Terrorist Financing on the Internet

By Michael Jacobson

SINCE THE SEPTEMBER 11 attacks on the United States, al-Qa`ida has come under growing international pressure. In response, the terrorist organization has increasingly relied on the internet to spread its message and gain support throughout the world. While its use of the internet for propaganda and recruiting purposes has received wide publicity, al-Qa`ida has also utilized the internet for a variety of other purposes, including terrorist financing. Al-Qa`ida is far from alone among terrorist organizations in exploiting the internet for financing. A wide range of other terrorist groups—including Hamas, Lashkar-i-Tayyiba and Hizb Allah—have also used the internet to raise and transfer needed funds to support their activities.

The internet offers broad reach, timely efficiency, as well as a certain degree of anonymity and security for both donors and recipients. Although governments throughout the world now recognize that the internet is an increasingly valuable tool for terrorist organizations, the response 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. This article provides an example of early terrorist use of the internet, explains how and why terrorists launder and raise funds through websites, and examines the challenges of countering this problem effectively.

Early Terrorist Financing on the Internet

While terrorists' use of the internet for finance-related activities dramatically increased after 9/11, it began well before. 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 until his arrest in 2004.[1] Beginning in 1997, Babar ran an entity called "Azzam Publications" and a number of associated websites that 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 move both themselves and money to conflict zones.[2] The website was explicit in its purpose.[3]

To persuade individuals to donate, Babar used a familiar argument: supporting jihad in some fashion was an obligation incumbent upon every Muslim. Babar noted that even if one could not fight in the jihad, they nonetheless had a religious obligation to contribute funds. He argued that the

> first 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...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]

Babar's case is just one example of early terrorist use of the internet for financing purposes.

Financing Earned through Online Criminal Activity

One of the primary ways that terrorist groups use the internet to raise funds is through criminal activity. Younis Tsouli, a young British man better known by his internet code-name "Irhabi 007,"[5] may today be the best known virtual terrorist. Tsouli began his "career" by posting videos depicting terrorist activity on various websites. He came to the attention of al-Qa`ida in Iraq (AQI),

1 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. For more, see *U.S.A. v. Babar Ahmad*, "Affadavit in Support of Request for Extradition of Babar Ahmad," September 2004 and indictment of Ahmad in *U.S.A. v. Babar Ahmad*, District Court of Connecticut, 2004.

2 "Affadavit in Support of Request for Extradition of Babar Ahmad."

3 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."

4 "Affadavit in Support of Request for Extradition of Babar Ahmad."

5 "Irhabi 007" means "Terrorist 007."

whose leaders were impressed by his computer knowledge and ambition. He quickly developed close ties to the organization.[6] AQI began feeding videos directly to Tsouli for him to post.[7] At the outset, Tsouli uploaded these videos to free webhosting services, and at this point he had few expenses and little need for funds. These free sites, however, 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 that forced him to raise money.[8]

Not surprisingly, given his expertise, Tsouli turned to the internet to raise the funds 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.[9] 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.[10] Tsouli laundered money through a number of online gambling sites, such as absolutepoker.com and paradisepoker.com, using the stolen credit card information. They conducted hundreds of transactions at 43 different websites in total. Any winnings were 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.[11] In total, Tsouli used 72 of these credit cards to register 180 websites, hosted by 95 different companies.[12]

Charities

Charities and non-governmental organizations (NGO) 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."[13] Charities are especially susceptible to abuse by terrorists and their supporters for whom charitable or humanitarian organizations are particularly attractive front organizations. 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. It is a significant challenge for law enforcement, intelligence officials, and charity headquarters personnel to effectively monitor funds distributed in conflict zones, which can be easily diverted away from the intended cause. Another challenge for governments that makes charities an attractive vehicle for terrorist groups is that banned or exposed charities tied to terrorism can shut down one day, and reopen the next under a new name—a tactic often used successfully by terrorist organizations.[14]

Charities and NGOs that are tied to terrorist organizations are often open about their fundraising activities 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 the U.S. Treasury Department for its ties to al-Qa`ida and the Taliban.[15] On its website, the 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 cards, and wire transfers, among other means.[16] In reality, the charity was set up and run for years by Rabih Haddad, who was allegedly a previous member of *Maktab al-Khidmat* (Services Bureau), the "precursor organization to al Qaeda."[17]

"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."

