The Columbia
SCIENCE AND TECHNOLOGY LAW REVIEW
www.stlr.org

THE CYBER-FRONT IN THE WAR ON TERRORISM: CURBING TERRORIST USE OF THE INTERNET

By Todd M. Hinnen *

As an affordable, anonymous, secure, geographically unbounded, and largely unregulated medium for commerce and communication, the Internet provides users with an unprecedented global marketplace in which to conduct financial transactions and exchange ideas. These same characteristics, however, render the Internet an inviting environment for vast fraud schemes, money laundering, and communication among criminal coconspirators. It has become increasingly clear that terrorist organizations avail themselves of the opportunities afforded by the Internet to recruit and train adherents and foot soldiers, to raise and move funds, and to plan and execute attacks. This Article explores law enforcement's ability to combat terrorist organizations' use of the Internet to raise and move funds, communicate, and orchestrate acts of terror. First, the Article examines the online mechanisms through which terrorist organizations raise funds online, citing examples in which terrorists have raised money by soliciting funds directly over the Internet, exploiting facially-legitimate online charities, or garnering the proceeds of Internet crimes. Second, the Article explores the online commercial applications through which terrorist organizations transfer resources from these fund-raising sources to their operational corps. Third, the Article investigates the online means by which terrorist organizations communicate to recruit and indoctrinate supporters, to orchestrate fund-raising and disbursement

* The author is a Trial Attorney with the United States Department of Justice's Computer Crime & Intellectual Property Section. His duties with the Department of Justice include serving as a consultant in federal terrorism investigations and prosecutions that involve the Internet and co-chairing an inter-agency working group on online terrorist financing with Juan C. Zarate, Deputy Assistant Secretary of Treasury for Terrorist Financing and Financial Crime. The views expressed in this Article are those of the author and do not necessarily represent the views of the Department of Justice.

efforts, and to devise and implement violent operations. With regard to each of these topics, the Article discusses the challenges posed to the United States government's efforts to prevent, investigate, and prosecute such conduct under United States law.

I. Introduction

For more than 2,000 years, military strategists have recognized the truism that armed conflict cannot be waged until it has been financed.[1] Accordingly, shortly after the September 11 terrorist attacks on the United States, President Bush observed that the country's first strike in the war against terrorism would target terrorists' financial support.[2] As former Secretary of the Treasury Paul O'Neill stated in October, 2001, "[o]ur goal must be nothing less than the disruption and elimination of the financial frameworks that support terrorism and its abhorrent acts."[3]

Since September 11, the United States has made remarkable strides in disrupting and interdicting the flow of financial resources to terrorists.[4] The United States has twice amended its laws to provide additional tools for preventing, investigating, and prosecuting terrorist financing.[5] The country has engaged in capacity-building around the globe, encouraging other countries to establish appropriate money-laundering legislation and effective oversight of their banking and financial systems.[6] The United States has led

---

[1] *See* Sun Tzu, The Art of War 72–73 (Samuel B. Griffith trans., Oxford University Press 1963).

[2] Comments of President George W. Bush, Delivered at the Dep't of the Treasury, Nov. 7, 2001.

[3] Press Release, United States Dep't of the Treasury, Remarks by Paul H. O'neill, U.S. Sec'y of the Treasury, Before the Extraordinary Plenary Meeting of the Financial Action Task Force (Oct. 29, 2001), *at* http://www.treas.gov/press/releases/po735.htm.

[4] The terms "terrorists" and "terrorist organizations" as used in this Article include the 36 organizations currently designated as Foreign Terrorist Organizations ("FTOs") by the Secretary of State pursuant to 8 U.S.C. § 1189 (2000) and the 315 individuals and organizations designated as Specially Designated Global Terrorists ("SDGTs") pursuant to International Emergency Economic Powers Act. In addition, they include any person or organization that intends to carry out, aid, assist, or support an act of domestic or foreign terrorism as those terms are defined by 18 U.S.C. §§ 2331(1) and (5) (2000). *See also* 22 U.S.C. § 2656f(d) (2000) ("The term 'terrorism' means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents. . . .").

[5] *See generally* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[6] *See generally* Press Release, U.S. Dep't of the Treasury, Testimony of Kenneth W. Dam, Deputy Sec'y Dep't of the Treasury, Before the Senate Committee on Banking, Housing, and Urban Affairs, *Terrorist Financing: A Progress Report on Implementation of the USA PATRIOT Act and the 2002 National Money Laundering Strategy* (Oct. 3, 2002), *at* http://www.treas.gov/press/releases/po3496.htm.

initiatives in multi-lateral fora to develop and implement legal and regulatory controls on alternative means of value transfer, such as *hawala*.[7] It has also coordinated with the private sector and the international community to develop best practices to prevent terrorists from exploiting charitable organizations to raise funds.[8]

In cooperation with other countries and with international bodies, the United States has led the international community in freezing funds and assets worth more than $139 million and seizing funds and assets worth more than $60 million.[9] Furthermore, the Secretary of the Treasury has frozen the assets of, and prohibited financial transactions with, 315 individuals and organizations by identifying them as Specially Designated Global Terrorists ("SDGTs") under the International Emergency Economic Powers Act ("IEEPA").[10] Countries around the globe are following the United States' lead—as of August 1, 2002, more than 160 foreign countries had instituted blocking orders affecting accounts worth more than $70 million.[11]

Indeed, one government official recently observed, "Terrorists can no longer safely use the international banking system. . . . As formal financial systems are purged of terrorist finance, terrorists naturally are inclined to resort to other, more costly and

---

[7] *Hawala* is a trust-based value transfer mechanism in which a payor in one geographic location, for instance the United States, visits a *hawaladar* and purchases a promise of payment to a payee in another location, for instance Pakistan. The U.S. *hawaladar*, relying on a network of trusted colleagues often developed over generations, communicates to a Pakistani *hawaladar* a request for payment in a certain amount to be made to the payee. If, at the end of a fixed period of time the transfers made between these two *hawaladars* do not balance out, they settle their accounts with one lump payment. *See* Patrick M. Jost & Harjit Singh Sandhu, *Hawala: The Hawala Alternative Remittance System and its Role in Money Laundering* (noting that for communication between *hawaladars* "email is becoming more and more common"), *available at* http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/default.asp (last visited Feb. 28, 2004). This Article uses the term "*hawala*" when referring to any trust-based informal value transfer system. Such systems have different names, however, in different geographical regions. They are called *hawala* in the Middle East, Afghanistan, and parts of Pakistan; *hundi* in India and parts of Pakistan; *fei ch'ien* in China; and *phoe kuan* in Thailand. *See Informal Value Transfer Systems*, 33 FinCEN Advisory (U.S. Dep't of the Treasury Financial Crimes Enforcement Network), Mar. 2003, *at* http://www.fincen.gov/advis33.pdf; Patrick M. Jost & Harjit Singh Sandhu, *Hawala: The Hawala Alternative Remittance System and its Role in Money Laundering*, Appendix A (Interpol General Secretariat, Lyon 2000).

[8] *See supra* note 6.

[9] *See* United States Dep't of the Treasury, Office of Management and Budget, *at* http://www.whitehouse.gov/omb/budget/fy2005/treasury.html (Feb. 9, 2004).

[10] *See* 50 U.S.C. §§ 1701–1706 (2000). The Department of the Treasury's current list of SDGTs, which is maintained as part of its list of Specially Designated Nationals and Blocked Persons, is available online at http://www.treas.gov/offices/eotffc/ofac/sdn/t11sdn.pdf.

[11] *See supra* note 6.

uncertain, but still serviceable mechanisms for moving resources."[12] Although this observation may be overly optimistic in one respect—terrorists and terrorist organizations do still use the international banking system—it correctly emphasizes that as the banking system is subject to increased scrutiny, terrorists must turn to other mechanisms to transfer funds. While maintaining vigilance over traditional means of value transfer, the United States must also focus on alternative means—trading in commodities such as gold, gems, and precious stones and metals; non-bank online remittance systems; and informal value transfer systems such as *hawala*.

The Internet provides an infrastructure that suffuses both traditional and alternative means of resource and money transfer. The manner and method in which terrorists use the Internet to raise and transfer funds is informed in part by the Internet's evolution as an anonymous, geographically unbounded, and largely unregulated international communication and commercial network. A brief explanation of the genesis and evolution of the Internet serves to illustrate this point.

The Internet was conceived in 1961 and delivered into a primordial stage of existence by a consortium of government scientists and academics in 1969.[13] The two original nodes, at UCLA and Stanford, exchanged the first Internet communication in October 1969.[14] During the 1970s, the Internet evolved into an open-architecture network that accommodated diverse network interfaces and a decentralized, redundant network that ensured reliability if any of its "nodes" malfunctioned.[15] A common language, or set of protocols, was agreed upon and applications such as electronic mail and file transfer were invented.[16] In the 1980s, the U.S. government encouraged the development of private networks and commercial applications.[17] The resulting tripartite partnership between government, academia, and private industry accelerated the growth rate and application diversity of the Internet.[18] The modern Internet reflects in a number of its signature characteristics the open, multi-disciplinary community out of which it evolved—it remains an open, interoperable, decentralized, and largely unregulated

---

[12] *Financial War on Terrorism: New Money Trails Present Fresh Challenges: Hearing Before the Comm. on Finance, U.S. Senate*, 107th Cong., S. Hrg. 107-880 at 43 (Oct. 9, 2002) (prepared statement of Hon. Alan Larson, Under Secretary of State for Economic, Business and Agricultural Affairs), *available at* http://www.senate.gov/~finance/hearings/84922.pdf.

[13] *See* Barry M. Leiner et al., A Brief History of the Internet, *available at* http://www.isoc.org/internet/history/brief/shtml.

[14] *See id.*

[15] *See id.*

[16] *See id.*

[17] *See id.*

[18] *See id.*

network.[19]

The Internet today is a global network of interconnected communication and information systems. A user at any Internet terminal in the world can access the vast wealth of information available on the World Wide Web[20] or communicate, share documents and stored information, and engage in commercial transactions with millions of other users throughout the world. The 2002 CIA World Factbook estimates that worldwide there are more than 10,000 Internet Service Providers ("ISPs") and more than 600 million Internet users.[21]

Several of the Internet's cardinal characteristics are essential to its use by terrorists to raise and transfer funds. First, Internet users enjoy a large measure of anonymity. Many Internet interactions are memorialized only by computers' exchange of unique numeric identifiers, called Internet Protocol ("IP") addresses, assigned to them by their respective ISPs.[22] Although it is theoretically possible to determine which user was assigned the IP address involved in a transaction, there are a number of practical obstacles to such a determination.

Even when it is possible to identify the IP address assigned to an Internet customer involved in a communication or transaction, the Internet provides several information security applications that allow customers to conceal the content of their communications or the details of their transactions. Internet customers can use widely-available encryption tools to convert a message into "ciphertext" for secure transmission or embed a message into an image, sound, or other file through a process called "steganography." Steganographic files appear indistinguishable from the millions of regular files transiting through or posted on the Internet. Unless one possesses the proper key to decode encrypted or steganographic files, it may be impossible to determine their content. Encoding methods such as encryption and steganography have important and

---

[19] *See id.*

[20] The terms "Internet" and "World Wide Web" are often, but incorrectly, used interchangeably. The Internet describes the network itself—the computers, the physical or virtual connections, and all of the protocols and applications they support—whereas the World Wide Web describes the resources available on that network through the use of one particular protocol, the hypertext transfer protocol ("HTTP"). *The Difference Between the Internet and the World Wide Web*, Webopedia, *at* http://www.webopedia.com/didyouknow/internet/2002/web_vs_internet.asp.

[21] *See* 2002 CIA World Factbook, *available at* http://www.cia.gov/cia/publications/factbook/geos/xx.html.

[22] An IP address is a unique numeric identifier assigned to each computer connected to the Internet. An ISP normally controls a range of hundreds or thousands of IP addresses, which it assigns to customers for their use. ISPs may assign IP addresses "dynamically" or "statically." In the case of dynamic assignment, each time the user accesses the ISP to connect to the Internet, the ISP assigns one of the available IP addresses it controls to the customer's computer for the duration of the customer's session (i.e., until he or she disconnects). Each time the customer connects to the Internet, she may receive a different IP address. By contrast, a user with a static IP address commonly has a permanent, 24-hour Internet connection and an IP address that remains constant over weeks or months. *See What is an IP Address?*, adNet, *at* http://www.adnetadvertising.com/whatis_ipaddress.html.

legitimate e-commerce, information security, and privacy protection applications. As with many characteristics of the Internet, however, anonymity and readily available encoding applications are double-edged swords. They also pose obstacles to investigations of Internet users who engage in illegal conduct.[23]

Second, the Internet is, for all intents and purposes, geographically unbounded. An Internet user in Washington, DC can as easily exchange e-mail, engage in "chat," visit a web page, or conduct web-based financial transactions with a user or server in a foreign country anywhere in the world as with another user or server in Washington, DC. Although it is theoretically possible to locate an Internet user in geographic space, several practical obstacles complicate the process of pinpointing a user's location. As a result of the Internet's global nature, regulation and investigation of communications and transactions on the Internet often involve two or more countries, which may or may not be on cooperative terms and may or may not have similar procedural and substantive laws.[24] Differences in regulatory and legal systems are mediated to a large degree in the area of terrorist financing, however, by a number of international legal instruments and by the work of several multilateral organizations.[25]

---

[23] Daniel A. Morris, *Tracking a Computer Hacker, at* http://www.cybercrime.gov/usamay2001_2.htm.

