2013-08

Terrorism Financing Methods: An Overview / Perspectives on Terrorism / Vol. 7, Issue 4

Freeman, Michael; Ruehsen, Moyara

Monterey, California. Naval Postgraduate School

Perspectives on Terrorism, August 2013, v. 7. No. 4
https://hdl.handle.net/10945/35989

I. Articles

Terrorism Financing Methods: An Overview

by Michael Freeman and Moyara Ruehsen

Abstract

How do terrorists move money? This article examines six of the most widely used methods: cash couriers, informal transfer systems (e.g. hawala), money service businesses, formal banking, false trade invoicing, and high value commodities. When terrorists move money, they choose methods that take into account issues of: volume, risk, convenience, simplicity, costs, and speed. This article analyzes the methods according to these issues. It draws on multiple cases and examples, including the most recent cases of Hezbollah's and al Shabaab's use of money service businesses, and many others.

Shortly after the 9/11 attacks, U.S. federal agents received a tip-off from a confidential informant that a Yemeni sheik was raising money in Brooklyn for al-Qaeda. The sheik had allegedly boasted in recorded conversations that he had raised as much as US $20 million for Osama bin Laden. Some of the money was raised in cash donations, but cash is bulky and difficult to move. Depositing the cash in a formal bank and wire transferring it to Yemen would have raised red flags. So the sheik arranged to have the bulk cash shipped in cargo. When the agents arrested two men at Kennedy Airport in October 2001, they found US $140,000 of cash hidden in cardboard boxes along with honey jars.[1] It wasn't the first time the honey trade had been used to disguise the movement of money. In the months leading up to 9/11, the same Yemeni honey trading businesses imported over-invoiced honey to disguise money flowing *to* the United States. [2]

How terrorists move money, and how this can be disrupted, is often overlooked. Instead, scholars and policy-makers focus on either the sources of terrorist financing or the things terrorists spend money on, like weapons and the attacks themselves.[3] Yet the movement of money is a critical intermediary step. Terrorist groups often raise money in places different from where they are located and different from where attacks might take place. For terrorist groups to be effective, they must be able to move money from its origins to the operational areas where it is needed. These transfers of money represent potential weak points which the state can target to more effectively disrupt the terrorist organization and its operations.

Given the range of possible methods for terrorists to move funds, why do terrorist groups choose a particular method or combination of methods from the possible options? The following section will explore what the broad attributes might be for the movement of money. The

subsequent section will describe the primary methods used to transfer money and will include how each method has advantages and disadvantages according to the attributes laid out in the earlier section. The final section will discuss how better countermeasures can be developed to better address the movement of terrorist finances.

Attributes

When terrorists move money, what kinds of issues might they be thinking of? Based on some evidence, as well as assumptions and inferred behavior, terrorists seem to choose methods of moving funds that take into account issues of: volume, risk, convenience, simplicity, costs, and speed.[4]

Volume: The ability to move more money with each transaction makes it easier for terrorist groups to fund an operation. However, not all methods are capable of moving an equal volume of funds. Methods like formal banking, hawalas, and money transfer businesses can theoretically transfer an infinite amount of money in a single transaction. In contrast, moving bulk cash is limited by the size and weight of the cash being transferred, with US $1 million in US $100 bills weighing over 20 pounds; and in US $20 bill denominations, more than 100 pounds. Such a load would also take up a lot of space. Despite what is often portrayed in the movies, a typical briefcase can fit just over US $250,000 in used US $100 bills, or a mere US $50,000 in US $20 bills.

Risk: For terrorist groups, there are several types of risks they might face depending on the method of fund transfer. Among the most obvious risks is that the transfer itself will be detected by authorities. For example, a transfer between two banks is much more likely to be monitored, recorded, and discovered, than a transfer of cash that crosses the border between Afghanistan and Pakistan. A related element of risk comes from the varying degrees of anonymity associated with each method of moving funds. Some methods, like formal banking, require institutions to follow "know your customer" (KYC) practices, while others, like hawalas or cash, allow for more anonymity.

Another risk for terrorists is the reliability of different methods. There is a high degree of certainty that transfers made between banks and between hawalas, for example, will be made accurately and completely. Cash transfers, on the other hand, may be less reliable because of the opportunities for theft along the way. And because of their bulk, they may be more vulnerable to seizure by law enforcement.

Convenience: Depending on their physical location, some methods for moving funds may be more or less convenient for a terrorist group. For example, using cash or hawalas to move money into or out of tribal areas in Iraq or Afghanistan is much more convenient than using formal banks. Likewise, al-Qaeda's alleged trade in West African conflict diamonds was more convenient than using cash or gold to move funds.[5] West Africa is geographically distant from South Asia, but diamonds are easy to hide, and therefore much more convenient than cash. Gold is less

convenient because of its weight and bulk, but given the importance of gold for dowries in both South Asia and the Middle East, and the number of large gold souks throughout the region, large shipments of gold in the form of high-end jewelry will not attract much notice. The convenience of a particular method will clearly depend on geographic/topographic features (like an uncontrolled border) as well as demographic (cultural, ethnic, linguistic) factors.

Simplicity: Everything being equal, terrorists would prefer methods that require the fewest number of steps, the lowest level of technology, and the least amount of skill. Given these parameters, terrorists are less likely to engage in elaborate money laundering schemes that involve numerous actors and that require dozens of complicated steps to obscure the trail of money. Using a scheme like the black market peso exchange, for example, would be much more complicated than a series of wire transfers through multiple bank accounts.[6]

Costs: Put simply, moving money requires the payment of fees. Western Union and MoneyGram charge users a transaction fee that can range anywhere from 1-10% depending on the amount being transferred and other transaction variables. Likewise, hawalas charge between 0.5-2.5% on each transaction. Even moving cash across borders may require side payments to border guards or customs officials.

Speed: Terrorists want to move money as quickly as possible to their final destination in order to fund their operational needs. Hawalas, for example, allow for transfers to occur relatively quickly, while formal banking may require deposits to sit for a day before they clear. Bulk cash smuggling can vary depending on how far the cash needs to move, and how many borders it needs to cross. A false trade invoicing scheme probably requires the longest amount of time to complete.[7]

Methods

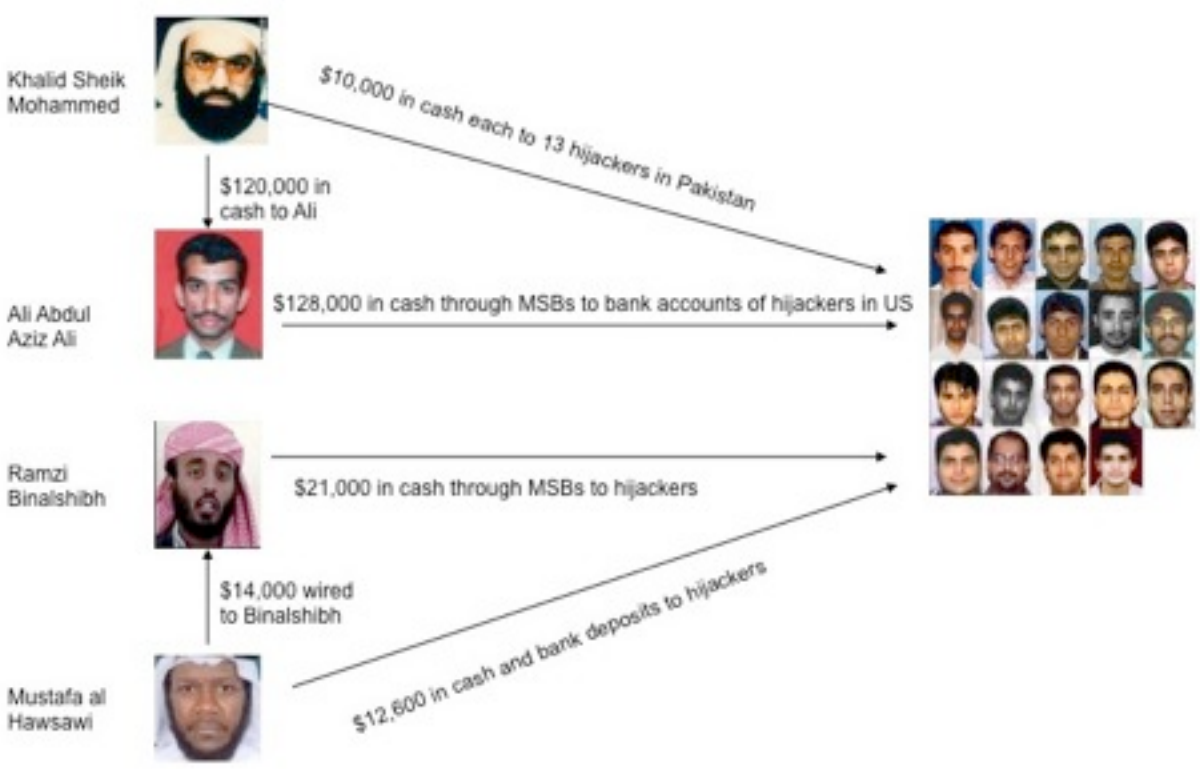
This section highlights the most used methods as well as some methods that are not used, but have been raised as potential future methods. For each method, we offer a description of the method, some examples of how terrorists have used the method, and how we might think about each method according to the attributes described above. The methods are presented from most simple to most complex.

