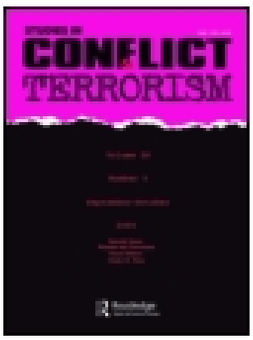

Studies in Conflict & Terrorism

ISSN: 1057-610X (Print) 1521-0731 (Online) Journal homepage: http://www.tandfonline.com/loi/uter20

Terrorist Financing and the Internet

Michael Jacobson

To cite this article: Michael Jacobson (2010) Terrorist Financing and the Internet, Studies in Conflict & Terrorism, 33:4, 353-363, DOI: 10.1080/10576101003587184

To link to this article: http://dx.doi.org/10.1080/10576101003587184

Studies in Conflict & Terrorism, 33:353–363, 2010

ISSN: 1057-610X print / 1521-0731 online
DOI: 10.1080/10576101003587184

Routledge
Taylor & Francis Group

Terrorist Financing and the Internet

MICHAEL JACOBSON

Stein Program on Counterterrorism and Intelligence
The Washington Institute for Near East Policy
Washington, DC, USA

While al Qaeda has used the Internet primarily to spread its propaganda and to rally new recruits, the terrorist group has also relied on the Internet for financing-related purposes. Other Islamist terrorist groups, including Hamas, Lashkar e-Taiba, and Hizballah have also made extensive use of the Internet to raise and transfer needed funds to support their activities. The Internet's appeal in this regard for terrorist groups is readily apparent–offering a broad reach, timely efficiency, as well as a certain degree of anonymity and security for both donors and recipients. Unfortunately, while many governments now recognize that the Internet is an increasingly valuable tool for terrorist organizations, the response to this point has been inconsistent. For the U.S. and its allies to effectively counter this dangerous trend, they will have to prioritize their efforts in this area in the years to come.

As Al Qaeda has come under growing international pressure, the terrorist organization has increasingly relied on the Internet to spread its toxic message and drum up support throughout the world. While its use of the Internet for propaganda and recruiting purposes has received wide publicity, Al Qaeda has also utilized the Internet for a variety of other purposes, including terrorist financing. Al Qaeda is far from alone among terrorist organizations in exploiting the Internet for this type of activity. A wide range of other terrorist groups, including Hamas, Lashkar e-Taiba, and Hizballah have also made extensive use of the Internet to raise and transfer needed funds to support their activities. It is not difficult to understand the appeal of the Internet in this area, as it offers a broad reach, timely efficiency, as well as a certain degree of anonymity and security for both donors and recipients. Unfortunately, while governments throughout the world now recognize that the Internet is an increasingly valuable tool for terrorist organizations, the response to this point has been inconsistent. For the United States and its allies to effectively counter this dangerous trend, they will have to prioritize their efforts in this area in the years to come.

Terrorists' Early Use of the Internet

While terrorists' use of the Internet for finance-related activities dramatically increased after 9/11, it began well before this. Of course, in many cases, the U.S. government and the general public only learned about these early activities after the 11 September 2001 attacks,

Received 15 June 2009; accepted 2 July 2009.
Address correspondence to Michael Jacobson, Senior Fellow, Stein Program on Counterterrorism and Intelligence, The Washington Institute for Near East Policy, 1828 L Street NW Suite 1050, Washington, DC 20036, USA. E-mail: mjacobson@msn.com

when investigative efforts were dramatically stepped up. The most prominent example was Babar Ahmad, a young British citizen from South London, who put his computer expertise to use early on in support of the *jihadist* cause.[1] Beginning in 1997, Babar ran an entity called "Azzam Publications" and a number of associated websites, which were primarily focused on supporting the Taliban in Afghanistan and the *mujahidin* in Chechnya. On these sites, Babar solicited funds, attempted to recruit fighters, and even provided detailed instructions on how individuals could get both themselves and money to these conflict zones.[2] The website was quite explicit on its purpose. On a question and answer page, Babar wrote that "Azzam Publications has been set up to propagate the call for Jihad among the Muslims who are sitting down, ignorant of this vital duty. . . ." Thus the purpose of Azzam Publications is to 'incite the believers' and secondly to raise some money for the brothers. Babar was arrested in 2004 by the United Kingdom, on the basis of an extradition request by the United States. Babar's appeals of the extradition request are still currently pending.[3]

