a. the Islamic Resistance Movement) as a Foreign Terrorist Group, pursuant to the Immigration and Nationality Act, as amended by the Antiterrorism and Effective Death Penalty Act of 1996. Fact Sheet: Secretary of State designates Foreign Terrorist Organizations, http://www.fas.org/irp/news/2001/10/fr100501.html (last visited Aug. 22, 2006). The Immigration and Nationality Act defines terrorist activity to mean:

> [a]ny activity which is unlawful under the laws of the place where it is committed (or which, if committed in the United States, would be unlawful under the laws of the United States or any State) and which involves any of the following: (I) The high jacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle). (II) The seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained. (III) A violent attack upon an internationally protected person (as defined in section 1116(b)(4) of title 18, United States Code) or upon the liberty of such a person. (IV) An assassination. (V) The use of any-(a) biological agent, chemical agent, or nuclear weapon or device, or (b) explosive or firearm (other than for mere personal monetary gain), with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property. (VI) A threat, attempt, or conspiracy to do any of the foregoing. (iii) The term "engage in terrorist activity" means to commit, in an individual capacity or as a member of an organization, an act of terrorist activity or an act which the actor knows, or reasonably should know, affords material support to any individual, organization, or government in conducting a terrorist activity at any time, including any of the following acts: (I) The preparation or planning of a terrorist activity; (II) The gathering of information on potential targets for terrorist activity; (III) The providing of any type of material support, including a safe house, transportation, communications, funds, false documentation or identification, weapons, explosives, or training, to any individual the actor knows or has reason to believe has committed or plans to commit a terrorist activity; (IV) The soliciting of funds or other things of value for terrorist activity or for any terrorist organization; (V) The solicitation of any individual for membership in a terrorist organization, terrorist government, or to engage in a terrorist activity.

Id.

The United States Department of Treasury describes Hamas as a terrorist organization

> [t]hat has intentionally killed hundreds of innocent civilians and continues to kill and maim with the aim of terrorizing a civilian population. Hamas was formed in 1987 as an outgrowth of the Palestinian branch of the Muslim Brotherhood. Hamas activists have conducted many attacks—including large-scale suicide bombings—against Israeli citizens and military targets. In the early 1990s, they also targeted U.S. citizens, suspected Palestinian collaborators and Fatah rivals.

See Press Release, U.S. Department of Treasury, U.S. Designates Five Charities Funding Hamas and Six Senior Hamas Leaders as Terrorist Entities (Aug. 22, 2003) [hereinafter U.S. Charities Funding Hamas], *available at* http://www.ustreas.gov/press/releases/js672.htm.

sia, Ukraine, Malaysia, Indonesia, the United Arab Emirates, the United Kingdom, and the United States.[68] The most strategically significant Hamas sites were hosted by ISPs in East Asia, where Hamas may perceive that government monitoring of Internet content and activities is least aggressive.[69] The official Web site of Hamas' terrorist-operational wing, the Izz al-Din al-Qassam Brigades,[70] responsible for dozens of suicide attacks on Israeli targets,[71] is hosted by an ISP in Malaysia.[72] The main Internet headquarters of Hamas, has three Web addresses with separate IP addresses and ISPs located in countries less vulnerable to American pressure.[73]

The ITIC concluded that the global decentralization of the Hamas Web infrastructure "is an indication, in our assessment, of a deliberate policy of the Hamas movement to avoid storing their first and second priority Web sites on American Internet service providers."[74] The ITIC emphasized that Hamas' strategy illustrates the group's "cautiousness and the movement's desire to preserve the flexibility and survivability of its Internet infrastructure over a prolonged period of time."[75]

Many terrorist groups maintain Web sites on multiple Internet servers to ensure that a site taken down on one server can be re-launched from another server within hours, most likely in a different country. A Chechen militant group site, Kavkaz Center, includes a section on its front page

---

[68] ITIC Marketing of Terrorism Study, *supra* note 62.

[69] *Id.*

[70] Izz Al-Din Al-Qassam Brigades, Islamic Resistance Movement, http://www.alqassam.info (last visited Oct. 30, 2006).

[71] The Izz al-Din al-Qassam Brigades "employ a variety of tactics, including kidnapping, assassinating Israeli soldiers, attacking Israeli civilians and ambushing Israeli vehicles. The group's military activities during the second Intifada have been characterized by the use of suicide bombings against targets such as buses, restaurants, coffee shops, hotels and other civilian locations in Israel." Jane's Terrorism and Security Monitor Intelligence Review, Izz al-Din al-Qassam Brigades, http://www.janes.com/security/international_security (follow news) (last visited Aug. 22, 2006).

[72] ITIC Marketing of Terrorism Study, *supra* note 62.

[73] See Hamas Web sites: The Palestinian Information Center, http://www.palestine-info.info (last visited Aug. 26, 2006) (registered in Dubai, United Arab Emirates); The Palestinian Information Center, http://www.palestine-info.net (last visited Aug. 26, 2006) (registered in Malaysia); and The Palestinian Information Center, http://www.palestine-info.com (last visited Aug. 26, 2006) (registered in Beirut, Lebanon).

[74] ITIC Marketing of Terrorism Study, *supra* note 62. It is important to note, however, that other terrorist networks appear to be less cautious about the locations they select for the posting of their Internet sites. For instance, the cyber jihad watch-dog group, Internet Haganah, estimates in a January 2005 study on the Internet infrastructure of the U.S. designated Hezbollah terrorist group, that the terrorist network maintains at least 25 websites worldwide. Of these sites, twenty–two are hosted by ISPs in Iran, while 22 are hosted by companies in the United States. Internet Haganah, *Who Keeps Hizballah Online*?, http://haganah.org.il/harchives/003473.html.

[75] *Id.*

noting the location of the site's six operating servers, providing visitors with the option of visiting any of the six mirror sites if the main site is incapacitated by Russian government security services.[76]

Other cyber jihadists utilize their computer skills to hack into the servers of companies and other organizations, and use those servers, unbeknownst to the provider, as de facto ISPs or proxy servers.[77] This tactic allows cyber jihadists to post their sites and deliver their communications while obscuring their own IP address.[78] For example, a publication by Mustapha Setmarian Nasar, a major Al Qaeda propagandist, was first released via a hacked American Web site, http:///www.carriagehouseglass.com, where it was secretly hidden in a file directory.[79] In addition, "[t]his same hacked Web site also published over 700 megabytes of video lessons given by Nasar and numerous other documents written by him."[80] Another cyber jihadist, known by the pseudonym Irhaby 007,[81] "hacked his way into an unprotected file directory on an Arkansas state government Web site, and used it to host beheading videos and other propaganda" for Al Qaeda in Iraq.[82]

Other cyber jihad Web sites rely on the knowledge that ISPs worldwide are not required to monitor content or to control access to sites on their servers until they are made aware of egregious contents on a particular site.[83] For example, the posting of the Nicholas Berg beheading video on the Internet became world news almost instantly, Acme Commerce, the Malaysia-based Web host for the Al-Ansar Al-Islam terrorist group's site, acknowledged that it was

---

[76] *See Chechen Separatist Basayev's Web site Back Online in Finland After Lithuania Shutdown*, MOSNEWS.COM, Oct. 11, 2004, http://mosnews.com/news/2004/10/11/websitereopen.shtml. The addresses of these mirrored sites include: kavkaz.tv; kavkaz.uk.com; kavkaz.org.uk; kavkazcenter.com; kavkazcenter.net; kavkazcenter.info (last visited Oct. 30, 2006). If one of these Kavkaz Center Web sites were taken down, viewers could also visit a web archive site such as http://www.webarchive.org in order to obtain the addresses of the mirrored sites.

[77] *See* Evan Kohlmann, *Al Qaeda and the Internet: Online Discussion*, WASH. POST, Aug. 8, 2005, [hereinafter *Kohlmann Online Discussion*]; Joseph Farah, *Islamist Terror Still Promoted on Web*, WORLD NET DAILY, Nov. 29, 2001, http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=25485 (last visited Aug. 24, 2006) (describing how the Al Qaeda affiliated Azzam.com Web site established mirrored sites in different countries to enable the site to quickly relaunch when a country shuts down one version of the site.).

[78] *Kohlmann Online Discussion*, *supra* note 77.

[79] *Id.*; Michael Levenson, *Crafts Website Hacked by Terrorists*, BOSTON GLOBE, May 7, 2006.

[80] *Kohlmann Online Discussion*, *supra* note 77.

[81] The actual identity of Irhaby 007 is believed to be Younis Tsouli, who was detained in the United Kingdom in the fall of 2005. Rita Katz & Michael Kern, *Terrorist 007, Exposed*, WASH POST, Mar. 26, 2006, at B1.

[82] Kohlmann Online Discussion, *supra* note 77.

[83] Molnar, *supra* note 47, at 26–30.

not aware of the existence of the site containing until "huge numbers of people trying to view the video overloaded its systems" and crashed its server.[84]

Many ISPs in the U.S. are notorious for providing hosting services to terrorist groups. In November 2005, the Tampa Tribune reported that a U.S.-based ISP, HostDime.com, was hosting two Web sites, shikaki.net and rabdullah.net, controlled by the designated terrorist group Palestinian Islamic Jihad.[85] When the HostDime.com manager was notified by the newspaper and agreed to take down the terrorist sites, he expressed the sentiment of many ISPs which host violent and terrorist-related content on their servers: "[w]e screen accounts as best we can. . . . If we sell hosting space to someone who is hosting something illegal, we don't know about it until somebody brings it to our attention."[86] In late August 2006, the Internet Haganah[87] Web site posted a detailed instruction manual first discovered on the prominent Islamic extremist site, http://www.alhesbah.org/v/,[88] entitled a "Plan of Action for the Jihad Fighter:

---

[84] Jonathan Kent, *Berg Video Website Shut Down*, BBC, May 13, 2004, http://news.bbc.co.uk/2/hi/asia-pacific/3710709.stm.

[85] *Altman*, *supra* note 37. *In* October 1997, the United States Department of State named Palestinian Islamic Jihad (PIJ) a Foreign Terrorist Group, pursuant to the Immigration and Nationality Act, as amended by the Antiterrorism and Effective Death Penalty Act of 1996, Fact Sheet: Secretary of State Designates Foreign Terrorist Organizations, *supra* note 67. PIJ was subsequently listed as a Specially Designated Global Terrorist entity by the U.S. Department of Treasury. Press Release, Treasury Designates Charity Funneling Money to Palestinian Islamic Jihad, U.S. Department of Treasury (May 4, 2005), *available at* http://www.ustreas.gov/press/releases/js2426.htm.

[86] Altman, *supra* note 37.

[87] For an extensive database of current and recently taken down jihadist Web sites, visit Internet Haganah, http://haganah.org.il/haganah/index.html (last visited Nov. 20, 2006). According to the organization's Web site, Internet Haganah "is a global open-source intelligence network dedicated to confronting Internet use by Islamist terrorist organizations, their supporters, enablers and apologists. Internet Haganah is also a grass-roots activist organization which encourages businesses to not provide services to Islamic extremists." Internet Haganah, http://haganah.org.il/harchives/003218.html (last visited Nov. 20, 2006). Described by some observers as "Internet vigilantes," Internet Haganah utilizes a number of provocative and somewhat controversial tactics to confront terrorists on the Internet. *See* Brad Stone, *Heros or Mettlesome Hacks*, Business Edge_Newsweek-MSNBC.com, July 13, 2005, http://www.msnbc.msn.com/id/8560624/site/newsweek/. Haganah's activities include hacking sites identified as terrorist-associated cyber environments and mocking extremist Internet postings regarding Internet Haganah's exposure efforts. Other terrorism consultants, such as the SITE Institute's Rita Katz, have critiqued Haganah's efforts to shut down extremist sites as counterproductive, as terrorists predictably change tactics in the face of interdiction. *See* Nadya Labi, *Jihad 2.0*, THE ATLANTIC, July 1, 2006.

[88] As of August 30, 2006, Al Hesbah registered 8,219,475 unique visits to its site, http://www.al-hesbah.org/v/. *See* Benjamin Wallace-Wells, *Annals of Terrorism: Private Jihad*, THE NEW YORKER, May 29, 2005, (describing how Al Hesbah has become an important extremist Web site for postings and chat rooms after the web master of another site, Ansar, was arrested for playing a role in a terrorist plot).

How to Kill a Westerner in the Arabian Peninsula."[89] The Al Hesbah site is hosted by Wild West Domains, Inc., a Scottsdale, Arizona-based ISP[90] and its network access provider is Dallas, Texas-based Colo4Dallas, Inc.[91]

Ultimately, the effect of inaction in the face of a growing cyber jihadist threat is startling. The inability of national security officials, Internet regulators, and providers to require and enforce accurate disclosure of Internet registration information has enabled an entire generation of cyber jihadists to exploit the Internet for murderous gains.

C. Techniques and Tactics of Cyber Jihadists

Cyber jihadists exploit the Internet through a variety of free and widely available technologies and easily applied techniques that are exceedingly difficult for authorities to restrict. Among the tactics terrorists employ are: encrypted and coded e-mail; steganographic messages; e-groups and chat rooms; e-mail dead-drops; openly accessible and password protected Web sites; hydra web links; and spam mimicking.

1. Encrypted Messages & Files

As law enforcement and security services' interception of terrorists' messages in some countries has grown,[92] operatives have increasingly utilized encryption technologies to communicate online via e-mail.[93] As the Washington Post reported, "Al Qaeda members have taught individuals . . . how to use the Internet to send messages and how to encrypt those communications to avoid detection."[94] For example, Wadih El-Hage, Osama bin Laden's former personal secretary and a senior planner of the 1998 Al Qaeda bombings of U.S. Embassies in Kenya and Tanzania, "sent en-

---

[89] Internet Haganah, *Islamist Al-hesbah Website Plan of Action for the Jihad Fighter: How to kill a Westerner in the Arabian* Peninsula, Aug. 26, 2006, http://www.haganah.org.il/harchives/005709.html (last visited Oct. 30, 2006).

[90] Wild West Domains, https://www.wildwestdomains.com/gdshop/about.asp?se=%2B&prog%5Fid=wildwestdomains&ci=3299&nocos=1 (last visited Oct. 30, 2006).

[91] Colo4Dallas, http://www.colo4dallas.com/default (last visited Oct. 30, 2006).

[92] Patrick Jonsson, *New Profile of Home Grown Terrorist Emerges*, CHRISTIAN SCI. MONITOR, June 26, 2006, at 1 (describing the FBI's uncovering of a Miami-based group of extremists involved in terrorist planning activities over the Internet).

[93] To "encrypt" is "[t]o scramble data to prevent unauthorized access." THE AMERICAN HERITAGE DICTIONARY 281 (3d ed. 1994). Encryption involves complex algorithms—a procedure or formula for solving a problem. Breaking into encrypted information requires sophisticated computer skills and mathematics.

[94] Douglas Farah & Peter Finn, *Terrorism, Inc.; Al Qaeda Franchises Brand of Violence to Groups Across World,* WASH POST, Nov. 21, 2003, at A33.

crypted e-mails under various names to associates in Al Qaeda."[95] In addition, "Khalik Deek, an alleged terrorist arrested in Pakistan in 1999, used encrypted computer files to plot bombings in Jordan at the turn of the millennium."[96] The convicted planner of the 1993 World Trade Center bombing, Ramzi Yousef, "used encrypted files to hide details of a plot to destroy eleven U.S. airliners over the Pacific Ocean."[97]

2. Codes & Steganography

Terrorist groups, including Al Qaeda, use online coding techniques or programs, known as steganography,[98] which allow illicit computer users, to hide a message inside another message, image, or file posted on the Internet.[99] For example, French intelligence officials assert that "suspects arrested in an alleged plot to blow up the U.S. Embassy in Paris were to get the go-ahead for the attack via a message hidden in a picture posted on the Internet."[100] Other extremists utilize "Internet bulletin boards carrying pornographic and sports information" to relay steganographic operational information to associates located elsewhere in the world.[101]

According to Internet security expert Chet Hosmer, other terrorist operatives transfer messages via "images that might be in an email message . . . [inside an] image that no one else would be able to detect or see."[102] September 11th ringleader, Mohamed Atta, may have used steganographic tactics to encode e-mail messages to his co-conspirators. Atta was "seen

---

[95] STEPHANIE R. BETANCOURT, SANS INSTITUTE, STENOGRAPHY: A NEW AGE OF TERRORISM 2 (2004) [hereinafter BETANCOURT/SANS INSTITUTE].

[96] *Id.*

[97] *Id.*

[98] NEWTON'S TELECOM DICTIONARY 859 (22d ed. 2006). Steganography is defined as "a method of hiding one piece of information within another." *Id.*

[99] BETANCOURT/SANS INSTITUTE, *supra* note 95. According to the SANS Institute, "there are currently over 140 steganography programs available" for public purchase. *Id.* at 3. The steganography tools ("S-Tools") "range from software that hides data in images to software that hides data in spam." *Id.* The SANS Institute notes that, "[s]teganography tools for Microsoft Windows include several programs that process GIF images, BMP images, and audio WAV files." *Id.* Steganography tools also include "a variety of encryption capabilities including IDEA, MDC, DES, and Triple DES." *Id.* According to Andy Brown, the creator of S-Tools, a company that produces a popular steganography software program that "works by spreading the bit-pattern of the message file to be hidden across the least-significant bits of the color levels in the image. S-Tools tries to reduce the number of image colors in a manner that preserves as much of the image detail as possible." *Id.*

[100] Brian Ross, *A Secret Language Hijackers May Have Used Secret Internet Messaging Technique*, ABC NEWS, Oct. 4, 2001.

[101] *See* Sue Pleming, *Muslim Extremists Utilize Web Encryption,* REUTERS, Feb. 6, 2001; *see generally* Bruce Schneier, *Bruce Schneier On Crypto, the FBI, Privacy and More,* THE REGISTER, Oct. 3, 2001, http://www.theregister.co.uk/2001/10/03/bruce_schneier_on_crypto/.

