Medea Group
Innovative Security and Development

Internet Banking, Hawala and Terrorism

The Dynamics of Islamic Terrorist Groups:
Groundwork for Institutional Fraud

May 2007

Copyright Medea Group 2007

Introduction

This is the first in a series of six papers discussing the money laundering practices—and the implications—of Islamic terrorist groups. This paper presents a summary of methods, both active and not-yet-realized, which are currently available in the illegal and legal transfer of funds from one entity to another and how they might be exploited to ill-gotten gain. Subsequent articles in the series will provide a regional perspective and deeper analysis regarding terrorist groups and money laundering activities. The premise of this paper is that terrorist groups are intelligent, rational entities, well poised to take advantage of gaps in financial security infrastructures and opportunities provided by new technology to expand both funding models and operational objectives.

Why is money laundering a real concern in the analysis of Islamic terror activities and how much money is really involved? Before addressing the methods or monetary figures related to terrorist activity, it is essential to establish the enormity of the money laundering industry. A 1992 estimate for the value of money laundering was $1 trillion USD annually.[1] Today, it is safe to assume "the amount has not diminished since the drug trade and other illegal businesses have been on a steep increase."[2] How much larger is it today, probably double the 1992 figure—about 2 trillion USD or more.[3]

Terrorism is an expensive business. While it is commonly believed terrorist attacks are cheap, the network behind each strike must be maintained, and this requires money. In order to successfully fund a terrorist operation, money must move across borders as quickly and covertly as possible, a service the global money laundering community provides. "Terrorist money does not necessarily move through banks. Money sent by bin Laden's Al-Qaeda organization flew under the radar via Western Union, storefront money transfer businesses, and Hawalas."[4] [a] This paper will demonstrate how a money laundering nexus exists between informal fund transfer systems, charities, Islamic banks and the open waters of the Internet. These are the keys that allow illicit funds to reach the terrorist entities they feed, and by extension the means for shutting them down.

As Rachel Ehrenfeld stated, "To confront global terrorism, especially Radical Muslim organizations, we need to cut off their money. Thus, we must also fight their support systems: criminal organizations, money launderers, and illegal drug producers and traffickers."[5] The discussion will now outline the various forms of money laundering available to the 21st century jihadist.

Terrorist Use of Gold in Money Laundering

The use of gold, gemstones and diamonds has allowed terrorist finances to remain remarkably fluid for some time. "Gold has allowed the Taliban and bin Laden largely to preserve their financial resources, despite the military attack battering their militant forces in Afghanistan."[6] This was accomplished by sending hoards of money by courier through the porous border with Pakistan to the port city of Karachi. There through the

[a] Hawala is simple method of transferring funds within a network of Hawala dealers (Hawaladars) and the running balances between them without a paper trail or infrastructure which can be investigated.

Hawala system and by foot, the money made its way to the desert sheikdom of Dubai, where it was converted into gold bullion.[7] While al Qaeda also used African diamonds, tanzanite from Tanzania and other commodities to generate money and hide assets, as global currency gold played a particularly important role in the group's financial structure.[8] As one senior U.S. law enforcement officer remarked, "Gold is a huge factor in the moving of terrorist money because you can melt it, smelt it or deposit on account with no questions asked."[9] Additionally, "Since it is exempt from international reporting requirements for financial transactions, gold is a favored commodity in laundering money from drug trafficking, organized crime and terrorist activities."[10]

Dubai, conveniently located at the crossroads of the Arab world, is home to one of the largest and least regulated gold markets in the world. Pakistani financial authorities approximate courier flow of $2 million to $3 million a day from Karachi to Dubai, mostly to buy gold.[11] The bullion dealers of Dubai vehemently assert their businesses are clean and free of connections to either terrorist groups or their proxies, but some are willing to do business with anyone for the right price, as Douglas Farah of the Washington Post discovered when interviewing Abdul Razzak, the Pakistani owner of ARY Gold and one of the major players in Dubai's thriving gold market. When questioned over connection to Taliban flight capital he proclaimed, "I wouldn't like to deal with Taliban people, and we don't like Taliban people." However he continued, "If you say you want 100 kilos of gold, I can give you that wherever you want in 12 hours. What you do with it is your business."[12]

The remarkable qualities of gold are everyone wants it, and is instantly convertible into any hard currency. Once a terrorist entity has successfully transferred currency reserves into bullion, finances have moved beyond traceability. Short of stopping fist-sized gold nuggets at the border, authorities will be unable to pick up the money trail again until it reenters the market. However while this transfer of funds is highly effective, it lends itself to a certain amount of risk, particularly when crossing borders with large amounts of money in tow. There are other transfer methods however providing greater security, reliability and virtual untraceability.