To persuade individuals to donate, Babar used a familiar argument on his website—that supporting the *jihad* in some fashion was an obligation incumbent upon every Muslim. Babar noted that even if an individual could not go fight in the *jihad*, he nonetheless had a religious obligation to contribute funds, writing that the "[f]irst and most important thing that Muslims can do in the West is to donate money and to raise it amongst their families, friends and others . . . 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."[4]

Sami al-Hussayen, a Saudi graduate student at Idaho State University, also served as the webmaster for a series of extremist websites before 9/11. These included the site of al-Haramain, a Saudi-based nongovernmental organization (NGO) later designated by the U.S. Treasury Department for its ties to Al Qaeda.[5] Speeches and lectures promoting violent *jihad* in Israel were also one of the focuses of these sites. Of particular note, the websites included a special by invitation only discussion group where participants were urged to contribute funds to "to assist their brothers in their honorable jihad against the dictatorial Zionist Jewish entity." Al-Hussayen was indicted in 2003 for providing support to Hamas, with the government alleging that al-Hussayen "knew and intended" that his computer expertise and services would be used to "recruit and to raise funds for violent jihad in Israel, Chechnya and elsewhere and that he conspired to conceal the nature of his activities."[6] Al-Hussayen was eventually acquitted of these charges by an Idaho jury.[7] The jury appeared to buy al-Hussayen's defense that he should not be held responsible for the material on the website, regardless of how disturbing it might be. As al-Hussayen's attorney argued, "These are not Sami's opinions. It's not right to hold him responsible for what someone else said."[8] Leaving the merits of the legal case against al-Hussayen aside, the material the prosecution presented during the course of the trial does illustrate what was available in cyberspace, even before 9/11.

Growing Exploitation of the Internet Post-9/11

Since 9/11, terrorist groups have made increasing use of the Internet to further their organizations' goals and activities. Most of the activity on the Internet has revolved around propaganda, recruiting, and training, as terrorist groups have taken advantage of the vast and growing reach of the Internet to all corners of the world. Indeed, the number of websites associated with Al Qaeda has increased from 12 in 1998 to approximately 2,600 by 2006, according to a UN study. Many different terrorist groups have had websites or made active

use of the Internet at one point or another including Al Qaeda, Al Qaeda in Iraq, Laskhar e-Taiba, Chechen *mujahidin*,[9] as well as the Palestinian rejectionist groups.[10] As terrorists have turned to the Internet to spread their messages and to try to attract new recruits, they have also turned to the Internet for financing-related activities, such as raising and transferring funds needed to sustain the organizations. This was a trend the U.S. government predicted in a 2006 National Intelligence Estimate (NIE). The NIE warned that "groups of all stripes will increasingly use the Internet to obtain logistical and financial support." The report noted, more generally, that technology and globalization have also enabled small groups of alienated people not only to connect but to raise resources for attacks without need for an established terrorist organization.[11]

Criminal Activity on the Internet

One of the primary ways that terrorist groups are using the Internet to raise funds is through criminal activity. Younis Tsouli, a young British man better known by his Internet code name "Irhabi 007" (translated as "Terrorist 007") may today be the best known virtual terrorist. As Evan Kohlman, a well-known terrorism expert observed, "Over the space of only two years, he became the undisputed king of internet terrorism."[12] Tsouli began his "career" by posting videos depicting terrorist activity on various websites. He came to the attention of Al Qaeda in Iraq (AQI), whose leaders were impressed by his computer knowledge and his ambitiousness, and quickly developed close ties to this organization. Once he proved his bona fides, AQI began feeding videos directly to Tsouli for him to post.[13] At the outset, Tsouli put these videos on free webhosting services, and at this point he had few expenses and little need for funds. However, these free sites had limited bandwidth and soon came to slow Tsouli down as he ramped up his activities. Tsouli then turned to sites with better technical capabilities, but which also cost money.[14]

Not surprisingly, given his expertise, Tsouli turned to the Internet to raise the money to pay for these sites. Tsouli and his partner—Tariq al-Daour—began acquiring stolen credit card numbers on the Web, purchasing them through various online forums, such as Cardplanet.[15] By the time Tsouli and his partner were arrested, al-Daour had accumulated 37,000 stolen credit card numbers on his computer—which they had used to make more than $3.5 million in charges.[16] Tsouli laundered money through a number of online gambling sites, such as absolutepoker.com and paradisepoker.com, using the stolen credit card information, conducting hundreds of transactions at 43 different sites in all. Any winnings would be cashed in and transferred electronically to bank accounts specifically established for this purpose. In this way, the money would now appear legitimately won, and thus successfully laundered.[17] In total, Tsouli used 72 of these credit cards to register 180 websites, which were hosted by 95 different companies.[18] Tsouli also used these credit cards to purchase equipment for the *mujahidin*, by having it sent to sites or premises that he and his associate would rent on a short-term basis.