Cash Couriers: Using couriers to move physical cash is the "simplest and oldest way of moving value."[8] When criminals move cash across international borders, they typically conceal it in vehicles, packages, luggage, or anything else that can hold large physical volumes of cash.[9] Oftentimes, where borders are uncontrolled or where the state's resources are strained, criminals do not even conceal the cash.[10]

AQ relied on couriers to move money in the 1990s and before the 9/11 attack. According to the 9/11 Commission Monograph, al-Qaeda used money changers to transfer US $1 million from the UAE to Pakistan and then used couriers to transfer the funds as cash into Afghanistan. For the

9/11 attack itself, "Khalid Sheik Mohammed delivered…US $120,000 [in cash to] Abdul Aziz Ali in Dubai…[who] then used the cash to wire funds to the hijackers in the United States."[11] Khalid Sheik Mohammed also gave thirteen of the hijackers US $10,000 each as they left Pakistan. These hijackers brought cash and traveler's checks with them as they entered the U.S. and deposited the funds at banks such as Bank of America, SunTrust, and other smaller banks. Others, like Ramzi Binalshibh and Mustafa al Hawsawi also used cash to fund the attack. Zacarious Moussaoui brought in the most cash, US $35,000, which he declared with Customs as he entered the country. (See Figure 1 for some of the cash transactions before the 9/11 attack.)

Figure 1: Cash Transfers before 9/11 Attacks



Cash couriers are used by other groups as well. For example, foreign fighters traveling to Iraq to join AQI often brought cash with them. According to the captured records from Sinjar (on the Syrian border in northwestern Iraq), of the 590 records of foreign fighters, 149 brought cash to AQI after entering Iraq. In general, almost all the different nationalities had close to the same rate of fighters contributing money (about 20-30%), but the Saudi fighters contributed the largest amount in an absolute sense. They also comprised 22 of the 23 fighters who brought in more than US $1,000.[12] Overall, these cash transfers were estimated to make up over 70% of AQI's budget, highlighting the importance of this mechanism for both raising and moving funds into the organization.[13]

Likewise, Jemaah Islamiyah has used cash couriers in the past as their primary method of moving funds. Before the Bali bombings in 2002, JI used two Indonesian laborers working in Malaysia to transfer over US $15,000 between terrorist members. Khalid Sheik Mohammed, the al-Qaeda deputy and mastermind of 9/11, used a Pakistani courier to deliver US $50,000 to a JI leader in 2003 after the Bali attack.[14] JI also used cash transfers and couriers to move about US $8,500 to the bombers of the Atrium Mall in Jakarta in 2001.[15]

Security is an important consideration when using cash couriers. Terrorist networks will presumably use only trusted personnel to move the money. Another consideration is speed. Transferring funds with couriers is much slower than electronic means. It also requires some complex planning and coordination if couriers need to arrange the transfers.

Informal Transfer Systems: There are several types of informal financial networks, such as Hawala/Hundi in South Asia, Fei ch'ien in China, Phoe Khan in Thailand, and Door-to-Door in the Philippines.[16] These networks often have traditional roots and ethnic ties, and operate in places where the formal banking sector is less established or where large ethnic diasporas live. They are estimated to be part of a US $500 billion global remittance system.[17] Although most countries have legalized hawala (thinking that the networks will be easier to police if they operate openly), many hawaladars (hawala dealers) continue to operate illegally because of prohibitively high licensing and registration fees. Hawala networks were especially scrutinized after 9/11 due to evidence that al-Qaeda, the Taliban, and Al-Qaeda in Iraq (AQI) used them.

Hawala networks in the Middle East and South Asia operate in the following manner: a worker in Dubai wants to send US $1,000 back to his wife in Pakistan. He finds a hawaladar and gives him the funds. The hawaladar contacts a fellow hawaladar (often an extended family member running a linked operation) in Pakistan. The hawaladar in Dubai gives both the worker in Dubai and the hawaladar in Pakistan a transaction code. The worker's wife goes to the hawaladar in Pakistan and gives him the code. If the codes match, the hawaladar in Pakistan gives his wife the rupee equivalent of US $1,000 minus a small fee. (Note that no funds have actually crossed borders.)

To settle the accounts, the simplest method is for the hawaladars to wait for a similar value of transactions to move in the other direction. As this rarely occurs, the hawaladars will periodically (weekly, or monthly) balance their books by using money service businesses, smuggling high value commodities, or false trade invoicing transactions to transfer funds.

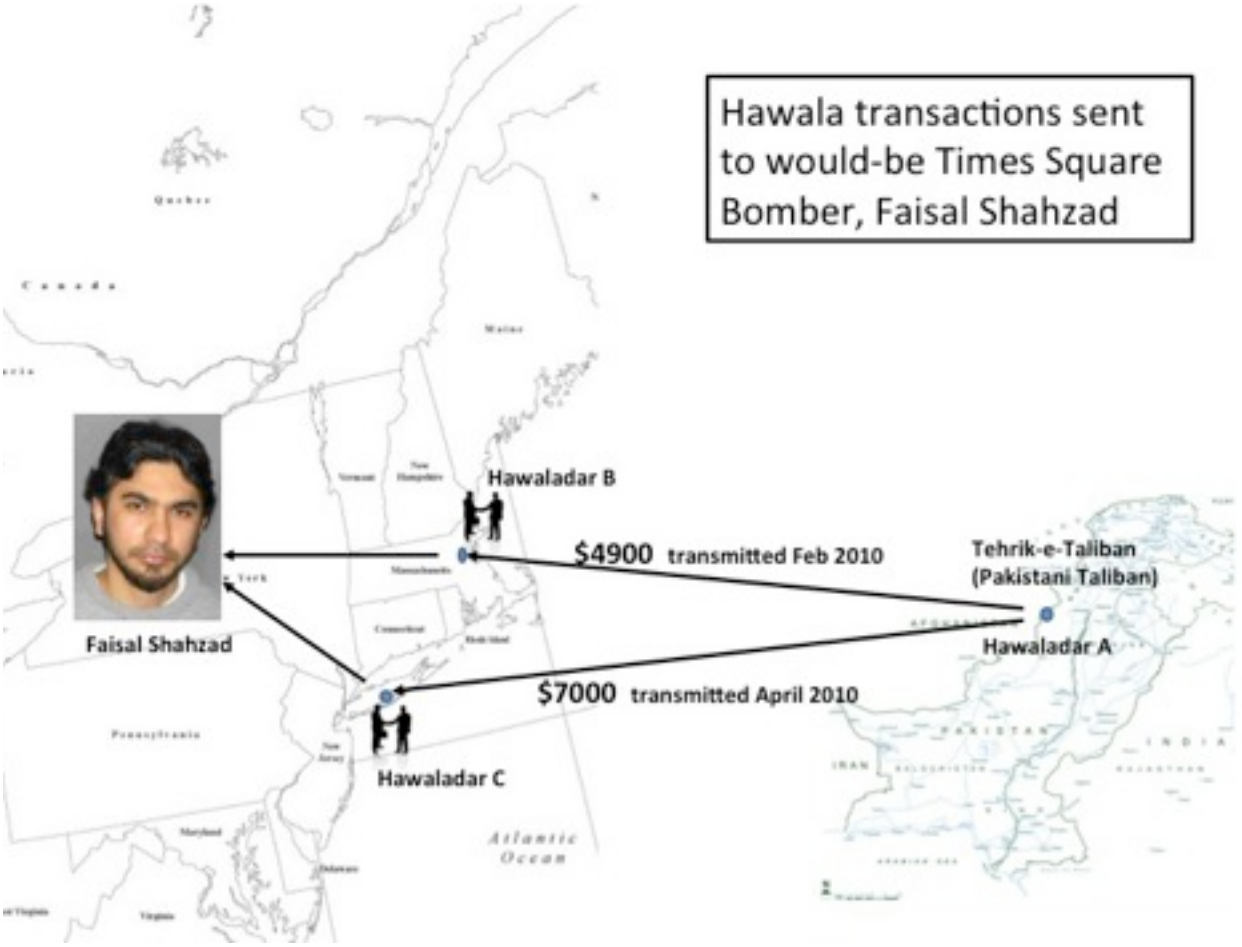
Although most customers use hawala for legitimate purposes, several terrorist groups have used hawalas to move money. Before 9/11, al-Qaeda "moved much of its money by hawala."[18] They used "about a dozen trusted hawaladars" (as well as some unwitting hawaladars) in Pakistan, Dubai, and elsewhere in the Middle East.[19] While AQ used hawalas prior to 9/11, they did not use them specifically for the 9/11 plot.[20]