Hawala

As mentioned above, Hawala is "money transfer without money movement."[13] It is a simple system relying on a network of Hawala dealers (Hawaladars) and the running balances between them. It leaves virtually no paper trail and is quicker and less expensive than bank wires.[14] Imagine person A in Mumbai wants to send $500 to his brother in Peshwar. He can simply go to his local Hawaladar with $500. This Hawaladar calls his counterpart in Peshwar and has him give $500 (or its equivalent in most major currencies or bullion) to the brother. The Hawaladars themselves keep a running tally of their transactions, and settle their accounts at a later date, commonly arranging for the transfer of funds by phone call, fax or even email.[15]

There is an extremely high level of trust between hawala dealers, as failure to come through with the money promised is tantamount to commercial suicide. Because no real

money has actually moved, there is no traceable link between the originator and recipient of the transfer. Even the records that hawaladars keep are usually in code and often destroyed after the completion of an individual transaction. This anonymity has been a contributing factor to the popularity and subsequent growth of this system, particularly in Islamic population centers (such as areas of Pakistan and Afghanistan) many of which lack formal banking infrastructure.

The existing tribal or familial link between the Hawaladar and the community are also important. A hawala dealer is commonly a trusted and respected member of society. Financial transfers to and from expatriate members of a community are often made through a locally known agent who has earned the respect and loyalty of those around. Furthermore, the Islamic expatriate community is commonly a male domain, and women left behind are expected to maintain minimal contact with the outside. This precludes women from a high level of access to public, commercial institutions such as banks. "A trusted hawaladar, known in the village and aware of the social codes, would be an acceptable intermediary, protecting women from having direct dealings with banks and other agents." [16]

These factors are relevant, but only secondary to the reliability and efficiency of the hawala system. First, a completed transaction is often processed within 24–48 hours, while international bank wires often take a week or more to finalize and can be easily misdirected or lost. Second, Hawaladars advertise more attractive conversion rates than banks while recording significant profit margins and are not subject to international bank regulations or exchange rates. Interpol confirms there are many legitimate hawala businesses, but still believes, "Hawala can, and does play a role in money laundering."[17] Hawala systems support the global flows of narcotics, smuggling, corruption, human trafficking and terrorism.[18] Aside from the question of legitimacy and financial transparency there remains the issue of the network's transfer of large amounts of funds within the Islamic community in support of jihadist activities such as recruitment, training, political propaganda and acts of terrorism.

Financial Implications – Real Numbers

The informal nature of the hawala system increases the difficulty of calculating the exact volume of funds funneled through this process. Pakistani officials have estimated that over $5 billion in hawala transactions pass through their networks each year.[19] India estimates the amount to be as high as $680 billion, roughly the size of Canada's annual GDP.[20]

Many imagine the hawala system is composed of small, one- or two-man operations run out of a little store front or home office. While this is certainly the case with many hawaladars, there are also major multi-national hawala empires.

Al-Barakat

One powerful example is the al-Barakat financial network, with over 187 offices in more than 40 countries, including the United States.[21] Al-Barakat, managed by Osama bin Laden associate Ahmed Nur Ali Jim' Ale, ran as a hawala based out of Dubai transferring

funds globally via opaque banks in the Gulf States.[22] The U.S. government froze the assets of the entire al-Barakat conglomerate after labeling the network an SDGT (Specially Designated Global Terrorist) following 9/11, but until its dissolution, Barakat Telecommunications, an al-Barakat subsidiary, actively assisted terrorist groups in the region by providing secure Internet and telephone connections.[23] Additionally, the banking division of Barakat Telecommunications reportedly handled $500,000 a month in financial transfers.[24]

Dahab Shil

Dahab Shil is a hawala bank functioning much like al-Barakat. Based in Somalia, the organization supports at least 87 branches worldwide, including offices in Canada, New Zealand, Australia and the United States.[25] On the website of the Central Bank of Kenya it is listed as an official Forex Bureau (although spelled Shill).[26] Despite the knowledge that Dahab Shil's infrastructure provided unquestioning support for al-Qaeda's Mohamed al-Owhali, convicted in the terrorist bombing of the U.S. Embassy in Nairobi, the organization continues to operate unimpeded.[27] Four days after he drove the truck bomb to the U.S. Embassy, al-Owhali received a $1,000 transfer from an al-Qaeda member in Yemen.[28]

A Tactical Advantage

Strategic use of these networks allows terrorists the ability to move money quickly with little to no traceability. This is a clear advantage for terrorists over local or international monitoring and law enforcement. The critical factor in the tracking of terrorist operations is timing. "Catching a common criminal or a political kleptocrat after the fact with evidence of money laundering that can be used in court is just fine; catching a terrorist after the fact can be a catastrophe."[29]

Despite efforts by various agencies to crack down on illicit use of the hawala system, monitoring, let alone controlling the flow of funds, is an unrealistic goal. A recent IMF study suggests that "as long as there are reasons for people to prefer such systems, they will continue to exist and even expand."[30] Indeed, as authorities crack down on some of the more public transfer methods, operations simply move underground as evidenced by the case of Western Union.