Charities

Charities and NGOs remain a major problem in the terrorist financing arena, and their activities on the Internet are no exception to this troublesome trend. According to the Paris-based Financial Action Task Force, "the misuse of non-profit organizations for the financing of terrorism is coming to be recognized as a crucial weak point in the global struggle to stop such funding at its source."[19] Charities are especially susceptible to abuse by terrorists and their supporters for whom charitable or humanitarian organizations are particularly

attractive front organizations. Indeed, terrorist groups have long exploited charities for a variety of purposes. Some charities are founded with the express purpose of financing terror, while others are existing entities that are infiltrated by terrorist operatives and supporters and co-opted from within. A particularly serious challenge not only for law enforcement and intelligence officials, but also for headquarters personnel of these charities, is how to effectively monitor funds distributed in conflict zones, which can be easily diverted away from the intended cause. Another challenge for governments which makes charities an attractive vehicle for terrorist groups is that banned or exposed charities tied to terrorism can also shut down one day, and reopen the next under a new name—a tactic often used successfully by terrorist organizations.

Charities and NGOs that are tied to terrorist organizations can be and often are quite open about what they're doing in terms of fundraising, since it is all ostensibly for humanitarian purposes. Therefore many of the terrorist-linked charities have had websites, openly advertising their activities and soliciting funds. This includes the Global Relief Foundation (GRF), an organization designated in 2002 by Treasury for its ties to Al Qaeda and the Taliban.[20] On its website, GRF said that the charity was "organized exclusively for charitable, religious, education and scientific purposes including to establish, promote, and carry out relief and charitable activities, projects, organizations, institutions and funds." GRF's mission statement focused on its work in emergency relief, medical aid, advancement of education and development of social welfare, noting that it will "act with goodwill towards all people." GRF accepted donations through its website, with donors able to pay through credit and debit card, and wire transfers, among other means.[21] Another Al Qaeda–linked NGO, the Al-Haramain Islamic Foundation, a Saudi-based NGO that was designated by the United States in November 2008 for its ties to Al Qaeda, also had a website.[22] (A number of al-Haramain's branches had been blacklisted by the United States and by the Saudis years earlier.)[23]

Other terrorist organizations also had charitable fronts operating online. These include the Holy Land Foundation, a Texas-based charity, whose leaders were convicted in 2008 for supporting Hamas. On the site, the Holy Land Foundation outlined their purported mission, explaining that it was to alleviate suffering through "humanitarian programs" helping "disadvantaged, disinherited and displaced peoples suffering from man-made and natural disasters."[24] The Union of Good (UG), which according to the U.S. government, is a Hamas front established by the organization's leadership in 2000 to "facilitate the transfer of funds to Hamas," also has a website to promote its activities. UG's English language website was hosted by Interpal, a U.K.-based organization that is a member of UG. Both Interpal and UG have been designated by Treasury[25] but continue to operate.[26]

Why the Internet?

Terrorists' increasing use of the Internet should hardly be surprising, and is being driven by a number of different underlying factors. First, the use of the Internet has expanded exponentially over the past decade throughout the world, and terrorists' and other illicit actors' use has risen right along side it.[27] Currently about 800 million people have access to Internet, and this will continue to grow in years to come—particularly in the Middle East (in 2006, Internet penetration in the Middle was only 8.6 percent, of 16 million).[28] Terrorists' use of the Internet to raise and transfer funds is also part of a broader global shift toward the use of technology in international commerce. There have also been dramatic shifts in how funds can be transferred from one destination to another, with new

technological developments. Transferring funds electronically—using the Internet to initiate transactions—has become increasingly common through such services as PayPal.[29] Transactions can also be conducted through cell phones in what are now better known as "M-payments." In countries where the formal financial sector is less than robust—such as in many African countries—using the Internet or cell phones to facilitate transfers is a far more attractive and readily available option. Online gambling sites and other similar entities have also made it easier to launder money on the Internet than it was in the past—a practice that terrorist groups have taken advantage of in recent years. While this type of activity could potentially expose them to detection, terrorists like Tsouli are able to mask their identities on the Internet when using these sites.

