The US Army War College Quarterly: Parameters

Volume 41
Number 1 *Parameters Spring 2011*

Article 13

3-1-2011

Tackling Threat Finance: A Labor for Hercules or Sisyphus?

Keving D. Stringer

Recommended Citation
Keving D. Stringer, "Tackling Threat Finance: A Labor for Hercules or Sisyphus?," *Parameters* 41, no. 1 (2011), doi:10.55540/0031-1723.2575.

Tackling Threat Finance: A Labor for Hercules or Sisyphus?

Kevin D. Stringer

In Greek mythology, the Gods gave the hero Hercules twelve, tremendously difficult labors, which he accomplished through clever strategy, tactics, guile, and divine support.[1] In contrast, they condemned Sisyphus, a Greek king, to an eternity at hard and frustrating labor. His assignment was to roll a great boulder to the top of a hill. Only every time Sisyphus, by the greatest of exertion and toil, attained the summit, the stone rolled back down again. Depending on the interagency strategy and policy approach chosen to address threat finance, the US government's resolution of it could produce either a Herculean or Sisyphean outcome.

While considered less critical than kinetic operations and therefore somewhat neglected, threat finance is an important subject in the US national security field with both domestic and international implications. Conceptually, the global financial network is a domain similar to its air, land, maritime, and cyber counterparts, requiring similar strategic and interagency approaches. Threat financiers exploit this sphere to the overall detriment of US national security interests. Hence a host of terrorism theorists, military operators, and intelligence officials all posit that the financing of terrorists and cartel groups is so pivotal to sustaining their operations, that their money systems have to become key targets in counter operations.[2] In reality, this aspiration proves exceedingly difficult to execute.

This article will explore threat finance by defining it, and then differentiating between its two subcomponents of terrorist financing and cartel money laundering. While acknowledging both the similarities and differences between these subelements of threat finance, this article will then detail the challenges of monitoring the financial networks supporting these illicit global flows, and show the difficulties in combating these criminal money transfers. After highlighting the progress to date, the article will then move beyond the foundational discussion to provide concrete interagency proposals and policy

Kevin D. Stringer is a 1987 graduate of the US Military Academy at West Point. He holds an M.A. in international relations from Boston University and a Ph.D. in international relations from the University of Zurich. A US Army Reserve Major, he is the designated Chair, Walker School of Business and Technology, Webster University Geneva, and is a Fellow at the Center for Advanced Defense Studies.

recommendations for further addressing the growing financial nexus between terrorist movements and criminal enterprises.

Threat Finance, Terrorist Financing, and Cartel Money Laundering

Threat finance is an umbrella term used to encompass various types of financing that support activities harmful to US national security. Within the US government and the Department of Defense, no singular, accepted definition of threat financing exists, and often the variance in definition reflects the particular nature of an organization; predominantly military or law enforcement, or an area of focus—strategic, theater strategic, or operational.[3] One reason for the lack of a clear and comprehensive definition may be the complexity of the topic, combined with the diversity of government actors involved. While the term *terrorist finance* is commonly used in international security literature to mean *threat finance*, it is too narrow, focusing only on organizations, cells, and individuals linked to terrorism. Other sources see threat finance as a much broader-based concept that includes:

- Proliferation and Weapons of Mass Destruction/Effects (WMD/E) funding.
- Terrorist financing.
- Narcotics trafficking.
- Organized crime.
- Human trafficking.[4]

The article supports this broader view which lends more utility when dealing with the highly adaptive, secretive, and flexible financing regimes and networks that straddle the criminal and terrorist worlds.[5]

This article defines threat finance through its two major subcomponents of terrorist financing (which subsumes WMD/E) and cartel money laundering (which includes organized crime, narcotics, fraud, corruption, and human trafficking). Terrorist financing is simply the process of raising, storing, and moving funds, obtained through illegal or legal means, for the purpose of terrorist acts or sustaining the logistical structure of a terrorist organization.[6] Cartel money laundering is the process designed to conceal the origin of money resulting from criminal activities.[7] For both, the degree of sophistication and complexity of illicit financing schemes is virtually infinite and is limited only by the creative imagination and expertise of the criminals or terrorists involved.[8]

The Differences

Yet while terrorist financing and cartel money laundering may share some characteristics since they are global in scope, transnational in operation, engage in jurisdictional arbitrage, and exploit the gray areas where state power is weak, there are some significant differences between the two.[9] Terrorism is unlike global crime in several critical ways: the direction of the related financial transactions; the tolerance for failure; the motivations of the participants; and the scale of the activity to be suppressed.[10] Terrorist financing generally involves financial flows that originate in legitimate activities to support illegitimate

activities rather than the reverse, introducing a significant complication for authorities following the money.[11] Terrorists take money and simply use it for attacks and their preparations.[12] Traditional money laundering involves a profit motive while terrorist financing often has no economic motive. Its objectives are usually political or ideological.

This differentiation, the noneconomic motives and funding from legitimate activities like charities, could be seen as a gap to more forcefully exploit against terrorist finance by focusing on psychological operations and public diplomacy instead of traditional anti-money-laundering procedures.

Variances also exist between the two types of threat finance. In their exercise of violence, transnational criminals act clandestinely by nature and seek to avoid exposure, while terrorists prefer to gain exposure through spectacular acts.[13] Conversely, unlike ordinary criminals, terrorists tend to avoid living conspicuous lifestyles that would alert authorities to the presence of extra income.[14] A final distinction between the two activities is in their scale: traditional money launderers deal with large cash flows while terrorists deal with a substantially smaller amount of money. For example, the International Monetary Fund puts the total amount of criminal money laundered globally each year at around $600 billion. In contrast, while the amount of money flowing to terrorist organizations overall is unknown, those whose finances have been documented appear to require much less money than previously estimated. The Provisional Irish Republican Army (PIRA) operated on a budget of some £1.5 million per year. The Real IRA and the Ulster Defence Association required only £500,000.[15] This smaller scale of demand makes detecting terrorist financing a more difficult task, leading to assertions from skeptics that tracking money is a marginal strategy in countering terrorism.[16]

Even this exercise in differentiation between the two activities has its critics. One expert is convinced there is little or no essential difference between these categories of behavior or instruments, and that the distinction derives instead from the labels attached to various groups. Terrorist groups, organized criminal cartels, and insurgent organizations often engage in a range of licit and illicit activities to fund operations and purchase influence. While their ambitions may vary, this is a product of strategic choice rather than essential organizational or instrumental difference.[17]