Western Union, an old favorite for terrorist fund transfer, was particularly exploited by bin Laden and his associates prior to September 11. A Harvard report on tracking terrorist finances specifically mentioned, "There was a tendency to use Western Union to wire money."[31] Ignorant to the aid they offered terrorists by expediting the flow of their finances, Western Union officials initially balked at accepting some of the more stringent regulations regarding customer identification, because it would impact their profit margin.[32]

After 9/11 and a crackdown by the Department of the Treasury, Western Union altered its practices and instituted a profiling method designed to reduce the likelihood of unsavory characters using their services. This reduction in accessibility has driven terrorist groups back to the Islamic hawala networks and the nearly untraceable waters of the Internet. A

Pakistani taxi driver, Munir Ahmed, said, "Sending money by hawala is cheaper and it does not get checked by banks, so it is quicker. They say it is not legal, but it is a reliable alternative to Western Union."[33]

Hawala has come to the forefront in Iraq where the insurgency rages through the assistance of illicit financing schemes. In a country lacking a sophisticated financial infrastructure, and where "the banking system does not allow the transfer of monies"[34], hawala "can actually stand in for a mature financial system."[35] As time progresses and Iraqi financial networks become more sophisticated, new strata of Islamic banking options may further muddy the waters and make tracking terrorist finances more arduous. Indeed individuals with personal finances are finding a new home among the ever expanding world of Islamic financial institutions, both secured by the Islamic code of banking and out of reach for Western investigators.

Islamic Banking

As of 2002, there were more than 200 Islamic financial institutions managing funds in excess of $200 billion and growing at an average annual rate of 10-15 percent.[36] The core of these banks operates in Kuwait, Malaysia, United Arab Emirates, Sudan, Pakistan and Bahrain, all members of the Organization of the Islamic Conference. Islamic banks will soon be able to manage half of the deposits of the Islamic world[37] by increasing profit margins through western banks while enabling unmonitored transfers throughout the Middle East. An unknown percentage of these transactions are managed away from the prying eyes of the western world and western intelligence agencies, rendering them increasingly incapable of creating effective profiles of these networks or potential threats.

edea Group
Innovative Security and Development

Islamic financial institutions strictly adhere to the concept of banking secrecy and confidentiality. Dr. Fath El Sheikh, legal adviser to the Kuwait Investment Authority explains:

> In all their investment and banking modalities, Islamic banks adhere ardently to the concept of banking secrecy and confidentiality. This concept is reflected in their dealings with customers and each other. In the appropriate contract of each detail, it is normally expressly stated that the parties should treat all communications under the contract as confidential, and under no circumstances shall relevant information be divulged to third parties except by court order or in compliance with operative law. Non observance of such a contractual provision amounts to breach of contract, giving the aggrieved party the right to take the appropriate legal action to vindicate its claim.[38]

Islamic banks have maintained a well established connection to money laundering practices and terrorist funding models while turning a blind eye to their implications. The Jordan based Arab Bank (with over 400 branches through out the Arab world, Western Europe Australia and the United States),[39] has long been a favorite for transferring money to terrorist groups in the Palestinian Territories.[40] According to a sworn declaration by the Arab Bank's chief banking officer, "beginning in December of

2000, the Saudi Committee made approximately 200,000 payments into Palestine through Arab Bank branches totaling over US$90,000,000."[41] The Committee is a known and documented supporter of Hamas.[42] Furthermore, an al-Qaeda logistical cell working in Spain to support the 9/11 attacks is known to have moved money from Spain to Pakistan and Yemen through the Arab Bank.[43] More recently, Arab Bank's New York branch was fined $24 million by US banking regulators for failing to implement anti-money laundering controls.[44]

Terrorist Banking Networks

Two infamous Islamic banks, al-Taqwa and al-Aqsa, were established explicitly to help launder and move terrorist finances. Bank al-Taqwa operated as a loosely affiliated, offshore banking conglomerate. Founded with significant support from the Muslim Brotherhood,[45] it enjoyed close contact from infamous terrorist money men Ahmed Idris Nasraddin and Yusif Nada.[46] Up until its closure, al-Taqwa counted Dr. Yusuf Abdullah al-Qaradawi as a board member and one of its largest shareholders. Al-Qaradawi is famous, among other things, for issuing *fatwahs* in support of martyrdom operations and being an outspoken supporter of Hamas and Islamic Jihad. Bank al-Taqwa is known to have transferred funds for bin Laden from "Kuwait and the United Arab Emirates to al-Taqwa's affiliates in Malta and then on to Switzerland and the Bahamas."[47] Al-Taqwa's American assets were frozen in November, 2001. In August 2002, "the United States and Italy, in cooperation with the Bahamas and Luxembourg, designated 25 individuals and institutions as terrorist entities and blocked their assets. These include fourteen businesses owned or controlled by Ahmed Idris Nasraddin or Yusif Nada and linked to al-Taqwa."[48]

Hamas founded al-Aqsa Islamic bank in 1997 to launder money. The shell business provided a legitimate front to its banking activities and acted as a buffer between Hamas and its donors. While popular in the Palestinian territories, al-Aqsa had difficulty operating in Israel. To move funds to its operatives inside Israel, al-Aqsa branched out, embarking on joint projects with Citigroup in order to intertwine itself with Citibank's Israel division and make its funds accessible to operatives in Israel and the territories.[49]

Soon, al-Aqsa and Citibank shared a single database for Israel. Money deposited into al-Aqsa accounts in Europe or other parts of the Middle East became accessible from Israel through Citibank chapters. When Citibank was opening an office in Tel Aviv in January 2001, Israeli authorities formally questioned its ties to al-Aqsa, prompting Citigroup to request advice from the U.S. Treasury Department. Citigroup has not released any information on the Treasury Department's response, but has since severed its ties to al-Aqsa. Israeli counterterrorism authorities estimate that over $1 million has been deposited into al-Aqsa accounts for Hamas since its affiliation with Citibank. At least some of this money reached Hamas through Citibank.[50]

Under executive order 13224 on December 4, 2001 the United States labeled al-Aqsa Islamic Bank "a financial arm of Hamas."[51] As a result the US froze the bank's American and European assets and denied access to collaborative banking relationships, thereby eliminating its usefulness.[52] The bank is now defunct, although this situation underscores the resilience and creativity of terrorist fund raising projects.