Terrorist cells' involvement in criminal activity is not a phenomenon limited to the Internet, as they are increasingly engaged in crimes across the spectrum. The primary reason is that the Al Qaeda core is no longer providing funding to support terrorist cells and operations. Before 9/11, Al Qaeda funded and controlled operations directly from its base in Afghanistan. The group provided funding for the East Africa embassy bombings in 1998, the 2000 attack on the U.S.S. *Cole* in Yemen, and the September 2001 attacks. Today, the terrorist threat is far more decentralized, and Al Qaeda's central command is not funding operations as it once did. Left to their own devices, budding terrorist cells have resorted to criminal activity to raise the funds for attacks.

There are numerous examples of this growing trend. The cell that executed the devastating 2004 Madrid train bombing plot, which killed almost 200 people, partially financed the attack by selling hashish. The terrorists who carried out the 7 July 2005, attacks on the transportation system in London were also self-financed, in part through credit card fraud.[30] In Southeast Asia, the Al Qaeda–affiliated Jemaah Islamiyah (JI) financed the 2002 Bali bombings, in part, through jewelry store robberies.[31]

Another factor that is likely fueling the increase in terrorists' criminal activity on the Internet, is that key terrorist leaders and operatives have specifically encouraged their followers to pursue this path. For example, Imam Samudra, a former JI operative convicted for his role in the 2002 Bali bombings, wrote a book during his imprisonment that included a chapter entitled "Hacking, Why Not?" In that section of the book, Samudra urged other *jihadists* to attack U.S. computer networks, referring to them as vulnerable to credit card fraud and money laundering.[32] While Samudra does not offer specific instructions in the chapter on how this could be done, he did point readers to specific websites that would help individuals get started, and to chat rooms where they could find hacking "mentors." An Internet-security training company director said that this would be invaluable to would-be hackers, noting that "this is exactly the kind of advice you would give someone who wanted to get started in cyber-crime."[33]

Of particular note, Samudra's hacking activities had at least the implicit blessing of Abu Bakr Bashir, JI's leader, who ruled that hacking into foreigners' bank accounts was religiously permissible, saying that "[i]f you can take their blood; then why not take their property."[34] Tsouli tried to encourage others to participate in hacking as well, posting a "Seminar on Hacking Websites," to a popular *jihadist* forum at one point.[35] He also provided advice on how to mask one's identity on the Internet, so that his fellow *jihadists* could avoid detection.[36]

Perhaps the most obvious reason, however, as to why terrorist groups, cells, and operatives have increasingly turned to the Internet is for the security it offers. As the United States and the international community have cracked down on Al Qaeda and affiliated terrorist organizations, the terrorists have tried to find new ways to avoid detection. The Tsouli case again provides a good example of the ways in which terrorists are able to exploit

security gaps and opportunities for anonymity that exist on the Internet. Even while he was engaging in extensive criminal activity on the Internet, Tsouli was able to cover his tracks, paying for transactions with stolen credit cards and identification information, and never using his real identity.[37] Tsouli also used a variety of techniques to hide his computer's Internet Protocol (IP) address, including anonymizing software and proxy servers.[38]

In fact, at one point, authorities suspected that Tsouli was in the United States, after he hacked into and uploaded data to an Arkansas state website and a George Washington University site.[39] Illustrating how seriously Tsouli generally took security matters, he had never even met Tariq al-Daour, his co-conspirator in this effort.[40] Interestingly, in the end, Tsouli was not caught through cyber-investigation, but through old-fashioned detective work. In October 2005, Bosnian police arrested two men whom they suspected were involved in a terrorist attack. In the search of their phone and email records, they uncovered Tsoulsi and his colleagues.[41] Babar was also very careful in his tradecraft, using aliases and post office boxes to conceal the fact that he was the one operating these extremist websites, and often paying the fees through cash and money orders. Babar also used encryption for his email communications as well as to protect data stored in his computer.[42]