[24] A compendium of the substantive computer crime laws in 44 different countries can be found in The Legal Framework—Unauthorized Access to Computer Systems, Moss District Court, Norway, *at* http://www.mosstingrett.no/info/legal.html.

[25] For instance, the International Convention for the Suppression of the Financing of Terrorism, which was adopted by the United Nations in 1999 and has been ratified by 61 countries, requires countries to establish substantive and procedural laws pursuant to which acts of terrorist financing can be effectively investigated and prosecuted and the proceeds of terrorist financing can be frozen or seized. *See* International Convention for the Suppression of the Financing of Terrorism, G.A. Res. 54/109, U.N. GAOR, 4th Sess., U.N. Doc. A/RES/54/109 (1999). The United Nations Security Council also passed immediately after the September 11 attacks a resolution requiring all 189 member nations to forbear from making funds available to terrorists and their supporters and to freeze the financial assets of persons and entities who commit or attempt to commit terrorist acts. *See* S.C. Res. 1373, U.N. SCOR, 56th Sess., 4385th mtg., U.N. Doc. S/RES/1373 (2001). The 31 members of the Financial Action Task Force on Money Laundering ("FATF") have endorsed eight Special Recommendations on Terrorist Financing, which encourage countries to develop regulations and laws facilitating the prevention, investigation, and prosecution of terrorist financing, and to cooperate internationally in the enforcement of such regulations and laws. *See* Special Recommendations on Terrorist Financing, *available at* www.fatf-gafi.org/SRecsTF_en.htm. Similarly, on June 3, 2002, the General Assembly of the Organization of American States ("OAS") entered into a comprehensive treaty to prevent the financing of terrorism, strengthen border controls, and increase cooperation among law enforcement authorities in different OAS countries. The OAS Inter-American Convention against Terrorism is available online at http://www.oas.org/juridico/english/treaties/a-66.htm. The UN, the G8, the OAS, the Asian Pacific Economic Cooperation ("APEC") group, the Association of Southeast Asian Nations ("ASEAN"), the International Organization of Securities Commissions ("IOSCO"), and other bilateral and multilateral fora continue to explore the ways in which

Finally, the Internet is subject to very little regulation. Because the Internet developed as an open, interoperable network, regulations are few in number and impose only minimal constraints. Moreover, because the Internet is global and decentralized—there is no single point or even set of points through which all information transiting the Internet must flow—its architecture is not easily susceptible to regulation. To a large degree, the only "regulations" imposed on Internet users are those that are essential to the Internet's functioning.

This Article explores the ways in which terrorists use the Internet to raise and move funds and law enforcement's ability to prevent, investigate, and prosecute such conduct under United States law.[26] Section I discusses the methods terrorists use to raise funds over the Internet, and the challenges these methods pose to federal efforts to prevent, investigate, and prosecute such conduct. Section II addresses terrorists' online efforts to move such funds without attracting the attention of law enforcement. Section III discusses terrorist use of the Internet as a medium for communication, whether to publish a *fatwah* endorsing violence against United States citizens, to impart the details of a financing scheme, or to plan an attack. The Article concludes with observations about how United States law enforcement can best meet the challenges posed by terrorists' use of the Internet and successfully prevent terrorists from using the Internet to raise and transfer resources, investigate individuals and organizations involved in such conduct, and prosecute them under United States law.

II. Terrorist Use of the Internet to Raise Funds

The terms "financing" and "fund raising" are used in this Article as shorthand for the accumulation of any of the material resources necessary for terrorists to maintain their organizations and carry out their operations. United States law defines "material support or resources" as

> currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine or religious materials.[27]

The support sought by, and provided to, terrorist organizations is often not in the form of cash. Terrorist organizations may also use the Internet to solicit other fungible

---

international cooperation can facilitate the prevention, investigation, and prosecution of terrorist financing.

[26] This Article does *not* discuss other means of stopping the flow of resources to terrorist organizations, such as targeted military or intelligence operations against terrorist organizations.

[27] 18 U.S.C. § 2339A(b) (2000) (making it a crime to provide material support to terrorists).

goods (gold or gems, for instance),[28] accumulate supplies, or recruit foot soldiers.

It may be tempting to treat terrorist financing just as one would any other form of money laundering or financial fraud, but terrorist financing often has some distinguishing characteristics. First, terrorists and terrorist organizations are not profit motivated. Their ultimate goal is not to amass wealth; it is rather to inflict harm and instill terror. Although the maintenance of a terrorist organization may be costly, terrorist operations such as the September 11 attacks can often be carried out on relatively low budgets.[29] Accordingly, the funding of terrorist operations may involve fund transfers that are too small to arouse suspicion or trigger regulatory scrutiny. The financial operation of a terrorist cell may be much more modest, and therefore much more difficult to detect than, for instance, the money laundering operation for a drug cartel.

Second, whereas money laundering generally involves financial transactions designed to conceal the illicit origin of funds, the funds used to finance terrorism are often not derived from an illicit source or generated by illicit activity. Law enforcement may uncover money laundering during the investigation of the predicate crime that produced the funds to be laundered—for instance, in the investigation of a drug cartel. Sometimes terrorist financing is linked with other crimes, such as fraud or narcotics trafficking, and may be discovered during the investigation of those crimes. In other instances, the funds used to finance terrorism derive not from other criminal conduct, but from donations or business proceeds. These facially legitimate fund raising mechanisms are not associated with separate criminal conduct that might arouse law enforcement suspicion. Moreover, in such cases, there may be no "victim" to report the fundraising activity.

Finally, the most important distinction between terrorist financing and money laundering, however, is this: terrorist financing supports acts of atrocity and violence against innocent victims in the United States and around the world. Any discussion of terrorist financing must be informed by the stark reality that what leaves the United States as currency or material resources may return as bombs, biological agents, or other means of destruction. Interdicting terrorist financing thus accomplishes more than frustrating a particular type of criminality or recovering criminal proceeds. It presents an opportunity to deprive terrorist organizations of the funding on which their operations depend, to unearth their networks and identify their members before they can act, and to disrupt them before they take more innocent lives.[30]

---

[28] *See* Jeannine Aversa, *Cutting Terror Funds Said Effective*, Associated Press, Sept. 10, 2002, *available at* 2002 WL 26545883 (reporting that Treasury officials had emphasized "money flowing through nontraditional financial channels, such as trading in diamonds or gold" as one challenge in interdicting terrorist funding).

[29] The FBI estimates the budget required to perpetrate the September 11 attacks at between $300,000 and $500,000. *See* Matthew A. Levitt, *The Political Economy of Middle East Terrorism*, Middle East Review of International Affairs Journal, Vol. 6, No. 4 (Dec. 2002), *available at* http://meria.idc.ac.il/journal/2002/issue4/jv6n4a3.html.

[30] Former FBI Director Louis Freeh, testifying before Congress in 1999, indicated that the 1993 attack on the World Trade Center could have been much more devastating, but the perpetrators lacked sufficient funds to build a larger bomb. He also attributed a strong investigative lead to

Terrorists use the Internet in four primary ways to solicit and collect such resources:

1. They solicit donations, indoctrinate adherents, share information, and recruit supporters directly via websites, 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; and

4. They use the Internet as a pervasive, inexpensive, and anonymous medium of communication to organize and implement fund raising activities.

A. *Direct Solicitation*

Terrorist organizations use websites, chat rooms, and targeted mass e-mailings to solicit funds directly from their supporters. Several terrorist organizations maintain websites, accessible to any Internet user, which celebrate past acts of terrorism, exhort adherents to further violence, and request donations in support of their causes. A prominent example was the site www.azzam.com, a site named after Abdullah Azzam, Osama bin Laden's mentor who conceived of and established international terrorist training camps in Afghanistan.[31] The site sold Islamic extremist publications, including a book by Omar Abdel Rahman, the mastermind behind the 1993 World Trade Center bombing. The site also included a page entitled "What Can I Do to Help Jihad and the

---

the perpetrators' lack of adequate funding—they were identified in part by their attempt to recover the deposit fee on the rental truck used to transport the bomb. *See Counterterrorism Efforts: Hearing Before Senate Comm. on Appropriations*, *Subcomm. for the Dep'ts of Commerce, Justice, and State, the Judiciary, and Related Agencies*, 106th Cong. (1999) (statement of Fed. Bureau of Investigation Dir. Louis J. Freeh).

[31] *See* Jonathan Fighel, *Sheikh Abdullah Azzam: Bin Laden's Spiritual Mentor*, *available at* http://www.ict.org.il/articles/articledet.cfm?articleid=388 (Sept. 27, 2001). Most of the examples cited in this Article involve terrorist organizations based in the Middle East and founded upon a militant, anti-American form of Islamic ideology, because these organizations pose the gravest and most immediate threat to the United States. The author does not intend to impugn the countries of the Middle East or the vast majority of Islamic sects and communities, many of whom have been among the United States' closest allies in waging the war against terrorism. The discussion and conclusions contained in the Article are equally applicable to all terrorists and terrorist organizations, regardless of where they come from, whether they are foreign or domestic, or what their underlying motives or objectives may be.

Mujahideen?" which read:

> Around the Muslim world, the Jihad is being entirely funded by donations from individuals. . . . Jihad is a profitable investment that pays handsome dividends. For someone who is not able to fight at this moment in time due to a valid excuse they can start by the collection and donation of funds. . . . Azzam Publications is able to accept all kinds of Zakah and Sadaqah donations and pass them on where they are most needed. . . . The Jihad . . . consists of . . . the one who organizes the weapons and ammunition [and] the one overseas who raises the money . . . .[32]

Several other terrorist organizations have used the Internet to solicit funds and material resources. A recent article in a Pakistani newspaper reported that five Pakistani jihad organizations currently maintain websites, some of which receive up to 300 visitors each day.[33] The following examples are illustrative of the direct solicitation sites that have been on the Internet since September 11:

- Hamas' military wing, the Izz al-Din al-Qassam Brigades, posted communications on a website recruiting suicide bombers and encouraging supporters "to donate . . . what you can to assist the cause of Jihad and resistance until the occupation is eliminated and every span of the Muslim Palestine is liberated."[34]

- Hizballah's television station Al-Manar maintained a website that urges contributions "for the sustenance of the Intifadah," listing bank accounts in Lebanon to which donations should be made.[35]

- The Global Jihad Fund published a website urging donations "to facilitate the growth of various Jihad Movements around the World by supplying them with sufficient funds to purchase weapons and train their individuals." The site listed bank accounts in Pakistan and featured links to websites supporting terrorist organizations, including the Taliban, Lasker Taiba, Hamas, and Hizballah.[36]

- A website entitled "Al Qa'ida University for Jihad Sciences" appeared in

---

[32] Jeff Breinholt, *Terrorist Financing*, 51 U.S. Att'ys Bull. No. 4 at 24 (July 2003), *at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usab5104.pdf.

[33] *See* Amir Rana, *Jihad Online*, Lahore Daily Times, Apr. 20, 2003.

[34] *See* Anti-Defamation League, *Jihad Online: Islamic Terrorists and the Internet* 23, *at* http://www.adl.org/internet/jihad_online.pdf (2002).

[35] *See id.* at 28.

[36] *See* Levitt, supra note 29, at 57 (*quoting* Chris Hastings & David Bamber, *British Cash and Fighters Still Flow to bin Laden*, London Sunday Telegraph, Jan. 27, 2001).

November 2003, offering online instruction in "jihad sciences" such as "suicide operations."[37]

1. Prevention & Investigation

It is difficult, if not impossible, to prevent such solicitations from occurring through websites, bulletin boards, and chat rooms and to investigate such solicitations if they do occur. Even assuming that the perpetrator uses a United States ISP—and in the post September 11 atmosphere of strict counter-terrorism practices, that is an assumption that would rarely be met—preventing and investigating such a website, bulletin board, or chat room may be difficult for four reasons. First, the Internet may be used anonymously. If the perpetrator is Internet savvy, he can mask his identity even as he hosts a public site on the Internet. Users can access the Internet from a public library or a cyber café without providing any identifying information. A user can even register a website from his home computer without identifying himself by first visiting a site called an anonymizer, which replaces the IP address for the user's home computer with another IP address that cannot be traced back to the user. See Figure 1. Investigation of such cases will determine that the website was registered from a public library, a cyber café, or an anonymizer, but will be unable to identify the person in the library or café, or the user who visited the anonymizer.

[37] *See* American Foreign Policy Council, Eurasia Security Watch (Ilan Berman ed.), *at* http://www.afpc.org/esw/esw7.shtml (Nov. 26, 2003).

