THE GEORGE WASHINGTON UNIVERSITY
HOMELAND SECURITY POLICY INSTITUTE

HSPI Issue Brief Series

THE NEXT DECADE OF COUNTERING THREAT FINANCE: RISKS, OPPORTUNITIES, AND LIMITATIONS

HSPI Issue Brief 15
June 12, 2012
Scott Helfstein

Almost ten years after the September 11 attacks, domestic terrorist plots linked to Islamic extremism continue rising. The evolving nature of sub-state threats makes it critically important to evaluate the strengths and weaknesses of the counterterrorism toolkit in the hope of maintaining an efficient and effective security posture. Counter threat finance has proven a valuable instrument in hindering terrorist activity over the past decade, making it all the more important to evaluate existing shortfalls and consider opportunities for future action.

Counter threat finance is the practice of attacking the financial lifelines of those intent on harming the Unites States, its citizens, and its allies.[1] There are many different elements associated with countering financial activities of illicit actors such as monitoring flows, stopping transfers, prosecuting criminal activity, and seizing funds bound for illicit use. It is difficult to quantify the impact of these efforts, but anecdotal evidence suggests that it has been reasonably effective with some variation across domains. Since 2009, al-Qaeda leaders prioritized calls for financial support, which many see as an indication of funding troubles.[2] Financial tools have also been one of the few successful tools brought to bear in confrontations with drug cartels and curtailing North Korea's weapons proliferation.

To date, successful counter threat finance operations have resulted in the tracking and arrest of terrorists, international fund seizures, domestic prosecutions for material support to terrorists, and fines levied against financial institutions found in violation of federal law. The Department of Treasury has taken the lead by providing intelligence

support and policy guidance, but law enforcement agencies like the Federal Bureau of Investigation and the Drug Enforcement Agency, and Combatant Commands like U.S. Central and Pacific Commands, as well as other departments in the executive branch like Commerce and State all utilize these tools to differing degrees.

Despite the investment in building counter threat finance capability and the impressive array of accomplishments over the past ten years, this remains a relatively new tool in the security kit. The decentralization and adaptation of the terrorist threat, the evolution of technology, and emerging frontiers of international law and cooperation present a unique set of risks, opportunities, and limitations for countering threat finance.

A risk assessment reveals that many organizations and individuals involved in illicit activity are quite comfortable using the modern financial system. The interconnected nature of the financial industry and the global reach through correspondent banks offer illicit actors many ways of getting funds into and out of the system. Add to this rapid technological change associated with delivery of financial services such as mobile phone transfers, retail foreign exchange, prepaid debit cards, and the growth of online transactions. In theory, regulatory practices exist to monitor these activities, but financial institutions and government authorities are often overwhelmed by the data streams. These regulatory measures incentivize banks to build out compliance functions that are supposed to keep a watchful eye for suspicious activity with financial punishments looming for failure to follow prescribed procedure.

Despite an array of risks facing the public and private sectors, there are a number of opportunities to strengthen threat finance initiatives and build a better system for the future. Some of these changes are fairly small, while others are more substantial. The regulatory structure offers a place to start. The current approach does not necessarily incentivize financial institutions to adopt an activist role in counter threat finance, which means that authorities are not yet leveraging every tool at their disposal. With much of the Dodd-Frank Act yet to be written, there may be opportunities to change the tenor of counter threat finance interaction without passing further legislation. Regulatory change in itself may not be sufficient to promote change through greater activism, but it will play an important role in shifting the domestic and international mindset.

Technological innovation often associated with increased risks simultaneously offers a powerful tool for addressing some of the shortcomings in the current counter threat finance environment. In an environment where data streams grow ever larger and algorithmic information processing is constantly improving, it is important to consider how these tools may be best be applied to current and future challenges. As the technology of big data analysis develops, it will help to keep costs of monitoring, reporting and investigating low despite the steadily growing stream of information.

Complex analysis of large-scale data also places certain limitations squarely in focus. Both the public and private sectors face serious issues in maintaining the technological skill set to thwart financial activities of illicit actors as adversaries grow increasingly sophisticated. It may be possible to incentivize third parties like the hacker population to crowd source solutions, but this also involves risks. Further, technological tools aimed at intelligently exploiting patterns in data also raise serious privacy concerns. It is important to promote discussions about the benefits and costs associated with integrated information systems in countering threat finance.