Besides al-Qaeda, Lashkar-e-Toiba used hawala networks to move funds before their 2000 Red Fort attack in Delhi. Likewise, Dawood Ibrahim transferred funds via hawala networks before the 1993 Mumbai attack.[21] In Iraq, terrorist groups have used hawala: two Iraqi Kurds were arrested for using hawalas to move part of nearly US $150,000 to finance Ansar al-Sunna/Ansar al Islam.[22] Based on an author's interview with a U.S. Special Forces colonel, we also know of coalition operations undertaken against hawaladars that were knowingly moving funds for Iraqi insurgent groups. Jemaah Islamiyah also used hawaladars to transfer about US $2,500 before a 2001 attack.[23]

A more recent example is the case of the would-be Times Square bomber, Faisal Shahzad. In February 2010 Mr. Shahzad's handlers in Pakistan (Tehrik-e-Taliban)[24] arranged for US $4,900 to be sent via an unregistered hawala network operated by two brothers, one of whom, Aftab Ali Khan, was an illegal Pakistani immigrant living in Brookline, Massachusetts. On February 24 or 25th Mr. Ali Khan met Mr. Shahzad just outside of his Massachusetts apartment to hand over US $4,900 in cash.[25] There was no suggestion in any subsequent investigations that Mr. Ali Khan knew what the money would be used for. He was merely completing an anonymous business transaction.

In April Mr. Shahzad received an additional tranche of funds from the Pakistani Taliban. Perhaps because of the inconvenient distance between Boston and New York, another hawala network was used. This new network, operated by Mohammad Younis on Long Island and his brother in Pakistan, was also unregistered.[26] On April 10th, just three weeks before the bombings, Mr. Younis spoke to Mr. Shahzad by phone and arranged a meeting in a parking lot in Ronkonkoma, New York to hand over US $7,000 sent by Mr. Shahzad's Pakistani Taliban handlers.[27]

Figure 2: Finances for Faisal Shahzad



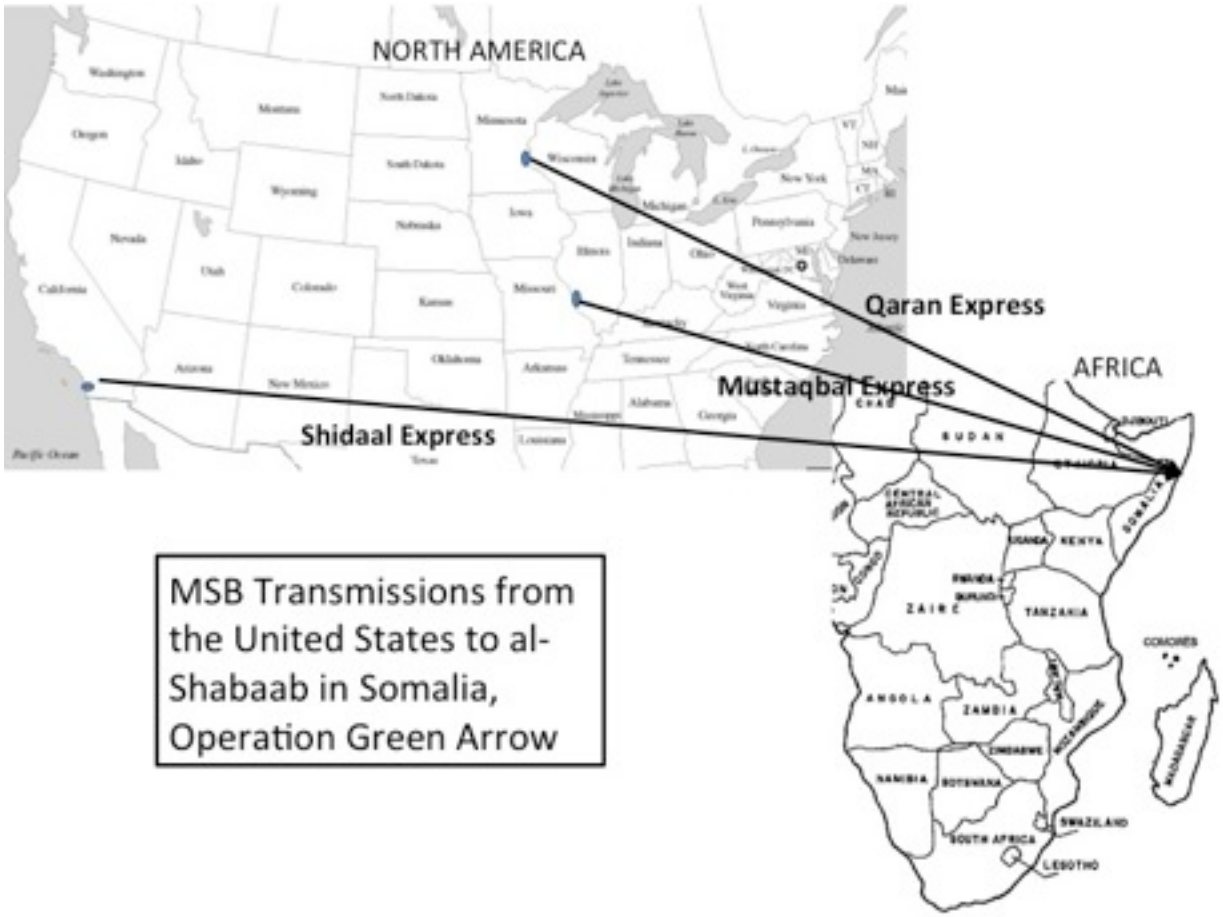
Hawala and other informal transfer systems are fast, with transactions happening usually within hours, perhaps up to a day or slightly more for transactions to the more remote regions.[28] They are also relatively anonymous. Hawaladars keep records, but these may often be done in their own shorthand, and their bookkeeping methods vary.[29] They may even be more reliable than other methods, like money service businesses, which serve similar communities.[30] They are also relatively inexpensive compared to other methods, charging just 1-2% for transfer fees and often offering a more competitive exchange rate –this is the primary reason why people use them. They are also convenient, operating in areas underserved by traditional banking. In Afghanistan, for example, Thompson notes that hawaladars operate in even the most remote areas of the country.[31] In the United States, informal transfer systems are required to register with FinCEN. In Afghanistan, there has been a similar effort to regulate the hawala network but both Afghanistan's geography and the weakness of its institutions have prevented much progress.[32]

Money Service Businesses: The Bank Secrecy Act (BSA) defines money service businesses (MSBs) as "currency dealers or exchangers; check cashers; issuers [or redeemers] of traveler's

checks, money orders, or stored value cards; and money transmitters."[33] In the United States alone there are over 33,000 registered MSB's.[34] Money service businesses are generally subject to the same regulations and laws as banks, and are subject to regulatory audits. However, unlike banks, MSBs do not follow similarly rigorous "know your customer" (KYC) procedures. Banks will only conduct transactions with people holding accounts at that bank, and those account holders must provide a significant amount of personal information when they open the account. MSBs, on the other hand, do not require that customers have existing accounts. Customers only need to present a valid form of ID. Most MSBs, and particularly the more established money transmitters such as Western Union, transfer funds quickly (within minutes to most locations), are minimally expensive for transfers larger than US $1,000, and offer low risks of detection, especially if the MSB is unregistered.