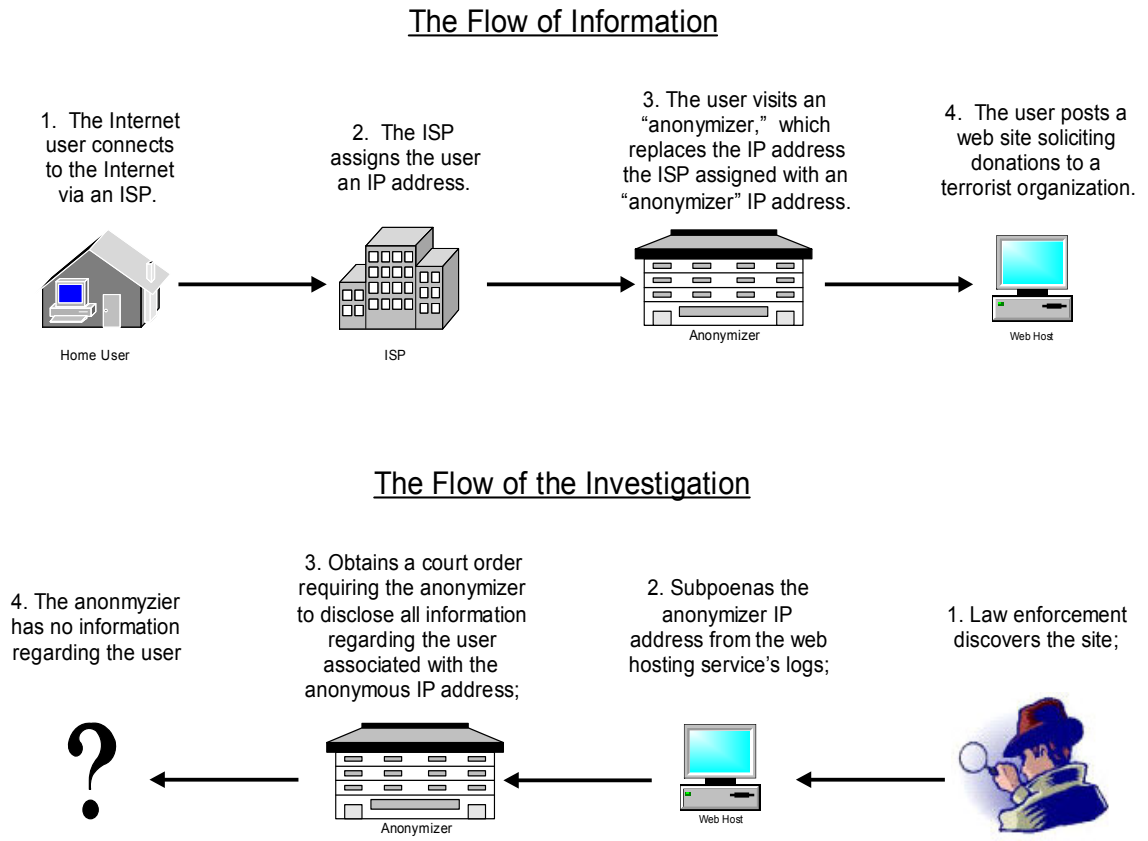

Figure 1

Second, the Internet is global. Among the more than 10,000 Internet service providers worldwide are several in countries that have large populations sympathetic to Islamic extremism or antagonistic to the United States. According to the 2002 CIA World Factbook, the seven nations currently listed by the State Department as "state sponsors of terrorism" maintain 19 ISPs.[38] Website hosts in these countries are not subject to United States regulatory jurisdiction, nor may these countries be eager to assist the United States in preventing terrorist organizations from soliciting funds on the Internet.

Third, the Internet is inexpensive. Many ISPs, including several in the United States, allow subscribers to register online for free web hosting services. These ISPs provide their services to subscribers free of charge and therefore have no incentive to accurately identify their subscribers. Nor do their subscribers have any disincentive to register a website that will be closed down after a short period of time—it costs them nothing, and they can simply open another one. Indeed, www.azzam.com used to inform its visitors: "We expect our web-site to be opened and closed continuously. Therefore,

[38] The nations currently on the State Department list are Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. *See* Patterns of Global Terrorism 2002 at 76, *available at* http://www.state.gov/s/ct/rls/pgtrpt/2002/pdf (Nov. 30, 2003).

we urgently recommend any Muslims that are interested in our material to copy all the articles from our site and disseminate them through their own web-sites, discussion boards and e-mail lists."[39]

Fourth, the Internet is largely unregulated. In most countries, there is no central government authority that reviews the content of websites before they are hosted online.[40] Moreover, most ISPs have neither the resources nor the desire to monitor the content of their customers' websites. Large ISPs have literally millions of customers; small ISPs generally have limited budgets and small staffs. Although law enforcement may search the Internet for public sites soliciting donations to terrorist organizations, they, too, lack the resources to maintain constant vigilance over the vastness of the Internet.

An example may be helpful in trying to understand how a terrorist operative might host a direct solicitation website while avoiding identification by law enforcement. Consider an al-Qaeda operative living in New York City. He receives, by regular mail, a diskette from Pakistan containing the content of a website praising the September 11 "martyrs" and encouraging supporters to send funds to three bank accounts in Karachi to support future attacks against the "infidels." The sympathizer accesses the Internet from a New York public library and registers online using false identification information with a free web-hosting provider (there are dozens, at least, in the United States). Law enforcement does not discover the website for several weeks. They compel the ISP to provide any information it has regarding the subscriber account, a process that may take additional time, and discover that the information is almost certainly false: the site was registered from a public library computer by John Doe at 315 Nameless Avenue, New York, NY, telephone 123-456-7890. Because the ISP keeps virtually no logs (records of activity on the site)—its business plan calls for low overhead, the ISP's representative explains, and logging and data storage cost money—law enforcement obtains, at most, IP addresses for the visits to the site over the last several days. The logs are not detailed enough to distinguish between someone who visited the site accidentally, leaving immediately when he discovered its content, and someone who printed out donation instructions or submitted a donation via credit card while on the site. See Figure 2.

---

[39] *See* Anti-Defamation League, *supra* note 34, at 14.

[40] The author serves as the Rapporteur for the G8 Subgroup on High-Tech Crime and the Head of the United States Delegation to the Organization of American States Group of Government Experts on Computer Crime, international bodies (see *supra* note 25) that cover 41 legal systems, and none of them have such a regulatory body.

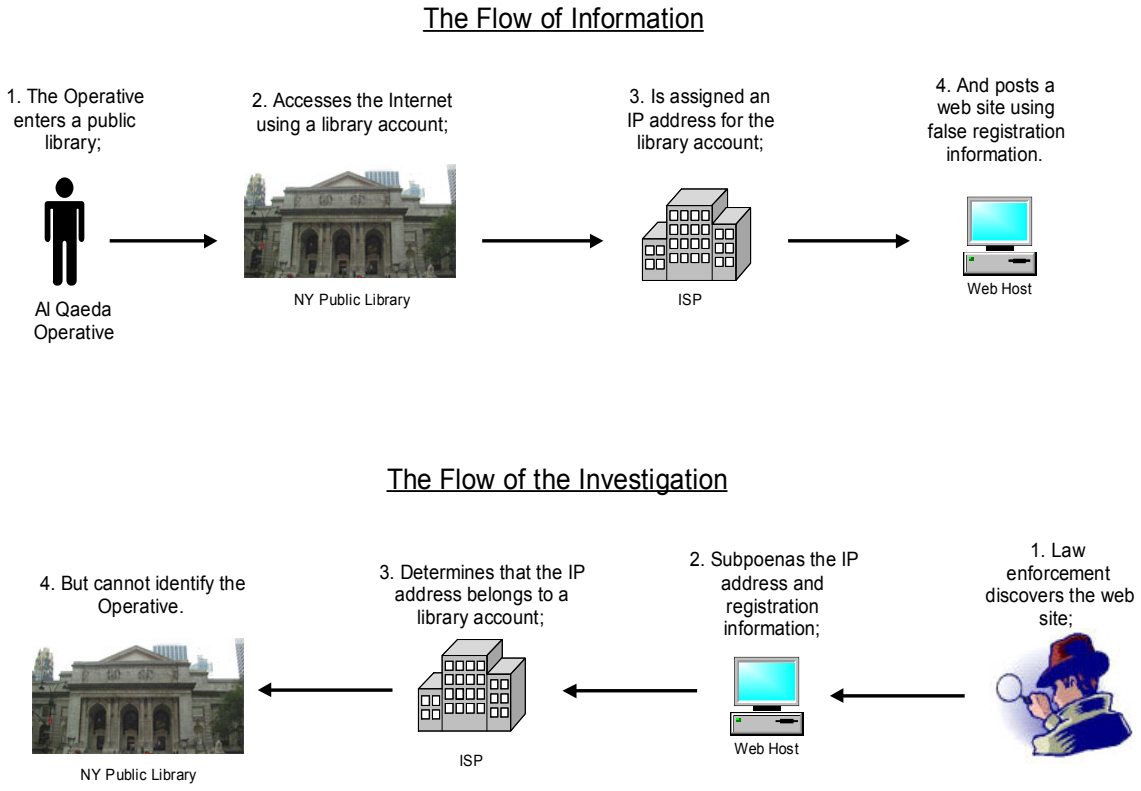

Figure 2

Investigation of the individuals who donate through such sites is subject to the same obstacles—use of public computer terminals or anonymizers, Internet accounts registered using false subscriber information, and failure of the web hosting ISP to retain logs of who visited the site and what they did there. Donors are susceptible, however, to an undercover investigative technique: law enforcement, posing as an online solicitor, can host such a site itself. Sites hosted by law enforcement for the purpose of attracting and gathering information on criminals are called "honey pots." Such a site would appear identical to the example discussed above (law enforcement could even re-open the site on a computer it administers). It would differ from the site above, however, in that it would record everything a visitor did while on the site and not actually send donations to the organizations. If a donor read a home page describing the site's purpose (i.e., to support a terrorist organization) and then filled out and submitted an electronic donation form, law enforcement would have good evidence that the visitor intended to donate money to support a terrorist organization.

Recent events suggest that terrorist organizations are aware of these and other features of the Internet. The capture of terrorist officials or infiltration of terrorist compounds is now often accompanied by the discovery of computers that have accessed the Internet.[41] In addition, many of the individuals and organizations in the United States

[41] *See, e.g.,* Alan Cullison & Andrew Higgins, *Suicide Watch: Al Qaeda Acolyte, One of Many, Vows to Die for the Cause*, Wall St. J., Dec. 30, 2002 at A1 (reporting on the contents of a

under investigation or facing prosecution for terrorist-related activities are highly trained in computer networks and communication systems.[42] Cybersecurity specialists also maintain that terrorists have probed the networked operation and security systems of several critical U.S. infrastructures, possibly in preparation for an attack on those systems.[43] Terrorist organizations are becoming increasingly adept at taking advantage of these features of the Internet.

2. Prosecution

If law enforcement is able to identify either a solicitor or a donor, and that individual or organization is located within the United States (if not, jurisdiction and extradition may pose separate challenges, depending on the United States' relationship with the country in which the defendant is located), establishing a substantive violation of United States law is generally not difficult. The United States criminal code contains strict prohibitions against providing financial or other material support knowing that it will be used to commit terrorist acts,[44] and knowingly providing material support to a designated "foreign terrorist organization."[45] The Code also prohibits conspiring within the jurisdiction of the United States to kill, kidnap, or maim any individual outside the United States, or to damage any property in a foreign country with which the United States is at peace, a prohibition that may apply to a perpetrator who solicits or donates funds in the United States knowing that they will be used to commit a specific act of terrorist violence abroad.[46] Moreover, the money laundering statute[47] applies to any individual other than the original donor who handles such a donation knowing that it will be used to support a terrorist organization, because each such individual conducts a transaction knowing that it involves the proceeds of illegal conduct (the donation) with intent to promote or continue the conduct. Finally, where a website, chat room, or e-mail solicits an individual to commit an act of terrorism that violates federal law, the

computer seized from a Taliban compound in Afghanistan); Kamran Khan, *Alleged Sept. 11 Planner Captured in Pakistan*, Wash. Post, Mar. 2, 2003, at A1 (reporting that computer equipment was seized from the house in which Khalid Sheik Mohammed was captured).

[42] *See, e.g.,* John Mintz*, 5 in Texas Jailed in Hamas Probe*, Wash. Post, Dec. 19, 2002, at A3 (reporting arrest of five executives of a Dallas computer firm who allegedly conspired to conceal financial transactions with an alleged terrorist leader); Susan Schmidt, *5 Tied To Islamic Charity Indicted in N.Y., Idaho*, Wash. Post, Feb. 27, 2003, at A2 (reporting that the five included a doctoral student in computer science).

[43] *See* Barton Gellman, *Cyber-Attacks by Al-Qaeda Feared,* Wash. Post, June 27, 2002, at A1.

[44] *See* 18 U.S.C. § 2339A (2000).

[45] *See* 18 U.S.C. § 2339B (2000).

[46] *See* 18 U.S.C. § 956 (2000).

[47] *See* 18 U.S.C. § 1956 (2000).

individual who posts or sends it may be charged under the criminal solicitation statute.[48] These criminal statutes impose substantial penalties for violations and, in conjunction with other statutes, enable the government to seize the proceeds of terrorist fund raising activities.

B. Exploitation of Charities & E-Commerce

Terrorist organizations have frequently and successfully exploited charities as vehicles for surreptitious fundraising. In some cases—as with Wafa al-Igatha al-Islamiya, Rabita Trust, Al Rasheed Trust, Global Relief Fund, Benevolence International Foundation, and Help The Needy—terrorist organizations have established a charity with an avowedly humanitarian purpose.[49] These charities have advertised in sympathetic communities' press and on websites and chat rooms with Islamic themes.[50]

For example, Al-Rashid Trust, a Pakistan based, al-Qaeda affiliated charity describes itself as "[a] prestigious welfare organization whose comprehensive services are benefiting all the Muslims of the world."[51] The Trust's website solicits donors with an impressive list of humanitarian accomplishments and a promise that "[m]ore attention shall be given to the departments of health, food, education, and employment."[52] Just days after the September 11 attacks, however, President Bush signed an executive order identifying the Trust as a financial conduit for the Taliban and al-Qaeda and freezing its

---

[48] *See* 18 U.S.C. § 373 (2000).

[49] *See* Office of Foreign Assets Control, *Specially Designated Nationals and Blocked Persons* (listing these purported charitable organizations as terrorist organizations), *at* http://www.treasury.gov/offices/eotffc/ofac/sdn/t11sdn.pdf.