[102] Ross, *supra* note 100.

repeatedly by witnesses using his Hotmail account at public libraries in Florida to surf the Internet, downloading what appeared to be pictures of children and scenes of the Middle East."[103]

Even where a terrorist's e-mail is not encrypted, terrorist operatives are known to utilize previously identified code words to signal that a particular event or action is going to take place. In the weeks preceding the September 11th attacks, September 11th ringleader Mohammed Atta e-mailed his Al Qaeda associates: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering."[104]

3. E-Groups

An e-group is a service offered by an ISP for users with common interests to exchange messages.[105] The original ISP or registrar of the group determines whether the group is open to all users or is password-protected.[106] Terrorist operatives and their sympathizers have exploited Web and e-mail providers, such as Yahoo, to create a virtual cyber communications center for carrying out terrorist-related activities.[107] For instance, at the Yahoo chat groups "Jehaad" and "The Jihad Group," "one can view sickening media presentations posted by Al Qaeda zealots. Videos of Russian soldiers being tortured by Chechen mujahedeen, mujahedeen vehicle bombing operations, sermons by jihadist sheikhs, [and] homages to bin Laden . . . ."[108] Other operatives visit these Web sites to leave coded or steganographic messages for their associates to review.[109]

4. E-mail Dead Drops

E-mail dead drops are another simple but effective tactic used by terrorist conspirators. E-mail dead drops involve the distribution of a user name and password for an e-mail account to members of a terrorist cell who can then

---

[103] *Id.*

[104] WEIMANN, *supra* note 13, at 10 (explaining that the references to the various faculties was apparently the code for the buildings targeted in the attacks and the 19 confirmations clearly relates to the 19 hijackers who carried out the suicide hijacking attacks on September 11th).

[105] *See* Todd M. Hinnen, *The Cyber Front in the War on Terrorism: Curbing Terrorist Use of the Internet*, 5 COL. SCI. & TECH. L. REV. 5, 40 n.148 (2004).

[106] *Id*. Hotmail provides free email accounts. *See* Microsoft Online Services, http://join.msn.com/hotmail/overview-std (last visited Oct. 30, 2000).

[107] Rita Katz & Josh Devon, *WWW.JIHAD.COM*: *E-Groups Abused by Jihadists*, NAT'L REV. ONLINE, Jul. 14, 2003, http://www.nationalreview.com/comment/comment-katz-devon071403.asp.

[108] *Id.*

[109] *Id.*

enter the account and save an unsent message in the draft folder for the other account users.[110] Because the message is never sent from the account, there is no identifying information to assist law enforcement officials in tracing the IP address or location of the message creator.[111]

Khalid Sheik Mohammed, a key planner of the September 11th attacks arrested in Pakistan in March 2003,[112] "used the e-mail dead drop technique to avoid having his e-mails intercepted by eavesdroppers in the United States or allied governments."[113] Mohammed or his operatives

> would open an account on a free, public e-mail service such as Hotmail, write a message in draft form, save it as a draft, then transmit the e-mail account name and password during chatter on a relatively secure message board. . . . The intended recipient could then open the e-mail account and read the draft . . . ."[114]

Because no e-mail message was sent, there was a reduced risk of interception by authorities.

5. Secure Web Sites

Terrorist operatives have exploited the electronic mail services provided by extremist Web sites in order to communicate with members of their terrorist network. Todd M. Hinnen, a senior George W. Bush administration counter-terrorism official, describes a scenario in which a cyber jihadist could use a secure site to communicate with his associates: "Imagine a secure Web site[:] www.jihad.com. The Web site supports basic e-mail services. An e-mail can be sent from one of its e-mail accounts (e.g., johndoe@jihad.com) to another (e.g., janedoe@jihad.com) without ever leaving jihad.com's servers. It cannot, therefore, be intercepted or tracked."[115] Most important, however, are examples that Al Qaeda utilizes secure Web sites to plan and coordinate terrorist attacks, including the September 11th attacks.[116]

---

[110] Renwick McLean, *Madrid Suspects Tied to E-mail Ruse*, INT'L HERALD TRIB., Apr. 28, 2006 (describing how the perpetrators of Al Qaeda's 2004 Madrid train bombings communicated with other members of the operational cell by saving messages for one another in the draft sections of pre-selected email accounts).

[111] Hinnen, *supra* note 105, at 10–12.

[112] *Officials: Alleged Paymaster in Custody*, CNN, Mar. 4, 2003, http://www.cnn.com/2003/WORLD/asiapcf/south/03/03/pakistan.arrests/.

[113] *Terrorists Turn, supra* note 15.

[114] *Id.*

[115] Hinnen, *supra* note 105, at 15.

[116] *See* discussion *infra* Part I (describing Al Qaeda operations planner Abu Zubaydah's use of secure Web sites to exchange planning information with other September 11th co-conspirators).

6. Hydra Web Links

Terrorists wishing to communicate particularly sensitive or timely information have recently employed the hydra web link technique in which numerous links to the same video or message are posted on a particular site or e-mail chat room.[117] The viewers of the message are encouraged to copy and repost the communication in other forums and sites in order to prevent the message from being intercepted before it is broadly disseminated to its target online audience.[118] As an example, the extremist online facilitator, Irhaby 007, posted an Al Qaeda in Iraq video entitled "All is for Allah's Religion" on the Web site www.alaflam.net/wdkl[119] and posted links to "numerous outlets where visitors could find the video. In the event that one of the sites was disabled, many other sources were available as backups. Several were based on domains such as www.irhabi007.ca and www.irhabi007.tv."[120]

7. Spam Mimicking

One of the newest techniques exploited by terrorist operatives is to visit the Spam Mimic Web site, http://www.spammimic.com, and "embed encrypted messages in spam in order to disguise the fact that confidential data has been exchanged."[121] According to the SANS Institute, users wishing to transfer secret messages need only visit the site, "choose 'encode' from the menu, type in a short message, and press enter. This generates a realistic spam message with the secret message embedded inside it."[122] Upon receipt of the message, the end recipient of the spam message can then visit the "Spam Mimic Web site to 'decode' the spam, and retrieve the original message."[123]

III. THE RISE OF THE CYBER JIHAD

A. Onward to Terror by Way of the Internet

While terrorist networks have long exploited various media and communications technologies,[124] the first Web site designed for the purpose of

---

[117] Katz & Devon, *supra* note 107.
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] Betancourt/SANS INSTITUTE, *supra* note 95, at 5.
[122] *Id.*
[123] *Id*
[124] For more than thirty-five years, terrorists have exploited the mass media to maximize the impact of their operations on civilian populations. The first televised terrorist attack was the March 31, 1970 Japanese Red Army hijacking of a Japanese Airlines B727. Lasting

promoting an Islamic extremist agenda did not emerge until the mid-to-late 1990s. In 1996, Babar Ahmad, a young Palestinian studying in London, launched the Azzam.com Web site, named in honor of Al Qaeda co-founder Abdullah Azzam, Osama bin Laden's spiritual mentor and one of the leading Arab-Afghan jihadists in Afghanistan during the 1980s.[125] According to Evan Kohlmann, Azzam.com "was the very first real al Qaeda Web site. It taught an entire generation about jihad,"[126] and spread extremist sentiment by exploiting the global reach of the Internet with inciteful messages and professional-looking imagery from ongoing conflicts in Bosnia, Chechnya, and Afghanistan during the 1990s.[127] Most significantly, Azzam.com served as a cyber jihad portal connecting Islamic extremist sympathizers to sister sites and message boards, such as Qoqaz.net and Waaqiah.com, both of which solicited funds for the jihad and recruited volunteers to attend terrorist training camps.[128]

While Azzam.com was eventually removed from the Internet, its existence, alongside dozens of other extremist sites, signified a new era in international terrorism.[129] As a spokesman for Azzam.com told the Wall Street Journal in late 2001, "one cannot shut down the Internet."[130] Indeed, the number and sophistication of extremist-related Web sites continued to

---

eighty-five hours, the hijacking transpired at airports in Fukuoka, Japan and Seoul, South Korea. After the Japanese Deputy Minister of Trade successfully offered himself up as hostage in place of the 80 remaining hostages, the plane flew into North Korea, where the attackers were granted political asylum. The plane safely returned to Japan with the crew and government minister on board. Airliner hijackings had entered the television age. PETER ST. JOHN, AIR PIRACY, AIRPORT SECURITY, AND INTERNATIONAL TERRORISM 23–24 (1991). Less than five months after the Japanese hijacking, the largest and "most remarkable event in the history of aerial piracy" involving five airliners, five governments (U.S, Germany, Switzerland, Israel, and Britain) and 769 hostages was carried out by the Palestinian Liberation Front ("PFLP"). *Id.* A TWA B707 flying from Frankfurt to New York was diverted to Dawson's Field. Simultaneously, a Swissair DC8 flying from Zurich to New York was hijacked. The third plane commandeered was an El Al B707 flying from New York to Tel Aviv with a stop in Amsterdam. The fourth airliner hijacked that afternoon was a Pan American jumbo jet, which was taken by two men who had failed to get on the El Al New York to Tel Aviv flight. The men directed the Pan-American jet to Cairo where the passengers were given eight minutes to vacate the plane before the $20 million aircraft was blown up. Finally, on September 8, the PFLP hijacked a British BOAC VC10 flying from London to Bahrain and Bombay in order to free one of the hijackers who had been captured. Four of the five planes were ultimately destroyed, representing a loss to the airlines of $52 million. *Id.*

[125] *See generally* EVAN KOHLMANN, AL QAIDA'S JIHAD IN EUROPE (2004); ROHAN GUNARATNA, INSIDE AL QAEDA (2002).

[126] Craig Whitlock, *Briton Used Internet as His Bully Pulpit*, WASH. POST, Aug. 8, 2005, at A1.

[127] *Id.*

[128] *Id.*

[129] *Id.*

[130] Stephanie Gruner & Gautam Naik, *Extremist Sites Under Heightened Scrutiny*, WALL ST. J., Oct. 7, 2001.

grow in the late 1990s and early 2000s, as terrorist groups and their sponsors realized the enormous operational potential of the Internet.[131] In the United States, several Al Qaeda and Hamas-front charities openly exploited the Internet for indoctrination, fundraising, and recruitment purposes related to terrorism.[132]

For instance, the Illinois-based Benevolence International Foundation (BIF) raised millions of dollars in the late 1990s for the covert support of Islamic extremism, in part by soliciting funds for what BIF described as "orphans" and other victims of war in Muslim conflict zones.[133] The BIF Web site offered donors a variety of ways to contribute funds for "charity," including online checking, debit, and credit card services, as well as electronic stock donations.[134] On November 19, 2002, the U.S. Department of the Treasury designated BIF a Specially Designated Global Terrorist entity[135] whose leadership "worked with others including members of Al Qaeda to purchase rockets, mortars, rifles, and offensive and defensive bombs, and to distribute them to various mujahideen camps, including camps operated by al Qaida."[136]

Several other individuals and organizations operating in the United States during the late 1990s and early 2000s exploited the Internet to promote and materially support Islamic terrorism. Sami Omar Al-Hussayen, a Saudi Arabian computer science doctoral student at the University of Idaho developed and maintained content for more than fifteen Islamic extremist Web sites and Internet chat rooms "which contained materials designed and intended to recruit mujahideen and raise funds for violent jihad."[137] Among the various items that al-Hussayen posted on his Web sites was the following *fatwa*[138] posted at www.alasr.ws in June 2001, just three months prior to the September 11th attacks:

> [T]he Mujahid (warrior) must kill himself if he knows that this will lead to killing a great number of the enemies, and that he will not be able to kill them without killing himself first, or demolishing a center vital to the enemy or its military force, and so on. This is not possible except by involving the human element in the operation. In this

---

[131] Whitlock, *supra* note 126; WEIMANN, *supra* note 14, 124–125.

[132] *See generally* COUNCIL ON FOREIGN RELATIONS, TASKFORCE REPORT, TERRORIST FINANCING (2002) (providing an in-depth analysis of terrorists' exploitation of charities for fundraising and facilitation purposes).

[133] *See* 9/11 COMMISSION REPORT, *supra* note 31, at 109.

[134] *See* Benevolence International Foundation archived Web site, http://web.archive.org/web/20030207191346/www.benevolence.org/donate.asp.

[135] Press Release, U.S. Department of Treasury, Treasury Designates Benevolence International Foundation and Related Entities as Financiers of Terrorism, Nov. 19, 2002, *available at* http://www.ustreas.gov/press/releases/po3632.htm.

[136] *Id.*

[137] Second Superseding Indictment, United States v. Al-Hussayen, No. 03-040 (D. Idaho 2004).

[138] A fatwa is "a legal opinion or decree handed down by an Islamic religious leader." MERRIAM WEBSTER'S COLLEGIATE DICTIONARY 598 (11th ed. 2003).

> new era, this can be accomplished with the modern means of bombing or bringing down an airplane on an important location that will cause the enemy great losses.[139]

Interrogation transcripts of detainees at the U.S. military base at Guantanamo Bay, Cuba, released by the Department of Defense in early 2006, also make frequent references to how the detainees were inspired to join Al Qaeda and the Taliban prior to September 11, 2001 by *fatwas* they viewed online.[140]

Islamic extremists were successful during the late 1990s in utilizing the Internet to promote their jihad agendas. Many of these Web sites were quite overt in their jihad purpose and message. For instance, an April 2001 version of the London-based Global Jihad Fund ("GJF") Web site,[141] openly solicited funds for the jihad: "The jihad can be supported by two types [sic]: 1) By sending your donations directly to the jihad orgs in potentially hot countries; 2) By sending your donations to the jihad support network in potentially cold countries (e.g., Kosova)."[142] The site included bank account numbers and instructions on how to contribute to jihad movements.[143] The Web site also posted cyber links to the Web sites of terrorist groups, such as Hezbollah, Jamaat-e-Islami, and the Taliban, and provided bank account information for the Al Rashid Trust and the Pakistan-based Al Qaeda affiliated movements Harkat ul Mujahideen and Lashkar Taiba.[144] Shortly after the September 11th attacks, President Bush and the United Nations ("U.N.") identified these groups as major financial and logistical supporters of Al Qaeda and the Taliban.[145] Additionally, behind a link for "Jihad military training," the GJF site provided e-mail contact information for jihadist sympathizers interested in becoming involved in violent Islamic extremist activities: "Training for the mujahideen in several countries whose names cannot be disclosed here. For jihad training mail jtraining@muslimsonline.com."[146]

---

[139] *See* Criminal Indictment, United States v. Al-Hussayen, No. 03-040 (D. Idaho 2003) [hereinafter Al-Hussayen Criminal Indictment].

[140] Reprocessed Combatant Status Review Tribunal and Administrative Review Board Documents, Testimony of Detainees Before the Combatant Status Review Tribunal, (released Mar. 3, 2006), http://www.defenselink.mil/pubs/foi/detainees/csrt/index.html.

[141] *See* Internet Archive, http://www.archive.org/about/about.php., explaining that Webarchive.org "was founded to build an 'Internet library,' with the purpose of offering permanent access for researchers, historians, and scholars to historical collections that exist in digital format." *Id.*

[142] Global Jihad Fund, http://web.archive.org/web/20011109223219/www.ummah.net/jihad/ [hereinafter Global Jihad Fund].

[143] *Id.*

[144] *Id.*

[145] Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001).

[146] Global Jihad Fund, *supra* note 142.

B. Post-September 11th Cyber Jihad Environment

Following September 11th, a number of the most notorious terrorist Web sites, such as Azzam.com and Al Qaeda's http://www.alneda.com[147] were shut down, but hundreds of other sites directly affiliated with terrorist groups emerged in their place.[148] Overall, domestic and international efforts to combat terrorists' use of the Internet have been anemic at best.[149] Complex legal and investigative enforcement challenges have crippled joint initiatives restricting the use of the Internet for terrorist-related activities. This issue goes to the heart of whether states and international organizations can effectively regulate and enforce security and legal order in a landless and borderless cyber network.[150]

Not only have terror-related Web sites grown in number, but the technical sophistication and practical application of the sites have also evolved with astonishing speed and intensity.[151] Often with just superficial masking of language or imagery, notorious terrorist sympathizers, including Al Qaeda recruiters and financiers, maintain engaging, real–time Web sites designed to inspire and mobilize extremist audiences.[152] Yet, such terror-related Web sites continue to flourish with minimal threat of enforcement actions.[153]

C. Terrorists' Strategic Uses of the Internet

Terrorists today utilize the Internet for a growing number of strategic purposes including: public communications and media promotion; indoctrination and recruitment; online fundraising; as well as training and operational planning.[154]

---

[147] *See* Thomas, *supra* note 25, at 115 (reporting that Alneda.com was hosted for a period of time in the United States).

[148] Internet Haganah, Internet Haganah in a Nutshell, http://haganah.org.il/harchives/003218.html (last visited Oct. 30, 2006).

[149] *See* John D. Podesta & Raj Goyle, *Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World*, 23 YALE L. & POL'Y REV. 509, 518 (2005) (criticizing the Bush administration and Congress for failing to implement tougher prevention and enforcement measures against cyber terrorism as part of the wave of anti-terrorism legislation after the September 11th attacks); *see also* Katz & Devon, *supra* note 107.

[150] *See generally* Podesta & Goyle, *supra* note 149.

[151] TERROR ON INTERNET, *supra* note 14, at 49–171.

[152] Internet Haganah, *supra* note 89 (providing an online library of links to dozens of highly sophisticated terrorist Web sites and online chat rooms).

[153] Since September 11th, there has not been a single conviction of an individual in the United States involved in online terrorist activity. *See* Dep't of Justice, Fact Sheet: Department of Justice Terrorism-Related Convictions Since Sept. 11, 2001, June 23, 2006, http://www.usdoj.gov/opa/pr/2006/June/06_crm_388.html.