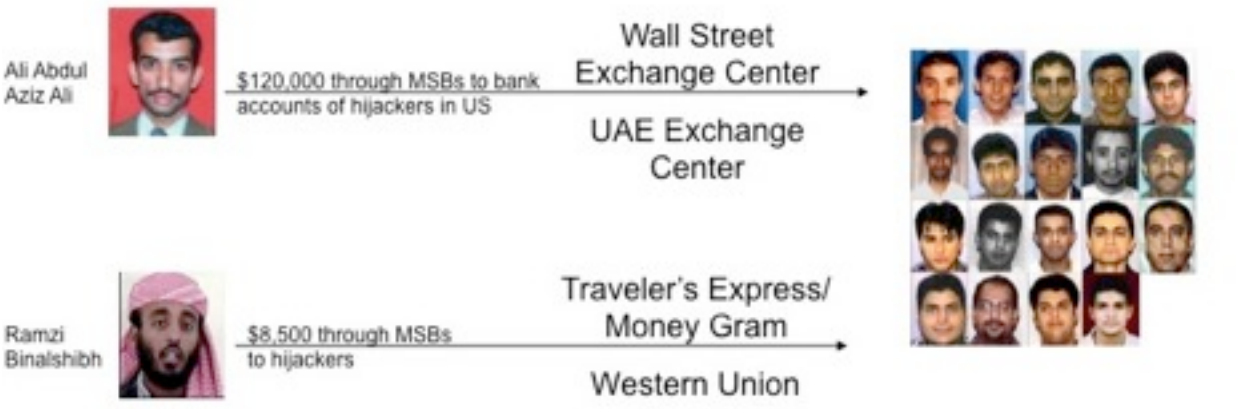
In February 2013, a federal jury in San Diego convicted four Somali immigrants of conspiring to fund al Shabaab, a militant terrorist group in Somalia.[35] While all four men were involved in raising funds, one of them, Issa Doreh, worked at the Shidaal Express, a registered MSB from which he sent funds directly to one of al-Shabaab's leaders, Aden Hashi Ayrow, who was in regular telephone contact with one of the other defendants. Months of wiretapped telephone conversations led to additional arrests in two related cases in St.Louis, Missouri and Minneapolis, Minnesota. Again, the goal was to raise funds for al-Shabaab and wire transfer those funds through registered MSB's, getting lost in the traffic of numerous legitimate remittances sent by the sizeable Somali immigrant communities in those cities. (See Figure 3)

Figure 3: Operation Green Arrow



Before al-Qaeda officially existed, Khalid Sheikh Mohammed, Ramzi Yousef, and Wali Khan Amin Shah used a large MSB in the UAE, Al Ansari Exchange Establishment (AAEE), to move funds for the Operation Bojinka plot in 1995.[36] Al-Qaeda also made extensive use of MSBs in their financing of the 9/11 attacks. An AQ financier, Ali Abdul Aziz Ali deposited almost US $120,000 at two MSBs in Dubai: the Wall Street Exchange Center and the UA Exchange Center. The money was transferred to the hijackers' U.S. bank accounts through the MSBs' correspondent accounts at the Royal Bank of Canada and Citibank, respectively. Even though the MSBs in Dubai required identification, Ali Abdul Aziz Ali used aliases. His transactions also appeared unremarkable among the millions of MSB transactions flowing out of that jurisdiction. A second financier, Binalshib, transferred about US $8,500 via two Traveler's Express/MoneyGram transactions and two Western Union transactions.[37] (See Figure 4)

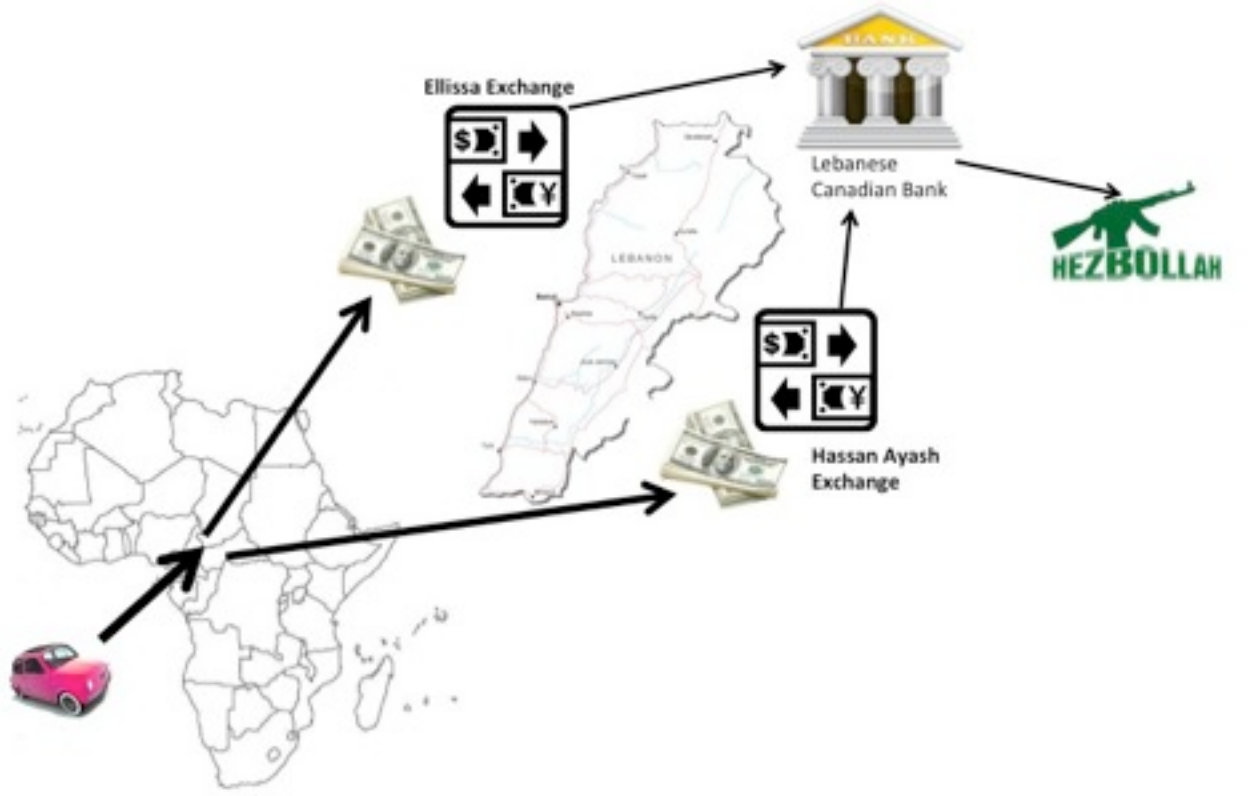
Figure 4: Money Service Business Transfers before 9/11 Attacks



Perhaps the terrorism financing case study that highlights the role of MSB's most glaringly is the complex Hezbollah financing case that entrapped and eventually undid Lebanese Canadian Bank in 2011. While the Lebanese Canadian Bank case has many layers (and more will be said about the case in the next section), one critical component of the money laundering operation allegedly run by Hezbollah involved the placement of cash into money service businesses located in Beirut. These MSB's had accounts with Lebanese Canadian Bank. The scheme originated in the Western Hemisphere with drug proceeds from Ayman Joumaa's drug trafficking network. Although Joumaa, himself, was not a member of Hezbollah, he had loose connections with the organization, and found in them a willing partner in crime.