Another al-Qa`ida-linked NGO, the al-Haramain Islamic Foundation, a Saudi-based NGO that was designated by the U.S. Treasury Department in November 2008 for its ties to al-Qa`ida, also had a website that encouraged donations.[18]

6 Gordon Corera, "The World's Most Wanted Cyber-Jihadist," BBC News, January 16, 2008.

7 Ibid.

8 "Cyber Operative Charged in Real World Terror Plot," Anti-Defamation League, March 1, 2006.

9 "U.S. Secret Service's Operation Firewall Nets 28 Arrests," U.S. Secret Service, press release, October 28, 2004. These forums obtained the credit cards through various online scams and e-mail viruses. See Brian Krebs, "Terrorism's Hook into Your Inbox," *Washington Post*, July 5, 2007.

10 For example, one New Jersey woman described how she received an e-mail asking her to verify eBay account information, which she completed, including sensitive financial information. Al-Daour ended up with her credit card information. For more, see Krebs.

11 Krebs.

12 Written statement from Andy Cochran at "Do the Payment Card Industry Data Standards Reduce Cybercrime?" Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Hearing, March 31, 2009. Tsouli also used these credit cards to purchase equipment for the mujahidin. The equipment was sent to locations or premises that he and his associate would rent on a short-term basis.

13 "Terrorist Financing," Financial Action Task Force, February 29, 2008.

14 The Treasury Department, for example, noted that the Bosnian branch of the al-Haramain Foundation "reconstituted" itself after its designation by the U.S. government in 2002, reopening under the name "Vazir." More recently, Treasury added new aliases for al-Rashid Trust and al-Akhtar Trust International, years after their designations by the U.S. and UN.

15 "Treasury Department Statement Regarding the Designation of the Global Relief Foundation," U.S. Treasury Department, press release, October 18, 2002.

16 "Jihad Online: Islamic Terrorists and the Internet," Anti-Defamation League, 2002.

17 The GRF also received funding from individuals linked to al-Qa`ida, and GRF officials had "extensive contacts" with Wadih el-Hage, a close associate of Usama bin Ladin, who was convicted by a U.S. jury for his role in the 1998 U.S. Embassy bombings. See U.S. Treasury Department, press release, October 18, 2002.

18 "Treasury Designates Al Haramain Islamic Foundation," U.S. Treasury Department, press release, June 19,

Why the Internet?

Terrorists' increasing use of the internet for financing purposes is being driven by a number of different underlying factors. The use of the internet has expanded exponentially and globally during the past decade, and terrorists' and other illicit actors' use has risen alongside this growth.[19] 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 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 services such as PayPal. 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 attempt to mask their identities on the internet when using these sites. 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.

"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."

Anonymity

Perhaps the most obvious reason 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 crack down on al-Qa`ida and affiliated terrorist organizations, 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. 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.[20] Tsouli also used a variety of techniques to hide his computer's Internet Protocol (IP) address, including anonymizing software and proxy servers.[21]

In fact, at one point, authorities suspected that Tsouli was in the United States because he hacked into and uploaded data to an Arkansas State website and a George Washington University site.[22] Illustrating how seriously Tsouli generally took security matters, he had never even met Tariq al-Daour, his co-conspirator in the effort.[23] Interestingly, in the end Tsouli was not apprehended through cyber-investigation, but through traditional detective work.[24]

Babar was also 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 used encryption for his e-mail communications as well as to protect data stored in his computer.[25]

In fact, terrorists appear so confident about the security that the internet provides that some 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 Lashkar-i-Tayyiba is suspected of perpetrating, the cell members communicated through internet telephone calls, which were routed through a Texas server.[26]

Increased Caution for Electronic Payments

Nevertheless, while terrorist groups have increasingly turned to the internet to spread their extremist message, they are at the same time growing more weary about the risks of electronic payments specifically, as governments have begun to crack down on the practice. A

2008. A number of al-Haramain's branches had been blacklisted by the United States and by Saudi Arabia years earlier. See U.S. Treasury Department, press release, June 2, 2004.