Regardless of how the activities are categorized, a nexus exists between the two categories. Already in 2001, Osama Bin Laden was channeling profits from the sale of narcotics arriving in Western Europe via the Balkan route to local governments and political parties, with the goal of gaining influence in Albania or Macedonia. This transfer of funds may have been accomplished through the Albanian criminal groups who dominate the narcotics and human trafficking trades in the region.[18] Such terrorist-cartel cooperation has only increased in the intervening years, and the two are often interwoven in new and dangerous manners that threaten the welfare and security of the United States.[19]

The Nature of the Threat and its Challenges

Given the complexity of threat finance, the challenge of mounting an interagency attack on it is daunting. Preventing illicit financial flows seems an almost impossible task. The problem has a number of facets, but the main points are threefold. First, the enemy can readily adapt within the global financial realm, which is both virtual and physical, to avoid law enforcement and regulatory scrutiny. Terrorists and criminals use a wide, imaginative, and evolving series of tactics, techniques, and procedures to transfer money throughout their networks, from high-tech means to low-tech or no-tech means.[20] The money may come from enterprises ranging from legitimate businesses (e.g., taxi companies and donations to charitable organizations) to illegitimate activities like smuggling, intellectual property theft, and drug trafficking.[21] Transfer methods can include physical couriers, invoice manipulation, trade-facilitated hidden transactions, and the use of correspondent banking accounts and sophisticated transactions between financial institutions on- and off-shore.[22] Transfers can be physically carried across international borders, and transformed into high-value and often hard-to-detect commodities such as precious stones.[23] Other common techniques are for front companies to overvalue or undervalue merchandise or fabricate shipments altogether.[24]

Second, the organizations can hire financial, banking, legal, and tax experts with abilities that exceed those of US government personnel, and deploy them without regard to bureaucratic or national boundaries. In contrast, US government organizations are hamstrung by a lack of unity of command, bureaucratic structures that inhibit collaboration, budget constraints, and political and legal limitations. Also, the knowledge and skills required to understand these financial networks are often found only in the private sector.[25]

Third, the volume of money transferred globally is huge and difficult to monitor. One of the effects of globalization is the rapid movement of money. The consequence is that cartel and terrorist financial flows are often intermixed with legal foreign investment, immigrant remittances, credit card transactions, and e-commerce.[26] For example, in the legal money system, more than $2 trillion is transferred worldwide by wire in 700,000 daily transactions; it is estimated that .05 to .1 percent of those transactions are laundered monies, amounting to an estimated $300 million per day.[27] From a currency perspective, the main US dollar international payment system processes more than $1.5 trillion a day;[28] a similar ratio would mean that approximately $224 million per day of illicit cash flows in US dollars alone. On the terrorist side, The National Commission on Terrorist Attacks Upon the United States (The 9/11 Commission) estimated that the 1998 East African embassy attacks required funding of only $10,000. The 2002 Bali bombings cost al Qaeda approximately $20,000. Despite the devastation caused by the 9/11 attacks, the total amount spent on the actual operation was estimated at between $400,000 and $500,000.[29] Monitoring and tracking such vast amounts of money in real-time in an effort to find specific, and sometimes small, amounts is extremely difficult, especially when one considers the aforementioned currency volume does not include the informal money transfer

conduits. In fact, the techniques created primarily for countering conventional money laundering are not as useful for the more difficult-to-trace informal methods like *hawalas* (an informal value transfer system used by a huge network of money brokers) and trade-based money laundering.[30]

These systems make the challenge associated with detection even greater since threat organizations increasingly turn to cash couriers and bulk cash smuggling to transfer funds.[31] Informal transfer services such as *hawala*, diversions of charitable contributions, trans-border cash transfers through the postal service or FedEx, trade-based smuggling, and falsified trade documentation are popular techniques for the transfer of funds.[32] According to the 2009 National Drug Intelligence Center (NDIC) assessment, Mexican and Colombian cartels alone launder between $18 and $39 billion every year.[33] The 2010 assessment is even more damning, noting that tens of billions of dollars are laundered each year by drug traffickers operating in the United States. There are no current estimates for the amount of money laundered domestically or smuggled out of the United States by drug trafficking organizations (DTOs) annually.[34] A 2007 NDIC study showed that from 2003 through 2004, at least $17.2 billion was smuggled into Mexico in bulk cash shipments.[35] Additionally, drug proceeds (perhaps totaling several billion dollars) are laundered each year through various techniques such as the use of the Black Market Peso Exchange (BMPE), money transmissions, front companies, real estate transactions, and structured deposits in traditional institutions. Because the predominant techniques used by DTOs to launder illicit drug proceeds have proven successful, DTOs continue to rely on these methods.[36]

To address threat finance, the US government needs to pursue a multipronged approach to disrupt these illicit methods of transfer given the fungible nature of money and the number of permutations that permit the discrete transfer of money and assets. This "money war" is mainly fought by intelligence, diplomatic, and law enforcement organizations. Key components of this war are the capabilities of America's financial intelligence organizations. Renewed emphasis on this capability is in keeping with the recommendation of the *9/11 Commission Report* to engage in "vigorous efforts to track terrorist [or cartel] financing." Stuart Levey, Undersecretary for Terrorism and Financial Intelligence at Treasury, emphasized that "counterterrorism officials place a heavy premium on financial intelligence" in part because "money trails don't lie."[37] The challenge is that while the terrorist money, when found, provides objective evidence and leads, the actual conduits for transmitting it are purposely shrouded and misleading in an effort to avoid detection. This is especially true for the cartels and their financing.