Today, while terrorist groups continue to use and exploit Islamic banks, many have turned their attention to the less regulated Internet where they can recruit, fund raise and move their finances—all with just the click of a mouse.

E-Jihad

As the popularity of the Internet as an effective communications tool continues to increase, so does its impact to an expanding Jihadist network.

"The web now serves these groups as a platform for e-jihad: planning, recruitment, fund-raising, training indoctrination, and propaganda. As of July 2006, the number of jihadist websites has grown from a dozen to 4,800."[53] These websites represent a strategic marketing approach by the terrorist community to enter the mainstream.

Terrorist organizations use chat rooms and targeted mass e-mailings as a method of soliciting funds directly from their supporters.[54] Setting up a website is easier than ever before; by utilizing IP Spoofing through an anonymizer, a user can even register a website from his home computer without identifying himself.[55] By making it appears as if a user's computer is connected to the Internet through a different IP address:

> Anonymizer sites access the Internet on your behalf, protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you, enabling you to remain at least one step removed from the sites you visit.[56]

The Internet is a particularly effective tool for terrorist "front" charities. A computer crime and intellectual property expert with the U.S. Department of Justice noted two ways in which they exploit the system:

> 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 worldwide donors. Second, an online charity is not subject to the scrutiny of donors or regulators in the way that predominantly brick-and-mortar charities are.[57]

As use of the Internet spreads through the Islamic world, more jihadists will also find their way online. This trend will expand in the coming decade as younger, more computer savvy militants navigate into the realm of online, Islamic propaganda.

If past performance is any indicator, terrorist use of the Internet will continue to increase over the next several years. The number of global Internet users has ballooned from approximately 600 million in 2002[58] to over 1 billion in 2005.[59] This represents an increase of almost 70% in just three years. This global increase is diminutive in comparison to increases ranging from 155% in the United Arab Emirates to more than

5,000% in Sudan, both of which are centers of the Jihadist movement and terrorist support infrastructure.

Increase in Number of Internet Users in Islamic Countries 2002 - 2005[60]

Country	No. of Users – 2002	No. of Users – 2005	% Increase
Indonesia	**4,400,000**	**16,000,000**	**363**
Iran	**1,326,000**	**7,500,000**	**565**
Lebanon	**300,000**	**700,000**	**233**
Pakistan	**1,200,000**[a]	**10,500,000**	**875**
Saudi Arabia	**1,453,000**	**3,200,000**	**220**
Sudan	**56,000**	**2,800,000**	**5000**
Syria	**60,000**	**1,100,000**	**1833**
United Arab Emirates	**900,000**	**1,397,000**	**155**
West Bank and Gaza (combined)	**60,000**[b]	**243,000**	**405**

a = 2000 data
b = 2001 data

The expansion of Internet usage demonstrates two residual effects. First, the community at large has embraced the concept of being able to bank and conduct business online. In 2005, HSBC reported a 500% rise in its online business transactions compared to 2004 numbers and the number of consumers banking online in Europe grew from 39 million in 2002 to 63 million in 2005.[61] In the United States at least half of all bills will be delivered online by 2010.[62]

The second effect is an increased vulnerability to phishing scams, online fraud and subsequent identity theft.

Online Fraud and Identity Theft

When legitimate business thrives, so does the potential for fraudulent activities. In the first half of 2006, UK banks reported a 55% increase in losses from fraudulent online transactions compared to the same period in 2005.[63]

Phishing is a global threat. It is generally used by petty criminals who send fraudulent emails, usually "representing" legitimate financial institutions to unsuspecting victims, exhorting them to reply with personal information. The responses received include passwords, login information, credit card numbers and personal details which are

normally sold or traded to an online community of bidders. A British watchdog organization reported £23.2m ($45 million) stolen in the first half of 2006 by online phishing scams. Another £22.5m ($44 million) is estimated to have been taken by the end of the year, a 90% increase over 2005 numbers.[64] The incidents of phishing between January and June 2006 were 5,069, a 1,624% increase from the 312 incidents reported the year before.[65] Online banking fraud in the UK increased 8,000% between 2004 and 2006.[66]

While these perpetrators of online fraud present a serious problem for the commercial banking and investment sector, the situation is far more dire: "Terrorists have used stolen identities 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."[67]

The coupling of identity theft with terrorist networks presents a legitimate danger to security models, particularly in an environment where terrorist organizations can pick and choose new identities for their operatives and simultaneously manipulate digital currencies. This triad represents limitless dangers, not just from a potential attack but also from their expanding ability to move resources under a transparent camouflage of IT protocols and web pages. The discussion now shifts to the dangers inherent in terrorist manipulation of digital currencies.