[50] *See, e.g.,* http://web.archive.org/web/20011127193351/english.islamway.com/ (displaying a banner for the Global Relief Foundation, a charity that has subsequently been designated as a foreign terrorist organization); The Muslim Student Association's Web Site, *available at* http://web.archive.org/web/20011218180645/www.msa-natl.org/chechnya/ (providing a link to the Benevolence International Foundation, another charity that has subsequently been designated a foreign terrorist organization. Islamic populations may be particularly susceptible to the exploitation of charitable organizations because the Quran requires Muslims to give a portion of their money to charity. The Quran divides alms giving into the obligatory ("zakat") and the voluntary ("sadaqa"). Devout Muslims may give contributions directly to Islamic organizations or needy individuals. In some Islamic countries, however, the collection and distribution of charitable funds is managed by the government. For example, the Islamic affairs councils of various states in Malaysia collect and disburse contributions, while Pakistan imposes a 2.5% annual income tax upon its Sunni Muslim residents. Unfortunately, terrorist organizations exploit this admirable Islamic practice to support their mission of violence.

[51] *See* UMMAH.com, *Al-Rasheed Trust—A blessing for the Muslim world* (Apr. 22, 2003), *available at* http://web.archive.org/web/20030608204207/http://www.ummah.net.pk/dharb/services.htm.

[52] *Id.*

U.S. assets.[53]

The Benevolence International Fund ("BIF") provides another example of how terrorists can simultaneously raise funds and avoid scrutiny by cloaking themselves as a charitable organization. In 1993, the United States Internal Revenue Service ("IRS") granted BIF tax-exempt status under 26 U.S.C. § 501(c)(3) (2000).[54] BIF raised millions of dollars each year during the 1990s, in part by accepting donations on its website www.benevolence.org.[55] Authorities have uncovered evidence that BIF transferred money to al-Qaeda, including funding two al-Qaeda attempts to purchase radioactive materials; to the Islamic extremists involved in the 1993 World Trade Center bombing; and, as recently as April 2000, to a Chechnyan extremist faction trained by al-Qaeda.[56] The Department of Treasury has listed BIF as a financier of terrorism.[57] In October 2002, BIF's leader, Enaam Arnaout, was indicted for, among other things, providing material support to terrorist organizations, including al-Qaeda.[58] In 2003, Arnaout pled guilty to lesser charges involving diversion of charitable contributions to armed militant groups in Bosnia and Chechnya.[59]

In other cases, terrorists have infiltrated branches of existing charities to raise funds surreptitiously. Many such organizations provide the humanitarian services advertised: they feed and clothe the poor, educate the illiterate, and provide medical care for the sick and the suffering—and it is important not to presume that charitable organizations have terrorist affiliations simply because they serve regions or religious or ideological communities with which terrorism may be associated. Some such organizations, however, in addition to pursuing their public mission of providing humanitarian aid, pursue a clandestine agenda of providing material support to the militant groups that seek violently to "liberate" their particular region or expand the influence of their particular religion or ideology. These organizations' propaganda may or may not provide hints as to their darker, more secret purpose.[60]

The Qatar Charitable Society ("QCS") illustrates how a terrorist organization can infiltrate a legitimate charity and exploit its funding base. At the trial of the conspirators who planned the bombings of the U.S. Embassies in Kenya and Tanzania, a former al-

---

[53] Exec. Order No. 13,224, 66 Fed. Reg. 49079 (Sept. 23, 2001).

[54] *See* Indictment, United States v. Arnaout, No. 02-CR-892 (N.D. Ill. Nov. 1, 2002), *available at* http://news.findlaw.com/hdocs/docs/terrorism/usarnaout10902ind.pdf.

[55] *Id*.

[56] *Id*.; *see also* Anti-Defamation League, *supra* note 34.

[57] *See* Indictment, *Arnaout*, No. 02-CR-892.

[58] *Id.*

[59] *See* Plea Agreement, United States v. Arnaout, , No. 02-CR-892 (N.D. Ill. Nov. 1, 2002), *available at* http://news.findlaw.com/hdocs/docs/bif/usarnaout203plea.pdf.

[60] *See supra* note 50 and accompanying text.

Qaeda member and QCS employee identified QCS as an al-Qaeda front and a financial conduit for militant jihadists around the globe.[61] The mission statement on its website did not foreshadow such involvement: "QCS aims to offer relief and help to orphans, victims of war and disasters by supporting them financially, socially and culturally up to the age of 18. QCS aids widows to meet living expenses particularly those who lost all relatives and friends."[62]

Terrorist exploitation of such charities is of particular concern because, as one commentator recently observed, "The operation under tax-exempt status in the United States of organizations that actively fund terrorist activities abroad, has meant that the U.S. government, and all U.S. taxpayers, indirectly finance" terrorists and terrorist organizations.[63]

Terrorist-affiliated entities and individuals have also established Internet-related front businesses as a simultaneous means of facilitating communications among terrorist cells and raising money to support their mission. For example, InfoCom, a Texas-based ISP, was indicted along with its individual corporate officers in December 2002 on thirty-three counts relating to its provision of communication services, in-kind support, and funds to terrorist organizations such as Hamas and the Holy Land Foundation for Relief and Development (HLFRD).[64] According to the indictment, InfoCom also exported advanced computer technologies to designated State Sponsors of Terrorism Libya and Syria in violation of IEEPA.[65] Incorporated in Texas in 1992, InfoCom's capital was donated primarily by Nadia Elashi Marzook, wife of Hamas figurehead and specially-designated terrorist Mousa Abu Marzook.[66]

1. Prevention & Investigation

Charities continue to be an attractive vehicle for terrorist groups seeking to raise and move funds. Such organizations are often hard to distinguish from the scores of legitimate charities providing humanitarian aid, a task rendered more difficult by the fact

---

[61] *See Fund-Raising Methods and Procedures for International Terrorist Organizations, Hearing before the House Committee on Financial Services Subcommittee on Oversight and Investigations*, Feb. 12, 2002 (Testimony of Steven Emerson quoting Transcript of Trial Testimony, Jamal Ahmed Al-Fadl, United States v. Bin Laden, 329-30 (Feb. 6, 2001)), *available at* http://financialservices.house.gov/media/pdf/021202se.pdf.

[62] QCharity, *at* www.qcharity.org/qenglish/index.html.

[63] Mindy Herzfeld, *Restricting the Flow of Funds from U.S. Charities to International Terrorist Organizations—A Proposal*, 56 Tax Law. 875, 875 (2003).

[64] *See* Indictment, United States v. Elashi, Cr. No. 3:02-CR-052-R (N.D. Tex. Dec. 17, 2002), *available at* http://news.findlaw.com/hdocs/docs/infocom/uselashi121702sind.pdf.

[65] *Id.*

[66] *Id.*

that organizations that bankroll terrorist groups also often finance legitimate charitable projects. The Internet exacerbates this problem in two respects. First, a charity may locate itself anywhere in the world—in a state that sponsors terrorism, for instance, or a country that does not regulate charitable organizations—and, through the Internet, obtain access to donors worldwide. Second, a charity that exists primarily online is not generally subject to the scrutiny of donors or regulators in the way that predominantly brick-and-mortar charities are. Donors do not, for the most part, visit the charity's offices or speak to one of its representatives.

The United States' effort to prevent terrorist groups from raising and moving money through charities focuses largely on domestic regulation and international cooperation. To obtain charitable status in the United States an organization must file an Application for Recognition of Exemption (Form 1023) with the IRS.[67] The application requires the organization to list its name, address, phone number, website, and general information about its formation or incorporation and its activities and operations. The organization must also provide information regarding its financial support, fundraising program, officers or directors, and the basis upon which it qualifies for exempt status.

Once the IRS grants an organization tax-exempt status, the organization must file annually a Form 990 containing its name, address, website, and phone number; contributions and other forms of income or revenue; operational expenses; charitable activities and accomplishments; officers and directors; and a list of contributors who donated more than $5,000 during that year.[68]

With regard to charities located overseas, the United States relies heavily on the host country's help in preventing abuse. To this end, the Special Recommendations on Terrorist Financing adopted by the FATF in October 2001 exhorted member countries to review their laws and regulations governing charitable organizations and ensure that such organizations are not subject to misuse.[69] In addition, the United States has actively

---

[67] If the organization seeks the exemption for any subsection other than 501(c)(3), they provide similar information on a Form 1024 instead.

[68] The Internal Revenue Code specifies the procedures that the IRS must follow in order to revoke the exempt status of any organization. *See* 26 U.S.C. § 7428 (2000). The Code also provides the organization with the right to contest a determination that its tax-exempt status should be revoked in the United States Tax Court, and appeal an adverse decision from the Tax Court to the appropriate United States Court of Appeals. *See id.* In order to revoke an organization's tax-exempt status, the Commissioner of Internal Revenue must: (1) conduct an examination of the organization; (2) issue a letter to the organization proposing revocation; and (3) allow the organization to challenge that determination in administrative proceedings. *See id.* The actual letter of revocation may be issued only at the conclusion of that administrative process. During any subsequent Tax Court proceeding or appeal to the Court of Appeals, the organization continues to enjoy tax-exempt status. This process may take years to complete. As a result, an organization that has had its assets frozen pursuant to a presidential order may continue to remain tax-exempt under the Code for years. To address this situation, the Senate is currently considering a bill that would suspend an organization's exempt status as soon as it is identified as a terrorist organization. *See* CARE Act of 2003, S. 272, 108th Cong. (2003)

[69] *See* Special Recommendations on Terrorist Financing, *supra* note 25

availed itself of bilateral meetings and multilateral fora to encourage other countries to strengthen regulatory control over charities within their borders.[70]

Greater awareness and caution on the part of donors may also help curb online terrorist fund raising. In this respect, the Internet provides some of the means to cure its own ills. The government may educate donors both by waging a proactive media campaign to raise awareness of online charities associated with terrorist organizations and by encouraging donors to take advantage of the vast resources on the Internet regarding charitable organizations. For instance, the site www.guidestar.org provides information on every charitable organization recognized by the IRS. Donors may also take advantage of the websites of organizations such as InterAction, the Better Business Bureau Wise Giving Alliance, and the National Association of State Charities Officials, which provide reports on charities, promote standards of accountability for charities, and alert donors to current charity frauds.[71] The Treasury Department, too, has promulgated guidelines encouraging charities to operate with appropriate transparency and accountability in order to discourage criminals and terrorists from exploiting charitable organizations.[72] By publicizing terrorists' use of charity websites to raise funds and by encouraging donors to learn about a charity before contributing to it, government and private organizations can reduce the amount of unwitting donations made to terrorist groups.

Investigation of a charitable organization with an online presence generally begins with discovery of that organization's affiliation with a terrorist organization. In a rare case, it may be possible to demonstrate the affiliation by online investigation. For instance, if a charitable organization's website includes a hyperlink to a terrorist propaganda page or vice versa, this may form the basis for further investigation. The information provided regarding a particular charity by online information services, such as www.guidestar.org, may also provide grounds to suspect that a charitable organization has terrorist connections. More often than not, however, the affiliation will be discovered through offline investigative techniques.

---

[70] *See* Testimony of Kenneth Dam, *supra* note 6.

[71] *See* InterAction Homepage, *at* http://www.interaction.org; Give.org Donor Information, *at* http://www.give.org/donors/index.asp; NASCO Homepage, *at* http://nasconet.org.

[72] *See* U.S. Department of the Treasury Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities, *available at* http://www.treas.gov/press/releases/docs/tocc.pdf.

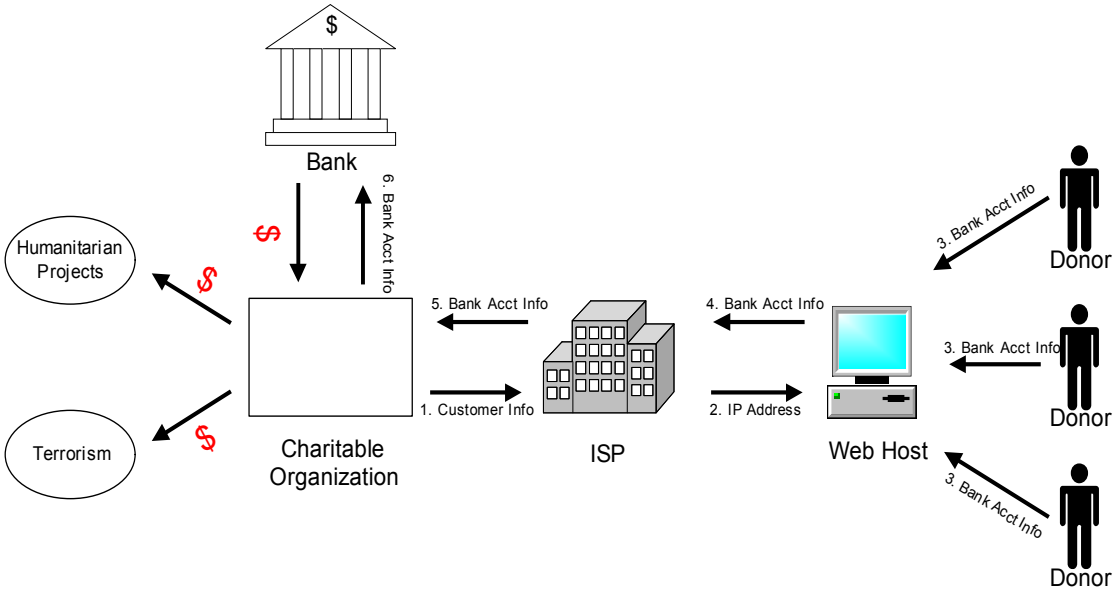

Figure 3

Once the affiliation is identified, there will be several sources of information online. The ISP that hosts the charity's website may have logs that indicate who created the site, who has visited it, and what they have done there. See Figure 3. In addition, such charitable organizations may keep electronic records of their donors, so that the charities can contact the donors again for future donations. Records regarding the accounts associated with the organization may be subpoenaed, and affiliated electronic mail accounts can be searched for communications with members of terrorist organizations or regarding terrorist activities. In addition to these online sources, law enforcement may obtain a charitable organization's Form 1023 or 1024 and its Form 990s.[73]

2. Prosecution

Once investigation demonstrates the affiliation between a charity and a terrorist group, the case against the charity or individuals associated with the charity is made. Law enforcement still has an important decision to make, however, before prosecuting such a charity and/or its donors. A charity that provides funds and resources to a terrorist organization may be a valuable source of information regarding that organization. If the ISP that provides web hosting service to the charity is located within the United States, law enforcement can obtain logs showing the IP addresses from which the site was

[73] As a result of amendments to the tax laws passed in the Victims of Terrorism Tax Relief Act of 2001, Pub. L. No. 107-134, 115 Stat. 2427 (Jan. 23, 2002), law enforcement now has expanded authority to obtain tax returns and return information for the purpose of preventing or investigating terrorist incidents, threats, or activities. *See* 26 U.S.C. § 6103 (2000).

accessed and the donations submitted online, as well as the electronic communications of the website operators (assuming that they provide their own electronic mail service through the website), which may identify individuals involved in the terrorist organization or reveal details about imminent operations. Law enforcement must assess in each investigation whether the benefit to be gained by prosecuting the individuals who are abusing the charitable organization outweighs the benefit to be gained by monitoring them as they continue to act.