In fact, terrorists appear so confident about the security that the Internet provides that many of the terrorist websites are actually hosted by companies in the United States. The U.S. sites are appealing, experts say, because of the high quality and low costs. There are numerous examples of websites linked to terrorist groups being hosted by U.S. companies. For example, a site tied to the Taliban was hosted by a company in Texas, on which the terrorist group bragged about attacks in Afghanistan on U.S. forces. Perhaps even more disturbingly, in the 2008 attack in Mumbai, which the Pakistani-based group Laskhar e-Taiba is suspected of perpetrating, the cell members communicated through Internet telephone calls, which were routed through a Texas server.[43] In at least one case, Hamas took matters into its own hands, establishing its own Internet Service Provider as part of its network in the United States. Infocom, which had ties to the Holy Land Foundation, received some seed money from Hamas leader Abu Mousa Marzook.[44] Infocom's leaders were eventually convicted for violating U.S. export control laws, for providing services to Libya and Syria.[45]

Increased Caution for Electronic Payments

Ironically, while terrorist groups have increasingly turned to the Internet to spread their extremist message in part due to the security and anonymity it offers, they are at the same time growing more weary about the risks of electronic payments specifically, as governments have begun to crack down. A participant in a recent discussion on al-Fallujah, one of the well known extremist forums, cautioned others about how they pay for online services. Governments, this extremist warned, are carefully tracking and monitoring electronic payment services, and through this have been able to identify *jihadists* and eventually unravel entire networks.[46] The extremist noted that even "If your use of the electronic payments has not brought you woes, then that does not mean it is safe." He recommended that when using Internet for payment that the brothers use "circumvented ways and methods," to make it more difficult to trace.[47] This type of security was only becoming necessary, in the view of this *jihadist*, as the governments were becoming increasingly vigilant in monitoring and tracking electronic transactions.

Hamas has also instructed potential donors on what steps they should take to avoid getting caught. For example, on its Qassam Brigades website, Hamas told donors to use "fake" names when sending e-mails regarding contributions. Hamas also reassured donors

that they will use "secure handling" for the donations to the fighters. Hizballah, likewise, has bragged about their sophistication in using the Internet, particularly in using encryption to protect the communications from detection. Hizballah spokesman Ahmed Jabril said that with this "brilliant" encryption, it was possible to "send a verse from the Koran, an appeal for charity and even a call for jihad and know it will not be seen by anyone hostile to our faith, like the Americans."[48]

The Way Forward

Terrorists will continue to exploit the Internet for all aspects of their operations, including raising and moving funds. This trend is only likely to increase as the scope and scale of the Internet expands, and with other related technological developments. There is widespread agreement at this point among governments that the Internet creates serious counterterrorism vulnerabilities, and that action is needed to counter this growing threat. However, there is far less agreement on what steps need to be taken.

The United States has taken aggressive actions unilaterally in this area, specifically designed to address the use of the Internet for terrorist financing purposes. This has included a number of prosecutions of suspected terrorists for their Internet-related activity, including al-Hussayen and Babar. The United States has also used its law enforcement tools more broadly, targeting money remitters without adequate anti money laundering/counterterrorist financing internal compliance systems. The United States has even gone after money remitters based outside of the United States that were marketing online to U.S. citizens, charging them with failing to register in the United States, as required by law.[49] The United States has complemented this with a softer approach, reaching out to individual Internet service providers (ISP) who are hosting troublesome websites, asking these ISPs to voluntarily shut down the sites. After completing a 60-day comprehensive policy review, the Obama administration also took a broader step to address the cyber-threat, creating a "Cyber-czar" at the White House to coordinate the government's efforts.[50]

The United Kingdom has been increasingly aggressive as well on this front. Like the United States, the United Kingdom is reportedly creating a cybercrime coordinator, who will be located in Whitehall and will lead the government's efforts in this important area.[51] The United Kingdom has also used its law enforcement tools to target those using the Internet for terrorist purposes. While the Tsouli prosecution was the highest profile case, there have been others as well. The outcomes have not all been successful, however, demonstrating what a difficult challenge this is. For example, Sulayman Zainulabin, a London chef who was offering training courses called the "Ultimate Jihad Challenge" through his website, was acquitted of the charges against him.[52]

Of potential promise, the European Commission is now reportedly moving into this arena more assertively as well, and will be putting out recommendations that the European member states increase criminal penalties in cybercrime cases. The Commission may also press member states to improve cooperation on cyber-investigations, publishing guidelines on how quickly countries should respond to investigative requests for assistance in these types of cases. There are currently no time restrictions in place.[53]

For a variety of reasons, however, not all countries have been as aggressive as the United States or the United Kingdom on this front. First, many countries lack the technical capabilities necessary to investigate online terrorist activity. In fact, Interpol's Secretary General stated that the international community needs to increase its efforts in this area 100, or 1,000 times, if we are serious about combating this threat.[54] For example, the United Arab Emirates (UAE) government is only now learning how to track Internet Protocol

addresses, and more generally, still has only a limited understanding of how to follow the money. In fact, the UAE has only two analysts in the Dubai police who are responsible for Counterterrorist Financing (CTF) issues—far too few to cover this area in the Middle East's leading international financial center.[55] Second, there is still a debate about how far governments should go in cracking down on Internet-related activities. Some governments are concerned that taking these steps will abridge the right to free speech. There is also an active debate about what works best from a counterterrorism perspective—particularly whether it is more valuable to monitor terrorists' activities on the Internet for intelligence purposes, or to shut them down.