It is appealing to view these integrated tools as a catch all capable of crippling the activities of illicit organizations while also providing early warning on radicalized individuals at a time when the strategic center of gravity in terrorism is devolving. In many ways, this assumption is a failure of lexicon, and one that establishes an unreasonable standard. Estimates suggest that illicit activity might be as high as one-third of global GDP and confronting radicalized individuals through the financial toolkit amid this deluge of illicit activity may be akin to finding a needle in a haystack.[3]

The importance of leveraging the tool and identifying illicit activity should not be underestimated. David Coleman Headley, the Lashkar-e-Taiba operative in charge of reconnaissance for the deadly 2008 Mumbai attack, had a history of illicit business and financial activity. In that case, the system's inability to link the illicit commercial activity with terror connections created space for a massive attack when it could have served as a warning.

Work on countering threat finance to date offers good reasons for optimism, and there is great opportunity to improve capabilities in the future. Policy making and implementation efforts must be clear about the aims of counter threat finance efforts by setting priorities and expectations appropriately across range of threats.

Known and Hidden Hazards

Among the tools that the United States and its partners can bring to bear against terrorist and other illicit transnational actors, countering threat finance is reasonably low cost. The benefits of integrating counter threat finance with more traditional tools over the past decade offered a new way to engage enemies, but it would be a disservice to ignore the remaining and emerging risks. With ten years of data since the September 11 attacks behind us, it is important to reassess the assumptions undergirding risks and priorities associated with threat finance especially at a time when government will be asked to do more with less.

The risk of terrorist exploitation of the financial system is by no means new and quite well-documented. The September 11 hijackers allegedly received money through wire transfers from the United Arab Emirates to Florida-based SunTrust Bank.[4] Since then, significant resources have been devoted to denying illicit actors access to the financial system, but these measures have not deterred many that seem quite comfortable with the global financial system. A rational deterrence theorist might argue that these actors must believe that punishment is unlikely or find significant benefits to utilizing the system.

Cases around the world reflect that illicit actors remain content using the global financial system. It is an advantageous way to move, launder, store, and generate funds. In April 2011, the Brazilian authorities arrested Khaled Hussein Ali, who had been running a media and fundraising network for al-Qaeda while possibly planning attacks in Latin America.[5] Many details of the case remain shrouded in secrecy, but the Brazilian government noted that there were a number of legitimate financial transfers to the Middle East.

The Hawallah System

In the years following the September 11 attacks, a great deal of time was spent talking about the hawallah system as means for funneling funds to terrorist organizations outside the watchful eyes of law enforcement and intelligence officials.[1] Hawallahs are informal money transfer outlets common throughout the Middle East, North Africa and South Asia. These businesses operate based on trust among the counterparties transferring funds. There is little record keeping and those that exist are often handwritten ledgers. Substantial sums of money flow through these outlets, which are the most common form of money transfer and remittance throughout a large part of the world.

The large sums of money, the tradition of secrecy, and the minimal record keeping in these transfer outlets offered good reason to generate concern. It is one area where officials have struggled to make any inroads. At the same time,

Charitable organizations like the Holy Land Foundation and Benevolence International are attractive fronts to raise funds and access the financial system with little suspicion.[6]

In June 2011, the U.S. government took steps to seize control of al-Qaeda assets that were used to open an investment account at Chicago-based R.J. O'Brien & Associates. The brokerage account was opened by Abu al Tayyeb in 2005 with a deposit of $26.7 million, which was raised in Saudi Arabia allegedly through an investment scheme.[7] Within a year, the account value declined to $7 million courtesy of a poor investment strategy. Without passing judgment on al-Qaeda's asset management prowess, the group clearly believed that US capital markets offered refuge to hide cash and perhaps even secure a positive return for future illicit activity.

Other terror financiers like Mansour al-Kassar proved far more adept at generating positive returns on ill-gotten gains that likely funded future illicit activity.[8] The international arms dealer and supporter of jihad had bank accounts in Europe's largest institutions, investments in hedge funds, and real estate interests on multiple continents. This financial empire, built on illicit activities, is an important reminder that there is more to be done.

the intense focus on this area may not be the best place to focus on going forward for two reasons. First, time and historical evidence have proven that reducing illicit actors' use of the legitimate financial system represents as much of a challenge if not more so.[1] Second, the current legal means and analytical resources offer little leverage in addressing this issue. Quite simply, there are other areas that offer greater potential gains for an identical investment.