If law enforcement does prosecute such a case as discussed above, providing money or material support to a terrorist organization may violate 18 U.S.C. § 2339A, § 2339B (if the organization has been designated a FTO), or 18 U.S.C. § 956 (making conspiracy to cause injury abroad a crime). Soliciting donations over the Internet from donors who believe their money is being used for humanitarian purposes, when in fact it is being used to support violent extremism and militancy, may violate the wire fraud statute.[74] Transferring funds received by a charity to another organization to further such unlawful activity may violate the money laundering statute, 18 U.S.C. § 1956. In all likelihood, the organization will have submitted false tax documents as well, a violation of 26 U.S.C. § 7206(1) and 18 U.S.C. § 1001.

Prosecuting contributors to such organizations will, in most instances, be inappropriate—they intended to contribute to a humanitarian organization, not to a terrorist front. To prosecute a contributor for a violation of §§ 956, 1956, or 2339A, the government must first prove that a contributor knew that a charity was affiliated with a terrorist organization and would use the funds contributed in support of an act of terrorism. If an organization has been designated an FTO, however, the prosecutorial burden is somewhat diminished—under § 2339B, the government must prove only that the contributor knew the organization was an FTO; it need not prove that the contributor knew the funds would be used to support terrorist activities.

C. *Proceeds of Online Crimes*

In addition to soliciting funds, either directly or through charitable or e-commerce front organizations, terrorists use the Internet to raise funds by perpetrating online crimes. The same qualities that protect individual privacy on the Internet make Internet users particularly susceptible to fraud and deception. The anonymity users enjoy online also allows the perpetrator of a fraud to pose easily as someone else—an identity theft victim or a fictitious person. Terrorists have used identities they have stolen through online fraud schemes to obtain cover employment within the United States, access to bank and credit card accounts, and even entry into secure locations.[75]

It requires very little expertise to change the "from" information on an e-mail so

---

[74] 18 U.S.C. § 1343 (2000).

[75] *See The Identity Theft Penalty Enhancement Act before the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information*, 108th Cong. (2002) (statement of Dennis M. Lormel Chief, Terrorist Financial Review Group Federal Bureau Of Investigation), *available at* http://www.fbi.gov/congress/congress02/idtheft.htm.

that it appears to come from an ISP's billing department, a credit card company, or a bank. Slightly more skill allows a user to design a fraudulent web page that purports to be an ISP's, the credit card company's, or the bank's customer service center. The ease and efficiency with which an Internet user can communicate with hundreds or thousands of other users, regardless of geographic location, makes the Internet an environment particularly conducive to vast fraud schemes with numerous victims.

Online auction fraud is another common e-crime gambit—the perpetrator offers to sell a valuable item, such as a piece of jewelry, through an online auction service, receives payment, and never sends the item. The purchaser attempts to obtain recourse from the seller, only to find out that he has provided fraudulent contact information. Online securities frauds, such as "pump and dump" schemes in which an investor publishes online fraudulent information about a security to inflate its value and then sells large quantities of the security at the inflated price, might also provide a source of funding for terrorist organizations.[76] Finally, commentators have recently suggested that the proceeds of intellectual property piracy may also be supporting terrorist organizations.[77]

1. Prevention & Investigation

Regulation of ISPs and of Internet users would prevent some online crimes. If electronic communications services, remote computing services, web hosting services, and other ISPs were required to obtain and verify valid contact information for each of their subscribers, for instance, the number of investigations that would dead-end at false registration information would diminish significantly. Similarly, if ISPs were required to retain logs regarding the use of their services, more information would be available to law enforcement investigating online crimes. The United States does not require by law or regulation, however, that ISPs retain such information.[78] ISPs are understandably

[76] For a thorough discussion of online securities frauds, *see* John Reed Stark, *Enforcement Redux: A Retrospective of the SEC's Internet Program Four Years after Its Genesis*, 57 Bus. Law. 105 (2001).

[77] *See* Levitt, supra note 29.

[78] Most European countries have also shied away from requiring ISPs to retain information. "[T]o ensure . . . protection of . . . the right to privacy, with respect to the processing of personal data in the electronic communication sector," the European Union obligates its 15 member countries to pass laws requiring ISPs to delete information regarding electronic communications if it is no longer being used to ensure the integrity of the communication service or for billing purposes. European Union Directive on Privacy and Electronic Communications, 2002/58/EC (July 31, 2002), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf. Several European countries, including France, Spain, Ireland, and Denmark, have, however, taken advantage of an exception to the "data protection" requirement that permits countries to adopt legislation requiring ISPs to retain data "for a limited period . . . to safeguard national security, . .

reluctant to have imposed upon them business practices that facilitate law enforcement investigations, rather than profit generation. Internet users are understandably protective of their privacy and anonymity.

For these reasons, the problem of Internet crime may be better prevented by encouraging increased security by ISPs and online businesses and by educating Internet users regarding the danger of online fraud. ISPs and online businesses can significantly reduce Internet crime by many means, some as simple as actively notifying their subscribers of current scams and swindles. Similarly, Internet users can abate online fraud by following simple rules such as "never provide your credit card number over the Internet except over a secure connection with a merchant you trust." As such measures reduce Internet crime in general, they will also reduce the amount of money flowing to terrorist organizations.

Deterrence, also, may play an important role in diminishing terrorists' commission of online crimes in order to raise funds and resources. In both the USA PATRIOT Act and the Homeland Security Act, Congress strengthened the statutory penalties for some computer crimes.[79] The Homeland Security Act also directed the United States Sentencing Commission to amend the United States Sentencing Guidelines to reflect adequately the prevalence and seriousness of computer crimes.[80] In addition, federal, state and local investigative and prosecutorial agencies have improved their ability to respond to such crimes. As these steps make punishment for online crimes more likely and more severe, the Internet will become a less appealing environment for criminal activity.

United States law enforcement's capacity to investigate and prosecute computer crimes has increased over the last several years. This is due, in part, to amendments in the USA PATRIOT Act and the Homeland Security Act concerning the procedural laws applicable to investigations of online activity.[81] These two Acts amended the laws that prescribe the procedures by which law enforcement may obtain information regarding online communications,[82] effectively streamlining these procedures while protecting the

---

. defence, public security, and the prevention, investigation, detection and prosecution of criminal offenses." *See id.* at Art. 15(1).

[79] *See* USA PATRIOT Act, Pub. L. No. 107-56, Title VIII, § 814, 115 Stat. 272 (2001); Homeland Security Act, Pub. L. No. 107-296, Title II, § 225, 116 Stat. 2135 (2002).

[80] *See* Homeland Security Act, Pub. L. No. 107-296, Title II, § 225, 116 Stat. 2135 (2002).

[81] Some of the amendments in the USA PATRIOT Act are subject to a sunset provision which will remove them from the code on December 31, 2005 unless they are affirmatively renewed. *See* Pub. L. No. 107-56, Title II, § 224, 115 Stat. 272 (2001). If these provisions are permitted to sunset, it will be a tremendous setback to law enforcement's ability to investigate and prosecute online crimes.

[82] Generally speaking, these laws are the Wire Tap Act, 18 U.S.C. § 2510 (2000), the Electronic Communications Privacy Act, 18 U.S.C. § 2701 (2000), and the Pen Register/Trap & Trace statute, 18 U.S.C. § 3121 (2000). *See also* the Dep't of Justice's manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, *available at* http://www.cybercrime.gov/s&smanual2002.pdf.

autonomy of ISPs and the privacy of Internet users. The Acts also amended the substantive laws applicable to computer crimes,[83] explicitly taking new strains of Internet criminality into account and strengthening penalties for many online crimes.

Law enforcement's increasing capabilities in investigating and prosecuting computer crimes are also due, in part, to the dedication of increased resources to this area and to federal, state, and local law enforcement entities' concomitant development of expertise. Many such entities now have cybercrime squads that are trained to investigate crimes committed via the Internet.[84] These experts complement traditional investigative techniques with Internet investigative techniques (such as legally obtaining information from ISPs and using publicly available online resources) and computer forensics.

The investigation of computer crimes has also been a fertile ground for international cooperation over the past several years, resulting in a greater ability to track computer crimes that cross international borders. The G8 Roma and Lyon Groups were established to combat transnational terrorism and transnational organized crime. They maintain a group of international computer crime experts, the G8 Subgroup on High-Tech Crime, which has promulgated principles and best practices regarding the prevention, investigation, and prosecution of computer crimes.[85] The Subgroup also maintains a network of computer crime experts from 35 countries who are available 24-hours-a-day, 7-days-a-week to respond to computer crime emergencies.[86] In addition, in November 2001, the Council of Europe completed negotiation of the Convention on Cybercrime, which commits its 35 signatories to pass procedural and substantive computer crime laws and to provide assistance to other signatory countries investigating cybercrimes.[87] Such cooperation and capacity-building in the international community is essential if the United States is to investigate effectively a mode of criminality that often transcends international borders.

It is worth noting that the measures for effectively preventing Internet crime and those for effectively investigating it are complementary. Adequately secured ISPs, well-educated users, strong, comprehensive procedural and substantive laws, and enhanced

---

[83] The primary substantive law applicable to computer crimes is the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000).

[84] For instance, each federal prosecutorial district now has an expert "Computer and Telecommunications Coordinator" to oversee prosecution of computer crime cases. *See* U.S. Dep't of Justice, Cybercrime Homepage, *at* http://www.cybercrime.gov/enforcement.html.

[85] *See, e.g.,* G8 Justice and Interior Ministers, *Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations*, *available at* http://www.g8j-i.ca/english/doc2.html; G8 Justice and Interior Ministers, *Principles on the Availability of Data Essential to Protecting Public Safety*, *available at* http://www.g8j-i.ca/english/doc3.html; G8 Justice and Interior Ministers, *Data Preservation Checklists*, *available at* http://www.g8j-i.ca/english/doc4.html.

[86] *See* 24-Hour Contacts for International High-Tech Crime (on file with the author).

[87] *See* Council of Europe, *Convention on Cybercrime*, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

law enforcement capacity all support effective prevention and investigation of online crimes and deprive terrorists of the proceeds of such crimes as a source of funding.

2. Prosecution

Federal, state, and local prosecutors, like investigators, have enhanced their ability to respond to Internet crimes. The United States Department of Justice, for instance, maintains the Computer Crime and Intellectual Property Section, a team of approximately 40 attorneys with expertise in the prevention, investigation, and prosecution of computer crimes.[88] This team forms the nucleus of a network of federal computer crime experts that includes at least one Computer and Telecommunications Coordinator ("CTC") in each of the United States' 94 federal law enforcement districts and Computer Hacking and Intellectual Property ("CHIP") units in several of the larger districts.[89]

As mentioned above, prosecutors are now armed with procedural laws designed to expedite the gathering of electronic evidence that encompass more destructive online behavior and punish such behavior more severely. Although one should not expect fraud or unauthorized intrusions to be eradicated from the Internet any more than fraud or burglary have been eradicated from the brick-and-mortar world, as network security, user education, and investigative and prosecutorial capabilities all continue to improve, Internet crime may well decrease, and with it the proceeds terrorist organizations derive from Internet crime.

III. Terrorist Use of the Internet to Move Funds

The term "moving funds," as used in this Article, encompasses any conduct proscribed and punished by 18 U.S.C. § 1956(a)(2) (2000), making it a crime for:

> Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States . . . with the intent to promote the carrying on of specified unlawful activity.

In addition, it includes transporting, transmitting, or transferring funds *within* the United States with the intent to support terrorists, and making funds available to terrorists by providing them with the means of access, such as a debit or credit card, a PIN number, or a password.

---

[88] To learn more about the Department of Justice's efforts to combat computer crime and intellectual property violations, visit the U.S. Dep't of Justice, Cybercrime Homepage at http://www.cybercrime.gov.