[154] Since 1999, a number of scholars have analyzed topics related to terrorists' use of the Internet. *See generally* U.S. ARMY TRAINING & DOCTRINE COMMAND, CCSINT HANDBOOK NO. 1.02: CYBER OPERATIONS AND CYBER TERRORISM (2005), http://www.mipt.org/pdf/Cyber-Operations-Cyber-Terrorism.pdf; Gabriel Weimann, *Terrorist and Their Tools*, YALE GLOBAL ONLINE, Apr. 16, 2004,

1. Public Communications

While terrorist groups and their affiliated sympathizers have exploited the Internet as a communications platform for delivering messages to the media since the first days of Azzam.com, the latest generation of cyber jihadists use the medium to deliver announcements crafted to be picked up by the media as news. Infamously, on May 10, 2004, the notorious leader of Al Qaeda in Iraq, Abu Musab al Zarqawi, was videotaped beheading American contractor Nicholas Berg.[155] Within hours of the beheading, the video of the execution was posted on the Al-Ansar Web site and entitled, "Shaykh Abu-Musab al-Zarqawi slaughters an American infidel with his own hands and threatens Bush with more."[156] A few hours after the video's posting online, it was broadcast to tens of millions of viewers on TV channels worldwide, while millions more viewed the video online.[157]

Other jihadist Web sites continue to disseminate statements from their leaders and communicate strategic plans and alliances between groups. For example, in May 2006, Al Qaeda posted a sixty-three page document written by Abdul Aziz bin Rasheed al-Anzy, an important Al Qaeda ideologue, on an extremist Web site, in which religious justification was made for the (foiled) February 24, 2006 plot to blow up the Abqaiq oil refinery facility in Saudi Arabia.[158] In 2004, negotiations to merge terrorist networks were conducted over the Internet between Abu Musab al-Zarqawi and Osama bin Laden.[159] When Zarqawi pledged his allegiance to bin Laden in late 2004, extremist Web sites broke the news.[160] On January 20, 2006, Al Qaeda operatives posted a 17-minute recording of Osama bin Laden's deputy, Ayman al-Zawahiri, to refute American claims that he had been killed in the bombing of an Al Qaeda hideout.[161] Earlier that month, leaders of a number of insurgency groups in Iraq used the Internet to communicate a new strategic alliance among terrorist groups in Iraq and announce the creation of an umbrella body called the Muja-

---

http://yaleglobal.yale.edu/display.article?id=3768; Thomas, *supra* note 25, at 112–16. (evaluating terrorists' exploitation of the Internet for profiling, anonymous-covert communications, generating cyber fear, mobilization and recruitment, mitigation of risk, theft and manipulation of data, and misinformation).

[155] *War on Terror Digest*, BBC MONITORING INT'L REP., *supra* note 8. This article describes how Zarqawi delivered a political statement regarding the U.S. occupation of Iraq prior to executing Nicholas Berg: "We are giving you good news which will displease you. Your worst days are coming, with the help of God. You and your soldiers will regret the day when your feet touched the land of Iraq and showered your bravery on shelters of Muslims." *Id.*

[156] *Id.*

[157] *Web as Weapon*, *supra* note 5.

[158] Mariam Fam, *Document: Al-Qaida Encourages Oil Attacks*, ASSOC. PRESS, March 2, 2006.

[159] *Web as Weapon*, *supra* note 5.

[160] Bamford, *supra* note 7; *see also* Global Terror Alert, *Communique from Al-Tawheed wal Jihad Movement (Abu Musab al-Zarqawi) in Iraq*, http://www.globalterroralert.com/zarqawi-bayat.pdf.

[161] *Bin Laden's No. 2 releases poetry tape*, CNN, Jan. 20, 2006.

heddin Shura Council in Iraq.[162] In 2005, the Al Qaeda-affiliated media operation, Global Islamic Media Front, began launching a series of online weekly magazines ("e-zines") updating readers on its international terrorism campaign.[163] Upon release, the e-zines are quickly distributed to a network of cyber jihadists, who repost the e-zine on numerous sites to frustrate removal by intelligence authorities.[164]

2. Indoctrination and Recruitment

In addition to providing a method of outward communication, jihadist Web sites glorify Islamic militancy in video testimonials of jihad operations. Sympathizers and potential recruits are thereby indoctrinated with virtuous messages of jihad and martyrdom that justify and legitimize violent action against non-Muslims.[165]

A video entitled "The Attack on the Hotels: 'Badr al-Baghdad,'" posted on a Zarqawi-affiliated site in December 2005, glorifies strikes on foreign targets in Iraq by taking viewers inside a terrorist cell's pre-attack surveillance.[166] The video chronicles planning and practice runs for the suicide bombings of the Sheraton Ishtar and Meridian Palestine Hotels in Baghdad.[167] The video includes laudatory biographical profiles of the suicide bombers as well as their martyrdom statements.[168]

Palestinian Islamic Jihad ("PIJ") exploits the Internet to glorify the purported courage and selflessness of suicide bombers who attack Israeli targets.[169] The aim is to inspire new sympathizers and recruits to commit to sacrifices for the terrorist group.[170] Visitors to PIJ's Qudsway.net Web site hear background music and the voice of the group's founder, Fathi Shiqaqi, proclaiming that the

---

[162] Hala Jaber, *Zarqawi sleeps in suicide belt*, TIMES ONLINE, Jan. 22, 2006, http://www.timesonline.co.uk/article/0,,2089-2003822,00.html.

[163] Thomas Hegghammer, *Global Jihadism After the Iraq War*, 60 MIDDLE EAST J. 1, 17 (2006) (describing a number of Al Qaeda online magazines, including: *Sawt al-Jihad* [Voice of Jihad] (29 editions) *Mu'askar al-Battar* [Camp of the Sabre] (22 editions), and *al-Khansa* (1 edition) and *Dharwat al-Sanam* [Peak of the Hump]); *see also* Bouchaib Silm, *A More Animated Approach to Jihad*, STRAITS TIMES (Singapore), Jan. 11, 2006 (describing activities and postings on the Al Qaeda-affiliated Global Islamic Media Front Web site).

[164] *See* discussion *supra* Part II.C.6 (discussing terrorists' use of hydra web links to distribute information online).

[165] *Hegghammer, supra* note 163, at 11–18.

[166] BATTLES OF MESOPOTAMIA, *supra* note 6.

[167] *Id.*

[168] *Id.*

[169] THE PALESTINIAN ISLAMIC JIHAD INTERNET INFRASTRUCTURE AND ITS INTERNET WEBHOSTS, INTELLIGENCE AND TERRORISM INFO. CTR. AT THE CTR. FOR SPECIAL STUDIES (2005) [hereinafter PALESTINIAN ISLAMIC JIHAD INTERNET INFRASTRUCTURE], *available at* http://www.intelligence.org.il/eng/eng_n/internet_e1205.htm.

[170] *See generally* ROBERT PAPE, DYING TO WIN: THE STRATEGIC LOGIC OF SUICIDE TERRORISM (2005) (providing an in-depth historical analysis of the indoctrination, recruitment, training and deployment of suicide bombers worldwide).

"Islamic nation's covenant [is] with blood."[171] The site features the picture of the suicide bomber who carried out the December 5, 2005, attack on a shopping mall in Netanya, Israel, that killed five Israeli citizens. The caption reads: "The suicide bomber Abu Sa'ad . . . waited for the Zionists to approach, smiled a broad smile and blew himself up."[172] The site also includes official PIJ publications, which can be downloaded by individuals who wish to learn about PIJ operations.[173]

3. Terrorist Financing

According to Todd Hinnen, a terrorist financing expert who serves on the Bush administration's National Security Council, terrorists use the Internet in "four primary ways to solicit and collect funding and equipment in support of terrorist operations."[174] Terrorists:

> (1) solicit donations, indoctrinate adherents, share information, and recruit supporters directly via Web site chat groups, and targeted electronic mailings;
>
> (2) they take advantage of charitable organizations, soliciting funds with the express purpose of clothing, feeding, and educating a population, but with the covert intent of exploiting contributors' largesse to fund acts of violence;
>
> (3) they perpetrate online crimes such as identity and credit card theft, intellectual property piracy, and fraud, and support their mission with the proceeds of such crimes;
>
> (4) and they use the Internet as a pervasive, inexpensive, and anonymous medium of communication to organize and implement fund raising activities.[175]

The U.K.-based Hamas front-organization Interpal is one of the largest Internet-based fundraising organizations and utilizes many of the above methodologies. In addition to being a principal conduit through which funds are funneled (under the guise of charity) to Hamas, "Interpal is [a] fundraising . . . coordination point for other Hamas-affiliated charities. . . . [As such, Interpal] supervis[es] activities of charities, develop[s] new charities in targeted areas, instruct[s] how funds should be transferred from one charity to another, and even determine[es] public relations policy."[176] Despite enforcement actions by the United States and Israel to freeze the assets of Interpal and to shut down the Web site, the organization continues to operate and raise funds online.[177]

Some prominent Islamic extremists issue public statements and writings referring followers to Web sites that provide instructions on how to exploit the Internet to raise funds for their deadly campaigns. Imam Samudra, Indonesian Al Qaeda terrorist and the leader of the 2002 Al Qaeda Bali

---

171 PALESTINIAN ISLAMIC JIHAD INTERNET INFRASTRUCTURE, *supra* note 169.
172 *Id.*
173 *Id.*
174 Hinnen, *supra* note 105, at 10.
175 *Id.*
176 U.S. Charities Funding Hamas, *supra* note 67.
177 Interpal, http://www.interpal.org/web/101.htm (last visited Oct. 30, 2006).

bombings,[178] recently released an autobiography from his jail cell containing a chapter entitled, "Hacking, Why Not?"[179] The chapter "details basic information on money laundering, online credit card fraud, and computer programming languages, exhorting all would-be terrorists to use cyberspace to further jihad."[180]

Other terrorist networks have combined multiple communications media to raise funds for terrorism-related operations. For example, Hezbollah maintains its own popular television station, Al Manar,[181] which is broadcast throughout the Middle East, and promoting violence against Israel and the United States. Al-Manar's Web site urges contributions "for the sustenance of the Intifadah" and provides bank accounts in Lebanon to which donations can be made for the purpose of carrying out violence against Israeli interests.[182]

Each of these Internet fundraising techniques illustrates terrorists' technological sophistication and strategic manipulation of readily-available technology in order to raise funds for militant campaigns.

4. Operational Training and Strategic Planning

Many violent extremist Web sites have become one–stop terrorist training and planning centers. As traditional means of travel and communication have become increasingly difficult for many terrorist operatives since September 11th,[183] a number of terrorist-related sites have expanded their use of the Internet as a command and control platform.[184] With horrifying openness and audacity, jihadi webmasters utilize multimedia Web technologies to create virtual training and planning command centers.

"If you want to conduct an attack, you will find what you need on the Internet."[185] During 2005 and early 2006, a series of high-quality training films shot

---

[178] Alan Sipress, *An Indonesian's Prison Memoir Takes Holy War into Cyberspace*, WASH. POST, Dec. 14, 2004, at A19; *Alleged Terror Hackers Arrested*, JAKARTA POST, Aug. 24, 2006, (reporting that a follow-up investigation resulted in the August 16, 2006 arrest of Agung Setyadi in Indonesia for smuggling a computer into prison for Imam Samudera and the August 12, 2006 arrest of Mohammad Prabowo for registering the anshar.net Web site on the UK hosting site, www.openhosting.co.uk, as a tool for exchanging information on terrorist operations).

[179] Sipress, *supra* note 178.

[180] Podesta & Goyle, *supra* note 149, at 518.

[181] *See* Al Manar Television, http://www.manartv.com.lb/NewsSite/News.aspx?language=en (last visited Oct. 30, 2006). On March 23, 2006, the U.S. Treasury Department designated Al-Manar as a Specially Designated Global Terrorist Entity pursuant to Executive Order 12334. Press Release, U.S. Treasury Dep't, U.S. Designates Al-Manar as a Specially Designated Global Terrorist Entity: Television is Arm of Hizballah Terrorist Network (Mar. 23, 2006).

[182] ANTI-DEFAMATION LEAGUE, *supra* note 10.

[183] *See* 9/11 STAFF REPORT ON TERRORIST TRAVEL, *supra* note 31.

[184] See discussion *supra* Part III.

[185] *Terrorists Turn*, *supra* note 15.

in Afghanistan were posted on Web sites associated with Al Qaeda affiliated groups. These Web videos include instructions for conducting a roadside assassination, raiding a house, shooting a rocket propelled grenade, blowing up a car, attacking a village, destroying a bridge and firing an SA-7 surface-to-air missile.[186]

Al Qaeda operatives planning the March 14, 2004, Madrid train bombings studied a report on the Al Qaeda-affiliated Global Islamic Media front Web site, "in which a committee of al-Qaeda experts suggested an attack in Spain before the general elections of March 14, 2004."[187] In late 2003, a Web site entitled "Al Qa'ida University for Jihad Sciences" offered an online instruction manual for various terrorist attacks including "suicide operations."[188] In August 2005, a site maintained by an Iraqi insurgency group posted an instructional pamphlet entitled "The New Road to Mesopotamia" for prospective foreign fighters seeking to enter Iraq to fight against U.S. and allied forces.[189] The pamphlet included very specific tactical recommendations for crossing the Syria-Iraq border, based on what appeared to be first-hand accounts of fighters who had previously made the trip:

> Arrange your trip to take place over two stages. The first stage is to learn the area, the people and the roads, and then head toward the city of Dayr Al-Zawr [Syria] near the Iraqi border. It is recommended to enter the city using a car and do not carry large sums of money. If anyone asks, say you are here on a vacation and have come to go fishing in the Euphrates—therefore, bring some fishing equipment and another person with you so you won't look suspicious. It is an inexpensive region and usually you will end up paying $300 for 15 days in a four star hotel. A tank of gas will cost you around $10 . . . .[190]

A number of other Web sites include remarkably detailed instructional booklets on how to make suicide explosive belts. For instance, a 26-minute video on the Al-Ansar forum site discovered by the SITE Institute in December 2004 "shows how to estimate the impact of an explosion, how best to arrange the shrapnel for maximum destruction, how to strap the belt onto the bomber's body, [and] even how to avoid the migraine headache that can come from exposure to the recommended explosive chemicals."[191]

---

[186] *Id.*

[187] Pamela Rolfe, *29 Indicted for Roles in Madrid Bombings*, WASH. POST, Apr. 11, 2006.

[188] ILAN BERMAN, AMERICAN FOREIGN POLICY COUNCIL, EURASIA SECURITY WATCH NO. 7 (2003), *available at* http://www.afpc.org/esw/esw7.shtml (last visited Oct. 30, 2006).

[189] GLOBAL TERROR ALERT, AL-MUHAJIR AL-ISLAMI THE ROAD THROUGH SYRIA TO JIHAD IN IRAQ 1–3 (2005), http://www.globalterroralert.com/pdf/0805/roadtoiraq0805.pdf.

[190] *Id.*

[191] *Web as Weapon*, *supra* note 5, at A1. According to its Web site, the U.S.-based SITE Institute:

> locates links among terrorist entities and their supporters. Once a potential terrorist entity is identified, either through SITE's ongoing internal research or via a client's specific query, SITE conducts a comprehensive investigation on the target and entities affiliated to it, scouring corporate records, tax forms, credit reports, videotapes, internet newsgroup postings, and owned websites, among other resources, for indicators of illicit activity.

Other sites have published a 15-page document authored by Al Qaeda operational leader Mustafa Setmariam Nasar with instructions for deploying potential biological weapons agents.[192] The document explains how to develop a crude biological weapons delivery mechanism: "inject carrier animals, like rats, with the virus and how to extract microbes from infected blood . . . and how to dry them so that they can be used with aerosol delivery system."[193] Online manuals discovered by the Terrorism Research Center instruct operational activities on "how to extract explosive materials from missiles and land mines. Another offered a country-by-country list of explosive materials available in western markets . . . ."[194]

The cyber jihad watchdog organization, Society for Internet Research, has noted that certain instructional documents illustrate a nexus between online extremist communications and subsequent terrorist operations.[195] On September 25, 2005, a known Al Qaeda facilitator using the name Abu Muhammad al-Hilali published a call to action on the Internet in which he provided instructions for additional terrorist attacks on the Sinai Peninsula in Egypt following suicide bombings in October 2004 and July 2005.[196] The communication is considered to be the first operational command to emerge on the Internet from a 1,601-page book on jihad authored by Islamic extremist Abu Mus'ab al-Suri.[197] This direct nexus between online ideological communications and subsequent attacks demonstrates the growing operational significance of the Internet to terrorist groups.[198]

IV. U.S. RESPONSES TO THE CYBER JIHAD

Despite notice beginning as early as the mid-1990s that terrorists were using the Internet as an operational and communications hub,[199] the U.S. has fundamentally failed to respond to the seriousness of the cyber jihad threat.[200] Instead of developing and implementing domestic and interna-

---

See SITE Institute, http://www.siteinstitute.org/mission.html.

[192] *Id*.

[193] *Terrorists Turn*, *supra* note 15, at A1.

[194] *Id.*

[195] *See* REUVEN PAZ, AL-QAEDA'S SEARCH FOR NEW FRONTS: INSTRUCTIONS FOR JIHADI ACTIVITY IN EGYPT AND SINAI, SOC'Y. FOR INTERNET RESEARCH 1–3, 10 (2005) (*citing* Abu Muhammad al-Hilali, *Risalah ila Ahl al-Thughour fi Sina'*, *A Message to the People of the Frontiers of Sinai*, http://www.alhesbah.org/v/showthread.php?t=33241).

[196] *Id.*

[197] *Id. See* Abu Mus'ab al-Suri, *Da'wah lil-Muqawamah al-Islamiyah al-'Alamiyyah (A Call for the Islamic Global Resistance)*, www.fsboa.com/vw/index.php?subject=7&rec=27&tit=tit&pa=0 (last visited Aug. 22, 2006).

[198] PAZ, *supra* note 195.

[199] ARQUILLA & RONFELDT, *supra* note 119 (providing notice in 1996 of the threat posed by cyber operational planning).

[200] *See* Podesta & Goyle, *supra* note 149, at 516–522 (criticizing the Bush administration and Congress for failing to implement tougher prevention and enforcement measures

tional regulatory measures to prevent terrorists and other criminals from gaining access to and exploiting the Internet, policymakers have focused their energies on national-level laws that rely heavily on deterrence and prosecution of online terrorist activities.

This strategy has failed to curb the exponential growth in Internet use as an operational center for cyber jihadists: U.S. law enforcement officials have yet to successfully prosecute a single case against a reputed cyber jihadist.[201] These failures illustrate a lack of imagination and courage to institute fundamental reforms that would make the Internet and the world a safer place.

A. Congressional Action: A Failure to Respond Creatively to the Threat

Since September 11th, the U.S. government has taken a number of regulatory steps to bolster Internet security and prevent the Web from becoming a breeding ground and safe-haven for terrorist activity.[202] Unfortunately, these measures have been insufficient and misdirected. Specifically, provisions addressing Internet security issues focus almost solely on strengthening penalties for cyber attacks on U.S. government infrastructure.[203] By focusing exclusively on the deterrence dimension of combating online terrorist-related activity, lawmakers have failed to consider grand-scale prevention measures to disrupt cyber jihad activities.

1. U.S.A. PATRIOT Act

In the weeks following the September 11th attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Re-

---

against cyber terrorism as part of the wave of anti-terrorism legislation after the September 11th attacks).