One solution might be to develop a profile of legitimate for-profit and not-for-profit enterprises likely to engage in terrorist activity; however, it is difficult, if not impossible, to discern patterns in financial transactions that signify terrorist activity. Indeed, New York Clearinghouse, an organization of the largest money-center banks, concluded after a post-9/11 two-year study that it simply cannot be done.[38] Despite repeated efforts to develop typologies

appropriate to terrorist finance, the Financial Action Task Force (FATF) reached a similar conclusion.[39] The profiles developed tend to rely on ethnicity and nationality, raising a multitude of problems that range from inaccuracy and counter-productivity to the infringement of individual rights.[40]

While the purpose of money-laundering investigations is to prosecute perpetrators and obtain the funds, terrorist financing investigations also need to accomplish other important goals, such as interrupting the flow of money and preventing successful operations, whether or not the investigation concludes in a prosecution. Interrupting the flow of money through the regulated sector either by "freezing" it or by introducing sweeping legislation can do great harm to important national security objectives of the state: law enforcement not only loses a conviction, but authorities may be unable to trace the funds as extensively as required to interrupt operations or to establish links to terrorist networks.[41]

Results to Date and Proposals

Despite a plethora of law enforcement, diplomatic, economic, and military measures, the efforts to stem threat finance in the United States have been spectacularly unsuccessful in making any significant inroads against terrorist or cartel operations.[42] Focusing on the terrorist side, the initial objective was "concentrating intelligence resources on gathering financial information related to terrorism . . . identifying and blocking assets of terrorists as well as those who support terrorist organizations and . . . deploying diplomatic resources to ensure international cooperation against terrorist financiers and networks abroad."[43] This shotgun approach was effective in the immediate aftermath of 9/11, enabling the United States and international law enforcement agencies to freeze and seize various funds, but that initial success is now providing diminishing returns.[44] The initial achievements as of November 2002, were 251 individual organizations designated under Executive Order 13224 as financial supporters of terrorism, and the freezing of terrorist assets in over 165 countries, including more than $112 million in terrorist assets contained in some 500 accounts.[45] More than $34 million of the assets were frozen in the United States.[46]

Despite this limited success, only a year following the 9/11 attacks, the United Nations released a report stating that al Qaeda financial sources remained intact, with between $30 million and $300 million available through links to legitimate business enterprises.[47] Various international intelligence and law enforcement agencies have reached similar conclusions.[48] In the face of such evidence, even the US administration backpedaled: Alan Larson, the Undersecretary of State for Economic Affairs, confirmed in October 2002 that it was "unquestionably true" that al Qaeda still had the financial means to carry out devastating attacks against the United States. He continued, "I don't think lack of resources is a major impediment to the operations of terrorist organizations at this stage."[49]

One of the major challenges is that both formal and informal accounting measures in the antiterrorist finance realm rely on traditional money-laundering

metrics to gauge success. In the United States, for instance, annual money laundering reports examine the number of states with blocking orders in force, the number of entities with seized assets, and the value of money frozen as indications of success. While such exercises may prove helpful for public relations purposes, the standards they set for those agencies attempting to interrupt the financial flow of illicit funds are out of synch with the true indicators of success. Because metrics play such a key role in determining what agencies focus on, the use of incorrect standards may influence the effectiveness of counterterrorist efforts. More reliable indicators include the conviction rate of those responsible for supplying money, or the level of responsibility within the terrorist or cartel network of those apprehended.[50]

Metaphorically, the approach is that of a systematic and structured fishing expedition, where the lake represents the global financial transactional world, and the fish are the criminals and terrorists swimming in this body of water. The fishermen represent the multiple agencies of the United States and its allied governments. The fishermen have to place a number of nets and poles at different locations and depths to disrupt the fish and ultimately catch them. Given the environment, not all fishing instruments will result in a catch, but the goal is to deny the fish freedom of movement and "to detect, collect and process information on, and to target, disrupt or destroy financial systems and networks, which support activities that threaten US interests."[51] Given the aforementioned results to date, the following section offers prescriptive proposals, some which may be familiar, but deserve rethinking from a different perspective. Success in reaching the goal of threat finance disruption requires evaluating several Herculean policy options that encompass four specific dimensions: unifying command; influencing donors that supply money to organizations in support of terror groups; taking specific actions against priority financial centers; and boosting cooperation in the banking sector in an effort to analyze its domain knowledge.

Unity of Command

Unity of command for interagency efforts seems to be a weakness for most of the complex security issues confronting the United States—stability and reconstruction operations, counterinsurgency, and counterproliferation.[52] Threat finance is no different. The organizational landscape is occupied by a number of hardworking agencies, each in its own lane, coming together in various task forces, operations, and working groups. One example is Operation Green Quest, led by the Customs Service. It includes the Internal Revenue Service, the Secret Service, the Federal Bureau of Investigation, the Financial Crimes Enforcement Network, and the Bureau of Alcohol, Tobacco and Firearms.[53] Another example is the FBI's Interagency Terrorism Financial Review Group, consisting of the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the Drug Enforcement Administration, and most of the agencies in Operation Green Quest.[54]

The current system is predicated on these various agencies putting aside legitimate differences with respect to focus, priorities, resources, and mission requirements, and working together in a collegial manner to accomplish what is often a poorly orchestrated and resourced effort. While the current system has merit and historical precedent, it has a tendency to rely heavily on force of personality and informal relationships between the various organizations rather than on any mandated structural mechanism to achieve its objective. The disruption of terrorist finances needs to be addressed within the overarching context of threat finance, and threat finance has to be integrated and resourced as part of a holistic approach in any operations against terrorists and cartels.[55] One solution would be to give an existing organization like the National Security Council or the Treasury Department the full mandate and funding authority to coordinate and direct threat finance actions for all US Government agencies (without stifling their flexibility or resources) against terrorists and cartels.[56] This directive can only come from the President.

Organizationally, such an initiative would imply the designation of a fully empowered threat finance czar and the selection of a cadre of interagency professionals capable of executing policy and operations. The goal would be to achieve a seamless effort—from collection of intelligence or evidence on the battlefields of Afghanistan and in the drug labs of California, to the application of counterthreat policy at embassies worldwide. The ultimate impact of this unification of command is hard to forecast, but it would bring together disparate strands in a complex effort under one commander. This approach aligns with how the military addresses major challenges in complex environments. The key hypothesis to test is does complete unity of effort have a discernible impact on financial interdiction or does the current organizational friction mask underlying flaws in the instruments or strategies employed?

Diplomacy and Psychological Operations

In some respects, terrorist organizations are similar to nonprofit organizations. Not only do they need to earn, store, and transmit sums of money, but they also need charitable sponsors and donors. This generic need is true for terrorist organizations worldwide. The Irish Republican Army (IRA), for example, and its various offshoots, profited from charitable contributions originating in North America. By far the most publicized and well known sources for such funding came from the United States. The Irish Northern Aid Committee (Noraid), founded in 1969 by Irish civil war veterans, provided important ideological and financial support to the Provisional IRA which Noraid claimed was humanitarian aid for people in Northern Ireland.[57] In combating Islamic terrorism, there is an additional religious component to take into account when confronting threat finance, and that is the concept of *zakat*. In Islam, one of the five pillars of religion next to *salat* (prayer) is *zakat* (alms). *Zakat* is the name of what a believer returns out of his or her wealth to the neediest of Muslims for the sake of the Almighty Allah. The obligatory

nature of *zakat* is firmly established in the Koran, the *Sunnah* (or *hadith*), and is supported by a consensus of Muslim scholars.