E-Currencies — The "Gold" Standard

While the creation of an e-currency—or digital currency—streamlined online commerce, backing it by gold was pure genius. In this globalizing world, the need to perform transactions in multiple currencies has become increasingly common. While there are certain dominant currencies (dollar, euro, pound sterling, yen etc) there is no overarching global currency that can be used for all transactions. Enter e-currencies. Companies like e-gold[68] or e-bullion[69] offer members the ability to exchange money from any major currency into gold units. These units hold their value based on the current exchange of gold to global currencies. When a user makes an online purchase with an e-gold account, the item is paid for in gold. If something costs $1,000, the account holder pays the equivalent amount in bullion and the merchant receives $1,000.

One of the most important factors in laundering funds is the liquidity of the finances in question. The more quickly they can be moved or converted into another form, the more difficult to track or trace. Traditionally, the easiest way to do this was by converting the original currency into bullion or gemstones, moving across borders and converting into a second currency on arrival. Since e-currency has freedom of movement across borders and is backed by bullion, it is ripe for exploitation by terrorist entities. As regulators and law enforcement officials continue to pressure the international banking arena and monitor transactions to and from areas and individuals of suspect, illicit entities have been working to establish more fluid, less regulated methods of transfer. Bullion backed e-currency allows them the flexibility and anonymity to do just that.

The operators of e-currency services are not ignorant to the threat of exploitation. The Company E-gold requires a user to fund an account through an independent exchange service (IES). IES transfers hard currency to and from e-currency. E-bullion allows users to contribute through its main website as well as through IES. Exchange services themselves vary in their security precautions with no overarching regulations to monitor their operations. Reputable exchanges like Euro Gold Sales[70] or the Omni Exchange[71] require an account to be funded through an authorized bank wire only. Other services like "electrum" allow you to fund your e-gold or e-bullion account with any Visa, Master Card or American Express.[72] For $35, e-bullion offers an anonymous, numbers-only debit card which can be used at point of sale and almost every ATM location globally.[73] While these debit cards are currently only available to members in the United States, other companies provide global debit services. Best Gold Card[74] and Eternity Bank[75] allow users to purchase and fund a debit card with their e-gold accounts and then use it at "more than 17 million ATM locations around the world."[76] This service is available to a global community[77] including those residing in money laundering hubs of the Middle East and Central Asia.

When coupled with identity theft, the tools provided by digital currencies become increasingly dangerous. A terrorist with one stolen credit card, an e-gold account and a linked debit card has streamlined his entire financing operation. The credit card funds the e-gold account which can be withdrawn at ATMs or used to purchase goods anywhere in the world. This cycle of laundering and fraud can be used to finance a near limitless supply of terrorist activity. These online accounts are more disturbing when you consider at least 40 million identifying records have been stolen or lost in the last year.[78] Even at this level, there is failure to appreciate the full potential of e-commerce and digital currency to finance terrorist operatives and initiatives, commercially and through charitable donation, both of which will be discussed in the following sections.

Innovative Security and Development

Commercial Implications

At the end of the month, or a pre-set period of time, hawaladars settle their accounts. To facilitate this activity, many hawaladars are known to run import/export businesses and as a way of settling accounts, over- or under-invoice the shipment. For example, if one hawaladar from Pakistan owes $5,000 to another from England, he can invoice a legal shipment he is making from his company to company B for $15,000 instead of $10,000 and thereby settle his account. The same concept can be applied with even greater ease online.

Paypal and eBay are very secure sites, both with active fraud protection systems. They are not however looking for over-invoicing. Online conversion services like World Exchanger allow a client to transfer digital currencies from one format into another. E-gold can be moved into e-bullion, and vice-a-versa, but also into several other e-currency formats, including Paypal.[79]

With over 100 million users, Paypal is the goliath of the online currency exchange business. Paypal users can send money with ease to one another, anywhere around the globe. They can also bid and pay freely on eBay for products which may or may not

exist. In an attempt to settle accounts or launder funds, an individual could easily list an item for sale on eBay creating a pseudo-bidding war with real and imagined users. No mechanism exists to confirm if and when a shipment is finalized between these users unless a complaint is logged on line. Additionally, a seller on eBay could list an item without any intention to deliver it upon completion of the auction. When payment has been received, the seller could simply create another persona, or suffer the sting of negative feedback and post again. In fact, a recent report from the U.S. Federal Trade Commission remarked that twelve percent of fraud complaints received was connected to online auction sites,[80] of which eBay is far and away the largest. Consequently, terrorists can create 'legitimate' online businesses which only serve as a funnel to transfer cash funds.