There is little evidence that terrorists striking the U.S. homeland, with the possible exception of the Time Square bomber Faisal Shahzad, have made significant use of the hawallah system to fund attacks.[1] Even if illicit organizations were using this informal system to covertly transfer vast sums, many would still look for somewhere to store the money. Undoubtedly, there are funds funneled to illicit organizations through these outlets, but there is also significant use of the legitimate financial system. This is a difficult issue, yet it is one that the U.S. government is far better equipped to address.

Current approaches to countering threat finance draw from anti-money laundering (AML) laws, a seemingly reasonable place to start.[9] It is important to recognize, however, that AML has more data points for banks and authorities to exploit. With

AML, parties have the chance to observe the criminal activity generating the illicit funds, or the banking behavior tied to laundering the money. By contrast, much of the funding that goes to terrorist activity is perfectly legitimate until it gets used for illicit purposes. In the instances where terrorist funds are procured illegally, the dollar amounts involved are usually far below those associated with criminal activity perpetrated for profit.

The power of terrorism lies in the psychological power of a small group of political dissidents with few resources attacking civilian targets. Al-Qaeda in the Arabian Peninsula (AQAP) claims that the 2009 mail bombs intercepted before reaching Chicago cost $4,200.[10] At the top end of the range, the September 11 attacks cost approximately $500,000. Given the amount the US has spent on counterterrorism in the past ten years, that is a return on capital making Warren Buffet's annualized 28% percent seem paltry.

Licit money transfer systems also present a unique set of problems. A cyber security expert, posing as a westerner interested in jihad, approached some users on a radical online bulletin board. After communicating in English and Arabic, and continually expressing his interest in jihad, an individual with a French Yahoo email account told him to participate in financial jihad. He was subsequently instructed to procure a fake identification and then map all of the local Western Union and Money Gram outlets. The handler told him to send small denominations using different stores, all going to the same location in Paris, France.

These licit transfer services are invaluable to the global economy as remittances play a large role in underdeveloped economies. It is easy, however, to exploit these services for nefarious purposes. Clearly, extremists and terrorists are not deterred from using these licit payment systems throughout the West. Given the volume of legitimate transfers that go through these systems on a daily basis, it seems easy to hide illicit activity among normal commerce.

The foreign exchange (FX) market, particularly the emerging arena of retail FX, is another challenge given the transaction volume associated with this newly emerging financial platform. FX markets deal with approximately $4 trillion dollars of transactions daily, and a terrorist attack costs a tiny fraction of that volume. It is the largest exchange by volume globally.

Retail foreign exchange platforms, which emerged so that smaller investors could access markets usually restricted to large investors, do have some important controls to prevent terrorist use. The systems appear to offer open access to the foreign exchange market, but the interfaces are actually proprietary systems where the company trades in the markets on behalf of the investor using a closed platform. These brokers are also subject to rules requiring them to know their counter parties, but the prospectus of one such company notes that 55% of its business is conducted in jurisdictions that are not subject to regulatory requirements.

The frontiers of finance, capital markets, and intermediation also pose unique challenges to counter threat finance. In many instances products and markets are introduced before proper precautions are established to deny illicit use. For example, the newly developed carbon trading exchange aimed at promoting environmental conservation was defrauded of millions. It is speculated that some may have gone to fund terrorism. Those developing new markets and products must be proactive in developing countermeasures to ensure that these financial innovations do not serve as lucrative outlets.

Similarly, emerging technologies pose a similar challenge. Growth of virtual worlds such as Second Life, World of Warcraft and Facebook inadvertently create unregulated markets and economies. Mobile banking and trading offer technology savvy actors new ways of defrauding the financial system, and prepaid debit cards offer a method to launder funds in small and medium size denominations. Given the strategic nature of the adversaries, it is important to remember that innovation and progress might inadvertently spawn new hazards.

Prospects for Improvement and Innovation

Despite the array of persistent and emerging counter threat finance risks, there is opportunity for improvement and innovation that builds on the success to date. Three of these prospects seem particularly pertinent: the incentive structure constructed by regulatory activity, international cooperation, and technological solutions.

In the aftermath of the September 11 attacks, threat finance initiatives focused on tightening the regulatory structure to deny illicit actors access. Part of this involved an ever increasingly complex set of regulations and overseeing bureaucracy, which fostered a compliance-oriented approach to security issues. The system cultivated a "check-the-box" mentality, increasing the likelihood that institutions are reactive

rather than proactive. This is coupled by a one way flow of information where compliance officers at financial institutions provide reports to government, but rarely learn whether and what types of information are useful.