This makes *zakat* an integral part of religious life for all Muslims, but the potential for its misuse is great. For example, by mixing religious beliefs and interpretations of the Koran for financial purposes, without adequate regulations and controls, Saudi Arabia became an avenue for terrorism financing based on the tradition of *zakat*. By abusing this pillar of Islam and taking advantage of the Saudi regulatory vacuum, al Qaeda was able to receive between $300 million and $500 million over the last ten years, a sum representing about 20 percent of the Saudi Gross National Product (GNP). Many of these donations were from wealthy businessmen and bankers, through a web of charities and companies that acted as legitimate fronts. Most of this financial infrastructure is still in place and capable of supporting fundamentalist organizations.[58] By using the concept of *zakat,* Muslim charities in other countries have successfully served as conduits for terrorist financing.

If government agencies are going to successfully counter this phenomenon, the key goal should be to influence the "finance" battlefield before monies are actually placed in the system. Once money is in the network, it becomes almost impossible to track and stop. To be successful, the United States should launch a focused interagency information, public diplomacy, and military psychological campaign directed at the sources of *zakat* in an effort to influence giving behavior and direct it to more legitimate humanitarian and charitable organizations. The key message would be how al Qaeda and related organizations actually misuse *zakat* to kill Muslims and destabilize Islamic societies on a global scale. This type of communication would be a strategic message from the highest levels of civilian and military organizations, with execution of such a policy coming from a joint effort of the Departments of State and Defense, operating under the auspices of the aforementioned unified command.

A related approach would be for the United States to work with regional partners in the Islamic world to create a system and standard for certifying and auditing Islamic charities and humanitarian organizations that are known to direct their resources to nonterrorist affiliated activities. This certification could take place under the auspices of key regional allies like Jordan or moderate Islamic religious organizations like those of the Aga Khan. Successful charity certification would notify *zakat* givers that their gifts were going directly into the hands of the truly needy. Such an undertaking would also be part of a US effort to combat Islamic extremism by supporting "Islamic renewal"—a diffuse but growing social, political, and intellectual movement whose goal is profound reform of Muslim societies and politics.[59] Such a campaign would need to be embedded in an interagency public diplomacy and psychological operations framework capable of steering *zakat* contributors to the precertified charities. Again, the measurement of success would be challenging, especially since the United States government does not currently have a means of knowing the total value of monies flowing to al Qaeda or its affiliates. Removing the money from the Western regulated sector is not going to help matters. A greater effort

needs to be expended on putting resources, first, into finding out how much money there actually is and, second, into discovering how it is moved. These actions would give the state a much better indicator of the level of funding it is intercepting. This means putting more funding into alternative areas, such as signals and human intelligence, to aid in strengthening the financial picture.[60]

Focus on Priority Financial Centers

The Financial Action Task Force (FATF), a Paris-based, multilateral organization, has played a critical role in attempting to regulate global financial centers with regard to threat finance. The FATF's Forty Recommendations on Money Laundering and Nine Special Recommendations on Terrorist Financing are widely acknowledged as the international standard for an anti-money laundering (AML) and anti-terrorist financing framework.[61] Even though these recommendations are not manifested in a binding legal commitment for the international community, a majority of the countries in the world have made a political commitment to their implementation. The Forty Recommendations cover criminal law, state regulations, and interstate cooperation. The cornerstone of the FATF strategy is the know- your-customer (KYC) approach. This includes eliminating anonymous accounts, identifying all customers, maintaining records of transactions for at least five years, making all records available to legal authorities upon request, and notifying appropriate authorities if unusual or suspicious transactions have transpired.[62] The main challenge for the FATF is to get the recommendations robustly enforced in relevant financial centers.

The criticality of overseas financial centers to threat finance harkens back to a 1980s presumed link between criminal finance and the appeal of zero-tax jurisdictions, with the associated regulatory laxity and a premium on offering discretionary services.[63] Today, a more accurate assessment is that most financial centers are used to some degree for money laundering. As a recent US Department of State report noted:

> The current ability of threat financiers to penetrate virtually any financial system makes every jurisdiction a potential money laundering center. There is no precise measure of vulnerability for any financial system, and not every vulnerable financial system will be host to large volumes of laundered proceeds.[64]

Concerned that offshore banking, subject to minimal supervision, provided potential terrorists and criminals with too much anonymity (making it difficult to trace the proceeds of crime), Congress amended the Bank Secrecy Act and gave the Secretary of the Treasury discretionary authority to place restrictions on foreign jurisdictions, institutions, and accounts if they posed a "primary money laundering concern" to the United States.[65] (No terrorist link was required.) Treasury could require financial institutions to maintain additional records for certain transactions, to identify foreign owners of accounts located at US financial institutions, and to identify customers opening foreign accounts at various banks within the United States. (Treasury has only used these powers twice since 9/11: both in support of the US FATF Non-Cooperative

Countries and Territories process for Ukraine and Nauru—neither instance was tied directly to terrorism.)[66]

But as one researcher remarked, "The most egregious examples of banking secrecy, money laundering and tax fraud are found not in remote alpine valleys or on sunny tropical isles but in the backyards of the world's biggest economies."[67] Given the number of world financial centers, the focus should be on those that are the most likely and probable conduits for threat finance and investments. This criteria would place a spotlight on the US, Caribbean, and Venezuelan financial centers. These three centers are priorities for a number of reasons. First, they are in close geographical proximity to the United States, and as threat financing moves more and more to a strategy of physical delivery to avoid tracking, physical location is critical. Second, these are also financial centers where the US government can exercise its full panoply of national power more effectively. Third, European financial centers like London, Zurich, and Frankfurt, are already under heavy regulatory scrutiny and have in general already implemented FATF recommendations. Fourth, these three major financial centers are the ones that still have critical weaknesses related to threat finance. Finally, international trade theory and related studies dealing with trading distances, geographical borders, proximity, and common cultures and languages, imply that the domestic US market, and the proximate Caribbean and Latin American regions, are the natural catchments for the movement of illicit money.[68]