Islamic Charities as Money Laundering Conduits

Online funds transfer is not limited to the world of buying and selling. Certainly many individuals find it a convenient way to donate to charities of choice. It is quick, easy and in most cases tax deductible to make a charitable donation online. When a political injustice is identified by the international community, a charity or fund pops up to provide support for those being oppressed. Not all charitable entities perform the work they mandate. Many take advantage of this unregulated influx of funds. "For the terrorist, charities represent a perfect cover for collecting large amounts of money and arms to be used for terrorist operations."[81] Although its primary benefit is financial, charities associated to terrorist groups also serve as recruiting centers and provide employment for its operatives.[82]

Several Islamic terrorist groups take advantage of this opportunity both for funding and to create an aura of political viability. Hamas, is known to be financed through the Union of Good, an umbrella organization of over 50 Palestinian charities including Interpal in the UK, the Committee for Palestinian Charity and Aid (Comité de Bienfaisance et de Secours aux Palestiniens) in France, and the Associazione Benefica di Solidarieta con il Palestinese in Italy.[83] Through these groups, Hamas is able to provide social services to the Palestinian people. This increases popularity at home and political clout abroad, while simultaneously allowing it to move money straight through to its military wing.

These money laundering practices are well known to international law enforcement officials and their efforts to contain and hinder these terrorist flows are the subject of the next section.

International Response

Law enforcement officials and the international community at large are no strangers to terrorist money-laundering practices and have been actively working to reduce their effectiveness. The greatest impediment towards accurate and effective monitoring of terrorist finances, particularly with regard to the international banking network, has been turf warfare and a lack of desire to cooperate. French regulators for example are not too keen on allowing American investigators unfettered access to banking archives. In other

locales, a legal structure requires judicial intervention prior to external access to a resident's personal information. Considering the speed of financial movement, it is no wonder that law enforcement has been falling behind.

The world is aware of these problems and in an effort to counter money laundering practices, global bodies have worked to remedy the situation. The United Nations has attempted to lay out the ground work for an individual country's responsibilities regarding money laundering through the passage of the International Convention for the Suppression of the Financing of Terrorism[84] and Security Council Resolution 1373.[85] In the resolution, the Security Council:

> Decides that all states shall….Prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of personas and entities acting on behalf of or at the direction of such persons…[86]

In order to counter cross-border financial movement by terrorist entities, a consortium of governmental and law enforcement agencies from 33 countries created the Financial Action Task Force on Money Laundering (FATF).[87] The FATF statutes, which include the Forty Recommendations on Money Laundering and the Nine Special Recommendations on Terrorist Financing, strive to counter the global financing of terrorism through enhanced international cooperation. This contentious issue is clearly addressed in Special Recommendation number five, which states:

> Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organizations. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organizations, and should have procedures in place to extradite, where possible, such individuals."[88]

The FATF is the vanguard in the war against terrorist financing in the world today. It should be commended for its actions to bring money laundering to the forefront of an international consciousness normally preoccupied with less sensitive and pervasive issues. Unfortunately, the FATF is doomed to failure for the same lack of effectiveness as other international treaties and regulations. There is no true way to enforce these practices. While the FATF contributes to additional pressure on law enforcement organizations, there is no mechanism to enable competing agencies into collaborative action. While this consortium is pregnant with political capital, it comes up short when everything is on the line.

The UN Security Council completed the bureaucratic circle with the passage of resolution 1617 (2005), section seven of which "Strongly urges all Member States to implement the comprehensive, international standards embodied in the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering and the FATF Nine Special Recommendations on Terrorist Financing."[89] Strongly urging international cooperation does not reflect a successful history,

Conclusion

Many think of Islamic terrorists as irrational beasts ready to kill anyone or anything for a headline or in support of Jihad. Perceptions are not always factual. It is imperative to recognize terrorist entities are run by highly intelligent individuals, often calm and calculating. Terrorist groups will continue to find new ways to finance themselves and perpetuate their existence and operations.

As new technologies develop particularly those designed to alleviate impediments to international trade, terrorists will find ways to exploit them by expanding their existing networks. International law enforcement agencies must commit to working as a more cohesive unit, in order to better understand, investigate and counter terrorist financing efforts. All of these bodies and resolutions help, but still amount to more suggestions than action, more resolution than solution.

The international community must concede that the volume of funds available to terrorists will always be larger than the amount that can be effectively confiscated or frozen. In order to truly combat terrorist financing and the money laundering upon which it thrives, we must not simply go after the source; we must destroy the mechanisms behind the source. This change in methodology provides a baseline upon which future actions can be designed, launched and monitored for measures of success.

---

[1] Ehrenfeld, R. 2002. "Funding Terrorism: Sources and Methods Confronting Terrorism – 2002," *Workshop held at Los Alamos National Laboratory*. March 25-29, 2002. Also available at http://library.lanl.gov/cgi-bin/getdoc?event=CT2002&document=30.

[2] Ibid.

[3] Ibid.

[4] Malkin, L. and Elizur, Y. 2002. "Terrorism's Money Trail," *World Policy Journal*, Spring, pp. 60–70. http://worldpolicy.org/journal/articles/wpj02-1/Malkin.pdf.

[5] Ehrenfeld, R. 2002. "Funding Terrorism: Sources and Methods Confronting Terrorism – 2002," *Workshop held at Los Alamos National Laboratory*. March 25-29, 2002. Also available at http://library.lanl.gov/cgi-bin/getdoc?event=CT2002&document=30.