[201] *But see* Superceding Indictment, United States v. Infocom Corp., No. 3:02-CR-052 (N.D. Tex. filed Dec. 17, 2002) (pending criminal case involving an ISP that allegedly provided material support to terrorist groups by developing, hosting, and maintaining Web sites which incited violent action against the U.S. and raised funds for terrorism-affiliated entities).

[202] Arguably the most significant legislative action taken in the wake of the September 11th attacks was the enactment of the U.S.A Patriot Act. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("PATRIOT") Act Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C., 22 U.S.C., 28 U.S.C., 31 U.S.C., 47 U.S.C., and 50 U.S.C.). Cyber terrorism–related provisions of the PATRIOT Act revise prohibitions and penalties regarding fraud and related activity in connection with computers to include specified cyber-terrorism offenses. The Patriot Act also directs the Attorney General to establish regional computer forensic laboratories, and to support existing laboratories, to develop specified cyber-security capabilities. *See* Pub. L. No. 107–56, Title VIII, § 816, 115 Stat. 385 (2001).

[203] *Id.*

quired to Intercept and Obstruct Terrorism Act ("PATRIOT Act"),[204] which was designed to address inadequacies in our nation's homeland security and to provide the necessary tools to address these problems.[205] In the area of cyber terrorism, however, the Act narrowly focuses on stiffer penalties for individuals who carry out offensive cyber attacks resulting in physical injury to American citizens, damage to U.S. facilities, or threaten public health or safety.[206] The legislation also authorizes additional funding for forensic laboratories to investigate cyber crimes.[207] However, the law does not include penalties for using the Internet to promote or communicate terrorism-related activities unrelated to cyber attacks. Instead, Congress appears content to allow terrorism-related activity on the Internet to be governed by anti-terrorism statutes.[208]

The Bush administration has emphasized that the PATRIOT Act encourages ISPs and e-mail providers to act as cyber watchdogs and report suspicious online activities.[209] In a July 2005 speech, President Bush argued that the PATRIOT Act enhances the security of the Internet by protecting ISPs from civil lawsuits "when they give information to law enforcement when it would help law enforcement prevent a threat of death or serious injury."[210] The statutory provision, however, *encourages* rather than *requires* ISPs to report threatening information on their sites.[211] To date, there is no

---

[204] *Id.*

[205] Press Release, The White House, Fact Sheet, The Patriot Act Helps Keep America Safe (June 9, 2005) [hereinafter The Patriot Act Helps Keep America Safe], *available at* http://www.whitehouse.gov/news/releases/2005/06/20050609.html.

[206] 18 U.S.C. § 1030a(5) (2001). The PATRIOT Act mandates criminal penalties of at least 1 year in prison where an individual carries out a cyber attack which results in aggregate damages over $5,000 to private computers, causes a public health or safety threat, results in injury or death of an individual or "damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security. *Id.*

[207] 28 U.S.C. § 509 Sec. 2357(3)(c) (2000). Section 816(a) of The PATRIOT Act authorizes the Attorney General to establish regional forensic laboratories and to support existing forensic labs to bolster their abilities in examining and investigating cyber crime. Pub. L. No. 107-56, Title VIII, § 816, 115 Stat. 385 (2001).

[208] *See* Antiterrorism Act of 1990, 18 U.S.C. § 2339B (2000) ("[p]roviding material support or resources to a designated foreign terrorist organization").

[209] *See* Press Release, President Discusses Patriot Act, Ohio State Highway Patrol Academy, Columbus, Ohio (June 9, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/06/print/20050609-2.html; The Patriot Act Helps Keep America Safe, *supra* note 205.

[210] The Patriot Act Helps Keep America Safe, *supra* note 205.

[211] PATRIOT Act, Title VIII, § 225(h) (codified at 50 U.S.C. § 1805(c)2B (2000). Section 225(h) of the PATRIOT Act stipulates that

> No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this this chapter for electronic surveillance or physical search.

available evidence to suggest that ISPs, Web hosts, or e-mail providers have increased their monitoring or reporting of suspected terrorism-related e-mails since September 11th.[212] Furthermore, the voluntary nature of this measure limits the likelihood that an ISP would shut down a Web site at the request of the government out of a fear that such action will raise civil liberties and prior restraint concerns.[213]

On the other hand, the PATRIOT Act does expand federal surveillance powers regarding e-mails and other electronic Internet communication by permitting the National Security Agency to filter and review potential terrorism-related e-mails and Web postings originating abroad.[214] Due to limited publicly available information regarding ongoing intelligence activities and pending terrorism investigations, the impact this provision has had on the government's intelligence gathering capabilities is unclear.[215] However, it appears that this surveillance authority was used in a number of terrorism related cases involving associates who maintained Web sites and conducted terrorism activities via e-mail.[216]

---

50 U.S.C. § 1805(i) (2000).

[212] Molnar, *supra* note 47, at 26–28.

[213] *See* Dino Bozonelos & Galen Stocking, *The Effects Of Counter-Terrorism On Cyberspace: A Case Study Of Azzam.Com*, 2003 J. INST. JUST. INT'L STUD. 88, 88–90 (2003). Internet scholars who advocate for strong free-speech protections online, such as University of Miami Law School Professor Michael Froomkin, argue that the doctrine of 'prior restraint' which prevents the government from blocking the publication of information except where that information poses a threat to the national security of the country, applies to content on the Internet. Prior restraint proponents argue that the government should be greatly limited in its ability to investigate and monitor Internet activities. E-mail from Michael Froomkin, Professor of Law, University of Miami School of Law, to Benjamin R. Davis (Mar. 24, 2006, 21:38:45 EST)(on file with author); *s*ee also Raphael Prober, Note*: Shutter Control: Confronting Tomorrow's Technology With Yesterday's Regulations*, 19 J.L. & POL. 203, 220–21 (2003) (describing the case law relating to the doctrine of 'prior restraint' and its application in the publication of national security related articles); Doe v. Ashcroft, 334 F. Supp. 2d 471, 489 (S.D.N.Y. 2004). In *Doe v. Ashcroft*, the court held that the disclosure bar was not narrowly tailored to further Government's interest in protecting the integrity and efficacy of international terrorism investigations in violation of the First Amendment free speech protections where an Internet service provider that had received an FBI National Security Letter that brought action challenging the Patriot Act provisions authorizing such letters and permanently barring disclosure of receipt of such letters. *Id.* The court also found that the NSL violated the Fourth Amendment as applied. *Id; s*ee also Craig M. Glasgow, Note, *Doe v. Ashcroft and its Place in the Judicial Trend: How the Courts Have Advanced Civil Liberties In Step With Advances In Technology*, 10 U. PGH J. TECH. L. & POL'Y 3, 4 (2006) (analyzing the recent *Doe v. Ashcroft* decision and its potential impact for placing boundaries on the government's ability to investigate online activities).

[214] 18 U.S.C. §§ 3121, 3123 (2000).

[215] *See* Gellman, *supra* note 37.

[216] The most notable of these cases was the 2004 trial of Sami Omar al-Hussayen. *See* Al-Hussayen Criminal Indictment, *supra* note 139.

2. Homeland Security Act

Another important piece of cyber terrorism-related legislation was the Homeland Security Act of 2002 (the "Act").[217] In addition to establishing the Department of Homeland Security, the largest reorganization of government in fifty years,[218] the legislation bolstered the government's institutional ability to combat offensive cyber terrorist threats.[219] The Act authorizes the Department of Homeland Security to share cyber security information and provide technical assistance to state and local governments, as well as private entities that develop or maintain critical information systems.[220]

The law also requires federal judges to consider a number of factors in determining sentences for individuals found guilty of cyber attacks on U.S. targets.[221] However, in light of lawmakers' repeated efforts to strengthen penalties for cyber terrorism-related offenses, the Department of Justice

---

[217] Homeland Security Act of 2002, Pub. L. No. 107–296, § 225, 116 Stat. 2135. Section 225 of the Homeland Security Act specifically directs the U.S. Sentencing Commission to review and amend Federal sentencing guidelines and otherwise address crimes involving fraud in connection with computers and access to protected information, protected computers, or restricted data in interstate or foreign commerce or involving a computer used by or for the Federal Government. The Act requires that the U.S. Sentencing Commission report to Congress on actions taken and recommendations regarding statutory penalties for violations. The Act exempts from criminal penalties any disclosure made by an electronic communication service to a Federal, State, or local governmental entity if made in the good faith belief that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay. The Act requires any government entity receiving such a disclosure to report it to the Attorney General. *Id.*

[218] William B. Cassidy, *The Big Push*, TRAFFIC WORLD, Dec. 11, 2002 at 11 (describing the largest reshuffle of federal agencies since the Department of Defense was established in 1947, involving the consolidation of 22 separate agencies, including the Transportation Security Administration, U.S. Coast Guard, Customs Service, Immigration and Naturalization Service and Border Patrol into a single department).

[219] Homeland Security Act of 2002, Pub. L. No. 107–296, 116 Stat. 2135 (establishing an Under Secretary for Information Analysis and Infrastructure Protection, as well as defining information (or cyber) systems among the nation's critical infrastructures).

[220] *Id.*

[221] *Id.* at 2156–57. The Homeland Security Act requires federal sentencing judges who are evaluating the nature of the criminal offenses related to cyber terrorism activities to:

> [C]onsider the following factors and the extent to which the guidelines may or may not account for them—(i) the potential and actual loss resulting from the offense; (ii) the level of sophistication and planning involved in the offense; (iii) whether the offense was committed for purposes of commercial advantage or private financial benefit; (iv) whether the defendant acted with malicious intent to cause harm in committing the offense; (v) the extent to which the offense violated the privacy rights of individuals harmed; (vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice; (vii) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and (viii) whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person.

Id.

has failed to produce a single conviction in a cyber jihad case since September 11th.[222] Without effective enforcement, deterrence cannot work.

3. False Starts at Reform

The Internet is anonymous, borderless, and remotely accessible. As such, it is difficult for states to find perpetrators of Internet crimes, and even more difficult to prosecute extremists for their online activities. Despite the U.S. government's focus on deterrence and penalties to combat the cyber jihad, policymakers and cyber security advocates originally considered imposing increased fiduciary duties on ISPs to monitor and verify user registration information.[223] However, a number of these efforts were blocked from implementation by business interests reportedly concerned with added costs and potential exposure to liability.[224]

For instance, the Bush administration's *National Security Strategy to Secure Cyberspace*, released in early 2003, proposed important mandates to enhance Internet security. [225] The initial proposal envisioned requiring ISPs to provide firewalls to consumers and holding ISPs liable for content posted on and activities associated with sites hosted by a particular provider that resulted in damages from cyber-terrorist attacks.[226] It also proposed establishing an industry-supported cyber security fund and forming corporate security councils to regularly review business-continuity plans and risks posed by vendors.[227] The strategic provisions were primarily targeted at bolstering cyber security against offensive cyber attacks, but the focus on increased monitoring and disclosure duties for providers would have complemented efforts to limit terrorists' operational use of the Internet.[228] The proposed measures would have also forced providers to invest in the technology and manpower to track data and electronic traffic passing through their company's servers for potential terrorist activity.[229]

---

[222] *See* Al Goodman, *Terrorist Internet Plotter Jailed*, CNN.com, Apr. 3, 2006, http://www.cnn.com/2006/WORLD/Europe/04/03spain.justice.

[223] Carolyn Duffy Marson, *Bush Team Lays Out Cybersecurity Plan*, NETWORK WORLD, Sept. 23, 2002; Tom Foremski *A Toothless IT Security Plan*, FIN. TIMES, Sept. 29, 2002; Aaron Davis, *Internet Security Strategy Released*, SAN JOSE MERCURY NEWS, Feb. 15, 2003, at 1C; Jonathan Krim, *Cyber-Security Strategy Depends on Power of Suggestion*, WASH. POST, Feb. 15, 2003, at E1; Jennifer Lee, *White House Scales Back Cyberspace Plan*, N.Y. TIMES, Feb. 15, 2003, at A14; Podesta & Goyle, *supra* note 149, at 520.

[224] *See* Marson, *supra* note 223; Foremski, *supra* note 223; Davis, *supra* note 223; Krim, *supra* note 223; Lee, *supra* note 223.

[225] WHITE HOUSE, NATIONAL ADVISORY COUNCIL ON CRITICAL INFRASTRUCTURE, NATIONAL STRATEGY TO SECURE CYBER SPACE (2003), http://www.whitehouse.gov/pcipb/.

[226] *See* Marson, *supra* note 223; Foremski, *supra* note 223; Davis, *supra* note 223; Krim, *supra* note 223; Lee, *supra* note 223.

[227] *See* Lee, *supra* note 223; Podesta & Goyle, *supra* note 149, at 520.

[228] Lee, *supra* note 223; Podesta & Goyle, *supra* note 149, at 520.

[229] Lee, *supra* note 223, at 2.

Ironically, it appears that ISPs may agree, at least in part, with the contention that they have a greater duty to monitor and detect illicit activity on sites they host. In testimony before the House Judiciary Subcommittee on Crime, Clint N. Smith, President of the Internet Service Providers Association, indicated that providers might accept wide-ranging responsibility for controlling content. Smith testified that, "[t]he successful investigation and prosecution of crime on the Internet requires a legal framework that balances the powers of law enforcement, the privacy rights of individuals, and the responsibilities and liabilities of services providers."[230] Unfortunately, no legislation has been considered to provide such a framework since 2002, and only two substantive hearings on cyber terrorism issues have been held in the last three Congresses.[231]

Yet, Congress and the Bush administration's historical reluctance to intervene in efforts to force systemic improvements on Internet security issues may be shifting course by way of another grave Internet security issue—the proliferation of online child pornography.[232] In June 2006, the House of Representatives Energy and Commerce Committee held hearings on online child pornography and sexual solicitation of minors. [233] Legislative efforts to combat online child pornography may ultimately serve as a springboard for strengthening ISP and search engine enforcement actions and responsibilities in combating cyber jihad–associated activities. While the hearings did not examine terrorism–related issues, a number of ISP companies and search engine providers, such as EarthLink, Verizon, Google, Yahoo, and America Online ("AOL"), publicly acknowledged that they must do more to comply with and enforce policies and laws on the Internet.[234] In partial response to criticism that they have not done enough

---

[230] *The Cyber Security Enhancement Act of 2002: Hearing on H.R. 3482 Before the Subcomm. on Crime of the H. Comm. on the Judiciary,* 107th Cong. 38 (2002) (statement of Clint N. Smith, President, United States Internet Service Providers Association) [hereinafter Smith Testimony].

[231] *See The Cyber Security Enhancement Act of 2002: Hearing on H.R. 3482 Before the Subcomm. on Crime of the H. Comm. on the Judiciary,* 107th Cong. 38 (2002); *Terrorist Use of the Internet for Communications: Before the H. Select Intelligence Comm*., 109th Cong. (2006) (examining the use of the Internet by terrorists, particularly in Iraq, to indoctrinate and recruit potential jihadists with ideological messages of hatred and militant Islam).

[232] Joshua Brockman, *F.B.I. and Justice Dept. Are Faulted Over Child Predators on Web*, N.Y. TIMES, Apr. 7, 2006 (reporting on Congressional hearings where members of Congress questioned that child pornography cases have increased 445 percent the last four years).

[233] *Making the Internet Safe for Kids: The Role fo ISP's and Social Networking Sites: Hearing Before the Subcomm. On Oversight and Investigations of the H. Comm. On Energy and Commerce,* 109th Cong. (2006) [hereinafter *Hearing: Making the Internet Safe for Kids*].

[234] *See id.*.

to combat online child predators,[235] AOL, Microsoft, EarthLink, and United Online announced the launch of "an aggressive campaign against child exploitation on the Internet through a new center for child protection technologies. Through this center, industry leaders will come together to develop and deploy technological solutions to disrupt predators' ability to use the Internet to abuse children."[236] Other ISPs with representatives at the hearings, such as Comcast, announced that they were voluntarily extending the retention of all IP user data to 180 days to aid in law enforcement efforts.[237] Perhaps most significantly, many of the representatives from these ISP and search engine companies described renewed efforts to comply with their statutory requirements to report child exploitation to the National Center for Missing and Exploited Children ("NCMEC").[238] In addition, Representative Diana DeGette announced during the hearing that she planned to introduce legislation that would require ISPs to retain all IP data for one year,[239] a significant expansion to the current ninety day data preservation requirement.[240]

The about-face by ISPs and search engine companies illustrated during the June 2006 Congressional hearings is likely due to the Executive Branch's tougher enforcement approach with Internet providers. In April 2006, Attorney General Alberto Gonzales suggested that ISPs retain user data for a "reasonable amount of time" to improve efforts to combat online

---

[235] *See ISP Data Retention Takes Center Stage at Child Porn Hearing*, WASH. INTERNET DAILY, Apr. 7, 2006 (reporting on a Congressional hearing in April 2006 where a witness stated that up to 40 percent of ISPs do not comply with government requests to preserve IP data in Internet crime investigations).

[236] *U.S. Rep. Edward Whitfield (R-KY) Holds a Hearing on Internet Service Providers and Social Networking Sites' Roles in Children's Use of the Internet,* CONG. QUARTERLY (June 27, 2006) (statement of Elizabeth Banker, vice President and Associate General Counsel, Yahoo).

[237] *Id.* (statement of Gerard Lewis, Vice President, Deputy General Counsel, and Chief Privacy Officer, Comcast)..

[238] 42 U.S.C. § 13032(b) (2000) (creating a duty to report child pornography on the Internet to the National Center for Missing and Exploited Children's Cybertip line). The National Center for Missing and Exploited Children, http://www.missingkids.com/. According to its Web site:

> [T]he National Center for Missing and Exploited Children, in cooperation with the Federal Bureau of Investigation's Innocent Images Task Force, the Bureau of Immigration and Customs Enforcement, the US Department of Justice's Internet Crimes Against Children Task Force Units, and the US Postal Service work together with shared access to information to fight Internet crimes against children.

U.S. Rep. Edward Whitfield (R-KY) Holds a Hearing on Internet Service Providers and Social Networking Sites' Roles in Children's Use of the Internet, CONG. QUARTERLY (June 27, 2006) (statement of Rep. Diana DeGette).

[239] Hearing: Making the Internet Safe for Kids, *supra* note 233, at 46.