US Financial Centers

If the United States government is going to lean on other world financial centers, it needs to be self-critical and take domestic actions within the interagency process.[69] According to research, the US is potentially the world's leading money laundering center. This makes sense considering the US market is where a large portion of the global drug revenues are produced. Additionally, it represents a stable and secure location in which various entities can invest the monies. Even criminals run the risk of losing their assets in unsafe or higher risk locations.[70] The quantitative research of John Walker and Brigitte Unger reveals that locations like the United States are extremely attractive for money laundering, and the subsequent investment of its proceeds. In fact, in one study, the United States was second out of five desirable locations for money laundering: behind Luxembourg and ahead of Switzerland.[71]

Jason Sharman, a political scientist at Australia's Griffith University, concludes that, "In practice Organization for Economic Cooperation and Development (OECD) countries have much laxer regulation on shell corporations than classic tax havens . . . And the U.S. is the worst on this score, worse than Liechtenstein and worse than Somalia." [72] This conclusion was confirmed by a money-laundering threat assessment in 2005 conducted by the federal government which found that the corporate anonymity offered by Nevada, Delaware, and Wyoming rivaled that of some of the most infamous off-shore financial centers. In Nevada, its official website touts "limited reporting and

disclosure requirements" and a speedy one-hour incorporation service. Nevada does not ask for the names of company shareholders, nor does it routinely share information with the federal government. The state, with a population of only 2.6 million, incorporates about 80,000 new firms a year, currently totaling more than 400,000—roughly one for every six people. A study by the Internal Revenue Service found that 50 to 90 percent of those registering companies were already in breach of federal tax laws elsewhere.[73] Delaware and Wyoming have similar records.[74]

The possibilities for misuse are endless. If these state laws are not changed, the US threat financing campaign will not be credible in the international context, leaving America with a vulnerability gap on its own territory. The Congress, in cooperation with state authorities, needs to alter the legal landscape in a number of states if the United States is going to eliminate this home for threat finance. This will require the cooperation of several agencies to investigate existing shell corporations in various jurisdictions. This strategy, however, is fraught with the potential to generate a firestorm regarding federal control and states' rights, and will require sound legal steps to avoid political and judicial challenges. The lead for this effort should be the Department of Justice.

Caribbean Financial Centers

In interviews with international bankers having to deal with the increasingly rigorous Know-Your-Customer regulations, most Latin American financial centers were viewed with concern.[75] This group, composed of Diaspora nationals from countries in the region, have Latin American institutional and private clients as customers. Out of the entire group, the only financial center that received high marks for proper regulation and application of KYC and AML measures is Panama. Nevertheless, even though Panama may be the best-regulated, the ease with which Panamanians incorporate front companies, with opaque holding structures extending all the way to the British Virgin Islands, makes it difficult to identify the owners of companies, or to ferret out those with cartel or terrorist links. This group of banking professionals gave the various Caribbean financial centers rather low marks for KYC and robust AML laws and regulations. Particularly noteworthy for their regulatory and KYC weaknesses are the Cayman Islands, British Virgin Islands, St. Kitts and Nevis, and Antigua.[76] This professional perspective contradicts the official view since none of these financial centers are currently deemed noncompliant with FATF recommendations.[77] This difference may imply the subjective or political nature of FATF evaluations, and the difficulty of actually implementing the recommendations.

To address these issues, the US government needs to use robust diplomacy with the Caribbean financial centers to ensure greater and more rigorous implementation of FATF recommendations. This effort should be based on sound intelligence that reveals implementation is weak or insufficient at the various banking centers. This approach should follow the classic "carrot or stick" model. If countries are uncooperative, then the Department of State

should take the lead and institute diplomatic retorsion efforts to enforce compliance. These efforts may be as simple as cutting off visa issuance for all citizens of a particular country until it complies.[78] Such acts may seem trivial, but they are effective, since it is mainly the political elite who travel to the United States. An example of this strategy, albeit for a nonfinancial criminal issue, is Guyana. In October 2001, the United States placed visa sanctions on Guyana because the Guyanese government was avoiding issuance of travel documents for 113 Guyanese awaiting deportation in the United States. The visa sanctions were lifted in December after the Guyanese government issued the travel documents for the deportees.[79]

For compliant countries that make an effort to address threat financing, the US government should allocate additional funding to strengthen indigenous capabilities related to financial intelligence and law enforcement. The Department of State, supported by the Department of Justice, should take the lead in these efforts and oversee the providing of aid and assistance to partner nations that develop prosecutorial expertise related to money laundering and terrorist financing.[80]

Venezuela's Financial Center

The Venezuelan regime of Hugo Chavez, noted for increasing connections to Iran and its terrorist protégés, is fast becoming a potential nexus of terrorism, cartels, and state (Iranian) financing.[81] Despite Venezuela's adversarial posture, the United States has a number of financial weapons at its disposal. An initial step would be to scrutinize and monitor all electronic message transfers via SWIFT (the interbank messaging system) or wire transfers between the United States and Venezuelan banks. Given the regulatory and counterparty credit aspects of the banking business, the United States and other Western banks should only use trustworthy Venezuelan-based banks to act as payment agents for the transfer of Venezuelan bolivars and US dollars. This would make it highly unlikely that a locally owned Venezuelan bank could conduct such transactions directly. It also implies that the US government should focus its intelligence efforts, as a first step, on payments flowing through easily identifiable foreign-owned banking subsidiaries, since they would have the highest probability of receiving illegal monies.

A second important step would be to pass legislation or issue an Executive Order that would allow the US government to monitor all US dollar payments from The Clearing House Interbank Payments System (CHIPS) in New York. CHIPS is a bank-owned, privately operated electronic payments system that transfers funds and conducts transactions in US dollars. CHIPS enables banks to transfer and settle international payments. It processes over 95 percent of the US dollar cross-border payments. Leading banks, their correspondents, and customers around the world rely on CHIPS to process more than $1.5 trillion every day.[82] The CHIPS database shows that 27 Venezuelan banks are linked to the dollar payments system via various member banks. As of 2010, CHIPS has 49 members, all large US banks and American branches of

foreign banks.[83] Being domiciled in the United States, these members would all be subject to US laws and regulations governing the surveillance of payments to and from Venezuela.

Finally, restrictions could be applied to Venezuelan banks. Interestingly, while Iranian banks are sanctioned, their Venezuelan counterparts are not. Iran-to-Venezuela money transfers are both possible and probable. It is currently left entirely to the foreign banks involved to be selective in their dealings with Venezuelan counterparts. Such a relationship is clearly not flawless, and could certainly be improved. Naturally, measures directed at the three high risk financial centers require a great degree of interagency cooperation for successful implementation, and an equally great degree of support for the aforementioned unity of command strategy.