Third, the laws in this area have not kept up with the technological changes, and there is not agreement about what changes should be made to move forward. At present, there is no consistency at the national level in what laws are on the books.[56] For example, while in Italy, cyber-cafes are required to ask for identification, Rome is alone in the European Union in imposing this regulation. In India, some states mandate this, but others do not.[57] The United States has also interpreted its responsibilities and laws more expansively than many other countries, targeting entities outside of the United States for prosecution; others are hesitant to give their law enforcement agencies this broad, arguably extra-territorial, reach.

Fourth, while some countries favor the establishment of an international legal instrument or treaty which would govern this area, not all governments regard this as a necessary or helpful step forward.[58] Even the technocratic Financial Action Task Force (FATF), the Paris-based organization, which aims to set worldwide standards for anti-money laundering/terrorist financing, has been slow to move into this area. While the FATF has identified the Internet (and particularly Internet payment systems) as a major vulnerability in the financing arena, it has not put forth comprehensive guidelines for how countries should mitigate these risks.[59] There are still no universally agreed upon thresholds, for example, on what transactions Internet payment companies are required to maintain records—an area where FATF is uniquely qualified to weigh in. These types of records would be particularly valuable for law enforcement agencies throughout the world as they investigate reports of terrorist financing activity taking place through the Internet.

And finally, even when countries do decide to act, they will face an uphill challenge. In response to governmental efforts, terrorists are constantly adapting how they raise and transfer funds, in an attempt to continue evading detection. New technologies coming on the scene facilitate the terrorists' efforts and complicate governmental tracking efforts. Virtual currencies available only online that can be used for Internet-based transactions present one such challenge. Second-life, the biggest virtual economy based in the United States, now has a market of approximately $500 million annually, which gives a sense of the scale of these growing businesses. Even more difficult to monitor, from the U.S. perspective, is the rapidly increasing virtual currency market in China, which is now $800 million a year, and rising by 30 percent annually.[60]

Unfortunately, there are limits to what the United States or another other country can accomplish on its own in this area. The Internet crosses all geographic boundaries, and if the United States cracks down on what is taking place within its borders, terrorists can easily relocate to other jurisdictions that are less vigilant about monitoring and countering this type of illicit activity. Only when there is more of a collective and coherent global response, will a dent be made in terrorists' ability to use the Internet so easily to further their nefarious goals. The U.S. actions are a step in the right direction, but without broader international focus and cooperation on this issue, there are real limits to what is likely to be accomplished.