This is an unfortunate irony. Despite the bad rap from the financial crisis and the Occupy Wall Street Movement, many of those at the helm of the country's financial institutions are patriotic individuals that have no interest in unwittingly supporting illicit actors or their endeavors. Many in the financial services sector want to support government activity against terrorists and criminals, which means the next is step is figuring out how to adjust the incentive structure to promote greater activism.

Among the biggest constraints to greater activism are the legal and financial realities that institutions face. Banks may find themselves in legal and reputational troubles should they attempt to gather more information on customers without encouragement and monitoring by government entities. The second constraint is financial, as the costs of taking a more active role may rile investors who care more about profitability. Both of these issues must be addressed to change the tenor of cooperation.

There are three tools that undergird current countering threat finance efforts: know-your-customer (KYC) provisions, blacklists, and suspicious activity reports (SARs).

KYC calls on financial institutions to gather information and know the people using their services. The provisions are built on the notion that financial institutions know their customers better than government bodies responsible for denying access, but the incentives driving information collection are not uniform across financial products. For example, banks have much greater incentive to gather information on those that take loans, risking the bank's capital base, than those making deposits, which helps build the capital base that generates revenues. Given the incentive structure for financial institutions, this is perfectly reasonable, but it does challenge the assumptions underlying the KYC effort. Online banking and international correspondent banking relationships also complicate matters, despite industry norms to understand counterparty risk.

Blacklisting is a tool to designate individuals with whom financial institutions are prohibited from interacting. Financial institutions face penalties should they offer services to these entities knowingly or in ignorance of their status. There are limits to this as well given that blacklists have force of law. For example, summing across the lists maintained by the US, UK, Euro Zone and UN yields approximately 1,000 names

tied to terrorism. It is difficult to imagine one can successfully counter terrorist finance by denying service to 1,000 individuals.

SARs, which banks are required to submit on suspicious activities over $10,000, also face a series of challenges. Banks take these reporting requirements seriously, but there are two crucial questions in judging their efficacy. What constitutes suspicious activity and what level of activity should banks be required to report? Since terrorism is a relatively cheap tactic, the levels on SAR reporting have declined accordingly, but this also creates a new dilemma. Lower SAR initiation requirements mean more reports are filed through the course of ordinary business even if there is nothing particularly suspicious about the transaction. This increases financial and logistical burdens on banks and regulators, both of which feel overextended.

These three tools of KYC, SARs, and blacklisting provide a strong foundation, but it is equally important to assess the assumptions associated with the regulatory regime. As it currently stands, financial institutions have incentive to comply with the rules to avoid punishment, but the problem is that the expected costs of punishment are tremendously small. Consider the two pieces involved. The first is the likelihood of uncovering illicit activity, and the second involves penalties levied against offending institutions.

Both of these are relatively weak across many instances of counter threat finance. First, the likelihood of identifying the flow of funds tied to illicit activities is relatively small compared to the assets under management at many financial institutions. This one of the reasons terrorists and other illicit actors continue to use legitimate financial services. As the likelihood that illicit funds will be detected decreases, the punishments have to get disproportionately large. To date, the government has mixed record when it comes to punishment. Fines tied to banking with Iran have been quite large whereas those tied to terrorism have been comparatively small.

A quick situation assessment reveals great difficulty associated with strengthening threat finance measures, but there are a number of additional actions or new approaches that might yield incremental or drastic improvements. Larger punishments on institutions tied to terrorist financing would help to set the expected costs at levels more likely to deter rational actors.

It is also important to strengthen measures to penalize the individuals associated with accepting or managing illicit funds beyond the institutional punishments. Many financial institutions offer large incentives for raising capital, and individuals may believe that they can secure monetary gain from working with illicit actors. Government should take no quarter in pursuing, prosecuting, and punishing individuals, not just institutions, to develop a credible deterrent.

Despite such incremental changes to the existing structure, the regulatory approach has focused almost entirely on punishment or the cost side of incentive structure with less regard for positive incentives.

Establishing positive incentives for financial institutions to take an activist role might help change the counter threat finance dialogue and practice in meaningful ways. Rather than incentivize financial institutions to generate thousands of suspicious activity reports in order to limit costs associated with legal liability, there may be ways to encourage financial institutions to investigate, identify, report and take actions against illicit actors. This does, however, raise an important question. Should banks take action against only people of interest identified by governments or adopt activist policies independent of government bodies? If the latter, banks are likely to seek immunity for mistakes and charges of impropriety. Governments can offer incentives like tax breaks, seizure sharing agreements, rewards, and grants to institutions that participate. This might help foster a culture where financial institutions see themselves as partners in counter threat finance.