Greater Public-Private Partnership

One difficulty with threat finance is that the scope is large and multidimensional, and the required expertise is spread over a number of disciplines, organizations, and people—many found outside of government organizations. This implies a need for greater public and private cooperation.[84] Know-Your-Customer guidelines have been amplified by the new imperative to shut down threat financing networks completely. To be successful in this endeavor, pattern recognition and local knowledge are critical. These capabilities are generally found in only the most seasoned and culturally linked bankers, expert in dealing with specific regions and threats. These experts have a keener "sense" of context, connections, and culture when it comes to the ferreting out of implausible or suspicious transactions.

The US government should increase its outreach in a public and private partnership to provide these bankers with the educational and informational tools necessary so they might share the latest threat finance intelligence and trends. The banks have a strong incentive to cooperate if they desire to maintain their reputations. There is also reciprocal information to be shared from banks that are active in these critical regions. This information may also be useful for interagency initiatives. To initiate this proposal, the Department of Treasury could establish a closed forum for the exchange of information with the banking industry in specific regions.

Finally, the US military could more effectively draw on its reserve component personnel with banking experience and security clearances to support this effort. The use of reserve component personnel with banking experience could provide a critical asset in combating threat finance. Unfortunately, there are several obstacles preventing the efficient utilization of this talent. First, the US military personnel system cannot readily identify the requisite skills and experience required. This issue is part of a greater problem the military has in identifying the full skillsets available throughout the Reserve Components. Secondly, those Reservists with the requisite skills and knowledge would need to be slotted in organizations that focus on threat finance. Again, the challenge is an internal one—the military's human resource system is driven by

an industrial process of slotting positions according to conventional military skills, not civilian ones. Developing a true talent management approach would enable government agencies to tap these assets.[85] To implement this proposal, the Department of Defense needs to take the lead and mandate that the services conduct a detailed survey of personnel who have such skills. Once the "banking" pool is determined, Reservists could be assigned appropriately.

Conclusion

Fighting threat finance networks requires smart hierarchies that can quickly transcend bureaucratic boundaries, pass information and analysis rapidly to the appropriate place, and afford maximum latitude and support to operatives in the field.[86] To ensure success in the threat finance arena, interagency policy recommendations need to focus on four main themes: The US government needs to:

- Mandate a single and existing US government organization to direct all agencies involved in fighting threat finance in an effort to provide unity of command. This action will entail appointing a threat finance czar with a comprehensive mandate.
- Utilize public diplomacy and psychological operations to influence money donors in an attempt to steer their funds to precertified charities with no ties to terrorist organizations. This step will prevent funds funneling into the financial domain. The initial focus of this effort could be targeted at Islamic terrorist groups.
- Increase interagency efforts to address three specific financial centers (United States, Caribbean, and Venezuela) where large amounts of illicit funds are likely to transit or be stored.
- Boost coordination, information exchange, and the education of the banking sector, while tapping the latent banking expertise of selected Reserve Component soldiers.

While these measures require, in most cases, an interagency and political will of the highest order, their execution would avoid American efforts ending in Sisyphean frustration. For in the end, only by summoning the political will required for such decisions, can the United States truly slay the Hydra of threat finance.

Notes

1. The core idea for this article originated in a background paper written by the author for a Center for New American Security (CNAS) study. See Robert Killebrew and Jennifer Bernal, *Crime Wars: Gangs, Cartels, and U.S. National Security* (Washington, DC: Center for New American Security, 2010).

2. Adapted from Benjamin Bahney et al. *An economic analysis of the financial records of al-Qaida in Iraq* (Santa Monica, CA: RAND, 2010), xvii.

3. Deputy Secretary of Defense, Directive-Type Memorandum (DTM) 08-034, DoD Counterthreat Finance (CTF) Policy (December 2, 2008). This policy implicitly defines threat finance by outlining CTF activities, roles, and responsibilities. A counter threat finance definition is provided

in the glossary on page 13 and includes "terrorist revenue and logistics and other such activities that generate revenue through illicit trafficking networks." This definition is specifically focused on illicit financing means and does not account for legal generation or legal distribution activities.

4. Acting Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism James Q. Roberts, *Statement on Terrorist and Insurgent Financing,* House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats, and Capabilities and House Financial Services Subcommittee on Oversight and Investigations, 28 July 2005, http://www.dod.mil/dodgc/olc/docs/Test05-07-28Roberts.doc (accessed October 18, 2010); Thomas W. O' Connell, ASD/SOLIC, *Defense Perspectives: The War on Terrorism, PowerPoint Presentation, 2006,* http://www.dtic.mil/ndia/2006solic/oconnel.pdf (accessed October 18, 2010).

5. Major Clarence W. Bowman III, *Countering Threat Finance as a Critical Subset of Irregular Warfare: An Interpretive Case Study of Northern Nigeria* (Ft. Leavenworth, KS: United States Command and General Staff College, 2009).

6. Based upon internal definitions from several banks in the Wolfsberg Group.

7. Ibid.

8. See for example *Switzerland and the Fight Against Money Laundering* (Basel: Swiss Bankers Association, 2001); author has private copies of the original internal documents from several banks in the Wolfsberg Group; and Article 305bis of the Swiss Criminal Code, 21 December 1937, status as of 1 January 2010, http://www.admin.ch/ch/e/rs/3/311.0.en.pdf (accessed November 10, 2010).

9. Phil Williams, "Warning Indicators and Terrorist Finances," in Jeanne K. Giraldo and Harold A. Trinkunas, *Terrorism Financing and State Responses: A Comparative Perspective* (Stanford, CA: Stanford University Press, 2007), 75; Russell D. Howard and Colleen M. Traughber, "The Route of Terrorism and Trafficking from Central Asia to Western Europe," *Connections: The Quarterly Journal* 6, no. 1 (Spring 2007): 1-4.

10. U.S. Deptartment of State, *International Narcotics Control Strategy Report 2003* (Washington, DC: U.S. Department of State, 2003).

11. Peter Reuter and Edwin M. Truman, *Chasing Dirty Money: The Fight Against Money Laundering* (Washington, DC: Institute for International Economics, 2004).

12. Williams, 85.

13. Jahangir Arasli, "The Rising Wind: Is the Caucasus Emerging as a Hub for Terrorism, Smuggling, and Trafficking?" *Connections: The Quarterly Journal* 6, no. 1 (Spring 2007): 5-26.