[89] For a detailed description of the CTC and CHIPs programs, visit the U.S. Dep't of Justice, Cybercrime Homepage at http://www.cybercrime.gov/enforcement.html.

As § 1956 indicates, one of the difficulties law enforcement faces in identifying terrorist financing is the fact that it is often the intent that the resources transferred support a *future* act of terrorism that makes such transfers illegal. Because the parties' intent is often not visible on the face of their transaction, it may be difficult to distinguish legitimate transfers of value (to support an ailing relative in the sender's native land, for instance) from terrorist financing.

Terrorists may use the Internet to transfer funds in three primary ways. First, they use Internet banks, online banking, and other financial services.[90] Second, they use Internet-based alternative value transfer systems, such as Internet payment services and e-cash. Finally, terrorists communicate over the Internet regarding the movement of funds.

A. *Formal Online Financial Services*

Brick-and-mortar banks and other financial institutions increasingly offer their customers online financial services.[91] A recent article estimated that whereas in 1994 only .3% of United States households used online banking, currently 26% (a total of 21 million United States households) use such services.[92] The article projected that this figure would increase to 45% by 2010. An April 2002 report on Internet banking by Harvard University's Program on Information Resources Policy indicated that all the largest United States banks now offer Internet banking.[93]

As demand for the convenience of online services increases, Internet-only banks are also entering the market. Although there were only nine separately chartered virtual banks at the beginning of 2000, they were attracting a relatively large client base.[94] First-e, the virtual bank of online finance company Enba, attracted 71,000 customers in its first six months of business.[95] Online banking is equally popular abroad, with financial entities such as Egg and ING populating foreign financial services markets.

---

[90] Terrorists may move funds through a variety of formal financial institutions, including securities and futures brokerages, mutual fund companies, and investment companies. These institutions are included within the definition of "financial institution" set forth in the anti-money laundering provisions of the Bank Secrecy Act, and pursuant to the USA PATRIOT Act, they must establish anti-money laundering programs reasonably designed to prevent their use for money laundering or terrorist financing. *See* 31 U.S.C. §§ 5313(a)(2), 5318(h) (2000).

[91] Although this discussion focuses primarily on the banking system, the discussion also applies to non-banking financial services and to non-depository financial institutions.

[92] *The Rise in Online Banking*, The Philadelphia Inquirer, Feb. 10, 2003.

[93] Karen Furst et al., *Internet Banking: Developments and Prospects,* Program on Information Resources Policy, Apr. 2002, *available at* www.pirp.harvard.edu/publications.

[94] *Id.*

[95] *See* William Echikson, *Euro E-Bank Whiz*, BusinessWeek Online, May 15, 2000, *available at* http://www.businessweek.com/2000/00_20/63681105.htm.

The Internet infrastructure underlying online banking and other financial services allows customers more easily to take advantage of the global nature of the financial system. With a few clicks of the mouse, a customer in one country can set up accounts in several other countries. With a few more clicks, the customer can transfer money between these accounts. The convenience, speed, and fluidity of online financial services are tremendous assets to customers and to the global economy. These same features, however, make online financial services a potential vehicle for terrorists and terrorist organizations seeking to move funds. The efficiency of the Internet makes it easier to "layer" transactions and fund transfers, routing money through a number of accounts using a number of different instruments and transfer mechanisms within a short period of time. See Figure 4.

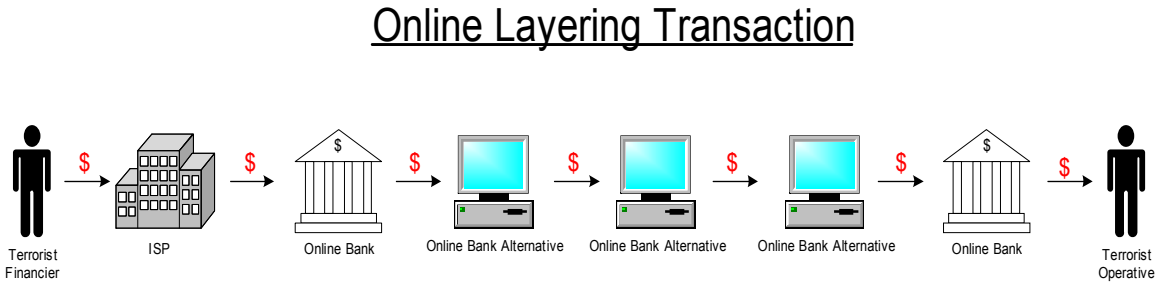

Figure 4

If any of the accounts used by the customer is in a country that does not require financial institutions to maintain information regarding such transactions or in a country that does not share such information, the ability to trace such transfers is severely hindered.

Terrorist use of online banking services is facilitated in part by banks that have terrorist ties. For instance, Al-Taqwa Bank, founded by the Muslim Brotherhood in the Bahamas in 1988, maintained branches in Algeria, Liechtenstein, Italy, Malta, Panama, and Switzerland, and provided banking services to al-Qaeda and Hamas until it was shut down by sanctions in the wake of September 11.[96] Similarly, Hamas established Al-Aqsa Bank in 1997.[97]

1. Prevention & Investigation

Regulation of the financial services industry is the primary tool for preventing terrorists from moving funds through the United States banking system. Banks often act as the gateway to the world of financial and fund transfer services. The first step in financial security is identifying a customer as she opens an account and verifying her

[96] *See* Testimony of Steven Emerson, *supra* note 61, at 19–21.

[97] *Id.* at 21–22.

identity.[98] For traditional brick-and-mortar banking, this process often involves meeting the customer, obtaining identifying documents that have photographs or list physical characteristics that match the customer's characteristics, and observing the customer's behavior. In an Internet banking context, none of these traditional techniques is possible.[99] Banks can, and do, ameliorate the risks inherent in online banking by requiring new customers to provide identifying information such as their social security number, driver's license number, address, and phone number, and by independently confirming that the information provided is valid.[100]

The USA PATRIOT Act directed the Secretary of the Treasury to promulgate regulations normalizing among all financial institutions[101] the process of identification and verification.[102] On April 30, 2003, the Secretary of the Treasury, in conjunction with the Federal banking agencies, the SEC, and the CFTC, released for final publication regulations requiring banks, broker-dealers, mutual fund managers, futures commission merchants, and introducing commodities brokers to adopt by October 1, 2003 a written Customer Identification Program ("CIP") setting forth procedures pursuant to which that entity will: (1) identify customers as they open accounts by obtaining information such as the customer's name, address, date of birth, and taxpayer identification number; (2) exercise reasonable efforts to verify the customer's identity; (3) maintain records of information obtained during the identification and verification processes; and (4) consult

---

[98] *See* Office of the Comptroller of the Currency, *Internet Banking: Comptroller's Handbook*, *available at* http://www.occ.treas.gov/handbook/intbank.pdf (Oct. 1999). Banks may also offer transferable monetary instruments such as money orders and value transfer services such as wire transfers without requiring a customer to open an account. Monetary instruments are subject to identification rules promulgated by FinCEN if they are purchased with more than $3,000 in cash. *See* 31 C.F.R. § 103.29 (2003). Likewise, money transfer services that involve more than $10,000 in cash are subject to FinCEN's currency transaction reporting rule. *See* 31 C.F.R. § 103.30 (2003). In addition, the purchase of money orders and the use of value transfer services are subject to the suspicious activity reporting requirements, discussed *infra*.

[99] *See* Office of the Comptroller of the Currency, *OCC Bulletin: ACH Transactions Involving the Internet*, *available at* http://www.occ.treas.gov/ftp/bulletin/soos-2.txt (Jan. 14, 2002); OCC, *Authentication in an Electronic Banking Environment*, *available at* http://www.ffiec.gov/PDF/pr080801.pdf (Aug. 8, 2001).

[100] *See* Ivan Schneider, *Banks Crack Down on Terror Funds*, *available at* www.banktech.com/story/whatsNews/BNK20020408S0002 (Apr. 8, 2002) (noting that "in the ongoing war on terrorism, banks and their technology providers can best serve the government by acting as a tripwire for criminals attempting to infiltrate the world financial systems").

[101] The statutory definition of "financial institutions" includes banks, credit unions, securities brokers and brokerage houses, currency exchanges, and several other, less formal entities offering financial services. *See* 31 U.S.C. § 5312 (2000).

[102] *See* USA PATRIOT Act, Pub. L. No. 107-56, Title III, § 326, 115 Stat. 272 (2001).

lists of individuals and organizations whose assets have been blocked or frozen.[103] The financial institution's CIP must enable it to form a reasonable belief that it knows the true identity of each customer.[104]

Financial institutions' role in ensuring the security and integrity of the United States' financial system does not end once a customer has opened an account. Financial institutions are also required to report to an appropriate federal law enforcement agency and to the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") any transaction exceeding $5,000 that attracts suspicion, either because it serves no evident business purpose or because it is unusual for that particular customer.[105] The United States, through participation in multilateral bodies, has encouraged other countries to adopt similar regulations.[106]

As these regulations indicate, much of the burden of securing online financial services against abuse by terrorist organizations must be borne by financial institutions. Both within the United States and internationally, oversight and regulatory bodies have offered guidance to financial institutions seeking to expand into the electronic market without becoming vulnerable to misuse by terrorist organizations and other criminals. For instance, in 2001 the Federal Financial Institutions Examination Council ("FFIEC") issued a report entitled *Authentication in an Electronic Banking Environment* that advises banks regarding how to verify effectively the identity of new customers who open accounts online and authenticate the identity of existing customers who initiate fund transfers or other transactions online.[107] The OCC and the Federal Reserve Bank of Chicago also offer guidance regarding secure electronic banking and fraud and intrusion prevention.[108] On the international front, in May 2001 the Basel Committee on Banking Supervision published its seminal document *Risk Management Principles for Electronic Banking*.[109] These documents encourage banks in the United States and abroad to consider the risks involved in offering electronic banking services and develop a strategy to manage those risks; to install and maintain adequate security to ensure that electronic

---

[103] *See* Press Release, Dep't of the Treasury, Treasury and Federal Financial Regulators Issue Final PATRIOT Act Regulations on Customer Identification (Apr. 30, 2003), *at* http://www.treas.gov/press/releases/js335.htm.

[104] *See id.*

[105] *See* 12 C.F.R. § 21.11(2003); 31 C.F.R. §§ 103.18, 103.19 (2003).

[106] For instance, the Special Recommendations on Terrorist Financing adopted by the FATF exhort countries to require of financial institutions and other business entities prompt reporting of suspicious transactions that may be related to terrorism. *See supra* note 25.

[107] *See* Authentication in an Electronic Banking Environment, *supra* note 99; *see also* OCC Bulletin: ACH Transactions Involving the Internet, *supra* note 99.

[108] *See* Internet Banking: Comptroller's Handbook, *supra* note 98; Chicago Federal Reserve Board, *An Internet Banking Primer* (on file with the author).

[109] *See* Basel Committee on Banking Supervision, *Risk Management Principles for Electronic Banking*, *available at* http://www.occ.treas.gov/ftp/release/2001-42a.pdf (May 2001).

banking services are not vulnerable to fraud or attack, either by an insider or an Internet user; to supervise actively electronic banking services outsourced to third-party providers; to establish adequate identifying and authenticating protocols for online banking customers, preferably involving multiple, complementary methods; and to effectuate measures to ascertain the accuracy, completeness, and reliability of banking information exchanged over public electronic networks.[110]

Investigation of terrorist use of online financial services to transfer funds generally begins with information provided pursuant to the banking regulations and security measures discussed above. FinCEN analyzes Suspicious Activity Reports ("SARs") filed by financial institutions, searching for trends and patterns, and assists law enforcement in tracing complex financial transactions back to criminal suspects. Law enforcement also investigates reports of electronic banking fraud, attacks on electronic banking systems, and intrusions into electronic banking computers. Such investigations rely heavily on the records maintained by the victim bank, but because they involve online conduct, law enforcement may rely on an additional source of information.

A perpetrator's abuse of an electronic financial service leaves an electronic trail. If the conduct simply involves accessing e-banking services to transfer funds to a terrorist suspect, the perpetrator leaves behind an IP address when he accesses the services. If the ISP through which he connected to the Internet is in the United States, or a cooperating foreign country, law enforcement can obtain the customer information associated with that user, pinpointing the computer from which the account was accessed (although there may still be significant obstacles to identifying the perpetrator if he used an Internet café, public library terminal, or anonymizer).

If the conduct involves fraud, the perpetrator leaves behind an IP address and a cache of electronic messages to and from the defrauded financial institution or individual. The financial institution very likely logs both the IP address from which the customer accessed the website and the customer's activity while on the website. Whereas an ISP may have little business incentive to maintain logs of its subscribers' communications for extended periods of time, a financial institution has every incentive to maintain thorough and accurate logs of customer and account activities. Not only is reliable verification of account activities central to the financial institution's business, it is required by regulation.[111] Moreover, for an online bank transfer to work, the customer must provide valid destination information. Investigation of online bank transfers therefore poses only one challenge—because such transfers appear much the same as legitimate transfers, it is often difficult to determine which transfers are worthy of investigation.

2. Prosecution

A bank transfer to a recipient that the transferor knows is a terrorist or terrorist

[110] *See supra* notes 103–105.