[6] Farah, D. 2002. "Al Qaeda's Gold: Following Trail to Dubai," *Washington Post*, 18 February. Also available at http://www.globalpolicy.org/nations/corrupt/2002/0218gold.htm

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Jost, P. M. and Sandhu, H. S. 2000. "The hawala alternative remittance system and its role in money laundering," *Interpol General Secretariat*, Lyon, January.
http://www.interpol.int/public/financialcrime/moneylaundering/hawala/

[14] Ibid.

[15] Ibid.

[16] El-Qorchi, M. 2002. "Hawala – How does this informal funds transfer system work and should it be regulated?" *Finance & Development*, a quarterly magazine of the IMF, December, vol. 39, no. 4. *Also available at http://www.imf.org/external/pubs/ft/fandd/2002/12/elqorchi.htm* (accessed April 4, 2007).

[17] Ibid.

[18] Gillespie, J. 2002. "Follow the Money: Tracing Terrorist Assets," *Seminar on International Finance, Harvard Law School*, April 15, 2002, p. 9. Also available at
http://www.law.harvard.edu/programs/pifs/pdfs/james_gillespie.pdf.

[19] Looney, R. E. 2002. "Following the Terrorist Informal Money Trail: The Hawala Financial Mechanism," *Strategic Insights*, November, vol. I, no. 9. Also available at
http://www.ccc.nps.navy.mil/si/nov02/southAsia.asp (accessed April 5, 2007).

[20] Ibid.

[21] Emerson, Steven. 2002. "Testimony Before the House Committee on Financial Services Subcommittee on Oversight and Investigations," *PATRIOT Act Oversight: Investigating Patterns of Terrorist Fundraising Fund-Raising Methods and Procedures for International Terrorist Organizations,* 12 February.
http://financialservices.house.gov/media/pdf/021202se.pdf

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] http://www.centralbank.go.ke/bankinfo/forexbureaus.asp (accessed April 16, 2007)

[27] Emerson Testimony

[28] Ibid.

[29] Malkin, L. and Elizur, Y. 2002. "Terrorism's Money Trail," *World Policy Journal*, Spring, pp. 60–70.
http://worldpolicy.org/journal/articles/wpj02-1/Malkin.pdf.

[30] Detmer, J. 2003. "Troubling analysis of terrorist banks – the business – International Monetary Fund on Hawala banking system – Brief Article," *Insight on the News*, 4 February.
http://www.findarticles.com/p/articles/mi_m1571/is_4_19/ai_97450999/print.

[31] Gillespie, J. 2002. "Follow the Money: Tracing Terrorist Assets," *Seminar on International Finance, Harvard Law School*, April 15, 2002, p. 12. Also available at
http://www.law.harvard.edu/programs/pifs/pdfs/james_gillespie.pdf.

[32] Malkin, L. and Elizur, Y. 2002. "Terrorism's Money Trail," *World Policy Journal*, Spring, pp. 60–70.
http://worldpolicy.org/journal/articles/wpj02-1/Malkin.pdf.

[33] Associated Press. 2006. "Western Union profiles Muslim names," *The Jerusalem Post*, 2 July. Also available at
http://www.jpost.com/servlet/Satellite?cid=1150885903063&pagename=JPost%2FJPArticle%2FPrinter.

[34] Iraq Study Group Report – pp. 21, Available online at
http://www.foxnews.com/projects/pdf/iraq_study_group_report.pdf (Accessed May 3, 2007)

[35] Altman, D. 2006. "Managing Globalization: Ins and Outs of Underground Money," *International Herald Tribune*, 12 July 12. Also available online at http://www.iht.com/articles/2006/07/11/business/glob12.php (Accessed May 3, 2007)

Media Group
Innovative Security and Development

[36] El Sheikh, F. 2002. "The Underground Banking Systems and their Impact on Control of Money Laundering: With Special Reference to Islamic Banking," *Journal of Money Laundering Control*, vol 6, no.1, pp. 42-45.
[37] Ibid.
[38] Ibid.
[39] Arab Bank Website available at http://www.arabbank.com/user_prof_world.asp (accessed May 3, 2007)
[40] Levitt, M. A. 2006. "The Political Economy of Middle East Terrorism," *MERIA Journal – Middle East Review of International Affairs*, December, vol. 6, no. 4. http://meria.idc.ac.il/journal/2002/issue4/jv6n4a3.html (accessed April 5, 2007).
[41] Levitt, M. 2006. *Hamas: Politics, Charity, and Terrorism in the Service of Jihad.* Newhaven and London: Yale University Press – published in cooperation with the Washington Institute for Near-East Policy, p. 191.
[42] Ibid.

[43] Ibid.

[44] Finextra Report. 2005. "Arab Bank fined $24m for anti-money laundering failures in US." 18 August. Available at http://www.finextra.com/fullstory.asp?id=14131

[45] Levitt, M. A. 2006. "The Political Economy of Middle East Terrorism," *MERIA Journal – Middle East Review of International Affairs*, December, vol. 6, no. 4. http://meria.idc.ac.il/journal/2002/issue4/jv6n4a3.html (accessed April 5, 2007).

[46] Emerson Testimony
[47] Ibid.

[48] Levitt, M. A. 2006. "The Political Economy of Middle East Terrorism," *MERIA Journal – Middle East Review of International Affairs*, December, vol. 6, no. 4. http://meria.idc.ac.il/journal/2002/issue4/jv6n4a3.html (accessed April 5, 2007).