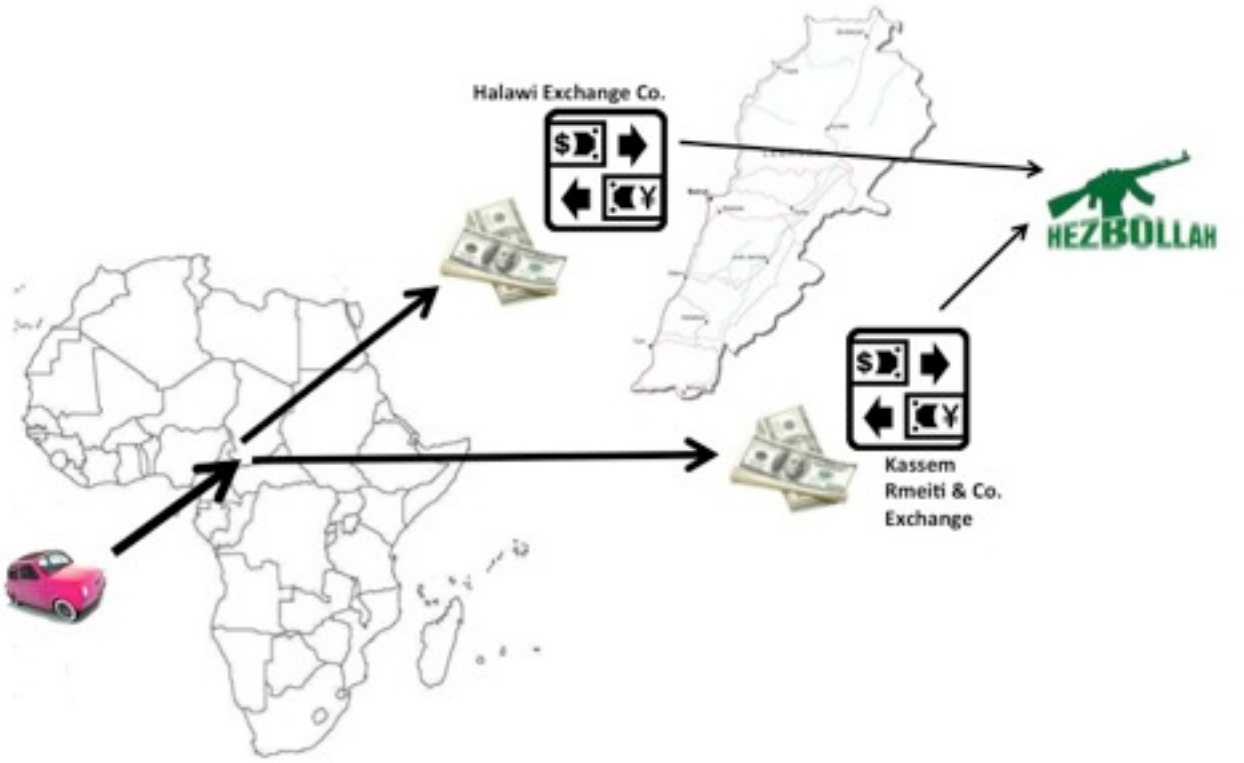
Joumaa's drug proceeds were laundered through a complicated scheme involving the purchase of used cars from Lebanese-owned dealerships in the United States.[38] The used cars were shipped to Africa where they were sold for cash. Additional drug cash was co-mingled with the proceeds of the car sales, and this cash was sent to at least two money service businesses in Beirut, including Elissa Exchange and the Hassan Ayash Exchange (See Figure 5). Both of these MSB's were allegedly complicit in the scheme, and allegedly earned commissions on their laundering services, which went straight into the coffers of Hezbollah. When the scandal was laid bare, both MSB's were shut down, and Joumaa's drug trafficking network was forced to find another channel through which to launder their funds.

Figure 5: Hezbollah Financing Scheme Pre-2011



According to a recent Treasury sanctions designation in April 2013, it did not take long for Joumaa to find a new channel for laundering his funds. Elissa Exchange and Hassan Ayash Exchange were soon replaced by two other Beirut-based, Hezbollah-linked money services businesses: Kassem Rmeiti & Co. for Exchange and the Hawali Exchange Co.[39] The designation by Treasury alleged that between March 2011 and October 2012 Rmeiti Exchange collected bulk cash, issued cashier's checks and facilitated cross border wire transfers for a variety of criminals, including "Hezbollah affiliates." (See Figure 6) Hawali Exchange was charged with similar, albeit more complex, transactions. Such designations essentially bring a financial institution's operations to a halt, as it becomes almost impossible to conduct U.S. dollar transactions. The designation decision set a new precedent, for it was the first time Treasury had used Section 311 of the Patriot Act against a money service business. Previous designations had been limited to formal banks.

Figure 6: Hezbollah Financing Scheme Post-2011



Up until this case and the successful efforts on the part of the U.S. Treasury Department to take down four well-known Lebanese money services businesses, MSB's had been considered an advantageous method for moving terrorist funds. They allow for the relatively inexpensive and speedy transmission of funds, their omnipresence is convenient, and even though their cash reporting threshold is low, it is still possible in theory to move a large volume of funds at any given time. But the risks have changed in recent years. Previously, MSB's flew under the radar and faced a lower risk of external audits or careful scrutiny by financial regulators. Renewed attention on their activities has put them in the spotlight, and many MSB's in North America are now finding it difficult to establish accounts with formal banks, who do not wish to take on the additional risks.

Formal Banking: The formal banking sector includes depository financial institutions (DFIs) – banks, saving and loans, and credit unions – which are the sole entities permitted "to engage in the business of receiving deposits and providing access to those deposits" through a payment system of checks, electronic networks, credit and debit cards, and bank-to-bank transfers.[40] The

formal banking sector is heavily regulated in the West, and increasingly so in most emerging market countries. In the U.S. laws like the Bank Secrecy Act (and its most recent amendments in Title III of the USAPATRIOT Act) require banks to maintain records, know their customers, report transactions over US $10,000 and report suspicious transactions of any amount. However, banks are still vulnerable to abuse by terrorists and other criminals.

Banks can be a vehicle for criminal financing in a variety of ways. The most convenient arrangement for a terrorist would be a bank that asks no questions, such as the former al-Madina Bank in Lebanon. Alternatively, the bank could have a crooked employee, who facilitates the laundering and movement of funds under the nose of unwitting supervisors, as happened with Lebanese Canadian Bank. And if a bank is not careful, it could also be used for criminal activity by way of correspondent accounts or payable-through-accounts of correspondent banks, as was the case with HSBC. And finally, there may be instances where a bank does all it is required to do with respect to customer due diligence, but the transactions still fail to set off any red flags, as happened with the 9/11 hijacker accounts.

Al-Madina Bank, and its subsidiary, United Credit Bank (UCB), represent a notorious case of deceitful corruption. When their crimes were uncovered in 2003, their unorthodox transactions caused the bank's collapse and the loss of depositors' funds. Purchased by two Lebanese-Saudi brothers in 1984, the bank soon fell under the *de facto* control of a woman named Rana Qoleilat, who started out as a mere executive assistant, but was soon given power of attorney to conduct transactions on behalf of the two owners. According to prosecutors' allegations, Ms. Qoleilat knowingly facilitated the laundering of funds by Saddam Hussein's sanctioned regime, conflict diamond dealers, Russian mafia groups, and an arms dealer for Hezbollah.[41] She is also alleged to have embezzled funds from the bank to enrich powerful Syrian generals and politicians during the Syrian occupation of Lebanon. However, because the bank was run like a Ponzi scheme, the entire operation eventually collapsed. Most depositors eventually recovered their funds, but the owners lost an estimated US $1.5 billion.[42]

The Lebanese Canadian Bank (LCB), mentioned earlier, was implicated in Hezbollah financing at a number of levels. The bank held accounts for money service businesses that were allegedly laundering and earning commissions for Hezbollah, but the bank was also held liable for allowing a handful of crooked senior bank managers to structure cash deposits right under the unwatchful eye of compliance staff.[43] These crooked employees received funds from Hezbollah couriers, who would bring the bulk cash directly from the airport, and deposit the funds at a nearby LCB branch.