[111] The regulations promulgated by the Department of Treasury under the Bank Secrecy Act requiring banks, other financial institutions, and individuals and businesses engaged in certain transactions to maintain records may be found at 31 C.F.R. §§ 103.11–103.39 (2003).

organization may be prosecuted under any of several criminal statutory provisions. If such a transfer is international, it may constitute money laundering[112] and may in addition constitute material support.[113] If the transfer may be traced to a conspiracy to commit particular terrorist acts, the transferor and the recipient may also be prosecuted for conspiracy to kidnap, maim, or kill a person or destroy property on foreign territory.[114] Finally, if the transfer is to an individual or entity that has been designated a terrorist or terrorist organization, it may violate the IEEPA[115] and § 2339A.

Any intermediary who possesses the requisite mental state—knowledge that the money will support a statutorily-defined act of terrorism under § 2339A and knowledge that the money is being given to a designated FTO under § 2339B—has also violated those sections. If the conduct involved fraudulent access to financial accounts or services or fraudulent use of customer information, the perpetrator may be tried under the criminal provision prohibiting wire fraud,[116] and potentially also the provisions protecting the privacy of a financial institution's customer information[117] and prohibiting fraud in connection with an access device such as an account number, PIN number or password.[118] If the conduct involved an intrusion into, or an attack on, an electronic banking system, the perpetrator may be tried under the Computer Fraud and Abuse Act.[119] In addition to prosecuting the perpetrator, the government may seek forfeiture of the funds and assets involved.[120]

---

[112] 18 U.S.C. § 1956 (2000), *amended by* USA PATRIOT Act, Pub. L. No. 107–56, Title III, VIII, X, §§ 315, 317, 318, 376, 805, 1004, 115 Stat. 273, 275 (2001).

[113] 18 U.S.C. § 2339B (2000), *amended by* USA PATRIOT Act, Pub. L. No. 107–56, Title VIII, §§ 810, 115 Stat. 275 (2001) if the recipient is a designated FTO; potentially 18 U.S.C. § 2339A (2000), *amended by* USA PATRIOT Act, Pub. L. No. 107–56, Title VIII, §§ 805, 115 Stat. 275 (2001) if the transferor knows that the recipient intends to carry out any of a number of enumerated violent crimes.

[114] *See* 18 U.S.C. § 956 (2000).

[115] *See* 50 U.S.C. §§ 1701–1706 (2000).

[116] *See* 18 U.S.C. § 1343 (2000).

[117] *See* 15 U.S.C. § 6823 (2000).

[118] 18 U.S.C. § 1029 (2000).

[119] *See* 18 U.S.C. § 1030 (2000), *amended by* USA PATRIOT Act, Pub. L. No. 107–56, Title V, Title VIII, §§ 506, 814, 115 Stat. 274, 275 (2001).

[120] *See* 18 U.S.C. § 981 (2000), *amended by* USA PATRIOT Act, Pub. L. No. 107–56, Titles III and VIII, §§ 319, 320, 371, 372, 806, 115 Stat. 272, 311–315, 336–339, 378 (2001). The USA PATRIOT Act broadened the scope of funds and assets subject to forfeiture actions, bringing within the ambit of § 981 funds in a United States interbank account, funds that are the proceeds of certain foreign crimes, funds and monetary instruments involved in currency smuggling, funds

B. *Internet-Based Banking Alternatives*

The Internet provides several new financial services and means of transferring value. Internet users can avail themselves of online non-bank payment systems such as AnonymousGold, PayPal, and StormPay; electronic currencies such as E-Bullion, E-Dinar, E-Gold, and Evocash; electronic checks such as those offered by PayNow and BankServ; and electronic debit cards such as "smartcards." Dollar-based electronic currencies such as Evocash and electronic checks are dependent on the banking system. Transactions involving these value transfer mechanisms must eventually pass value into or out of the traditional banking system, subjecting these transactions, at least second-hand, to the record-keeping and reporting requirements imposed on the banking industry.

Many of the online payment systems, gold-backed e-currencies, and smartcard applications, however, are not dependent on the banking industry.[121] For instance, the online payment system StormPay requires only an e-mail address to open an account.[122] Customers can fund their accounts, StormPay states, by credit card, check, electronic currency, another online payment system "and much more!"[123] StormPay even advertises its services as "MLM [multi-level marketing] friendly."[124]

transferred without complying with currency reporting requirements, and funds that are the assets of terrorist organizations.

[121] While these applications are developing largely independent of the banking system, some of them have implemented security, fraud prevention, and reporting practices similar to those imposed on banks. PayPal, for instance, has established an aggressive fraud prevention strategy, cooperated routinely with law enforcement investigations, and reported voluntarily suspicious use of its services that may implicate money laundering, other criminal conduct, or misuse by terrorist organizations.

[122] *See* Stormpay.com, *The Universal Payment System*, *at* http://www.stormpay.com/stormpay/ (last visited Feb. 15, 2004).

[123] *Id*.

[124] *Id*. The term "multi-level marketing" is sometimes used to conceal fraudulent "ponzi" or "pyramid" schemes. *See, e.g.,* Federal Trade Commission, FutureNet Defendant Settles FTC Charges, *available at* http://www.ftc.gov/opa/1998/11/huff.htm (Nov. 24, 1998).

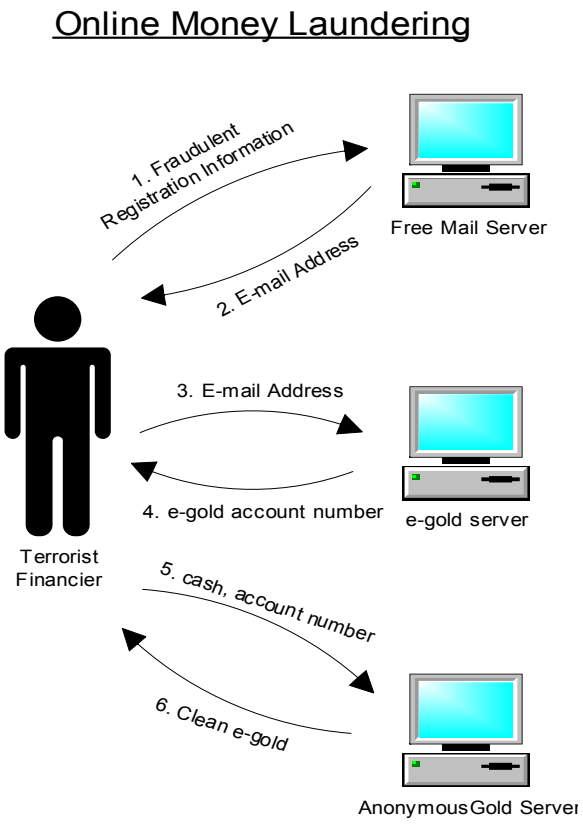

Figure 5

Similarly, AnonymousGold converts funds into or out of a gold-backed electronic currency.[125] To buy a quantity of the e-currency, a customer merely sets up an e-gold account, sends by mail to AnonymousGold cash and an order ticket that discloses only the customer's e-gold account number, and notifies AnonymousGold by encrypted e-mail to expect the purchase order.[126] See Figure 5. Likewise, to convert a quantity of the e-currency into cash, a customer simply transfers the e-currency into AnonymousGold's account, and then sends an encrypted e-mail to AnonymousGold notifying it of the address to which AnonymousGold should send cash or a blank money order by regular mail.[127] AnonymousGold states that it "do[es] not deal with banks" and that it "destroy[s] all of [its] transaction records upon completion of [a customer's] order."[128]

---

[125] *See* SecurityGold.com, *Buy Gold, at* http://www.securitygold.com/buy.htm (last visited Feb. 15, 2004).

[126] *Id.*

[127] *See* SecurityGold.com, *Sell, at* http://www.securitygold.com/sell.htm (last visited Feb. 15, 2004).

[128] *See* SecurityGold.com, *Buy Gold & Silber Discreetly and Privately!, at* http://www.securitygold.com/ (last visited Feb. 15, 2004).

Applications such as StormPay and AnonymousGold effectively protect the privacy of their customers. Without doubt, a vast majority of their customers use their services for legitimate business purposes and private transfers. But because they effectively mask the identity of their customers and destroy or refuse to disclose the records of monetary transactions, such services are also susceptible to abuse by terrorist organizations.

Electronic currency accounts with companies such as e-gold (backed by gold)[129] and e-dinar (backed by the Islamic dinar, a specific weight of gold minted according to Islamic law) may also be opened with only a valid e-mail address (both companies request contact information, but the information does not appear to be verified or essential to the initiation of an account or the provision of services).[130] E-gold can then be converted into any of eight different currencies or transferred instantaneously to any other e-gold account anywhere in the world.[131] Such accounts may be opened with the information of identity theft victims, funded with their credit cards, and then used to transfer money into the account of a perpetrator.

Magnetic stripe applications and smartcards are another stored value alternative that can interface with the Internet to transfer funds to users around the world. Magnetic stripe stored value applications, such as traditional credit and debit cards, utilize existing financial networks. Smartcards are microcomputers the shape and size of a credit card that contain small electronic data storage chips from which information can be read or to which information can be written with appropriate hardware. Smartcards have a number of useful applications, one of which is serving as a bearer-authenticated form of stored value—whoever holds the card can access the value stored on it. A customer can log on to a website, create a username and PIN, and fund the card using a check, money order, cashier's check, credit card number, or direct draw from a bank account. The card can then be sent to anyone in the world, and used as though it were cash. The information contained on the card is protected by strong authentication protocols and encryption and cannot be accessed without the appropriate key, PIN, or biometric identifier. If the smartcard or e-cash application relies on securities or brokerage accounts to hold its reserves, these transactions are invisible to the regulatory regime that scrutinizes traditional banking transactions—they appear to be normal, legitimate transactions. It is not difficult to imagine how these new alternative payment processes might be used by terrorists, either singly or in series, to transfer funds. The relative anonymity afforded by these processes, their ability to circumvent banking regulations, and their increasing use around the world render them vulnerable to exploitation by terrorists and terrorist

---

[129] Gold-based e-currencies back accountholders' value by physical reserves of gold or other precious metals. The gold remains in a central, secured vault. Customers pay each other by transferring electronically ownership of a quantity of that gold (GoldMoney, for instance, quantizes its transactions in units of value called GoldGrams). Accountholders can withdraw value from these companies by ordering a check or by ATM or debit card.

[130] *See* e-gold.com, *Account Creation, at* https://www.e-gold.com/newacct/ (last modified Dec. 20, 2003); e-dinar.com, *e-dinar Open Account*, https://www.e-dinar.com/en/index_1.html (last visited Feb. 15, 2004).

[131] *See* e-gold.com, *Benefits of Using e-gold Account, at* http://www.e-gold.com/unsecure/qanda.html (last visited Feb. 15, 2004).

organizations.

1. Prevention & Investigation

Abuse of alternative payment processes might be prevented, or at least diminished, by regulating vendors and requiring more information from customers. Although the regulatory landscape with regard to new technologies such as alternative payment systems, e-currencies, and smartcard applications is not clearly defined by statute or case law, these systems seem to fall within the broad definition of "financial institution" set forth in 31 U.S.C. § 5312 (2000).[132] Still, a balance must be struck in regulating these new technologies.

One might argue that these services, which essentially perform the functions of a bank, should be subject to the same oversight and regulation. The counter-argument is twofold: (1) most of these systems interface with the banking system at some point, so there is no need for onerous record keeping by alternative payment companies; and (2) these companies thrive on low overhead and the administrative burden of such tasks as reviewing transactions and filing SARs would impose an additional transaction cost on vendors.

Similarly, one might argue that customers of such services should be required to provide the same information that banking customers provide—at least names, social security numbers, driver's license numbers, valid addresses and phone numbers. There is an obvious trade-off with this measure, too. Customers use these services in part because of the privacy and anonymity that they provide.

Nor would an appropriate regulatory regime be a panacea for misuse of such new technologies. The borderless fluidity of the Internet poses unique challenges for such regulations. Customers can easily conduct online transactions that cross international borders or access foreign financial services from an Internet terminal located in the United States. Particularly when transactions span two or more regulatory jurisdictions, it can be difficult to differentiate legitimate from illegitimate transactions.

To the extent that these new technologies interface with the Internet, opening

[132] The statutory definition of "financial institution" appears to extend the Secretary of the Treasury's anti-money laundering and anti-terrorist financing regulatory authority to these new technologies. It includes both specific categories ("a dealer in precious metals, stones or jewels," § 5312(a)(2)(N); "a licensed sender of money or any other person who engages as a business in the transmission of funds," § 5312(a)(2)(R)) and catch-all provisions ("any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage," § 5312(a)(2)(Y); "any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters," § 5312(a)(2)(Z)). The definition also includes money services businesses, which FinCEN has defined to include providers of alternative payment and stored value services if those providers conduct more than $1,000 worth of transactions per day. *See* 31 C.F.R. § 103.11(uu). Although FinCEN's regulations require issuers, sellers, and redeemers of stored value to have anti-money laundering programs, they are not currently subject to other Bank Secrecy Act requirements.

accounts and using their services requires visiting a website. If the company logs traffic on its website and retains those logs (although in rare cases, such as those discussed above, companies proactively destroy business records to protect their customers' privacy, most of them retain logs so that they can investigate customers' claims of fraud or theft), it should, at the very least, have a record of the date, time, and IP address from which the account was accessed for every transaction. Subject to the investigative challenges discussed in Section II.A.1, *supra*, law enforcement can obtain this information for both accounts that are party to a transaction, i.e., the payor and the payee. From this information law enforcement can in theory determine who accessed each account and participated in the transfer of value.[133]

2. Prosecution

The potential statutes under which a transfer of funds to a terrorist or terrorist organization may be prosecuted are the same regardless of the means used to transfer the funds. See Section III.A.3 *supra*. If a suspect provides false registration information when opening an account, that individual might also be prosecuted under the wire fraud statute.[134]

IV. Electronic Communications

Terrorists' use of the Internet to communicate with one another constitutes perhaps the most prevalent use of the Internet to facilitate the raising and moving of funds. Communication, of course, is protected in the United States by the First Amendment unless it is in furtherance of some criminal conduct. Thus, for instance, the First Amendment protects an individual who transmits, without doing more, the message, "I believe that the only way to curb the spread of American capitalism, and the spiritual vacuum that accompanies it, is by waging war against the United States." Communications are often more, however, than a passive ideological statement. They may be an incitement to imminent unlawful action or a threat, neither of which is protected by the First Amendment.[135] A conspiracy to commit unlawful acts may also be

---

[133] In practice, this will depend on how long the ISP through which the customer accessed the Internet maintains information and whether it requires and confirms valid registration information.