14. Laura K. Donohue, "Anti-Terrorist Finance in the United Kingdom and United States," *Michigan Journal of International Law* 27, no. 2 (Winter 2006): 396.

15. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Title III, § 302(a)(1), Public Law 107-56, 107th Congress; H.C. 978-1, Table 1:18. Select Committee on Northern Ireland Affairs, The Financing of Terrorism in Northern Ireland, Fourth Report of Session 2001–2.

16. Kathryn L. Gardner, "Fighting Terrorism the FATF Way," *Global Governance* 13, no. 3 (July-September 2007): 325-345.

17. Written feedback from an anyonymous Naval War College reviewer of an earlier verison of this manuscript, January 2011.

18. Rex A. Hudson, *A Global Overview of Narcotics-funded Terrorist and Other Extremist Groups* (Washington, DC: Federal Research Division, Library of Congress, May 2002) http://www.loc.gov/rr/frd/pdf-files/NarcsFundedTerrs_Extrems.pdf (accessed October 18, 2010).

19. Killebrew and Bernal, *Crime Wars*, 6.

20. Roberts, *Terrorist and Insurgent Financing*.

21. Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2002–2003, February 14, 2003 (Paris: FATF Secretariat).

22. Jeanne K. Giraldo and Harold A. Trinkunas, "The Political Economy of Terrorism Financing," in *Terrorism Financing and State Responses* (Stanford, CA: Stanford University Press, 2007), 29.

23. Amelia Hill, "Bin Laden's $20M African 'Blood Diamond' Deals," *The Observer*, October 20, 2002, http://www.guardian.co.uk/world/2002/oct/20/alqaida.terrorism (accessed February 26, 2011).

24. Sina Lehmkuhler, "Countering Terrorist Financing: We Need a Long-Term Prioritizing Strategy," *Journal of Homeland Security,* April 2003, http://www.homelandsecurity.org/journal/articles/Lehmkuhler.html (accessed February 26, 2011).

25. Interview with US Army Colonel, U.S. Special Operations Command, January 2010.

26. Moises Naim. *Illicit: How Smugglers, Traffickers, and Copycats are Hijacking the Global Economy* (New York, NY: Doubleday, 2005), 154.

27. Jack A. Blum et al., "Financial Havens, Banking Secrecy, and Money Laundering," Issue 8 of *UNDCP Technical Series* (New York: United Nations Office for Drug Control and Crime Prevention, 2004).

28. CHIPS, The Clearing House Interbank Payments System, http://www.chips.org/home.php (accessed May 26, 2010).

29. John Roth, Douglas Greenburg, and Serena Wille, *National Commission on Terrorist Attacks Against the United States, Monograph on Terrorist Financing: Staff Report to the Commission*, 131, http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf (accessed February 26, 2011).

30. Lehmkuhler, "Countering Terrorist Financing."

31. Matthew Levitt and Michael Jacobson, "The U.S. Campaign to Squeeze Terrorists' Financing, *Journal of International Affairs* 62, no. 1 (Fall/Winter 2008): 67-85.

32. Roberts, *Terrorist and Insurgent Financing*.

33. U.S. Department of Justice, National Drug Intelligence Center, *National Drug Threat Assessment 2009*, December 2008, http://www.justice.gov/ndic/pubs31/31379/finance.htm (accessed November 3, 2010).

34. U.S. Department of Justice, *National Drug Intelligence Center, National Drug Threat Assessment 2010, Illicit Finance*, February 2010, http://www.justice.gov/ndic/pubs38/38661/finance.htm (accessed February 21, 2011).

35. The $17.2 billion estimate is based on a review of US banknotes repatriated from Mexico. The estimate represents only US currency returned to the United States, not all US currency that was smuggled to or through Mexico. This estimate is based on analysis of US banknotes purchased by US financial institutions from Mexican financial institutions from 2003 through 2004. See *National Drug Threat Assessment 2010*.

36. *National Drug Threat Assessment 2010, Illicit Finance*.

37. United States House Financial Services Subcommittee on Oversight and Investigations, testimony by Stuart Levey, Under Secretary for Terrorism and Financial Intelligence, U.S. Department of the Treasury, 109th Congress, 2nd Session, July 11, 2006, http://www.treasury.gov/press-center/press-releases/Pages/hp05.aspx (accessed May 24, 2010); U.S. Department of the Treasury, "Statement of Under Secretary Stuart Levey on the Terrorist Finance Tracking Program," 23 June 2006, http://www.treasury.gov/press-center/press-releases/Pages/js4334.aspx (accessed May 24, 2010).

38. Roth, *National Commission on Terrorist Attacks,* 56.

39. *Financial Action Task Force on Money Laundering*, 4.

40. Financial Crimes Enforcement Network, U.S. Department of Treasury, *SAR Activity Review—Trends, Tips and Issues* 4, August 2002 (Washington, D.C.: FinCEN Office of Strategic Analysis, 2002), http://www.fincen.gov/news_room/rpl/files/sar_tti_04.pdf (accessed November 10, 2010).

41. Donohue, "Anti-Terrorist Finance,"403.

42. Ibid., 390.

43. U.S. Departments of the Treasury and Justice, *National Money Laundering Strategy*, July 2002, 17-8, http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/ml2002.pdf (accessed December 1, 2010).

44. Lehmkuhler, "Countering Terrorist Financing."

45. "Update on Terrorist Blocking and Freezes," internal Treasury Department document, November 2002.

46. U.S. Department of the Treasury, "Contributions by the Department of the Treasury to the Financial War on Terrorism-Fact Sheet," September 2002.

47. Edward Alden, "The Money Trail: How a Crackdown on Suspect Charities is Failing to Stem the Flow of Funds to al Qaeda," *Financial Times*, October 18, 2002, 19.

48. Ibid.

49. Ibid.

50. Donohue, "Anti-Terrorist Finance," 405.

51. O'Connell, *Defense Perspectives*.

52. Kevin D. Stringer, "A Supreme Commander for the War on Terror," *Joint Forces Quarterly* (1st Quarter, 2007): 19-23. This article offers a view to the criticality of unity of command for an organization and its execution of operations.

53. Operation Green Quest Overview, CBP.gov, February 26, 2002, http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/legacy/2002/22002/02262002.xml (accessed February 26, 2011); Operation Green Quest brochure, U.S. Customs Service Office of Investigations, October 2002.