19 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. "Internet Crime," Federal Bureau of Investigation, press release, March 30, 2009.

20 Written statement from Andy Cochran at "Do the Payment Card Industry Data Standards Reduce Cybercrime?" Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Hearing, March 31, 2009.

21 Nadya Labi, "Jihad 2.0," *Atlantic Monthly*, July/August 2006. Tsouli apparently learned this 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 heeded.

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

23 Tsouli, however, 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. For more, see Corera and Labi.

24 In October 2005, Bosnian police arrested two men whom they suspected were involved in a terrorist attack. During the search of their phone and e-mail records, they uncovered Tsouli and his colleagues. See "Cyber Operative Charged in Real World Terror Plot."

25 *U.S.A. v. Babar Ahmad*, "Affadavit in Support of Request for Extradition of Babar Ahmad," September 2004 and indictment of Ahmad in *U.S.A. v. Babar Ahmad*, District Court of Connecticut, 2004.

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

participant in an early 2009 discussion on al-Fallujah, a well-known extremist forum, cautioned others about how to 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.[27] 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 the internet for payment that the brothers use "circumvented ways and methods" to make it more difficult to trace.[28]

Hamas has also instructed potential donors on what steps to take to avoid apprehension by security forces. For example, on its Qassam Brigades website, Hamas told donors to use "fake" names when sending e-mails about contributions. Hamas also reassured donors that they will use "secure handling" for the donations to the fighters. Hizb Allah, likewise, has bragged about its sophistication using the internet, particularly in utilizing encryption to protect communications from detection. Hizb Allah 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."[29]

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. There is far less agreement, however, 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. 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 pursued money remitters based outside of the country that were marketing online to U.S. citizens, charging them with failing to register in the United States as required by law.[30] It has complemented this with a softer approach, reaching out to individual web service providers who are hosting troublesome sites, asking the providers to voluntarily shut them down.

Not all countries have been as aggressive as the United States on this front. First, many countries lack the technical capabilities necessary to investigate online terrorist activity.[31] 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 their websites 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.[32] For example, in Italy cyber cafés 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.[33] The United States has also interpreted its responsibilities and laws more expansively than many other countries, targeting entities outside its borders for prosecution; others are hesitant to give their law enforcement agencies this broad reach. Finally, while some countries favor the establishment of an international legal instrument that would govern this area, not all governments regard this as a necessary or helpful step forward.[34]

There are limits, however, to what the United States or any one 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 limits to what is likely to be accomplished.

Michael Jacobson is a senior fellow in The Washington Institute's Stein Program on Counterterrorism and Intelligence. Previously he served as senior adviser in the Office of Terrorism and Financial Intelligence and as counsel on the 9/11 Commission. He is the author, with Matthew Levitt, of the 2008 Institute Publication, "The Money Trail: Finding, Following and Freezing Terrorist Financing."

27 "Jihadi Discussion Forum Posting on Safely Financing Jihad-Related Websites," translated by the NEFA Foundation, April 7, 2009.

28 Ibid.

29 "Jihad Online: Islamic Terrorists and the Internet."

30 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.

31 Raphael Perl, "Terrorist Use of the Internet: Threat, Issues, and Options for International Cooperation," Organization for Security and Cooperation in Europe, April 7-10, 2008.

32 Ibid.

33 "Indian States Make Cyber-Users Sign In," Associated Press, January 10, 2006.

34 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.