[134] *See* 18 U.S.C. § 1343 (2000).

[135] *See* Brandenburg v. Ohio, 395 U.S. 444, 447 (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."); Planned Parenthood of the Columbia/Williamette, Inc. v. Am. Coalition of Life Activists, 290 F.3d 1058, 1072 (9th Cir. 2002) (en banc) ("[W]hile advocating violence is protected, threatening a person with violence is not.").

punished, even if communications are the strongest indicators that a conspiracy exists.[136] Similarly, communications regarding criminal conduct may constitute information essential to the prevention of, or evidence valuable to the investigation and prosecution of, such conduct and may be obtained with appropriate legal process.[137]

Terrorist organizations have established websites to communicate regarding fund transfers. The most straightforward example of such communication is the listing on sympathetic websites of accounts to which funds for various terrorist organizations can be transferred.[138] For instance, the site http://www.ummah.net/jihad/support provided account numbers for the Al Rashid Trust at Habib Bank Limited, for Harkat ul Mujahideen at the Allied Bank of Pakistan, and for Lashker Taiba at Faisal Bank Limited.[139]

Many of the terrorists and terrorist organizations indicted by the United States have communicated via e-mail. For instance, the indictment of four members of the Islamic Group alleges that computers were used "to transmit, pass and disseminate messages, communications and information between and among IG leaders and members in the United States and elsewhere around the world."[140] Similarly, six individuals indicted in 2002 in Oregon allegedly communicated via e-mail regarding their efforts to travel to Afghanistan to aid al-Qaeda and the Taliban in their fight against the United States.[141] Mukhtar al-Bakri, indicted in 2002 for training with al-Qaeda to wage war against the United States, allegedly e-mailed with co-conspirators to discuss and plan acts of terrorism.[142] Finally, four members of a Colombian terrorist organization indicted in November 2002, allegedly used e-mail to broker a guns-for-drugs deal.[143] In addition, the Washington Post recently reported that "al Qaeda members have taught individuals from other groups how to use the Internet to send messages and how to encrypt those

---

[136] *See* Wisconsin v. Mitchell, 508 U.S. 476, 489 (1993) (noting that "[t]he First Amendment . . . does not prohibit the evidentiary use of speech to establish the elements of a crime or to prove motive or intent.").

[137] *See supra* note 73.

[138] *See* Levitt, *supra* note 29.

[139] *See* Global Jihad Fund, *at* http://web.archive.org/web/20011109223219/www.ummah.net/jihad/ (last visited Mar. 7, 2004).

[140] Indictment, United States v. Sattar, No. 02-CRIM-395 at 11 (S.D.N.Y Apr. 9, 2002), *available at* http://news.findlaw.com/hdocs/docs/terrorism/ussattar040902ind.pdf.

[141] *See* Indictment, United States v. Battle, No. CR 02-399 HA at 5 (D.Or. Oct. 2, 2002), *available at* http://news.findlaw.com/hdocs/docs/terrorism/usbattle100302ind.pdf.

[142] *See* Criminal Complaint, United States v. Al-Bakri, No. 02-M-108 at 8 (W.D.N.Y. Sept. 13, 2002), *available at* http://news.findlaw.com/hdocs/docs/terrorism/usal-bakri091302cmp.pdf.

[143] *See* Criminal Complaint, United States v. Varela, No. H-02-1008M at 9–10 (S.D.Tex. Nov. 1, 2002), *available at* http://news.findlaw.com/hdocs/docs/terrorism/usromero110102cmp.pdf.

communications to avoid detection."[144]

Terrorists may also pass PIN numbers, account passwords, or transfer instructions by e-mail, secure websites, or chat rooms. Increasingly, value transfer through *hawala*, the traditional alternative remittance system that has provided value transfer to the people of the Middle and Far East for centuries, relies on e-mail communications between *hawaladars* around the world.[145] Although the vast majority of *hawala* transfers are legitimate (it is estimated that there are tens of millions of dollars transferred through *hawala* annually), experts believe that much of al Qaeda's funds for September 11 transferred through *hawalas* in Dubai and that terrorist organizations continue to use *hawala* to transfer funds.[146] *Hawala* provides a cheap, efficient, less regulated means of moving money, particularly in and out of countries in the Far and Middle East.[147] The advent of e-mail as a preferred means of communication between *hawaladars* has at least one benefit—for the first time in the centuries-long history of this alternative remittance system, e-mail creates a record of transactions that law enforcement can obtain (or even intercept) to aid in an investigation.

Terrorists may be using sophisticated means of electronic communication to conceal their efforts to raise and move funds and to plan acts of violence. One common method is to provide the username and password of an e-mail account to all the members of a conspiracy. One member drafts, but does not send, an e-mail message. He then logs off (exits the e-mail account). His co-conspirators can log on from anywhere in the world, read the draft, and then delete it. Because the draft was never sent, the ISP does not retain a copy of it and there is no record of it traversing the Internet—it never went anywhere, its recipients came to it.

Another common method involves providing basic electronic mail services in conjunction with a terrorist-sympathizer website. Imagine a secure website www.jihad.com. The website 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. In fact, United States intelligence and law enforcement will never know about it unless they obtain access to jihad.com's servers or records. In addition, terrorists may use encryption and steganography to conceal the content of electronic

---

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

[145] *See* supra note 7; Christopher Blevins, U.S. Dep't of the Treasury, *Hawala: Issues & Policy Implications* (2002).

[146] *See* Karen DeYoung & Douglas Farah, *Infighting Slows Hunt for Hidden Al Qaeda Assets; Funds Put in Untraceable Commodities*, Wash. Post, June 18, 2002, at A1.

[147] The USA PATRIOT Act amended the definition of "financial institution" to include informal value transfer systems such as *hawala*. *See* 31 U.S.C. § 5312(2)(R). As a result, *hawalas* operating in the United States must now establish an anti-money laundering program, register with FinCEN, and comply with record keeping and reporting requirements. Several foreign countries, such as United Arab Emirates and Saudi Arabia, now regulate *hawala* transactions, while other countries, such as India and Pakistan, have banned the practice of *hawala* altogether.

communications regarding raising and moving funds.

Terrorist organizations also communicate through e-groups.[148] A user may register an e-group with only a valid e-mail address. If the user wishes, he can control who joins the group, what messages are posted for review by its readers, and whether its content is publicly available or password protected. E-groups appeal to terrorists for a number of reasons. E-groups may often be established free and without providing any authentic identifying information. They facilitate mass communication to geographically-dispersed groups—using one e-mail address, an e-group member can reach hundreds or thousands of other members across the globe. E-groups also tend to be available even in countries that strictly limit Internet use because they are established in subdirectories of innocuous Internet services such as Yahoo!. Finally, e-groups can be established with built-in security in the form of a password. E-groups may be broadly used by terrorist organizations for everything from ideological indoctrination and the dissemination of *fatwahs*, to providing directions to *mujahideen* training camps, to operational planning for future attacks.

1. Prevention & Investigation

One can no more prevent terrorists from communicating via the Internet than one can prevent them from communicating via telephone or regular mail. A regulation requiring ISPs to obtain and confirm valid subscriber information would discourage some such communications (and much of the other illicit conduct occurring on the Internet). Such a measure would, however, deprive Internet users of a certain degree of privacy and anonymity and impose business costs upon ISPs. As a result of the delicate balance between law enforcement's need for valid identifying information and computer users' right to privacy, no consensus for such regulation has developed in the international community. Even if the United States established such a regulatory regime, therefore, terrorists could simply use mail servers based in other countries. Moreover, as noted above, a terrorist group could easily establish basic mail service capabilities on its own website. In short, such regulation would limit the Internet's use as a global communication medium, a forum for international commerce, and an educational resource without effectively preventing terrorists from communicating over the Internet.

As noted in Section II.C.2, *supra*, the capacity to investigate terrorist

[148] An e-group is a service offered by an Internet Service Provider through which users with common interests can exchange messages. When the "owner" of an e-group registers that group, she can determine whether it is public (open to anyone) or private (open only to invited users possessing a password) and whether it is moderated (user messages may only be posted by a moderator who has reviewed the message) or un-moderated (users may post messages directly, without the intervention of a moderator). Users may elect to receive posted messages either by visiting the e-groups website, where recently posted messages are archived, by receiving each message in their e-mail accounts as it is posted, or by receiving a periodic digest of messages in their e-mail account. *See generally* Rita Katz & Josh Devon, *WWW.JIHAD.COM E-Groups Abused by Jihadists,* National Review Online (July 4, 2003) (providing an overview of how Islamic fundamentalists use Yahoo! Groups), *at* http://www.nationalreview.com/comment/comment-katz-devon071403.asp.

communications over the Internet has increased appreciably over the last several years due to amendments to procedural and substantive laws, increased cooperation and capacity-building in the international community, and the development by federal, state, and local law enforcement of computer crime expertise. If United States law enforcement has reason to believe that terrorists are using a particular electronic communications account to raise funds and solicit resources, and the ISP that serves that account is located in a cooperative country that has appropriate laws and expertise, law enforcement now has the legal tools it needs to obtain historical communications (to the extent they are retained by the ISP), trace electronic communications back to their source IP address or dial-up telephone number, and even intercept those communications as they occur, provided that law enforcement obtains the appropriate form of legal process.[149]

2. Prosecution

Before pursuing prosecution, law enforcement must again decide whether the benefit of prosecution outweighs the benefit of the information that might be gathered if prosecution is delayed and the terrorists are allowed to continue communicating so that law enforcement can continue to gather information. Once the decision has been made to prosecute individuals engaged in electronic communications as a means of soliciting material support for terrorist organizations, the individuals or organizations engaged in the communications may be prosecuted under the statutes prohibiting such solicitations, discussed in Section II.A.3, *supra*. In addition, providing a communication platform such as a website or e-group for the use of a FTO constitutes providing material support to that organization in the form of "communications equipment."[150]

V. Conclusion

The Internet is undeniably one of the most significant technological advances of our era. Its prevalence and accessibility have revolutionized the ability of individuals and organizations all over the world to communicate, share and access information, and conduct transactions. It has created an efficient, borderless marketplace for the exchange of ideas and for the transacting of business and financial affairs. This marketplace has been fertile ground for innovation, providing an infrastructure within which existing businesses can offer services with greater efficiency and convenience and new businesses can capitalize on the remarkable attributes of this new global network.

With this technological advance and these new opportunities, however, come new challenges. The very attributes that make the Internet an invaluable communication, educational, and business resource make it susceptible to abuse by criminals and

[149] If the ISP is subject to United States jurisdiction, law enforcement may obtain legal process compelling the production of such records and information under 18 U.S.C. §§ 2703(d), 3123, and 2516 (2000).

[150] 18 U.S.C. § 2339A(b) (2000).

terrorists. For legislators and for regulatory and law enforcement agencies, the challenge is to preserve the attributes that make the Internet such a remarkable innovation—the anonymity and privacy it offers users, the liberation from geographic boundaries, the speed-of-light efficiency, and the rarity of regulatory constraints—while at the same time making it less susceptible to criminal or terrorist abuse.

The war on terrorism is asymmetric in nature but the advantage belongs to us, not the terrorists. We will fight this campaign using our strengths against the enemyâ€™s weaknesses. We will use the power of our values to shape a free and more prosperous world.Â Our economic strength will help failing states and assist weak countries in ridding themselves of terrorism. Our technology will help identify and locate terrorist organizations, and our global reach will eliminate them where they hide. And as always, we will rely on the strength of the American people to remain resolute in the face of adversity. We will never forget what we are ultimately fighting forâ€”our fundamental democratic values and way of life. Most of the terrorist organizations have been using the technology for military training of their militants, preparation, and recruitment processes. Especially the internet is almost a virtual training slot for terrorist groups. Recent studies (Weimann, Stud Confl Terrori 29(7): 623â€“639, 2006; Rothenberger, Rom J Commun Public Relat 14(3):7â€“23, 2012) have revealed that the internet is served as the library for the terrorist groups to provide instruction manuals and videos on technical and tactical areas such as making a bomb, taking hostages, and guerilla combat.Â Hinnen TM (2004) The cyber-front in the war on terrorism: curbing terrorist use of the internet. Columbia Sci Technol Law Rev 5(5):1â€“42Google Scholar. Cyber-terrorism could thus be defined as the use of computing resources to intimidate or coerce others. An example of cyber-terrorism could be hacking into a financial institution, hospital computer system and changing someone's medicine prescription to a lethal dosage as an act of revenge.Â The Nigeria government in a bid to curb their excesses put together the joint task force comprising of the military and other offensives to curl them yet the have proven to be beyond the powers of the state as more heinous crime is on the rise using various methods which the military forces are totally incongruent with.Â THE IMPACT OF CYBER TERRORISM ON NATION STATES What would the impact be? Business, government and industry have all become addicted to information.