[240] 18 U.S.C. § 2703(f)(2) (2000) (imposing the 90 day retention of data requirement only upon specific request by a government entity).

child predators.[241] This was a reversal of the prior Justice Department position of opposition to strengthening data-retention laws.[242] There are also indications that stronger data retention laws are aimed not only at combating cyber predators, but cyber jihadists as well. Indeed, in a series of private meetings with Internet industry leaders in May and June 2006, the Justice Department reportedly requested that ISPs and search engine companies retain IP data as well as lists of e-mail traffic and Web searches for up to two years in an effort to improve government efforts to fight online child predators and Internet–based terrorist activities.[243]

B. Criminal Enforcement

In the rare instances of successful law enforcement identification, tracking, and detention of individuals for online terrorism-related activities, federal prosecutors have had difficulty overcoming high Constitutional hurdles that protect most forms of speech. In the 2004 trial of Sami Omar Al-Hussayen,[244] a Saudi national accused of providing material support to terrorist groups through affiliated Web sites, an Idaho jury found the defendant not guilty of terrorism-related charges due, in part, to free speech protections laid out by the Supreme Court in its landmark *Brandenburg v. Ohio* decision.[245]

In *Brandenburg*, the Court determined that speech must be "directed to inciting or producing imminent lawless action and is likely to incite or produce such action" in order to be suppressed or prosecuted by the government.[246] In the Al-Hussayen case, the jury was not convinced that the defendant's posting of inciteful material calling for violent action against the United States and soliciting financial support for Islamic fighters rose to

---

[241] U.S. Att'y Gen. Alberto R. Gonzales, Prepared Remarks at the National Center for Missing and Exploited Children (April 20, 2006), http://www.usdoj.gov/ag/speeches/2006/ag_speech_060420.html.

[242] Declan McCullagh, *Gonzales Pressures ISPs on Data Retention*, CNET NEWS.COM, May 26, 2006, http://news.com.com/2100-1028_3-6077654.html [hereinafter *Gonzales Pressures ISPs*] (describing the Bush administration's earlier opposition to data retention laws).

[243] *See* Jon Swartz, *U.S. Asks Internet Firms to Save Data*, USA TODAY, June 1, 2006; *Feds Put Squeeze on Internet Firms*, CNN.COM, May 30, 2006, http://www.cnn.com/2006/TECH/internet/05/30/internet.records/index.html; *Gonzales Pressures ISPs*, *supra* note 242.

[244] Al-Hussayen Criminal Indictment, *supra* note 139.

[245] Brandenburg v. Ohio, 395 U.S. 444 (1969) (holding that the constitutional guarantees of free speech and free press do not permit a state to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.); *see also* Thomas E. Crocco, *Inciting Terrorism on the Internet: An Application of Brandenburg to Terrorist Websites,* 23 ST. LOUIS U. PUB. L. REV. 451, 482–84 (2004) (proposing a narrowly expanded standard of "imminence" for online terrorist activities).

[246] *Brandenburg,* 395 U.S. at 447.

the level of a convictable offense under the *Brandenburg* "imminent danger standard."[247]

In *United States v. Ahmad*, a Palestinian national who maintained Al Qaeda's Azzam.com Web site presents the latest challenge for federal counter-terrorism prosecutors in pursuing justice against cyber jihadists.[248] While the *Ahmad* indictment implicates the defendant's online terrorism-related activities, prosecutors are mindful of the failures of the Al-Hussayen trial.[249] The core of the government's case against Al-Hussayen focused on his online activities.[250] In the *Ahmad* indictment, however, the charges focus on other aspects of the defendant's material support for terrorism, such as recruiting trainees for terrorist training camps.[251] In doing so, prosecutors seek to illustrate the broader impact of the defendant's cyber operations, while minimizing the defendant's speech activities that damaged the government's case against al-Hussayen.

Ultimately, cyber jihadists "walk a fine line between free speech and criminality when they set up Web sites. There are many factors you have to consider,"[252] said Assistant U.S. Attorney Robert O'Neill, prosecutor in *United States v. Babar Ahmad*.[253] Investigators must consider whether there are "legitimate connections to what is considered a jihadist group. You have to look at the Webmaster's background, [and the beliefs] that

---

[247] *Failed Prosecution of UI Student May Aid Terror Cause, Attorneys Say*, ASSOC. PRESS, Apr. 27, 2005.

[248] *See also* Superseding Indictment, United States v. Infocom Corp., No. 3:02-CR-052 (N.D. TX filed Dec. 17, 2002) (involving an ISP that allegedly provided material support to terrorist groups by developing, hosting, and maintaining Web sites which incited violent action against the U.S. and raised funds for terrorism-affiliated entities).

[249] The Sami Al-Hussayen case is cited by some legal scholars as an example of the misuse of the material support for terrorism statute, 18 U.S.C. § 2339B (2000), to reach First Amendment protected activities. *See* Robert Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV J. ON LEGIS. 1, 58 n.316 (2005) (emphasizing that online terrorist-related activity that falls short of the imminence standard in *Brandbenburg* would enable the defendant to defeat the prosecution on First Amendment grounds); Harvey Silvergate, *Opinion, Free Speech in an Age of Terror*, BOSTON GLOBE June 28, 2004, at A11 (arguing that prosecution of Saudi student Sami Omar Al-Hussayen raised free speech concerns); *see also* E-mail from Michael Froomkin, Professor of Law, University of Miami School of Law, to Benjamin R. Davis (Mar. 24, 2006, 21:38:45 EST) (on file with author).

[250] *See* Second Superseding Indictment, *supra* note 137. The Connecticut federal grand jury charged Ahmad with terrorism-related crimes, including running Web sites that provided material support to the Taliban and the Chechen *mujahideen* by supplying "expert advice and assistance, communications equipment, military items, lodging, training, false documentation, transportation, funding, personnel and other support." *Id.*

[251] Criminal Indictment, United States v. Ahmad, No. 3:04m240, at 1 (D. Conn. filed July 28, 2004) [hereinafter *Ahmad Criminal Indictment*].

[252] Altman, *supra* note 37.

[253] Ahmad Criminal Indictment, *supra* note 251.

person is espousing."[254] As Robert Altman emphasizes, "clearly the First Amendment doesn't give you the right to cry fire in a crowded theater."[255] However, defining speech protections in the context of cyber jihadists creates a difficult hurdle in their successful prosecution.

C. Pursuing ISP Accountability in the Civil Justice System

Suing ISPs for civil liability for failing to monitor and filter inappropriate content is another avenue to clamp down on extremist content on the Internet. Courts have generally conveyed strong hesitation in imposing negligence liability on ISPs, except where it can be shown that ISPs were aware, or should have been aware, of illegal activities taking place on sites they host, or where it can be shown that a breach of duty caused damage to a particular party.[256] To date, almost all successful civil litigation alleging ISP liability for content on hosted sites has involved copyright, trademark infringement, or defamation claims.[257] The lack of ISP content liability litigation involving terrorism is due, in part, to statutory protections under the Communications Decency Act,[258] and the difficulty that victims of ter-

---

[254] Altman, *supra* note 37.

[255] *Id.*

[256] *See* Bolin & Daniel, supra note 49; Justin Nackley, *"Oh What a Tangled [World Wide] Web We Weave." The Dangers Facing Internet Service Providers, and Their Available Protections,* 2005 SYRACUSE SCI. & TECH. L. REP. 2, 31-35 (2005) (describing a number of cases which found ISPs liable for content posted on Web sites which were hosted by the defendant ISP).

[257] *See, e.g.,* Gucci Am., Inc. v. Hall & Assoc., 135 F. Supp. 2d 409, 410-11 (S.D.N.Y. 2001) (finding that the Telecommunications Act of 1996 did not protect the defendant ISP corporation from liability for copyright information for information posted on a Web site by the company which was using the ISP services). *But see* Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003) (finding a Web site host non-liable for sending out emails sent to a listserve maintained by one of its sites under the Communications Decency Act (CDA)); Carafano v. Metrosplash.com, 339 F.3d 1119 (9th Cir. 2003) ("[P]roviders of interactive computer services . . . and their users [are immunaized] from causes of action asserted by persons alleging harm caused by content provided by a third party."); Ben Ezra, Weinstein & Co. v. Am. Online, 206 F.3d 980, 984-85 (10th Cir. 2000), *cert. denied*, 531 U.S. 824 (2000) (declining to impose liability for the posting of incorrect stock data); Blumenthal v. Drudge, 992 F. Supp. 44, 49-53 (D.D.C. 1998) (holding AOL not liable for hosting the content of an independent contractor's news reports, despite a contract allowing AOL to edit or remove content); Gentry v. eBay, Inc., 99 Cal.App.4th 816, 830 (2002) ("immuniz[ing] providers of interactive computer services . . . and their users from causes of action asserted by persons alleging harm caused by content provided by a third party"); Kathleen R. v. City of Livermore, 87 Cal.App.4th 684, 692 (2001) (holding that the city was immune under CDA Section 230 for a city library that allowed online access to pornographic material); Doe v. Am. Online, 783 So.2d 1010, 1013-1017 (Fla. 2001), *cert. denied*, 122 S.Ct. 208 (2000).

[258] Communications Decency Act, 47 U.S.C. § 230(b)(2000). The Communications Decency Act conveys Congress' interest in protecting speech on the Internet in that:

rorism encounter in proving that a particular Web site or Internet posting proximately caused a party's injury.[259] Furthermore, monitoring Internet traffic remains voluntary for providers and there are few criminal or civil penalties for either ISPs or online criminal perpetrators under U.S. law.[260] Without the threat of civil liability or affirmative statutory duties to track and monitor Internet traffic and content on their hosted sites, it is unlikely that providers or Internet-related technology companies will invest in developing the technology and personnel necessary to make the Internet a more difficult place for cyber jihadists and other online criminals to operate.[261]

V. INTERNATIONAL RESPONSES TO CYBER JIHAD

Although many countries, particularly in Western Europe and North America, have instituted policies strengthening penalties for cyber terrorist attacks and providing additional resources for governments and private organizations to monitor online activity,[262] the fight against online Islamic extremist activities remains an *ad hoc* endeavor.[263] While national security experts have praised the efforts of the international community in addressing the cyber terrorism threat,[264] these observers fail to point out that the actions multi-lateral bodies have taken to bolster Internet security focus primarily on online copyright and trademark fraud, child pornography,

---

> [I]t is the policy of the United States: (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services.

[259] *See* Note, *Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm*, 119 HARV L. REV. 2442, 2460 (2006) (citing Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable,* in THE LAW AND ECONOMICS OF CYBERSECURITY 221, 221–58 (2006)).

[260] The exception is where an ISP maintains editorial control over the content of the site, or the ISP is repeatedly notified that a site is notorious for illicit content or traffic. In such instances, civil and/or criminal penalties may be imposed. *Gucci Am., Inc.*, 135 F. Supp. 2d, at 417.

[261] *See* Molnar, *supra* note 47, at 26, 29–30.

[262] *See* Johnson & Post, *supra* note 39.

[263] *See* Legal Framework–Unauthorized Access to Computer Systems, *supra* note 40.

[264] *See* Hinnen, *supra* note 105 (praising the efforts of the international community to combat cyber-terrorism threats by pointing to the Council of Europe's adoption of the Convention on Cybercrime and the G8 countries development of an integrated multi-national cyber-terrorist threat monitoring and response unit).

privacy issues, and offensive cyber attacks, while ignoring cyber jihad activities.[265]

A. Multi-Lateral Treaties

The Council of Europe's Convention on Cyber Crime treaty ("Cyber Crime treaty") is often cited as a success in terms of measurably improving global Internet security.[266] To date, forty-two countries, including the United States in November 2001, have signed the Cyber Crime treaty.[267] While the treaty did take significant steps to institutionalize mutual assistance exchanges between signatory countries investigating computer-related crime, it failed to address the threat of online terrorist planning activity.[268] The convention's provisions focus on cyber fraud, copyright violation, and child pornography issues.[269] Moreover, the treaty illustrates the shortcomings of multi-lateral regimes to respond quickly to emerging international threats. As of September 2006, only thirteen countries had ratified and integrated the convention into domestic laws.[270] After years of debate over privacy concerns regarding law enforcement investigative powers in the treaty,[271] the United States became the sixteenth country to ratify the convention on August 3, 2006.[272]

The Group of Eight ("G8") leading industrialized nations has also expanded international cooperation to combat computer crimes. [273] In 1996, the G8 issued twenty-five measures to address new terrorist threats, developed by the G8's new Counter-Terrorism Experts Group, known as the

---

[265] *See, e.g.*, Convention on Cybercrime, Council of Europe, Jan. 1, 2006, ETS No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[266] *See* Hinnen, *supra* note 105, at 10; Rick Perera, *Thirty Countries Sign Cybercrime Treaty*, IDG NEWS SERV., Nov. 23, 2001.

[267] *Senate Urged to Ratify Cybercrime Convention*, WASH. INTERNET DAILY, Dec. 13, 2005.

[268] *See* Perera, *supra* note 266*;* Convention on Cybercrime, *supra* note 265.

[269] Convention on Cybercrime, *supra* note 265.

[270] Convention on Cybercrime, Treaty Open for Signature, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (last visited Oct. 30, 2006).

[271] David Quainton, *Lobby Group Urges Ratification of Cybercrime Convention,* SC MAGAZINE, Jul. 1, 2005; Letter from Electronic Privacy Information Center (EPIC) to U.S. Sen. Richard G. Lugar, Chairman, Senate Foreign Relations Committee (Jul. 26, 2005) (opposing Senate ratification of the treaty due to privacy concerns relating to the broad investigative powers granted in the treaty).

[272] Council of Europe, Convention on Cybercrime art. 7-13, Nov. 23, 2001, S. TREATY DOC. NO. 108–11 (2006); Dan Kaplan, *Senate Ratification of Cybercrime Treaty Praised,* SC MAGAZINE, Aug. 4, 2006; Declan McCullagh, *Senate Ratifies Controversial Cybercrime Treaty,* CNET NEWS.COM, Aug. 4, 2006, http://news.com.com/2100-7348_3-6102354.html.

[273] G8 Presidency, http://www.g8.gov.uk/ (last visited Aug. 26, 2006).

Lyon Group.[274] The recommendations were designed to combat transnational terrorism and organized crime activities, including computer crime-related activities, in G8 countries.[275] Within the Lyon Group, the G8 maintains a Subgroup on High-Tech Crime, which has "promulgated principles and best practices regarding the prevention, investigation, and prosecution of computer crimes."[276] The Subgroup also maintains a rapid response team of computer crimes experts who are available 24 hours a day, 7 days a week, "to respond to computer crime emergencies."[277]

Unfortunately, the approaches taken by both the G8 and the Council of Europe to fighting cyber crime and bolstering Internet security fail to encompass strategies against cyber jihad. The G8 has taken a passive enforcement approach, encouraging its member states to implement voluntary best practices for service providers and provider associations to retain "identified categories of traffic data and/or subscriber data for legitimate business or public safety purposes . . . [and] ensure data protection legislation . . . [allowing] retention and preservation of data important for network security requirements or law enforcement investigations or prosecutions . . . ."[278]

In December 2005, the European Parliament took aggressive action in addressing the need to equip intelligence and law enforcement authorities with greater access to Internet data relating to cyber crime and cyber terrorism–related activities when it passed a directive to strengthen electronic data retention laws in E.U. member states.[279] The directive requires E.U. member states to implement national laws to retain electronic communications data for between six months and two years.[280] The retention directive covers a wide range of electronic data including Internet and e-mail user identifications, Internet and landline telephone numbers dialed, IP addresses, as well as the date and time of log-ins and log-offs, and international calling data for mobile cellular phone usage.[281] While Internet and telephone industry representatives were critical of the added burdens the directive places on companies to comply with the new regulations, E.U.

---

[274] G8 RECOMMENDATIONS ON COUNTER-TERRORISM, G8 Foreign Ministers' Meeting (2002).

[275] *Id.*

[276] *See* Hinnen, *supra* note 105, at 25 n.85 (citing G8 Justice and Interior Ministers, Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations, http://justicecanada.ca/en/news/g8/doc2.html).

[277] *Id.*

[278] *Id.*

[279] Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Electronic Communication Services and Amending Directive, EUR. PARL. DOC. (COM 438) (2005) [hereinafter Data Retention Directive]; Jo Best, *Europe Passes Tough New Data Retention Laws,* CNET NEWS.COM, Dec. 14, 2005, http://news.com.com/2100-7350_3-5995089.html.

[280] Data Retention Directive, *supra* note 279, Parts V–VI.

[281] *Id.* at art. 5(1).

member states were careful to craft language that balances the civil liberties and privacy interests of E.U. citizens with the need for greater access to electronic data for security purposes. The directive explicitly includes language that prohibits the storage of "data revealing the content of the communication . . . ."[282] While it is likely to take several years for E.U. member states to develop and implement their own national laws to comply with the directive,[283] the E.U.'s action is unquestionably a significant step in providing counterterrorism authorities the tools they need to prevent and deter cyber jihadists from exploiting the Internet as an operational theater.

B. The United Nations and the International Telecommunications Union

The U.N. has engaged the largest number of countries and private organizations in addressing the contemporary security challenges of the Internet. The U.N. has even conveyed its concerns regarding the growing cyber security threats in U.N. General Assembly Resolutions 57/239 (2003)[284] and 58/199 (2004).[285] Both resolutions promote the "creation of a global culture of cyber security and the protection of critical information infrastructure."[286]

The U.N. has also taken a leadership role in examining significant legal and policy issues related to the governance of the Internet. Many United Nations member states also have inserted themselves into Internet governance issues via the U.N. subsidiary International Telecommunications Union ("ITU").[287] Through the ITU, which is responsible for telecommunications regulatory and policy issues, the U.N. hosted two major international

---

[282] *Id.* at art. 5(2).

[283] *Id.* at art. 15(3) (allowing E.U. member states up to 36 months to comply with the Internet, e-mail and Internet telephony provisions of the directive).

[284] G.A. Res. 57/239, U.N. Doc. A/RES/57/239 (Jan. 31, 2003).

[285] G.A. Res. 58/199, U.N. Doc. A/RES/58/199 (Jan. 30, 2004).

[286] World Summit on the Information Society, Oct. 14, 2005, Hammamet Tunisia, *WSIS Thematic Meeting on Cybersecurity: Outcome and Next Steps (*prepared by Robert Shaw*)*, *available at* www.itu.int/osg/spu/presentations/2005/shaw-cybersecurity-gsr-14-nov-05.pdf [hereinafter *WSIS Thematic Meeting on Cybersecurity*].