Notes

1. Affadavit in Support of Request for Extradition of Babar Ahmad, September 2004 and indictment of Ahmad in US v. Babar Ahmad, 2004.
2. Affadavit in Support of Request for Extradition of Babar Ahmad, September 2004.
3. Ibid.
4. Ibid.
5. The entire organization was designated in June 2008; many branches of al-Haramain had been designated years earlier. Treasury press release, "Treasury designates Al Haramain Islamic Foundation," 19 June 2008.
6. "Saudi National Charged with Conspiracy to Provide Material Support to Hamas and other Violent Jihadists," Justice Department Press Release, 4 March 2004. Available at http://www.usdoj.gov/opa/pr/2004/March/04_crm_137.htm
7. Bob Fink, "Idaho Graduate Student Acquitted of Using Internet to Support Terrorism," Associated Press, 11 June 2004. Available at http://seattletimes.nwsource.com/html/localnews/2001952936_webstudentacquitted10.html
8. Maureen O'Hagan, "A Terrorism Case that Went Awry," *Seattle Times*, 22 November 2004.
9. Fourth Report of the United Nations 1267 Monitoring Team, January 2006. Available at http://daccessdds.un.org/doc/UNDOC/GEN/N06/230/45/PDF/N0623045.pdf?OpenElement
10. "Jihad Online; Islamic Terrorists and the Internet," Anti-Defamation League, 2002.
11. Office of the Director of National Intelligence, "Declassified Key Judgments of the National Intelligence Estimate 'Trends in Global Terrorism: Implications for the United States' Dated April 2006." Available at http://www.dni.gov/press_releases/Declassified_NIE_Key_Judgments.pdf
12. Gordon Corera, "The World's Most Wanted Cyber-Jihadist," *BBC News*, 16 January 2008.
13. Ibid.
14. "Cyber Operative Charged in Real World Terror Plot," Anti Defamation League, 1 March 2006.
15. See US Secret Service press release. Available at http://www.secretservice.gov/press/pub2304.pdf. These forums obtained the credit cards through various online scams and e-mail viruses. Brian Krebs, "Terrorism's Hook into Your Inbox," *Washington Post*, 5 July 2007.
16. For example, one New Jersey woman described how she received an e-mail asking for her to verify eBay account information, which she completed, including sensitive financial information. Al-Daour ended up with her credit card information. Krebs, "Terrorism's Hook into Your Inbox."
17. Ibid.
18. Written statement of Andy Cochran, Congressional Hearing, 31 March 2009, For the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Hearing, U.S. House Committee on Homeland Security, "Do the Payment Card Industry Data Standards Reduce Cybercrime?" Interestingly, Tsouli's terrorist activities went beyond financial, to other types of logistical support. Of particular concern to U.S. authorities, British investigators discovered "casing" videos of targets in the United States, including various landmarks in the Washington, DC area. They were allegedly shot by two individuals living in the Atlanta, Georgia area. John Murgatroyd, "Two Views of Former Georgia Tech Student Drawn at Terror Trial," *CNN*, 2 June 2009. Available at http://www.cnn.com/2009/CRIME/06/02/georgia.jihad.trial/
19. Financial Action Task Force, *Terrorist Financing*, 29 February 2008. Available at http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf, p. 11.
20. Treasury press release, "Treasury Department Statement Regarding the Designation of the Global Relief Foundation," 18 October 2002. http://www.ustreas.gov/press/releases/po3553.htm
21. "Jihad Online; Islamic Terrorists and the Internet."
22. Treasury designation of al-Haramain as an organization, 19 June 2008. Available at http://www.ustreas.gov/press/releases/hp1043.htm
23. Treasury press release, 2 June 2004. Available at http://www.treas.gov/press/releases/js1703.htm

24. "Jihad Online; Islamic Terrorists and the Intenet."

25. Treasury designation of Interpal, 22 August 2003. Available at http://www.ustreas.gov/press/releases/js672.htm; Union of Good designation, 12 November 2008. Available at http://www.treas.gov/press/releases/hp1267.htm

26. Steve Merley, "The Union of Good: Interpal and the UK Member Organizations," NEFA Foundation, 23 March 2009. http://www.nefafoundation.org/miscellaneous/FeaturedDocs/nefaunionofgoodmemberorgs0309.pdf

27. Terrorists are also far from alone in using the Internet for illicit purposes. In fact, crime on the Internet has been growing rapidly, with the FBI estimating losses from Internet crime in 2008 at approximately $264 million. The agency received 275,000 such complaints from the public in that year alone. FBI press release, 30 March 2009. Available at http://www.fbi.gov/page2/march09/internet_033009.html

28. Fourth Report of the United Nations 1267 Monitoring Team.

29. It's important to note that the funds themselves would not actually be transferred through the Internet. The communication channel would instruct a service provider on what action to take.

30. David Aufhauser, Testimony Before the House Financial Services Oversight Committee, 18 May 2004. http://financialservices.house.gov/media/pdf/051804da.pdf

31. David Kaplan, "Paying for Terror: How Jihadist Groups are using Organized-Crime Tactics—and Profits—to Finance Attacks on Targets around the Globe," *U.S. News and World Report*, 27 November 2005. Available at http://www.usnews.com/usnews/news/articles/051205/5terror_print.htm

32. Written statement of Andy Cochran, Congressional Hearing.

33. Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War into Cyberspace," *Washington Post*, 14 December 2004.

34. "Irhaby 007's American Connections," NEFA Foundation, January 2008, citing Kaplan, "Paying for Terror."

35. Rita Katz and Michael Kern, "Terrorist 007, Exposed," *The Washington Post*, 26 March 2006.

36. Nadya Labi, "Jihad 2.0," *The Atlantic Monthly*, July/August 2006. This was apparently something Tsouli learned early in his Internet career. When he first began visiting a particular *jihadist* site, one of the members of the forum warned Tsouli not to access the site from his own IP address—a lesson Tsouli appears to have generally heeded.