Even when a bank carefully scrutinizes its employees, it can still be used for terrorism financing by way of contaminated correspondent accounts. Correspondent accounts are accounts set up to allow off-shore banks to conduct transactions in a key currency such as the U.S. dollar. For example, any foreign bank that wishes to conduct dollar transactions must first set up a

correspondent account with a U.S. bank to process those dollar transactions. Correspondent accounts are an unavoidable tool for conducting international transactions. The problem arises because the U.S.-based bank cannot guarantee that the foreign correspondent bank is carefully screening its own customers and its customers' activities. That is why correspondent relationships take time to establish. Most large international banks will not set up a correspondent relationship with an overseas bank without first conducting an on-site visit and evaluation of the other bank's risk compliance regime. Unfortunately, such due diligence and care was not undertaken by HSBC-US when it continued to maintain a correspondent account relationship with al-Rajhi Bank of Saudi Arabia, after several allegations of connections to terrorism financing. The first allegations arose in 2005 when two individuals were indicted for using al-Rajhi bank to send money to violent extremists in Chechnya. Additional concerns arose in 2007 when the contents of a 2003 CIA report were leaked. The report found that "senior al-Rajhi family members have long supported Islamic extremists and probably know that terrorists use their bank."[44] In spite of all of these red flags, HSBC-US continued to conduct correspondent account transactions with al-Rajhi Bank until they were investigated for many additional compliance failures.

In the execution of the 9/11 attacks, al-Qaeda used the formal banking sector as their primary method of moving and storing funds. All told, they deposited around US $300,000 in U.S. banks, and spent all but US $36,000 of that before the attacks. About US $130,000 of the funds the hijackers used came through bank-to-bank transfers (including through MSB correspondent accounts at banks) and the rest was deposited as cash. Once these funds arrived in the United States they were deposited in accounts at Union Bank of California and Sun Trust Bank in Florida, among others. All the hijackers opened accounts at these U.S. banks with their real identities. They accessed their funds with ATM and debit cards. An additional US $47,600 was deposited in overseas banks: US $9,600 in Saudi British Bank in Saudi Arabia, US $8,000 in a Citibank branch office in the UAE, and US $30,000 in a Standard Chartered Bank branch in the UAE. Two of the hijackers accessed these overseas accounts with ATM and Visa cards.[45] What is remarkable is that most of these transactions, because of their relatively small size and the lack of suspicion about the would-be hijackers, would not have set off any red flags even today.

Formal banking has several advantages and disadvantages for terrorist groups. In general, banks are largely regulated and therefore pose higher risks for terrorists of detection by investigators. Al-Qaeda, however, overcame some of these drawbacks by utilizing bank branches in the UAE and Pakistan, which at the time lacked much regulatory oversight, and by allowing mostly low-level (unknown to law enforcement) operatives to use banks for the 9/11 plot.[46] They are safe and convenient, but can be expensive (based on fees and exchange rates), and can be slow if the banks hold the money for a period of time before authorizing transfers.[47]

False Trade Invoicing: One of the most difficult laundering methods to detect is false trade invoicing, which is why it is estimated to be the one of the most heavily utilized methods by both

organized crime and terrorist groups for moving funds internationally.[48] False trade invoicing disguises the transmission of value from one jurisdiction to another. This can be done through over-invoicing or under-invoicing.[49] If a U.S.-based terrorist purchases some American honey, and then exports that honey to Yemen, he could overprice the shipment by US $100,000 without attracting much attention. When the Yemeni importer pays for the overpriced honey, some of that money will go towards paying off the U.S. honey producer. The additional US $100,000 goes right into the pocket of the fellow terrorist in the U.S., who arranged for the shipment. According to one government source, this is believed to have happened in the months leading up to 9/11.[50]

When investigators followed leads connected to the 9/11 hijackers they ran into a number of suspicious transactions related to the Middle East honey trade. Thanks to a tip-off from a confidential informant, agents rushed to Kennedy Airport to find two suspects stashing US $140,000 in cash inside a honey shipment bound for the Middle East.[51] Learning of the suspicious honey transactions, Professor John Zdanowicz at Florida International University took it upon himself to run through all of the Commerce Department data on honey imports and exports between the U.S. and al-Qaeda watch list countries in the months leading up to 9/11. What he found raised a number of eyebrows, particularly for honey exported to Yemen. Although Yemen is known for its honey trade, importing 600 metric tons per year and exporting its own special brand of honey from the ancient Sidr tree,[52] these transactions were nevertheless highly unusual, suggesting the surreptitious movement of funds from Yemen to the U.S. The investigation ultimately led to the listing of the Yemen-based Al Nur Honey Center, Al Nur Honey Press Shop and the Al-Shifa Honey Press for Industry and Commerce on OFAC's list of designated terrorism-related entities.[53]

Of all of the methods of moving terrorist funds, false trade invoicing offers many advantages for criminal organizations. While it is not simple and can be quite time consuming, it is incredibly convenient if the group already has front companies to conduct the transactions. Traditionally, the risk of detection has been quite low, but with the continued establishment of Trade Transparency Units (TTU's) around the world, this risk is rising. In addition to assisting with port security, Trade Transparency Units attempt to scour big data, searching for unusually priced transactions.[54] While this method is unlikely to catch falsely-invoiced shipments in real time, the paper trail related to the discovered transactions can be a starting point for money laundering and terrorism financing investigations.

High-value commodities: Valuable commodities like gold and diamonds offer yet another convenient method for transmitting value across borders. Gold is an especially reliable form of transportable payment during times of strife, or when fiat currencies are heavily devalued or not easily convertible. Gold can also be smelted into any shape and disguised for easy transport. Its weight, quality and price can be easily determined, and it is nearly impossible to trace its origin.[55] In addition to these advantages, gold is extremely important in Middle Eastern and South

Asian cultures. Bridal dowries are often presented in the form of high quality gold jewelry. The region is also home to the world's largest gold souks (markets), so the transport of gold by travelers is not likely to raise eyebrows. For these reasons, it should come as no surprise that gold has been offered as a reward incentive by both al Qaeda and the Taliban for would-be jihadists.[56] Other groups such as the militant right-wing Posse Comitatus in the U.S., and the Aum Shinrikyo cult in Japan, have been known to store and trade gold.[57]

Diamonds and their use by terrorists groups are more controversial, with researchers divided over the reliability and weight of the evidence. There is little doubt that Hezbollah has a hand in the diamond business, especially give the large Lebanese diaspora involved in the African diamond trade.[58] What is more controversial is the extent to which al Qaeda and its affiliates have used diamonds to store or move value. The first allegations arose not long after 9/11 when Douglas Farah, a *Washington Post* reporter at the time, declared a connection,[59] but there were many doubters. A brief FBI investigation soon after 9/11 turned up nothing, but more evidence began to surface in the following years, especially with the capture and questioning of Ahmed Ghailani in Pakistan in 2004. Ghailani, a senior al-Qaeda operative, confessed to buying conflict diamonds and spent a great deal of time traveling in and out of West African conflict zones between 1999 and 2002.[60] There were also a lot of questions raised about Aafia Siddiqui, an MIT-trained Pakistani microbiologist and al-Qaeda sympathizer, who was captured by U.S. forces and now sits in a Texas prison, sentenced to 86 years for trying to kill Americans. She is alleged to have traveled to Liberia to purchase conflict diamonds prior to 9/11.[61] Why would al-Qaeda resort to the diamond trade? After the 1998 East African embassy bombings the Clinton Administration froze more than US $220 million of assets belonging to the Taliban and al-Qaeda. The organization needed to convert its remaining assets into something transportable, which could not easily be traced or seized.[62]

Gold and diamonds clearly offer many obvious advantages for a terrorist. Diamonds are especially easy to transport and hide, and both are easy to convert into cash. But obtaining diamonds and gold from the source (such as African mines) is neither simple nor convenient. They need to be transported by hand, and that always carries the risk of seizure or theft. Where valuable commodities continue to play a major role is in settling hawala accounts, for both criminal and law abiding hawaladars.[63]

Other methods: The methods described above are the most common way terrorists move money. However, it is worth mentioning that there are other methods that criminals use, but, so far, have not been used extensively by terrorists groups. One relatively new, and widely discussed, method is the use of stored value cards (SVCs).[64] "Closed" cards are tied to a particular business, while "open" cards, like prepaid debit cards, can be used anywhere. These cards, especially the open ones, "provide a compact, easily transportable, and potentially anonymous way" to move funds.[65] While drug dealers and money launderers have used SVCs, terrorists

have not been known to use them in any meaningful way.[66] Likewise, casinos are often mentioned as a venue for criminal money laundering, but we have found no evidence that terrorists utilize them for moving funds. As another example, digital currencies, like Bitcoin, are increasingly being used by criminals, especially drug dealers, but we have seen little evidence that terrorists are using them.[67] A 2008 report lists several examples of criminals using new payment methods (NPMs), like digital currencies, stored-value cards, and mobile payments, but lists just a single example of terrorists selling phone cards to raise funds.[68]

Conclusion

To sum up, terrorist groups utilize multiple methods for moving funds, demonstrating how they are flexible and adaptive; when one method becomes riskier or costlier, they move to other methods. Terrorists also take advantage of legal and regulatory differences between states, finding the seams where they can work. This makes stopping terrorist financial flows a challenging problem.