[287] International Telecommunications Union, http://www.itu.int/aboutitu/overview/purposes.html (last visited Aug. 18, 2006). According to its Web site, the ITU:

> [w]as established last century as an impartial, international organization within which governments and the private sector could work together to coordinate the operation of telecommunication networks and services and advance the development of communications technology. Whilst the organization remains relatively unknown to the general public, ITU's work over more than one hundred years has helped create a global communications network which now integrates a huge range of technologies, yet remains one of the most reliable man-made systems ever developed.

Id.

conferences in 2003[288] and 2005[289] on transnational issues related to the durability, accessibility, and security of the Internet.[290] However, despite the pervasive attention in the world media to the growing threat of online terrorism-related activities, the U.N. has not specifically addressed the threat posed by terrorists' exploitation of the Internet for operational and planning purposes.

At the World Summit on the Information Society II in Tunis, Tunisia in December 2005,[291] for example, the agenda focused on expanding Internet access and information technology infrastructure to the developing world. The Summit's only reference to terrorism-related activity on the Internet was a statement of principle on the importance of countering terrorism on the Internet, buried as point 44 in the summit's 121 point agenda.[292]

---

[288] *Id*. World Summit on the Information Society, *First Phase*, Dec. 10–12, 2003, http://www.itu.int/wsis/geneva/index.html. The first World Summit on the Information Society (WSIS):

> [T]ook place in Geneva hosted by the Government of Switzerland from 10 to 12 December 2003. The objective of the first phase was to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake. At the Geneva Phase of WSIS nearly 50 Heads of state/government and Vice-Presidents, 82 Ministers, and 26 Vice-Ministers and Heads of delegation as well as high-level representatives from international organizations, private sector, and civil society provided political support to the WSIS Declaration of Principles and Plan of Action that were adopted on 12 December 2003. More than 11,000 participants from 175 countries attended the Summit and related events.

Id.

[289] World Summit on the Information Society, *Second Phase,* Nov. 16–18, 2005, http://www.itu.int/wsis/tunis/index.html [hereinafter Tunis Summit].

[290] The Tunis Summit participating states issued a proclamation which describes the agenda of ITU regarding Internet governance in the years to come. The Summit agreed that:

> We recognize that Internet governance, carried out according to the Geneva principles, is an essential element for a people-centred, inclusive, development-oriented and non-discriminatory Information Society. Furthermore, we commit ourselves to the stability and security of the Internet as a global facility and to ensuring the requisite legitimacy of its governance, based on the full participation of all stakeholders, from both developed and developing countries, within their respective roles and responsibilities.

World Summit On The Information Society, *Tunis Agenda For The Information Society*, ¶ 31, WSIS 05/Tunis/Doc/6(Rev.1)-E (Nov. 18, 2005) [hereinafter *Tunis Agenda For The Information Society*].

[291] The Tunis Summit was one of the largest gatherings ever held regarding policy issues relating to the Internet. It was attended by over 19,000 participants, senior officials from 174 countries, as well as 800 entities including UN agencies, private businesses, and civil society organizations. World Summit on the Information Society, Summit Newsroom–Tunis Phase, http://www.itu.int/wsis/tunis/newsroom/index.html (last visited Oct. 30, 2006).

[292] Tunis Summit, *supra* note 289. The inclusion of the terrorism-related language in the Statement of Principles was inserted at the last minute by conference participants reportedly due to the persistent urging of the Israeli Foreign Minister Silvan Shalom; *see* ITIC, Marketing of Terrorism on the Internet, http://www.intelligence.org.il/eng/eng_n/tunis_e.htm (last visited Aug. 26, 2006). The summit's pronouncement on combating cyber terrorism

Like the U.S. government, the ITU remains overly focused on implementing enforcement and prosecution strategies. In laying out a public policy framework of agreed upon principles for responding to cyber security threats, the ITU Tunis Conference participants emphasized international cooperation in investigating and prosecuting cyber crimes.[293] Instead, the summit participants could have used the opportunity to explore methods of prevention and interdiction of emerging and expanding cyber jihadist operations.[294]

Much of the substantive agenda at the Tunis Conference was overshadowed by the ongoing controversy regarding which organization or government(s) would control the administration and governance of the Internet.[295] During the conference, a number of participating states, including Brazil, Iran, China, Venezuela, Sudan, and the European Union, acting on fears that ICANN operates as a puppet of the U.S. government, sought to limit the powers and influence of ICANN.[296] This anti-ICANN coalition advocated for bolstering the clout and responsibilities of other multinational organizations, such as the ITU, which historically have been involved on the periphery of Internet policy-making issues, without the ability to wield any administrative or regulatory control.[297]

U.N. member states reached a compromise in late 2005, agreeing that "an international forum under U.N. auspices, will be set up to examine

---

stated: "We also underline the importance of countering terrorism in all its forms and manifestations on the Internet, while respecting human rights and in compliance with other obligations under international law . . . ." *Id.*

[293] Tunis Summit, *supra* note 289.

[294] The Tunis Summit stakeholders agreed in principle that:

> We seek to build confidence and security in the use of ICTs by strengthening the trust framework. We reaffirm the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cyber security, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks. This culture requires national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data. Continued development of the culture of cyber security should enhance access and trade and must take into account the level of social and economic development of each country and respect the development-oriented aspects of the . . . . We underline the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction but having effects in another. We further underline the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, inter alia, law enforcement agencies on cybercrime. We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks . . . .

Tunis Agenda For The Information Society, *supra* note 290, at ¶¶ 39–40.

[295] Rupert Cornwell, *US Wins Right to Keep Internet Control after Warning of Censorship*, FINAN. TIMES, Nov. 17, 2005.

[296] Tunis Summit, *supra* note 289.

[297] *Id.;* Bob Keefe, *Tug of War for Internet Goes Global,* ATLANTA J. CONST., Nov. 16, 2005, at A1; Ben Tanner, *U.S. Retains Domain Name Control*, DM ASIA, Nov. 17, 2005, *available at* http://www.digitalmediaasia.com/default.asp?ArticleID=11342.

Internet issues. But day-to-day management of the Internet will remain with the California-based ICANN."[298] Fortunately, the resolution of this controversy over the regulatory control of the Internet should permit policymakers and Internet governance experts to turn their attention and resources to significant administrative and governance challenges facing ICANN, including the rising threat of cyber jihad operations.

C. Internet Corporation for Assigned Names and Numbers ("ICANN")

In order to better understand the options for confronting the cyber jihad, it is important to examine the regulatory and administrative characteristics of ICANN, the primary organization responsible for governing the Internet.[299] Since 1998, when the U.S. government privatized it, the Internet has technically been governed by ICANN, a not-for-profit California-based corporation.[300]

The mission of ICANN is "to create an effective private sector policy development process capable of administrative and policy management of the Internet's naming and address systems."[301] ICANN, according to its mission, is intended to serve as a "more effective—more nimble . . . alternative to the traditional, pre-Internet model of a multinational government treaty organization."[302] According to ICANN's official bylaws, the organization's core values include the responsibility for "preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet."[303]

The ICANN Web site indicates that the organization is responsible for:

---

[298] Cornwell, *supra* note 295.

[299] ICANN, http://www.icann.org (last visited Nov. 15, 2006).

[300] Milton Mueller, *ICANN and Internet Governance: Sorting through the debris of 'self-regulation,'* 1 J. OF POL'Y REG. & STRAT. FOR TELECOMM. INFO. AND MEDIA 497, 498 (1999) (providing a history of the development of the ICANN organization).

[301] ICANN, ICANN President's Report, The Case for Reform, Feb. 24 2002, http://www.icann.org/general/lynn-reform-proposal-24feb02.htm.

[302] *Id.* Ironically, the focus on private control of the Internet resulted from the intervention of the Clinton Administration's Commerce Department in the debate surrounding the governance at a crucial time in the mid-1990s when the Internet was experiencing explosive growth and innovation. At a U.S. Congressional hearing on governance of the Internet, Larry Irving, then Assistant Secretary of Commerce and whose responsibilities included overseeing the administration of the Internet, told Congress that "[t]he private sector, with input from governments, should develop stable, consensus-based self-governing mechanisms for domain name registration and management that adequately defines responsibilities and maintains accountability." *Internet Domain Names Part I: Hearing* Before the H. Comm. on Sci., *Subcomm. on Basic Research,* 105th Cong. 4 (1997) (statement of Larry Irving, Asst. Sec. of Commerce for Commc'n and Info.). Irving also emphasized that "self governance mechanisms should recognize the inherently global nature of the Internet." *Id.*

[303] ICANN, Bylaws for Internet Corporation for Assigned Names and Numbers, http://www.icann.org/general/bylaws.htm#I (last visited Oct. 30 2006).

> [m]anaging and coordinating the Domain Name System (DNS) to ensure that ever address is unique and that all users of the Internet can find all valid addresses. It does this by overseeing the distribution of unique IP addresses and domain names. It also ensures that each domain name maps to the correct IP address. ICANN is also responsible for accrediting the domain name registrars. "Accredit" means to identify and set minimum standards for the performance of registration functions, to recognize persons or entities meeting those standards, and to enter into an accreditation agreement that sets forth the rules and procedures applicable to the provision of Registrar Services.[304]

As such, ICANN's regulatory authority over the DNS system "provides the control point from which to regulate users."[305] Because of its centralized control over the DNS system, Klein emphasizes that "ICANN realizes the governance potential in DNS, [by] leveraging Internet addressing to achieve global governance."[306] In fact, Klein suggests that ICANN is appropriately equipped to handle a wide array of regulatory challenges, including security-related initiatives.

At its core, ICANN is partially responsible for operating the thirteen root servers, ten of which are located in the United States, which drive the Internet.[307] In addition, ICANN governs the hosting and distribution of domain names through a "web of top-down contracts"[308] that specify the terms of the registrar or domain name holder contracts.[309]

According the Hans Klein, ICANN has taken on the following array of administrative and policy-making functions:

> ICANN defined and enforced new forms of intellectual property in Internet domain names, it regulated market entry and set prices in relevant industries, and it possessed (but did not immediately exercise) the awesome power to disconnect entire country domains from the Internet. With widespread recognition of its policy role came growing calls for a restructuring of ICANN to endow it with a degree of legitimacy appropriate to its powers.[310]

---

[304] ICANN, Frequently Asked Questions, http://www.icann.org/faq (last visited Oct. 30, 2006).

[305] Hans Klein, *ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy*, 18 INF. SOC'Y 193, 195 (2002).

[306] *Id.* at 201.

[307] Wolfgang Kleinwoechter, *From Self-Governance to Public-Private Partnership: The Changing Role of Governments in the Management of the Internet's Core Resources,* 36 LOY. L.A. L. REV. 1103, 1123 (2003).

[308] *See*, Jonathan Weinberg, *Backgrounder: ICANN and Internet Governance* (adapted from JONATHAN WEINBERG, INTERNET GOVERNANCE, TRANSNAT'L CYBERSPACE L. (2000)), http://www.law.wayne.edu/weinberg/mdrbackgrounder.pdf.

[309] "ICANN's power over domain name registration (and through it, possibly other aspects of Internet activity) ultimately derives from its ability to maintain the obedience of operators of top-level domain name root servers, which sit on top of a pyramid of servers that record and track Internet domain names . . . [and] enable Internet users to find and get access to Web sites or to send e-mail."
Id.

[310] HANS KLEIN, SOC. SCI. RES. CONS. INFO. TECH. & INT'L COOPERATION PROGRAM, RESPONSE PAPER 3: LEGITIMACY AND GLOBAL INTERNET GOVERNANCE (2004), *available at* www.ssrc.org/programs/itic/publications/knowledge_report/memos/kleinmemo3.pdf.

Despite ICANN's effectiveness in some administration areas, a number of experts argue that it is impossible for ICANN "to be all things to all people—simultaneously private and public, international and local, policymaking and a mere facilitator of technical management."[311] Critics question the efficacy of preserving the ICANN organization as the preeminent Internet governance organizations given its broad-ranging responsibilities, limited resources, and lingering ties to the U.S. government.[312]

In order to overcome hurdles to gaining more institutional legitimacy, ICANN must explicitly delineate the role of governments and other organizations in its regulatory process. Since 2002, the role of national governments in the administration and development of ICANN has been strengthened. ICANN struggled in its first few years to overcome a legitimacy gap; this was due in large part to its limited funding and lack of cooperation from governments that participated on ICANN's Government Advisory Committee.

Recently, ICANN regulators have taken note of rising threats to the "stability" and "security" of the Internet posed by the growing number of cyber jihadists and online criminals. Due in part to reform pressures from Internet governance experts and national governments, ICANN has begun to address the issues of prevention and accessibility. For example, ICANN established a Security and Advisory Committee ("SAC") tasked with tracking and resolving security threats to the naming and address system of the Internet.[313] Unfortunately, the SAC's purview does not specifically

---

[311] Weinberg, *supra* note 308, at 1.

[312] *See* Michael Froomkin, *ICANN 2.0: Meet the New Boss*, 36 LOY. L.A. L. REV. 1087, 1092, 1101 (2003); Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution,* 50 DUKE L.J. 17, 18–22 (2000); *see also* ICANN Watch, http://www.icannwatch.org/ (last visited Oct. 30, 2006).

[313] *See* ICANN Security Committee Charter, http://www.icann.org/committees/security/charter-14mar02.htm (last visited Aug. 27, 2006). The bylaws lay out the following responsibilities for the Special Advisory Committee:

> (1) To develop a security framework for Internet naming and address allocation services that defines the key focus areas, and identifies where the responsibilities for each area lie. The committee will focus on the operational considerations of critical naming infrastructure; (2) To communicate on security matters with the Internet technical community and the operators and managers of critical DNS infrastructure services, to include the root name server operator community, the top-level domain registries and registrars, the operators of the reverse delegation trees such as in-addr.arpa and ip6.arpa, and others as events and developments dictate. The Committee will gather and articulate requirements to offer to those engaged in technical revision of the protocols related to DNS and address allocation and those engaged in operations planning; (3) To engage in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and to advise the ICANN community accordingly. The Committee will recommend any necessary audit activity to assess the current status of DNS and address allocation security in relation to identified risks and threats.

Id.

include security initiatives relating to cyber jihadists and other online criminals, which would empower ICANN to address cyber terrorism-related issues.

In 2005 and 2006, ICANN also sponsored a reform taskforce to examine systemic problems in the WhoIs Web site address verification system.[314] The investigation uncovered the persistent failure of ICANN and its local providers to require accurate recording of site holders' identifier information on the WhoIs site, as well as the pervasive misrepresentations of information posted by WhoIs registrants.[315] Such issues in the WhoIs database can critically hinder investigative efforts to pursue cyber wrongdoers.

In order to successfully pursue a reform agenda, ICANN must further solidify its role as the primary regulator and administrator of the Internet. Noted Internet governance experts have recommended a multi-faceted approach to reform that would broadly enhance the ability of ICANN to carry out its mission, while retaining it as the primary organization for regulation of the Internet.[316] In a paper prepared for the World Summit on the Information Society in November 2005, Professor Klein recommended action to enhance the legitimacy and efficacy of ICANN:

> Political Authorization: A legitimate political authority (presumably an international body) should formalize the delegation of regulatory powers to ICANN; Legislative Mandate: That same political authority should spell out and delimit ICANN's mandate. This should be codified in an international legal instrument; Internal Processes: ICANN's system of stakeholder representation and decision-making should be reviewed for fairness and efficiency. Internal procedures should be clearly specified in a legal instrument, most likely its corporate charter and bylaws; Judicial Review: Mechanisms should be created by which ICANN's regulatory decisions can be appealed to higher authority. Any appellate body should have the power to enforce its decisions; and Political Oversight: The legitimate political authority described above should periodically review ICANN's actions and mandate. Political oversight should itself be highly constrained in order to insulate ICANN from political pressures.[317]

---

[314] "The purpose of WhoIs is to provide to third parties an accurate and authoritative link between a domain name and a responsible party who can either act to resolve, or reliably pass information to those who can resolve, technical problems associated with or caused by the domain." PRELIMINARY TASK FORCE REPORT ON THE PURPOSE OF WHOIS AND OF THE WHOIS CONTACTS, WHOIS TASK FORCE, GENERIC NAMES SUPPORTING ORGANIZATION, ICANN (2006), http://gnso.icann.org/issues/whois-privacy/prelim-tf-rpt-18jan06.pdf. In its preliminary taskforce report, ICANN notes that the taskforce was formed in an effort to fulfill its obligations in protecting the core values of the Internet including the security and stability of the Internet. *Id.*

[315] *Id.*

[316] *See generally* HANS KLEIN, ICANN REFORM: ESTABLISHING THE RULE OF LAW, INTERNET & PUBLIC POLICY PROJECT (2005) [hereinafter ICANN REFORM: ESTABLISHING THE RULE OF LAW], *available at* http://www.internetgovernance.org/pdf/ICANN-Reform-Establishing-the-Rule-of-Law.pdf.

[317] *Id.*

Professor Klein's recommendations provide a substantial foundation from which ICANN can build an effective organization that is empowered to address the long-term cyber jihad threat.

VI. PRINCIPLES FOR A CYBER VICTORY

While Internet governance stakeholders continue to debate the characteristics of an emerging Internet governance regime, experts have failed to keep up with the ever-intensifying threats facing the Internet. While many experts have focused their energies and analysis on macro-level issues, such as forming sustainable Internet governance institutions, serious attention to a number of vital Internet security issues has been lacking in the Internet governance literature. Without greater debate and innovative policy responses to these challenges, the visionaries of the Internet will be prevented from creating an "enduring global architecture" of innovation, security, and sustainability on the Internet.[318] To fill some of the gaps in the literature on the cyber jihad, it is important to identify, describe, and evaluate a number of principles and tactics central to mitigating the threat posed by cyber jihadist activities.

Five core mutually-reinforcing principles based on Professor Klein's ICANN reform recommendations should guide Internet policymakers in addressing the cyber jihad threat and formulating strategic responses: authority and legitimacy; enforcement and normalization; verifiability; flexibility; and balance of security and liberty interests.[319]

A. Authority and Legitimacy

In order to take aggressive action against the cyber jihad, ICANN needs to gain the legitimate authority to debate, develop, and implement bold new policies.[320] The Internet governing body needs cooperation from an array of public and private stakeholders who will continue to be involved in the Internet policy-making process.[321] Legitimacy must be viewed within the context of power and authority.[322] As Professor Klein argues, "[p]ower is the ability to realize one's intentions . . . . Relative to public policy, [legitimacy] usually refers to the exercise of power over societal entities, [such as] people, organizations, or nation-states. Authority is power en-

---

[318] *WSIS Thematic Meeting on Cybersecurity*, *supra* note 286.