37. Written statement of Andy Cochran, Congressional Hearing.

38. Labi, "Jihad 2.0."

39. Katz and Kern, "Terrorist 007, Exposed."

40. Corera, "The World's Most Wanted Cyber-Jihadist." Although Tsouli was extremely careless on several occasions, failing to anonymize his transactions, which led one private cyber-investigator to conclude that Tsouli was located in Ealing, England—a short distance from his actual home. Labi, "Jihad 2.0."

41. "Cyber Operative Charged in Real World Terror Plot," Anti Defamation League, 1 March 2006. http://www.adl.org/main_Terrorism/terrorist_077_younis_tsouli.htm

42. Indictment of Babar Ahmed, and Affadavit in Support of Extradition.

43. Joby Warrick and Candace Rondeauz, "Extremist Web Sites are Using US hosts," *Washington Post*, 9 April 2009.

44. Justice Department press release, 13 October 2006. Available at http://www.usdoj.gov/usao/txn/PressRel06/elashi_bayan_ghassan_basman_infocom_sent_pr.html

45. Ibid.

46. Jihadi Discussion Forum Posting on Safely Financing Jihad-Related Websites, Translated by NEFA Foundation, 7 April 2009. http://www.nefafoundation.org/miscellaneous/FeaturedDocs/nefafinancejihadsites0409.pdf

47. Ibid.

48. "Jihad Online; Islamic Terrorists and the Internet."

49. See, for example, the U.S. Justice Department prosecutions of MENAEXCHANGE.com, a money remitter that transferred funds between the United States, the Middle East, and North Africa.

50. Bonnie Johnson, "Obama to Create 'Cybersecurity' Chief," *The Guardian*, 29 May 2009. Available at http://www.guardian.co.uk/technology/2009/may/29/obama-cybersecurity

51. Chris Williams, "UK.gov to Create Central Cybersecurity Agency," *The Register*, 15 June 2009. Available at http://www.theregister.co.uk/2009/06/15/cabinet_office_cybersec_agency/

52. "Chef to Sue over Terror Charges," *BBC*, 13 August 2002. The British have been more successful in other Internet-related cases. According to British authorities, an Al Qaeda–associated individual in the United Kingdom was using multiple identities to finance the purchase and supply of explosives components for use in another country. Forensic financial investigation revealed that this person used multiple accounts to purchase high resolution maps of a third country over the Internet. Following the money enabled investigators to track the international travel of the conspirators as well as the delivery by international courier of components for improvised explosives to the same foreign country over several months. Multiple transactions involving accounts controlled by an associate of the original suspect revealed a wider conspiracy. In a joint operation with a foreign law enforcement agency, the original suspect was tracked to a third country where he was arrested in a makeshift bomb factory. HM Treasury, Foreign and Commonwealth Office, Government of the United Kingdom, "The Financial Challenge to Crime and Terrorism," February 2007. Available at http://www.hm-treasury.gov.uk/media/C/B/financialchallenge_crime_280207.pdf.

53. Jeremy Kirk, "Europe Looks to Step Up Fights against Cybercrime," *PC World*, 10 June 2009. Available at http://www.pcworld.com/article/166420/europe_looks_to_step_up_fight_against_cybercrime.html

54. "Terrorist Use of the Internet: Threat, Issues, and Options for International Cooperation," Rapahel Perl, OSCE, 7–10 April 2008, at the Second International Forum on Information Security.

55. Interview with State Department official, January 2008.

56. "Terrorist Use of the Internet."

57. "Indian States Make Cyber-Users Sign in," *Fox News*, 10 January 2006. Available at http://www.foxnews.com/story/0,2933,181221,00.html

58. For example, at an April 2009 conference in Spain organized by the Council of Europe and the Organization of American States that the author attended, the Russian Federation was pressing for an international treaty to govern this area, but the United States and others pushed back against the Russian proposals. The U.S. position is that the focus should be on improving the implementation of the Council of Europe's September 2001 Cyber-crime treaty.

59. FATF Report, entitled, "Money Laundering and Terrorist Financing: Vulnerabilities of Commercial Websites, and Internet Payment Systems," 18 June 2008. Available at http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

60. Olga Kharif, "Virtual Currencies Gain in Popularity," *Business Week*, 6 May 2009.