54. Robert S. Mueller, III, Director, Federal Bureau of Investigation, Testimony before the House Committee on Financial Services, "The Work of the Terrorism Financial Review Group," Washington, DC, September 19, 2002.

55. Wesley J.L. Anderson. Disrupting Threat Finances: Utilization of Financial Information to Disrupt Terrorist Organizations in the Twenty-First Century (Ft. Leavenworth, KS: School of Advanced Military Studies, 2007).

56. Ibid.

57. James Adams. *The Financing of Terror* (London: Hodder & Stoughton Ltd 1986), 165.

58. Jean-Charles Brisard. *Terrorism Financing: Roots and Trends of Saudi Terrorism Financing.* Report prepared for the President of the Security Council United Nations, December 19, 2002, http://old.nationalreview.com/document/document-un122002.pdf.

59. Abdeslam M. Maghraoui, "American Foreign Policy and Islamic Renewal," *Connections: The Quarterly Journal* 5, no. 4 (Winter Supplement 2006): 26-40.

60. Donohue, "Anti-Terrorist Finance," 406.

61. *The Financial Action Task Force (FATF) 40 Recommendations* (Paris: OECD, October 2003, with amendments until October 2004) and *FATF IX Special Recommendations* (Paris: OECD, October 2001, updated October 2004). (do you want to add a URL?)

62. Financial Action Task Force (FATF), Methodology for Assessing Compliance with the FATF Forty Recommendations and the FATF Nine Special Recommendations (Paris: OECD, 2004).

63. Don D. Marshall, "The New International Financial Architecture and Caribbean OFCs: Confronting Financial Stability Discourse," *Third World Quarterly* 28, no. 5 (2007): 917-938. This article is a rich analysis of the origins of money laundering and financial corruption; John Walker and Brigitte Unger, "Measuring Global Money Laundering: The Walker Gravity Model," *Review of Law and Economics* 5, no. 2 (2009): 821-853; and John Walker, *Modeling Global Money Laundering flows-some findings*, November 30, 1998, http://www.johnwalkercrimetrendsanalysis.com.au/ML%20method.htm (accessed May 21, 2010).

64. U.S. Department of State, *International Narcotics Control Strategy Report 2010* (Washington, DC: U.S. Department of State 2010).

65. USA PATRIOT Act of 2001.

66. U.S. Departments of the Treasury and Justice, *National Money Laundering Strategy, 2003, 13.*

67. "Finance and Economics: Haven hypocrisy: The G20 and tax," *The Economist*, Vol. 390, Issue 8624, March 28, 2009, 87.

68. J.C.P. McCallum, "National Borders Matter: Canada-U.S. Regional Trade Patterns," *The American Economic Review* 85, no. 3 (June 1995): 615-623; John F. Helliwell, "Language and Trade, Gravity Modelling of Trade Flows and the Role of Language" in Albert Breton, ed., *Exploring the Economics of Language* (Ottawa: Department of Canadian Heritage, 1999; John Walker and Brigitte

Unger, "Measuring Global Money Laundering: The Walker Gravity Model," *Review of Law and Economics* 5, no. 2 (December 2009): 821-853.

69. Interview with a confidential source who is an international tax and corporate structuring specialist, November 2010. This source requested confidentiality given the sensitivity of this subject in his professional field.

70. Giraldo and Trinkunas, "The Political Economy," 19.

71. Walker and Unger, "Measuring Global Money Laundering," 821-853;Walker, *Modeling Global Money Laundering*."

72. "Finance and Economics: Haven hypocrisy," 87.

73. Ibid.

74. Delaware, The 'Lectric Law Library Stacks, The United States The World's Largest Tax Haven* http://www.lectlaw.com/filesh/bbg33.htm (accessed May 24, 2010); Delaware-Taxation, City Data http://www.city-data.com/states/Delaware-Taxation.html (accessed May 24, 2010;Justin Hane, "Delaware: tax haven or just "advantageous"?", *Swissinfo.ch*, June 17, 2009, http://www.swissinfo.ch/eng/news/best_rated/Delaware:_tax_haven_or_just_advantageous.html?cid=7090 (accessed May 24, 2010).

75. Semi-structured interviews from January-August 2010 with: an Argentinean investment banker structuring solutions for private clients in Latin America; a Colombian private banker responsible for external asset managers in the region; a Venezuelan transactional banker dealing with Latin American financial institutions in payments and trade finance; and a Mexican economist focused on Latin American money flows. All interviewees requested anonymity given the sensititvy of this subject to their respective bank employers.

76. This current view comes from the interviewed group of front-line bankers dealing with real KYC assessments from potential clients in the region. For a historical view to the development of these financial centers in terms of money laundering see Esther C. Suss, Oral H. Williams, and Chandima Mendis, "Caribbean Offshore Financial Centers: Past, Present, and Possibilities for the Future," *IMF Working Paper WP/02/88*, revised June 26, 2002.

77. Financial Action Task Force: Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review (Paris: OECD, 2007). Currently, no countries are listed as noncooperative.

78. Kevin D. Stringer, "Visa Diplomacy," *Diplomacy and Statecraft* 15, no. 4 (December 2004) offers an overview of how to use visa diplomacy for retorsion.

79. Ambassador Odeen Ishmael (Guyana), "The Impact of the September 11, 2001 Terrorist Attack against the United States on the Caribbean Political Economy," lecture, Howard University, Washington, DC, January 30, 2003, http://www.guyana.org/Speeches/ishmael_013003.html (accessed December 10, 2010).

80. Roberts, *Terrorist and Insurgent Financing*.

81. Structured interviews with two transactional bankers working for two different global banks involved in the region, October 2010; Killebrew and Bernal, *Crime Wars,* 31-32.

82. CHIPS, The Clearing House Interbank Payments System, http://www.chips.org/home.php (accessed May 24, 2010).

83. See *About CHIPS*, Customers, http://www.chips.org/about/pages/033742.php (accessed May 24, 2010).

84. Derived from Roy Godson, "Transstate Security," in Richard Schultz, Jr., Roy Godson, and George Quester, *Security Studies for the 21st Century* (Dulles, VA: Brassey's, Inc., 1997), 93-95.

85. Kevin D. Stringer, "The War on Terror and the War for Officer Talent: Linked Challenges for the US Army," *The Land Warfare Papers*, No. 67 (Arlington, VA: Institute of Land Warfare AUSA, July 2008).

86. Killebrew and Bernal, *Crime Wars*, 9.