[319] *See* ICANN REFORM: ESTABLISHING THE RULE OF LAW, *supra* note 316; *supra* accompanying text Part IV.A.

[320] Benedict Kingsbury et al., *The Emergence of Global Administrative Law*, 68 LAW & CONTEMP. PROBS. 15, 22–24 (2005).

[321] *See* ICANN REFORM: ESTABLISHING THE RULE OF LAW, *supra* note 316.

[322] *Id.* at 2.

dowed with legitimacy."[323] Without this requisite legitimacy, ICANN became bogged down in battles over process and control that fundamentally limited the organization's ability to implement its vision for the future of the Internet.[324] Now that Internet regulatory stakeholders have resolved the major dispute regarding ICANN's administrative control of the Internet at the Tunis Conference in late 2005,[325] ICANN should be able to develop and preserve its institutional legitimacy in asserting full administrative and regulatory enforcement control over the Internet.

B. Enforcement and Normalization

The Internet community's "strongest method of enforcement is expulsion."[326] To date, true normalization of Internet activity by expelling bad actors has been all but abandoned by Internet policymakers on the national and international organization levels. The existing rules, regulations, laws, and contracts related to online terrorism-related activities are insufficient and rarely, if ever, enforced.[327] As a result, normalization of the Internet further erodes while criminals and terrorists continue to push the envelope of illicit online activities.[328] Until more stringent enforcement of Internet regulations is achieved, greater security against cyber jihadist threats will be unobtainable.

Once ICANN is truly granted the authority to develop and implement effective policies, it will be able to enact and enforce aggressive and innovative Internet security measures. The organization's ability to enforce laws and rules will lead to the normalization of Internet activities and the exclusion of nefarious elements, such as cyber jihadists, from the Internet. Once ICANN's ability to regulate and normalize the scope of permissible activities on the Internet increases, clearer legal and ethical standards of conduct in cyberspace will emerge. Standardization of behavioral norms throughout the Internet community will increasingly support ICANN in the expulsion of rogue users from that community so that "there is no longer any place [for cyber jihadists] to run to anymore, in which case enforcement, at least in theory, has attained its outer limit."[329]

---

[323] Hans Klein, Working with the Resources at Hand: Constraints on Internet Institutional Design, 9 J. MEDIA & CULTURAL STUD. 403, 404 (2004).

[324] *See infra* Part IV (describing the ongoing disputes between ICANN and its stakeholders for administrative and regulatory control over the Internet).

[325] *See generally* Tunis Summit, *supra* note 289.

[326] Viktor Mayer-Schonberger, *The Shape of Governance: Analyzing the World of Internet Regulation*, 43 VA. J. INT'L. L. 605, 633 (2003).

[327] *Id.*

[328] *See* Aron Mefford, *Lex Informatica: Foundations of Law on the Internet,* 5 IND. J. GLOBAL LEGAL STUD. 211, 212–13 (1997).

[329] *Mayer-Schonberger, supra* note 326, at 634.

C. Verifiability

Legitimate authority empowering decision-makers to produce sound and enforceable policy in a normalized Internet community is rooted in accurate and verifiable information about the individuals and organizations which constitute the users and ISPs.[330] A major difficulty in investigating and enforcing the rules of the Internet is verifying the registration information provided at Internet entry points, such as ISPs or registrar sites.[331] Although this information is explicitly required by ICANN rules, the enforcement of the rules to date has been lax.[332] As a result, law enforcement has no quick, reliable way of identifying parties responsible for Web sites.[333] The failure to ensure accurate and verifiable registration information undermines the legitimate authority of the entire Internet regulatory regime to investigate illicit uses of the Internet and to impose penalties.

D. Flexibility

In order to implement enforceable security policies aimed at eliminating the cyber jihad threat, ICANN must improve responsiveness to the rapidly-emerging innovations and challenges of the Internet. In order to attain the delicate mixture of legitimacy through verifiability, normalization, and flexibility, Internet policymakers need to approach solving the Internet security problems with balance, effectively weighing the needs and interests of the multitude of existing and future Internet stakeholders.

---

[330] Molnar, *supra* note 47, at 29–45.

[331] *Id.* at 30.

[332] *See* ICANN, WHOIS RECOMMENDATION OF THE SECURITY AND STABILITY ADVISORY COMMITTEE (2003), *available at* www.icann.org/committees/security/whois-recommendation-01dec02.pdf.

[333] *See id.* The report explains that:

> [T]he accuracy of Whois data used to provide contact information for the party responsible for an Internet resource must be improved, both at the time of its initial registration and at regular intervals. Whois records known to be false or inaccurate must be frozen or held until they can be updated or removed. Whois records that have information that can not be validated may be frozen or held until it can be verified . . . There are two principal reasons to maintain accurate contact information in Whois records: technical and legal. The technical rationale is that if there are problems with or abuse originating from a resource (e.g., a domain name, route, or IP address) the Whois entry for the resource is the only source for finding the responsible party. For legal problems accurate postal addresses are required for serving court papers to the responsible party.

Id.

E. Balancing Security and Liberty

Balancing the needs of regulation and security with the Internet's driving forces of innovation and the free flow of information is one of the great policy challenges of our time. However, "a regulation need not be absolutely effective to be sufficiently effective. It need not raise the cost of the prohibited activity to infinity in order to reduce the level of that activity quite substantially."[334] Thus, a balance should be sought in which the risks and costs of illicit behavior are dramatically reduced without impinging upon the freedom to conduct legal and beneficial activities on the Internet.[335]

VII. NEW TOOLS FOR WINNING THE WAR AGAINST THE CYBER JIHAD

As Internet policymakers and vested stakeholders take aim at combating the cyber jihad, key policy thinkers and decision-makers must develop a new set of regulatory tools and tactics that incorporate the principles outlined above. Not all of the following tactical recommendations for combating cyber jihadism are entirely new concepts or ideas to Internet regulators. But by adopting, implementing, and enforcing these policy and legal instruments, Internet regulators will begin to build a sustainable and enduring Internet governance architecture for future generations.

There are seven core legal and tactical tools which ICANN policymakers and other regulators should consider and implement in combating cyber jihadism: (1) identify and explicitly define what activities on the Internet are prohibited and punishable by ICANN; (2) require greater Internet registration disclosure and verification requirements akin to a user identification number for the Internet; (3) require ISPs and other providers to store user traffic data on a rolling basis for ten day intervals; (4) establish a centralized monitoring and enforcement section at ICANN to track illicit Internet activities; (5) create an Internet sanctions blacklist of banned users, providers and computers which are associated with illicit online criminal activity; (6) impose civil negligence fines and liability for providers who fail to monitor and enforce content restrictions; (7) develop and sustain sufficient

---

[334] Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1405 (1996). Professor Lessig argues that:

> [I]f regulation increases the cost of access to this kind of information, it will reduce access to this information, even if it doesn't reduce it to zero . . . If government regulation had to show that it was perfect before it was justified, then indeed there would be little regulation of cyberspace, or of real space either. But regulation, whether for the good or the bad, has a lower burden to meet.

Id.

[335] *Id.*

public and private funding and technology sources for building and protecting the Internet of the future.

A. Establish Universal Standards for Illicit Internet Activities

Any effort to improve the security and oversight of the Internet must begin with the collaboration of Internet regulators, mainly ICANN and the ITU, to develop common, universal definitions of prohibited online activities.[336] To date, neither the ITU nor ICANN have developed clear, accessible standards for prohibited Internet activities.[337] ICANN has deferred the standardization of Internet activities to local ISPs, who generally include in customer contracts language about permissible and prohibited Internet activities.[338] However, the issuance and enforcement of these standards pri-

---

[336] Now that the international community has reached a compromise agreement on the administrative control over the Internet and has preserved ICANN's administrative authority over the Internet, it should be more feasible for ICANN and ITU to build consensus on matters of substantive importance, as there is no longer a larger conflict regarding overall control of the Internet. Yet, substantial antipathy remains between the ITU and ICANN which must be overcome before substantive cooperation can take place. Id. But see E-mail from Michael Froomkin, Professor of Law, University of Miami School of Law, Benjamin R. Davis (Mar. 24, 2006, 21:38:45 EST) (on file with author). Professor Froomkin responded to the suggestion that ITU and ICANN will cooperate on policy reforms as a "pipe dream . . . seeing as they hate and fear each other." Id.

[337] *See* Amended Bylaws for Internet Corporate for Assigned Names and Numbers (Apr. 8, 2005); *World Summit on the Info. Soc, Geneva, Switzerland, Dec. 12, 2003, Declaration of Principles: Building the Info. Soc.: A Global Challenge in the New Millennium, Int'l Telecomm. Union*, WSIS-03/Geneva/Doc/4-E, ¶ 44, available at http://www.itu.int/wsis/index.html (under "WSIS Outcome Documents," select "Geneva Declaration of Principles" hyperlink, then select document according to preferred language and format); *Golden Book: Stakeholder Commitments And Initiatives, Second World Summit On The Info. Soc., International Telecomm. Union*, Tunis, Tunisia, Feb. 24, 2006.

[338] *See* Yahoo Terms of Service, ¶ 6 Member Conduct, http://uk.docs.yahoo.com/info/terms.html. The Yahoo Terms of Service stipulate that the user agrees:

> Yahoo may access, preserve, and disclose your account information and Content: (a) to its affiliated companies worldwide for the purpose of providing the Content to you in an efficient manner; (b) for the purpose of properly administering your account in accordance with the standard operating procedures of Yahoo or its affiliated companies; and (c) if required to do so by law or in the good faith belief that any such access, preservation or disclosure is reasonably necessary to: (i) comply with legal process; (ii) enforce the TOS; (iii) respond to claims that any Content violates the rights of third-parties; (iv) respond to your requests for customer service; or (v) protect the rights, property, or personal safety of Yahoo, its users and the public.

Id.; *see also* Molnar, *supra* note 47, at 26 (noting how registrars do not conduct any background checks, nor assumed any responsibility or liability due to customer's registration containing false or improper contact information despite being specifically required by ICANN accreditation rules to assure accurate registrant information); ICANN Registrar Accreditation Agreement, ¶ 3.7.8, http://www.icann.org/registrars/ra-agreement-17may01.htm.

marily have been undertaken by providers on a voluntary basis.[339] As a result, providers and Internet users have had virtually no incentive to comply with any existing contractual obligations regarding user conduct, having faced practically no repercussions for noncompliance.[340]

1. Define Prohibited Internet Activities

ICANN must work with its stakeholders to implement a standardized and legally-binding definition of prohibited Internet practices that can be referenced by both providers and users. In developing standardized language with public and private stakeholders, ICANN should assert its legitimate regulatory authority and articulate these standards for adoption by the legal systems of individual countries. The standardization of regulatory authority on the international level would enable more effective investigation and prosecution of Internet crimes and end the balkanization of national Internet regulations.

Key definitional language could address: activity related to the planning or coordination of a violent act;[341] "crimes against persons and related extortion that are of international significance;"[342] and support, solicitation, or provision of any and all types of assistance to U.N. 1267 Committee-listed terrorist individuals, groups, or affiliated entities.[343]

2. Establish Universal Internet User and Provider Contracts

The legal legitimacy and binding nature of these standards should be further enhanced by including the language in universally-recognized user contracts drafted and distributed by ICANN.[344] These contracts could be distributed for use by Web site hosts as well as service providers and users.[345] While the suggested language would certainly require subsequent additions and amendments, it is vital that the Internet regulators establish a common regulatory baseline. Most importantly, by establishing explicit definitions for prohibited Internet activities that are binding on all Internet providers and users, Internet regulators around the world would have the ability to hold complicit parties accountable for non-compliance with ICANN security regulations.

---

339 *See* Molnar, *supra* note 47.

340 *Id.*

341 *See generally* Thomas, *supra* note 25.

342 Organization of American States Convention on Terrorism, Convention to Prevent and Punish the Acts of Terrorism Taking the Form of Crimes Against Persons and Related Extortion that are of International Significance, Feb. 2, 1971, O.A.S.T.S. No. 24,381.

343 S.C. Res. 1267, *supra* note 3.

344 *See* Nackley, *supra* note 256, at 22–24 (proposing the introduction and distribution of a uniform registrar and ISP contract).

345 *Id.* at 12.

B. Surfing with Our Eyes Wide Open: Increasing Registration Disclosure

In order to reverse intensifying cyber lawlessness, regulators must establish, implement, and enforce realistic registration disclosure and verification mechanisms to reveal the true personal identity or organizational affiliation of an Internet user. While ICANN has addressed a number of the problems with its cyber registration regime through the ongoing Taskforce on the Purpose of WhoIs and of the WhoIs Contacts,[346] the organization must be more responsive to the registration concerns in the Internet community.

1. Establish a Universal Internet User Identification Program

To enhance the ability of providers and investigative authorities to identify cyber jihadists, ICANN regulators could create an Internet user ID system that requires a unique identification number for each individual upon completion of a brief registration process by an applicant. A prospective or existing Internet user could be required to electronically submit copies of some form of unique identifier information or two forms of photo identification to ICANN which would then process the request electronically. The user would then be provided with a unique log-on credential, which would enable the user to sign-on to the Internet with minimal delay or hassle, while greatly enhancing the ability of monitors and enforcement authorities to identify particular illicit online users. The only change from the present Internet environment would be that the illicit user's activities would then be traceable wherever that individual chose to visit online—whether a user visited a terrorist Web site, a jihadist chat room, or a company's hijacked Web site that contains terrorist training and operational materials.[347] The program would permit ISPs and investigators to reference another layer of identification information, in addition to the user's IP ad-

[346] ICANN, PRELIMINARY TASK FORCE REPORT ON THE PURPOSE OF WHOIS AND OF THE WHOIS CONTACT (2006), *available at* http://gnso.icann.org/issues/whois-privacy/prelim-tf-rpt-18jan06.htm.

[347] An earlier proposal by ICANN's Domain Name Supporting Organization (DNSO) presents a slightly different remedy for the online registration crisis in proposing a registration site with tiered levels of access. The tiered information system would enable registrars and ISPs to access additional registration data on a registered user while protecting a user's privacy interests against data and identity theft. ICANN, ICANN GENERIC NAMES SUPPORTING ORGANIZATION COUNCIL, TASK FORCE 3, IMPROVE THE ACCURACY OF DATA COLLECTED FROM GTLD REGISTRANTS PRELIMINARY REPORT 6 (2004) *available at* http://gnso.icann.org/issues/whois-privacy/TF3PreliminaryWithRCMR1.pdf. Critics of a user ID would likely argue that the user ID could easily be forged and would fail to bolster transparency on the Internet. *Id.* at 8. Requiring multiple forms of photographic identification is designed to make document forgery more difficult.

dress, and would likely expedite investigator's ability to pinpoint the individual's online operating location.[348]

A user ID system would not completely guard against fraud and misrepresentation; thousands of users would undoubtedly continue to find ways to falsify their identification information. But a user ID system would increase the challenges and risks for illicit users of the Internet while simultaneously adding to the virtual "paper trail."[349] Additional identification information made available to providers and investigative authorities could present a substantial deterrent to many existing illicit Internet users who would no longer be able to hide behind public Internet portals at cyber cafes or libraries.[350]

2. Need for Outside Support for Database of User Identifications

Implementing a user ID system could require ICANN, ISPs, and software developers to collaborate in developing a universal sign-on page to the Internet where the user would simply enter his ID number. An ID system would also require that governments signal their support for the initiative and possibly provide partial funding for the development of the requisite software and database technologies. The success of this and other security reform proposals will rely to a great extent on the ability of ICANN to solidify government and private industry support for the initiative.

To appease critics concerned about the civil liberty concerns associated with requirements for a user ID, the user identification number would not disclose the user's identity to anyone but the ISP and the centralized Internet regulatory body—most likely ICANN. Therefore, the disclosure of the information would pose little risk to users who feared that the information could be exploited by identity thieves or other online predators.

In addition, many Internet users are already required to disclose personal information in order to establish access accounts with providers. Users are often required to consent to limited disclosure of their online activities to affiliated ISPs and e-mail providers. In everyday life, individuals are required to possess identification to conduct numerous mundane activities such as driving a car, checking their bank account balances, and entering their places of work.[351] It is not unreasonable, therefore, to suggest that

---

[348] *Id.*

[349] *See* Lessig, *supra* note 334, at 1405.

[350] *See supra* Part I (describing how September 11th hijacker and plot ringleader Mohammed Atta was observed by multiple witnesses using the Internet at computer terminals in public libraries in south Florida in the weeks prior to the September 11th attacks).

[351] *See* SCOTT LEDERER ET AL., MANAGING PERSONAL INFORMATION DISCLOSURE IN UBIQUITOUS COMPUTING ENVIRONMENTS (2003), *available at* http://www.eecs.berkeley.edu/Pubs/TechRpts/2003/CSD-03-1257.pdf. This article argues that: "the emergence of a global heterogeneous real-time database composed of people,

users be required to disclose a unique identifying number in order to allow Internet regulators to track the user's activities should the need for an investigation be triggered.

C. Require ISPs and Other Providers to Store User Traffic Data for a Longer Period

Although the U.S. domestic ISP industry has signaled that it is open to assuming greater responsibilities in Internet monitoring,[352] particularly relating to cyber pornography issues, there has been little legal action outside of Europe to enhance the duties of ISPs to track and store content and activity records of individual Internet users.[353] The laws that have been implemented are watered down to the point of being ineffectual. For instance, the PATRIOT Act focuses on providing liability immunity for providers should they voluntarily choose to monitor the activity of suspected illicit users and voluntarily disclose this information to law enforcement officials.[354] These and other policy reforms subsequent to September 11th have been enforcement-focused, rather than prevention-oriented measures. ICANN and its stakeholders must develop and implement access prevention measures which enable providers and regulators to quickly identify and track users who perpetrate online jihad activities.

While many policymakers and Internet industry stakeholders have publicly opposed any proposals requiring ISPs to store user data for any substantial period of time due to cost and privacy concerns,[355] a number of providers have already implemented aggressive user tracking and data storage technologies. For example, AOL has maintained a program for years that closely monitors the activities of its account holders. Once a violation has been identified and the user information is verified, AOL contacts the user and places the user on notice regarding the prohibited nature of the conduct in question.[356] After a predetermined number of violations, the account is closed and the user is barred from establishing a new AOL account. There is little reason to believe that similar types of user

---

places, and things instead of records, tables, and fields, whereby any party with proper permissions can access one's personal information in real-time." *Id.*

[352] *See* Smith Testimony, *supra* note 230.