[49] Emerson Testimony
[50] Ibid.
[51] U.S. State Department. 2001. "Shutting Down Terrorist Financial Networks," *White House Fact Sheet on Hamas*, 4 December. Available at http://usinfo.state.gov/is/Archive_Index/Shutting_Down_Terrorist_Financial_Networks.html (accessed April 16, 2007).
[52] Ibid.
[53] Editors, Discover. 2006. "The Future of Terrorism," *Discover Magazine*, 25 July. http://discovermagazine.com/2006/jul/cover/article_view?b_start:int=0&-C=
[54] Hinnen, T. M. 2004. "The Cyber-Front in the war on Terrorism: Curbing Terrorist Use of the Internet," *The Columbia Science and Technology Law Review*, vol. 1, no. 42, p. 9. http://www.stlr.org/html/volume5/hinnen.pdf.
[55] Hinnen 11
[56] How Anonymizers Work - http://www.livinginternet.com/i/is_anon_work.htm - accessed April 15, 2007
[57] Hinnen 19
[58] 2002 figures provided by the 2003 CIA World Factbook, hosted by Bartelby at http://www.bartelby.com/151/fields/110.html (accessed on April 16, 2007)
[59] 2005 figures provided by the 2006 CIA World factbook, available online at https://www.cia.gov/cia/publications/factbook/rankorder/2153rank.html
[60] 2000, 2001, 2002 figures provided by the 2003 CIA World Factbook, 2005 figures provided by the 2006 CIA World Factbook
[61] "Potential of internet banking remains unfulfilled," *CBR Online*, April 5, 2007. Available online at http://www.cbronline.com/article_feature_print.asp?guid=C6389ECF-5713-4EB7-8D95-E73076B4B42D.
[62] "Online Banking Fastest Growing Internet Activity," *ITworld.com, Ecommerce in Action*, February 15, 2005. http://www.itworld.com/Tech/2409/nls_ecommerceonlinkebank050215/pfindex.html.
[63] Kirk, J. 2006. "Sharp rise for online banking fraud. UK banks lose £22.5m," *P.C. Advisor*. 8 November. Also available at http://www.pcadvisor.co.uk/news/index.cfm?newsid=7549.

Media Group
Innovative Security and Development

[64] Sharma, N. 2006. "Online Banking Fraud Witnesses 8,000% Rise In U.K.," *BizReport: Latest Headlines*, 15 December. http://www.bizreport.com/2006/12/online_banking_fraud_witnesses_8000_rise_in_uk.html.
[65] Ibid.
[66] Ibid.
[67] Hinnen, p. 22.
[68] www.e-gold.com (accessed April 13, 2007)
[69] www.e-bullion.com (accessed April 13, 2007)
[70] www.eurogoldsales.com (accessed April 13, 2007)
[71] www.omniexchange.net (accessed April 13, 2007)
[72] www.electrumx.com (accessed April 13, 2007)
[73] http://www.e-bullion.com/debit_us.php (accessed April 13, 2007)
[74] http://www.bestgoldcard.com (accessed April 13, 2007)
[75] http://www.eternitybanking.com (accessed April 23, 2007)
[76] http://www.bestgoldcard.com (accessed April 13, 2007)
[77] http://www.bestgoldcard.com (accessed April 13, 2007) – Although this service is not available to residents of Iran or Syria, it is available to all residents of the UAE, Saudi Arabia Indonesia, India, Lebanon, Macao and others.
[78] http://www.idtheft.com/intro.php (accesed April 23, 2007)
[79] www.worldexchanger.net (accessed April 13, 2007)
[80] 2005 Identity Theft Statistics, available online at http://www.guardmycreditfile.org/index2.php?option=content&do_pdf=1&id=555 (accessed April 23, 2007)
[81] Emerson Testimony
[82] Levitt, M. 2006. *Hamas: Politics, Charity, and Terrorism in the Service of Jihad.* Newhaven and London: Yale University Press – published in cooperation with the Washington Institute for Near-East Policy, pp. 81.
[83] Levitt, M. 2006. *Hamas: Politics, Charity, and Terrorism in the Service of Jihad.* Newhaven and London: Yale University Press – published in cooperation with the Washington Institute for Near-East Policy, pp. 157-161.
[84] "International Convention for the Suppression of the Financing of Terrorism." http://untreaty.un.org/English/Terrorism/Conv12.pdf.
[85] "UN Security Council Resolution 1373." http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement.
[86] "UN Security Council Resolution 1373." http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement (quote from section 1d).
[87] Financial Action Task Force (FATF) Website http://www.fatf-gafi.org (accessed on April 16, 2007)
[88] "Nine Special Recommendations (SR) on Terrorist Financing (TF) – FATF Standards #5 (v)." Available online at http://www.fatf-gafi.org/document/9/0,2340,en_32250379_32236920_34032073_1_1_1_1,00.html (accessed April 24, 2007).
[89] "UN Security Resolution 1617 section 7." Available online at http://daccessdds.un.org/doc/UNDOC/GEN/N05/446/60/PDF/N0544660.pdf?OpenElement (accessed April 24, 2007).