To counter the movement of terrorist funds, there are reporting requirements for banks and non-bank financial institutions, as well as a loosely coordinated international regime consisting of organizations like the Egmont Group of Financial Intelligence Units which share financial intelligence, and FATF-style regional bodies that evaluate member states' compliance regimes. It is beyond the scope of this article to describe the full regime here, as others have done so more than adequately.[69] This regime has had a mixed record of success, despite insufficient international coordination, deficient capacity, and inadequate implementation in many countries. For example, al-Qaeda especially, but also Jemaah Islamiyah, al-Qaeda in Iraq, Hamas, and the Abu Sayyaf Group have been unable to maintain their levels of violence because of financial difficulties.[70] Additionally, financial data has been a key component in prosecuting terrorism cases, with FBI special agents often making use of SAR filings. This is because financial transactions leave "footprints" for law enforcement agencies to intercept and follow. And even when investigations do not begin with suspicious financial transactions, financial records can provide key evidence in piecing together the details of a case, as it did with the would-be Heathrow liquid explosive bombers in 2006.[71]

Despite these successes, there are also failures and challenges. For example, as the 9/11 Commission noted, the regulatory regime in place before 9/11 did not fail, rather it was "never designed to detect or disrupt the transactions of the type that financed 9/11."[72] The point here is that there is no way to create a perfect regulatory and enforcement regime that can stop all criminal transactions. Nor would we want such a heavy regime, because then it would also impose costs on the vast majority of legal, legitimate transactions that occur within the financial system.

To return to the attributes described earlier, there is little countries can or should do to affect many of them, because so many methods are used for legitimate purposes. We do not want to decrease the potential volume of funds that can be transferred with any method (with the exception of cash transactions); nor do we want to make methods costlier, slower, more complex, or less convenient.

Instead, the focus should be on making the risks of detection higher. Specifically, this means enhancing regulatory compliance at the ground level and improving international collaboration, cooperation, and capacity building, as well as prioritizing enforcement with non-compliant countries.[73] Making the transfer of funds riskier can be especially effective against the many terrorist groups who place a high value on the internal control of their operatives, even at the risk of operational security. For many groups, like al-Qaeda and its affiliates in Iraq and North Africa, they obsessively demand that their members keep detailed records of their financial transactions. Their choice of "control" over "security" provides an important vulnerability that states can exploit.[74]

About the Authors:

Michael Freeman *is an Associate Professor in the Department of Defense Analysis at the Naval Postgraduate School in Monterey. He received a Ph.D. from the University of Chicago in 2001 and is the author of Freedom or Security: The Consequences for Democracies Using Emergency Powers to Fight Terror (Praeger, 2003), the co-editor of Gangs and Guerrillas: Ideas from Counterterrorism and Counterinsurgency, the editor of* Financing Terrorism: Case Studies *(Ashgate 2012), as well as the author of several journal articles and book chapters on terrorism, emergency powers, and terrorist financing.*

Moyara Ruehsen *is an Associate Professor in the Graduate School of International Policy Management at the Monterey Institute of International Studies. She is a certified anti-money laundering specialist (CAMS), who has lived, studied and worked throughout the Middle East, most recently in Iraq, where she worked for the USAID-financed Financial Sector Development Program. In addition to writing and consulting on the topics of money laundering and terrorism financing, she also teaches courses on Money Laundering, Terrorism Financing, Illicit Drug Markets, and International Finance.*

The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

Notes

[1] William Glaberson, "Behind Scenes, Informer's Path Led U.S. to 20 Terror Cases," *New York Times* (18 November 2004).

[2] "Honey Exports May Have Financed Terrorism," *Money Laundering Alert* (November 2001).

[3] See Jeanne Giraldo and Harold Trinkunas, eds., *Terrorism Financing and State Responses*, Stanford University Press, 2007; Thomas Biersteker and Sue Eckert, eds., *Countering the Financing of Terrorism*, Routledge, 2008; Sean Costigan and David Gold, eds., *Terrornomics*, Ashgate, 2007; Michael Freeman, ed., *Financing Terrorism*, Ashgate, 2012; and Nimrod Raphaeli, "Financing Terrorism: Sources, Methods, and Channels," *Terrorism and Political Violence*, Vol. 15, No. 4 (Winter 2003).

[4] Samuel Maimbo, "The Money Exchange Dealers of Kabul: A Study of the *Hawala* System in Afghanistan," World Bank Publication, Working Paper No. 13, 2003 has a similar approach of looking at the operational characteristics of the Afghan hawala network. His characteristics are: scope, international, transactional volume, speed, cost, reliability, documentation, settlement, and potential for financial abuse.

[5] cf. Douglas Farah, *Blood From Stones*, Broadway Books, 2004.; and Moyara Ruehsen, "Diamonds are a terrorist's best friend," www.moneylaundering.com (2005).

[6] For details, see "Black Market Peso Exchange Update," FinCEN Advisory Issue 12 (June 1999). Online at: http://www.fincen.gov/news_room/rp/advisory/html/advis12.html.

[7] See Financial Action Task Force, "Trade Based Money Laundering," June 23, 2006. Online at: http://www.fincen.gov/news_room/rp/files/fatf_typologies.pdf.

[8] Nikos Passas, "Informal Value Transfer Systems, Terrorism and Money Laundering," a report to the *National Institute of Justice*, 2003, p. 30.

[9] "U.S. Money Laundering Threat Assessment," December 2005, p. 34 notes that US $1 million in US $20 bills weighs over 100 pounds and would make a stack 18 feet high.

[10] "U.S. Money Laundering Threat Assessment," p. 35.

[11] John Roth, Douglas Greenburg, and Serena Wille, "National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing," p. 26 and p. 134.

[12] Joseph Felter and Brian Fishman, "Becoming a Foreign Fighter: A *Second* Look at the Sinjar Records," in Brian Fishman, ed., *Bomber, Bank Accounts, & Bleedout*, Combating Terrorism Center at West Point, pp. 53-54.

[13] Jacob Shapiro, "Bureaucratic Terrorists: Al-Qaida in Iraq's Management and Finances," in Brian Fishman, ed., *Bomber, Bank Accounts, & Bleedout*, Combating Terrorism Center at West Point, p. 73.

[14] Zachary Abuza, "Funding Terrorism in Southeast Asia: The Financial Network of Al Qaeda and Jemaah Islamiyah," The National Bureau of Asian Research, Vol. 14, umber 5, December 2003, pp. 20-21.

[15] Abuza, "Funding Terrorism in Southeast Asia," p. 54.

[16] Passas, "Informal Value Transfer Systems, Terrorism and Money Laundering," is the most thorough analysis of Informal Value Transfer Systems (IVTS). We are really describing what he calls "informal funds transfer systems" (IFTS), which are the more traditional, informal systems. Passas lists many more examples of informal transfer systems on pp. 25-26.

[17] "Remittance corridors: New rivers of gold," Economist April 28, 2012, p. 77.

[18] Roth et al, "Monograph on Terrorist Financing," p. 25.

[19] Roth et al, "Monograph on Terrorist Financing," p. 25.

[20] Roth et al, "Monograph on Terrorist Financing," pp. 17, 25.