[353] *See* Molnar, *supra* note 47.

[354] Pub. L. No. 107-56, 115 Stat. 272 (2001); *s*ee also discussion on the limitations of the PATRIOT Act, *supra* Part IV.A.

[355] *See* Molnar, *supra* note 47, at 35 ("domain name registrars worry about [the] cost and time required to implement better verification procedures; commercial, business and non-profit organizations fear a diminishing right to privacy . . . .")

[356] AOL Safety and Security Center, http://daol.aol.com/safetycenter (last visited Oct. 30, 2006).

tracking and data storage technologies cannot be utilized by other providers and Web hosts.[357]

As discussed above, U.S. law already requires ISPs to retain data for up to ninety days upon government request. The Congress could follow the European Union's lead and expand electronic data retention requirements to one to two years. The aggressive data retention policy passed by the European Parliament in late 2005 could provide a model for an international standard for Internet data storage.[358] Although the total amount of data stored by ISPs would significantly increase, ICANN or other stakeholders within the regulatory system could develop a common technology that could be distributed to providers for a small fee. By providing a universally-applied technology, the type and character of data stored would be very similar, regardless of the locality or size of the provider or host. Data standardization would allow more efficient and productive investigations by law enforcement around the world.

D. Establish a Centralized Monitoring and Enforcement Section at ICANN to Track Illicit Internet Activities

In order to further substantiate its international regulatory and enforcement legitimacy, ICANN could establish a centralized monitoring and enforcement division. This division could track online activities and identify illicit operations and threat nodes that require immediate enforcement action. While ICANN is empowered to take regulatory enforcement action against providers and hosts, it has declined to take any measurable action against non-compliant providers to date.[359] This failure to act may be due in part to the organization's lack of enforcement authority to actually track online activities and identify compliance failures which require enforcement actions.

Despite damage done to its legitimacy due to its failure to implement and enforce its own regulations, ICANN is uniquely positioned to carry out investigative and enforcement actions against illicit online actors. As the

---

[357] *Id.*

[358] On December 14, 2005, the European Union passed the Internet Data Retention Directive which requires that relevant Internet data must be retained for between six months and two years, depending on the domestic laws of the member state. *See* Sara Dethridge, *Industry Has Doubts over Data Retention Directive: A Real Tool Against Terror?,* COMPUTER WKLY., Mar. 14, 2006. The directive

> requires companies to keep a wide range of data such as incoming and outgoing phone numbers, the duration of phone calls, IP addresses that identify log-in and log-off times and e-mail activity details . . . will be made available to law enforcement agencies for the investigation, detection, and prosecution of "serious crimes."

Id.

[359] Molnar, *supra* note 47, at 32 (describing how ICANN has threatened to shut down only one registrar for negligently failing to enforce Internet registration policies).

primary guardian of the Internet's root servers, it has the ability to track and shut down illicit providers, domains, and individual users. Much of ICANN's core activity and duties in its early years has been focused on establishing clearer lines of governing responsibility and maintaining the site registration and accreditation system. As a result, the security dimension of ICANN's mission has suffered from neglect at a period in time when cyber security continues to be a significant issue of concern.[360]

To launch an investigation and enforcement arm, ICANN could consult with regional partnership organizations such as the G8's Lyon Group.[361] The multi-national G8 initiative is well-equipped to address these issues, as it includes a European-based team of cyber investigators and an around-the-clock response center to act on tips and emerging cyber threats.[362] However, ICANN should eventually establish its own unit to exercise similar capabilities over the entire Internet community in order to solidify its long-term institutional legitimacy.

E. Naming and Shaming: Blacklisting the Perpetrators of Online Crimes

In conjunction with ICANN's efforts to establish preventive mechanisms that make it more difficult for cyber jihadists and other criminals to exploit the Internet, it is equally important that the organization create new enforcement mechanisms to raise the costs for cyber jihadists conducting illegal business online, thereby deterring future illicit cyber activities.

One of the easiest and most cost-effective ways to punish and deter wrongdoers is to name and shame individuals and organizations that are banned from partaking in a particular activity. ICANN can implement this strategy by creating a consolidated blacklist of individuals and entities banned from using, benefiting, or profiting from the Internet. Publication of a list of banned users, providers, and registrars would alert ICANN stakeholders, the media, law enforcement officials, and the general public to the named *persona non grata* on the Web. This concept is modeled on the targeted terrorism sanctions regimes of the United Nations[363] and the United States, in which the assets of designated individuals are frozen and the individuals or groups are publicly declared to be supporters of terrorism. [364] The U.S. has had substantial success in creating public sanction

---

[360] *See International,* WASH. INTERNET DAILY, Oct. 6, 2005; *Business First*, THE AUSTRALIAN, July 26, 2005; *Question is Whether Attacks Will Strengthen or Hobble ICANN*, WASH. INTERNET DAILY, Sept. 24, 2001.

[361] Hinnen, *supra* note 105, at 10.

[362] Communiqué, Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, Russia, Oct. 19–20, 1999, *available at* http://www.mofa.go.jp/policy/i_crime/high_tec/conf9910.html.

[363] S.C. Res. 1267, *supra* note 3.

[364] Exec. Order No. 12,334, 31 C.F.R. § 591 (2000).

lists of individuals and entities designated as terrorists, drug traffickers, and proliferators of weapons of mass destruction.[365]

These sanctions lists also put banking institutions and American businesses on notice regarding the sanctioned targets, many of whom are major financial and material sponsors of transnational terrorism and weapons proliferation.[366] As a result, these actors are effectively expelled from participation in the legitimate commercial and financial sectors in the United States and other industrialized countries.

To promote the efficacy of blacklists, ICANN must ensure the legitimacy of the user ID system in order to empower providers to properly identify blacklisted users.[367] ICANN also must establish penalties for providers and hosts who negligently provide services to blacklisted users lists, much the same as the U.S. Government and the United Nations impose penalties on banks that conduct business with designated targets.[368]

To establish the sanctions list as a legitimate and authoritative enforcement mechanism, ICANN should bolster its existing audit and dispute resolution sections to process and evaluate evidence against the targeted users and providers. It must also develop a mechanism to hear and resolve challenges to the ban of a particular user or provider. Again, establishing an additional regulatory regime within ICANN will require broad stakeholder support and a larger resource commitment from ICANN and its financiers.

---

[365] *See id.;* Exec. Order No. 13,382, 31 C.F.R. § 539 (1999); Exec. Order No. 12,978, 31 C.F.R. § 598 (2000). The U.S. targeted sanctions programs are operated by the U.S. Department of Treasury Office of Foreign Assets Control ("OFAC"). According to its Web site the OFAC:

> administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under US jurisdiction.

OFAC, http://www.ustreas.gov/offices/enforcement/ofac/ (last visited Oct. 30, 2006).

[366] Each time that the U.S. Department of Treasury announces an anti-terrorism, counter-narcotics, or counter-proliferation designation, an electronic alert is distributed to banking and financial institutions worldwide putting them on notice regarding the action. By law, the institutions are then prohibited from conducting financial transactions with these individuals or entities. Violators of the regulations may face negative publicity and enforcement actions including fines. *See* Foreign Assets Control Regulations, 31 C.F.R. § 50 (2003); OFAC Frequently Asked Questions, http://www.ustreas.gov/offices/enforcement/ofac/faq/ (last visited Aug. 24, 2006).

[367] *See supra* Part VII.B.1.

[368] Molnar, *supra* note 47, at 34–36 (describing the ineffectiveness of ICANN and its sister organizations in monitoring and enforcing Internet regulations and an evaluation of Congressional legislation which would impose fines on registrars and users who provide false registration information).

At the national level, Congress could emulate the public–private partnership it mandated in the late 1990s to combat Internet child pornography and online predators.[369] In 1998, Congress passed legislation that required Internet providers to report child pornography and child sexual exploitation on the Internet to the NCMEC.[370] The legislation also mandated substantial fines for providers who fail to report child pornography or child exploitation on the Internet.[371] In compliance with the statute, the NCMEC compiled and continuously updates a nationwide list identifying child pornography Web sites and individual child predators.[372] The NCMEC Web site also provides a database of links to government and nongovernmental programs in other countries that track and enforce laws against child pornography.[373]

Congress could enact legislation to address terrorist-related activities on the Internet modeled after the child pornography prevention and enforcement regime. Such legislation should establish and fund a public–private information and enforcement clearinghouse on terrorism-related materials and content on the Internet in the model of the NCMEC. A National Center for Terrorism and Violence-Related Activities on the Internet would create a public face for the cyber terrorism issue and encourage industry and private citizens to track and feed information to law enforcement officials on terrorism activities while increasing the profile of this issue in the public eye. Once established, the National Center could also launch a global partnership of country-level centers on cyber terrorism–related activities that are interconnected to an international umbrella organization such as ICANN.

F. Impose Negligence Fines for Providers Who Fail to Monitor and Enforce Content Restrictions

Another enforcement and deterrence mechanism needed to bolster the overall Internet security environment are negligence fines. ICANN must impose fines on providers and hosts who repeatedly fail to comply with the monitoring requirements stipulated in the terms of standardized ICANN-issued accreditation contracts. In addition to a credible threat of being pub-

---

[369] 42 U.S.C. § 13,032 (2000).

[370] *Id*.

[371] *Id.* § 13,032(b)(4) (requiring fines for knowingly and willfully failing to make a report to the National Center for Missing and Exploited Children of not more than $50,000 for the first offense and not more than $100,000 for the second offense).

[372] National Center for Missing and Exploited Children Cyber Tipline Factsheet, http://www.missingkids.com/en_US/documents/CyberTiplineReportTotals.pdf (last visited Oct. 30, 2006).

[373] National Center for Missing and Exploited Children Global Network, http://www.missingkids.com (select countries from the drop-down menu under "Global Network" on the left tool bar) (last visited Oct. 30, 2006).

licly banned from the Internet, ICANN's ability to fine hosts and providers would create a significant incentive for enhanced monitoring of online content by the private sector.

In addition, ICANN regulators should examine the feasibility of including language within the provider and host contracts that would impose a negligence standard of tort liability upon providers for failure to comply with the contract terms. While the legal application of these terms would undoubtedly vary by individual country, the contractual language would signal ICANN's intent to hold negligent providers accountable and reinforce the legitimate authority relationship between ICANN and providers and hosts.[374] As such, ICANN would lead the effort to normalize Internet legal and professional standards while providing incentives for the private sector to increase monitoring and enforcement.[375]

G. Develop and Sustain Sufficient Funding and Technology Sources

In order for ICANN and its stakeholders to establish the organization as the preeminent regulatory body charged with overseeing and protecting the interests of the Internet, the organization's primary decision-makers must create guaranteed, long-term sources of funding and technological resources. As ICANN wrote in its 2004-2005 budget proposal:

> [m]eeting the needs of registration providers and consumers is already a significant element of ICANN's budget, but there are many activities that are under-funded and under-staffed in light of the demand for such services. To provide the level of service that appropriately fulfills ICANN's service goals will require substantial investments in systems, infrastructure, regional presence and personnel.[376]

Without the financial ability or technological know-how to hire and train capable personnel who could develop technological tools to assist in bolstering the security of the Internet, ICANN will be incapable of capitalizing on the opportunity to reverse the lawless spiral of Internet regulatory efforts and establish itself as the preeminent Internet governance organization.

To accomplish these recommendations, along with other substantial regulatory and administrative needs currently facing the Internet, ICANN policymakers must identify long-term guaranteed funding streams.[377] Sus-

---

[374] *See* Nackley, *supra* note 256, at 10-17 (recommending specific boiler-plate Web site hosting contractual language for distribution and use by providers and users).

[375] *See* Johnson & Post, *supra* note 39, at 1387–91 (describing how the Internet community will begin to develop legal norms to regulate online behavior as it becomes necessary).

[376] ICANN, PROPOSED FISCAL YEAR 2004-2005 BUDGET 11 (2004) [hereinafter 2004-2005 ICANN BUDGET], *available at* http://www.icann.org/financials/proposed-budget-14may04.pdf.

[377] *Id.* at 17. The ICANN budget proposal emphasizes the need to "develop alternate sources of funding in order to provide a more robust revenue base" by securing a more consistent base of funding from ICANN stakeholders. *Id.*

tainable and reliable funding of ICANN continues to be a problem for the organization.[378] A possible solution is the imposition of fees on providers and Web hosts, to be collected on regular intervals.[379] While many industry representatives have opposed the imposition of additional user access fees because of the small size and profitability of some providers,[380] the reality is that the administrative and security challenges facing the Internet require a greater resource commitment from those who benefit the most from maintaining access to the Internet. ICANN has indicated that it is considering such fees as a way to address its funding challenges.

Under "Alternate Sources of Revenue," the ICANN 2004–2005 budget proposal claimed that ICANN "could derive fees from the revenue stream flowing to registries as a result of new registry services."[381] In addition, in 2004–2005, ICANN sought to bolster its revenue by billing fees charged to registrants through registrars on a per transaction basis versus the previous quarterly basis billing cycle.[382] In early 2006, ICANN issued a new framework for collecting adequate "user fees" from registrars and Top Level Domain ("ccTLD") organizations.[383] In its document, "Guidelines for ccTLD Managers Accountability Framework Discussions with ICANN,"[384] ICANN states that it is "working . . . to ascertain a) an agreed amount within the total ICANN Budget that could be paid by ccTLD managers and b) a model by which to fairly apportion that amount between ccTLD managers." However, any contribution made by the ccTLDs will remain voluntary until ICANN and the Country Code Names Supporting Organization, the parent organization for TLDs, can reach a consensus agreement on regular annual fees for TLDs to make to ICANN.[385]

---

[378] *Id.*

[379] Klein, *supra* note 305, at 196.

[380] *Register.com Joins Industry Call for Changes to ICANN.com Proposals*, BUS. WIRE, Feb. 15, 2006; *Contracting the Internet: Does ICANN Create a Barrier to Small Business?: Hearing Before the H. Comm. on the Judiciary*, 109th Cong. (June 7, 2006)(statement of Mr. W.G. Champion Mitchell, Chairman and Chief Executive Officer, Network Solutions, LLC).

[381] 2004–2005 ICANN BUDGET, *supra* note 376, at 17.

[382] *Id.* at 14.

[383] ICANN, GUIDELINES FOR CCTLD MANAGERS ACCOUNTABILITY FRAMEWORK DISCUSSIONS WITH ICANN, http://ccnso.icann.org/announcements/af-guidelines-14dec05.pdf (last visited Aug. 24, 2006).

[384] *Id.*

[385] *See* ICANN, ICANN MANAGERS ACCOUNTABILITY FRAMEWORK 3 (2005). The ICANN Accountability Managers framework established a vaguely defined preliminary fee agreement that ccTLDs:

> [s]hall contribute to ICANN's cost of operations in the amount of [ ] per annum. It is acknowledged by both parties that the ccTLD community and ICANN are working together to obtain a formula to determine permanent and satisfactory contribution to ICANN. If there is no agreement on a permanent solution for ccTLD contributions to ICANN the parties agree to review in good faith . . . the contribution to ICANN set out above. . . . The review of the parties will take into account all relevant circumstances.

Another source of ICANN funding could be derived from assessing a reasonable fee on for-profit Web site merchants who earn a certain amount of revenue—perhaps over $100 million per year—from their Web site sales. ICANN appears to be evaluating similar proposals for assessing commercial user fees.[386] In its 2004–2005 budget, ICANN described the "substantial opportunity for commercial organizations that benefit directly from successful operation of ICANN's functions to contribute to some of the associated costs."[387]

VIII. CONCLUSION

Despite the fact that senior national security officials and Internet policy experts have been aware since the mid-1990s that terrorist groups were targeting the Internet as an operational and communications platform, far too little has been done to cut off the Internet from terrorist elements. Al Qaeda and affiliated terrorist movements continue to exploit the Internet as an operational platform for the indoctrination, recruitment, fundraising, training, and more recently, planning and coordination of terrorist attacks.[388] Cyber jihadists' unrestricted online activities continue to lead to the killing and maiming of thousands of innocent civilians worldwide each year. Domestic and international policies toward cyber jihadists' online activities that focus on deterrence and passive enforcement of content regulations are no longer tenable. Cyber jihadists pose an increasingly intolerable national security risk to the United States and its allies due to the sophisticated online planning and operational activities of potential attacks weapons of mass destruction and suicide terrorist attacks.

The time to act is now. Yet, the U.S. government, foreign governments, ICANN and other private stakeholders continue to fail to implement significant prevention and enforcement-oriented reforms that will make it more difficult for terrorists to exploit the Internet.[389] By establishing an aggressive timetable for Internet security reform while evaluating and implementing the seven core regulatory and enforcement tools proposed in this Comment for combating the cyber jihad threat, ICANN, sovereign governments, and private stakeholders can begin to stem the tide of terrorist exploitation of the Internet.

Id.

[386] 2004–2005 ICANN BUDGET, *supra* note 376, at 17–18.

[387] *Id.*

[388] *See* discussion *supra* Part III.C.

[389] *See* discussion *supra* Part IV–V.

Ending the cyber-jihad: Combating terrorist exploitation of the rule of law and improved tools for cyber governance. Comm Law Conspectus, 15, 119â€“ 186. Serious Organised Crime Agency Serious Organised Crime Agency SARs Annual Report 2011.Â Focuses on encryption technology and how it allows illegal use of the Internet in the form of cyber laundering and e-cash, and on the move by terrorists into narcotics production and trafficking - which is defined as nacre-terrorism. Describes efforts to proscribe cyber crime, including cyber laundering and cyber terrorism, including controls on privacy and encryption. Shows how business corporations can become involved with terrorism, including a case study on tanzanite. View. Though the cyber threat is one of the FBIâ€™s top priorities, combating terrorism remains our top investigative priority. As geopolitical conflict zones continue to emerge throughout many parts of the world, terrorist groups may use this instability to recruit and incite acts of violence. The continuing violence in both Syria and Iraq and the influx of foreign fighters threatens to destabilize an already volatile region while also heightening the threat to the West. Due to the prolonged nature and the high visibility of the Syrian conflict, we are concerned that U.S. persons with an interest in