[21] Matteo Vaccani, "Alternative Remittance Systems and Terrorism Financing," *World Bank Working Paper*, No. 180, 2010, p. 7.

[22] Vaccani, "Alternative Remittance Systems," p. 7.

[23] Abuza, "Funding Terrorism in Southeast Asia," p. 54.

[24] Tehrik-e-Taliban is also known as the Pakistani Taliban.

[25] Evan Perez, "Case Shows Rise of Non-Bank Transfers to Fund Terror," *Wall Street Journal* (17 November 2010).

[26] Neither hawaladar was ever convicted of knowing anything about the Times Square bomb plot. Aftab Ali Khan was jailed for visa fraud and operating an unlicensed hawala and subsequently deported to Pakistan in May 2011. Mr. Younis was granted leniency for coming forward and cooperating with law enforcement. He avoided jail, paid a small fine and was also deported back to Pakistan.

[27] Bray, Chad, "Plea in Bomb-Link Case," *Wall Street Journal* (19 August 2011).

[28] Maimbo, "The Money Exchange Dealers of Kabul," p. 10.

[29]Edwina A. Thompson, *Trust is the Coin of the Realm: Lessons from the Money Men in Afghanistan*, Oxford University Press, 2011, p. 203.

[30] Passas, "Informal Value Transfer Systems, Terrorism and Money Laundering," p. 32; and Thompson, *Trust is the Coin of the Realm*.

[31] Thompson, *Trust is the Coin of the Realm*. See Chapter 6, which explains well how they are critical for facilitating all manner of aid transfers, family remittances and foreign trade transactions.

[32] Based on interviews with former U.S. Department of Treasury officials.

[33] "U.S. Money Laundering Threat Assessment," p. 7.

[34] Financial Crimes Enforcement Network website. www.fincen.gov (accessed May 2013)

[35] "San Diego Jury Convicts Four Somali Immigrants of Providing Support to Foreign Terrorists: Defendants Sent Money to al-Shabaab in Somalia," Office of the United States Attorney, Southern District of California (22 February 2013).

[36] Abuza, "Funding Terrorism in Southeast Asia," p. 41.

[37] All figures taken from Roth et al, "Monograph on Terrorist Financing," Appendix A.

[38] *USA v. Saade, Maroun, et al.,* "Indictment," accessed March 3, 2013, http://www.investigativeproject.org/documents/case_docs/1483.pdf; Ginger Thompson, "Lebanese Bank Is Accused of Money Laundering," New York Times (10 February, 2011). Online at: http://www.nytimes.com/2011/02/11/world/middleeast/11hezbollah.html; and Jo Becker, "Beirut Bank Seen as a Hub of Hezbollah's Financing," *New York Times* (13 December 2011). Online at: http://www.nytimes.com/2011/12/14/world/middleeast/beirut-bank-seen-as-a-hub-of-hezbollahs-financing.html.

[39] "Treasury Identifies Kassem Rmeiti & Co. for Exchange and Halawi Exchange Co. as Financial Institutions of "Primary Money Laundering Concern," Press Release, U.S. Department of the Treasury, 23 April 2013.

[40] "U.S. Money Laundering Threat Assessment," p. 1.

[41] Mitchell Prothero, "Beirut Bombshell," *Fortune* (4 May 2006).

[42] Gary C. Gambill and Ziad K. Abdelnour, "The Al-Madina Bank Scandal," *Middle East Intelligence Bulletin* (January 2004).

[43] Jo Becker, "Beirut Bank Seen as a Hub of Hezbollah's Financing," *New York Times* (13 December 2011).

[44] Quoted in U.S. Senate Report, "U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History," 17 July 2012, Permanent Subcommittee on Investigations, p.189.

[45] Roth et al, "Monograph on Terrorist Financing," Appendix A.

[46] Roth et al, "Monograph on Terrorist Financing," pp. 25-26.

[47] Roth et al, "Monograph on Terrorist Financing," p. 67.

[48] Moyara Ruehsen, "Foreign Trade Detected as Refuge for Launderers Dodging Tougher Laws," *Money Laundering Alert* (May 2001).

[49] John Zdanowicz, "Trade-Based Money Laundering and Terrorist Financing," *Review of Law and Economics*, Vol.5, no.2 (December 2009).

[50] "Honey Exports May Have Financed Terrorism," *Money Laundering Alert* (November 2001).

[51] William Glaberson, "Behind Scenes, Informer's Path Led U.S. to 20 Terror Cases," *New York Times* (18 November 2004).

[52] "The World Market for Honey," USAID, CIAFS (September 2012).

[53] "Honey Exports May Have Financed Terrorism," *Money Laundering Alert* (November 2001).

[54] For a good explanation of TTU's, see http://www.ice.gov/trade-transparency/

[55] John Cassara and Avi Jorisch, *On the Trail of Terror Finance: What Law Enforcement and Intelligence Officers Need to Know*, Washington, DC: Red Cell Intelligence Group, 2010, chapter 6 "Gold and Diamonds."

[56] Cassara and Jorisch, *On the Trail of Terror Finance*, p. 97.

[57] Cassara and Jorisch, *On the Trail of Terror Finance*, p. 97.

[58] Moyara Ruehsen, "Diamonds are a terrorist's best friend," www.moneylaundering.com (2005).

[59] Douglas Farah, *Blood From Stones*, Broadway Books, 2004.

[60] NPR Interview with Bryan Bender of the *Boston Globe* (5 August 2004); Moyara Ruehsen, "Diamonds are a terrorist's best friend," www.moneylaundering.com (2005).

[61] Farah, *Blood From Stones.*

[62] Moyara Ruehsen, "Diamonds are a terrorist's best friend," www.moneylaundering.com (2005).

[63] Lisa C. Carroll "Alternative remittance systems distinguishing sub-system in Interpol member countries on the Asian continent" http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/EthnicMoney/default.asp; Cassara and Jorisch, *On The Trail of Terror Finance*, pp. 100-101.

[64] "U.S. Money Laundering Threat Assessment," includes SVCs as a MSB.

[65] "U.S. Money Laundering Threat Assessment," p. 20.

[66] "U.S. Money Laundering Threat Assessment," p. 20. The FATF report, "Money Laundering Using New Payment Methods," 2010, describes 33 cases, only one of which involves "possible" prepaid cards used by individuals involved in the 2008 Mumbai attack, p. 37. Likewise, Juan Miguel del Cid Gomez, "A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates," *Perspectives on Terrorism*, Vol. 4 No. 4, pp. 19-20 discusses "New Payment Methods" but does not offer any examples of terrorists using them.

[67] *Economist*, "Digital Currencies: A New Specie" April 13, 2013; Kara Scannell, "Cyber Crime: Without a Trace," *Financial Times* (1 June 2013).

[68] Jennifer Hesterman, "How Terrorists and Criminals Exploit E-Commerce to Store and Move Money" *The Counter Terrorist* September/ October 2008, p. 38.

[69] Roth et al, "Monograph on Terrorist Financing," chapter 4; Martin Weiss, "Terrorist Financing: U.S. Agency Efforts and Inter-Agency Coordination," CRS Report for Congress, August 2005; Matthew Levitt and Michael Jacobson, "The Money Trail: Finding, Following, and Freezing Terrorist Finances," The Washington Institute for Near East Policy, Policy Focus #89, November 2008, chapter 4, as well as numerous chapters in Giraldo and Trinkunas, *Terrorism Financing and State Responses* and Biersteker and Eckert, *Countering the Financing of Terrorism*.

[70] Levitt and Jacobson, "The Money Trail," pp. 40-41.

[71] Conference notes, International Anti-Money Laundering Conference, 21-23 March, 2011, Hollywood, Florida.

[72] Roth et al, "Monograph on Terrorist Financing," p. 131.

[73] Levitt and Jacobson, "The Money Trail," pp. 43-43 have a well-thought out list of recommendations on this topic.

[74] Shapiro, "Bureaucratic Terrorists" for examples of AQI. See also Rukmini Callimachi, "Idiosyncratic Terrorist Breaks Out on His Own in Sahara Bloodbath," Talking Points Memo, May 28, 2013, http://talkingpointsmemo.com/news/idiosyncratic-terrorist-breaks-out-on-his-own-in-sahara-bloodbath.php, for the AQIM example.