These positive incentives, particularly aspects like grants, can be used to encourage innovation in technological platforms. Promoting investment in innovative platforms will likely yield better results than one-off rewards. For example, many armchair jihadists have social networking websites on platforms such as Facebook and MySpace. Technology exists to integrate activity such as friend connections on these websites with financial transactions using automated systems and algorithms. These types of platforms may yield fruit where standalone financial forensics struggle. Investments like these might also help institutions address information asymmetries in financial intermediation to produce better returns with less risk in their core business.

Innovative efforts to counter threat finance, especially in the identification and tracking of financial transactions tied to illicit activity, need not be limited to banks and governments. Third parties may prove to be critically important actors if the incentive structure could be designed to promote positive engagement. One possible

target would be the hacker population, which has a technological skill set that the private and public sector entities involved in counter threat finance have a difficult time acquiring. Countering money laundering, that involves accessing and tracking data, may be one area where partnership with positively incentivized hackers proves to fill a current gap. Leveraging a crowd sourced approach and the technological skill set of a broader group could augment current capabilities in interesting ways.

The benefits from evolving technological platforms are not limited to data mining and information assessment. Widespread access to mobile phones and electronic payment platforms, often referred to as financial inclusion, are changing the nature of commerce in ways that may not be amenable to illicit activities, particularly in developing economies. By improving transparency, the risk associated with illicit activities such as terrorism, drugs, or corruption increases. Adoption of these systems in a manner sufficient to derive benefits will require time, and more importantly, significant social change that redefines people's use of financial services. Merchants and customers can break the natural inertia involved in such radical change should they find sufficient benefit in these new systems.

Taking steps to build a more productive partnership and encourage greater industry activism on security measures may also help crack the code on better international cooperation. Counter threat, and particularly counter terrorism, finance proves an area difficult to secure cooperation among international partners. This may stem from the financial benefits of looking the other way, a desire to downplay the presence of radical elements in a country, or a lack of political will to address the issue.

Within weeks of the terrorist attack on Mumbai, charitable fronts associated with the perpetrators, Lashkar-e-Taiba, were blacklisted by several international bodies. A few months later, groups operating under different names with almost identical rhetoric were back to business as usual. One advertisement used the same logo with a different color scheme, and below was a banking code identical to the one used before the attack. The organization names had changed, but the accounts remained the same.

Irrespective, an incentive structure that promotes activism may pave the way for the industry and its powerful lobby groups to promote international cooperation. Meaningful progress will require substantial cooperation in parts of the world where the U.S. struggles to exert influence in positive ways, and this is where industry may be well positioned to assist and drive for higher standards.

Expectations, Limits, and Priorities

There are many opportunities to improve counter threat finance efforts, but it is equally important to recognize the limitations if there is any hope of developing realistic goals and effective policies. The community has to decide whether threat finance will focus on individuals or groups, clearly outline the relationship between privacy and future innovation, and understand the limitations or develop alternatives to the "public-private partnership".

Despite much success, recent cases reflect limitations in leveraging counter threat finance as a tactical tool capable of providing early warning on decentralized threats. For example, the attempted Times Square bomber Faisal Shahzad, was in default on his house when he carried out his plot.[11] This is an example where the individual had a banking relationship, based on loans rather than deposits, used informal remittance systems to fund the attack, and never drew suspicion. While this is frustrating, it is also unreasonable to argue that the associated financial institutions should have identified him as a possible bomber based on current standards and capabilities.

Najibullah Zazi, the attempted New York subway bomber, also accessed the US financial system accruing $51,000 in personal debt.[12] He eventually declared bankruptcy and moved out of his uncle's house when he could no longer pay rent. There is no evidence to suggest that the borrowed funds played a role in acquiring materials for his subsequent plot, but they did sustain his lifestyle. Despite the financial incentives to know debtors, and the legal requirements to know your customer, Zazi escaped identification for months during planning. This anecdote reinforces the difficulty associated with countering terrorist finance in the current environment.

The number of attacks conducted by individuals inspired by al-Qaeda's ideology, those unconnected to the actual organization, increased drastically within the US over the past few years. It is important to recognize that efforts to counter terrorist finance, or using terrorist financial transactions for intelligence purposes, will yield little benefit when it comes to these small scale incidents.[13]

Scouring the financial system to find the next Shahzad or Zazi will only overwhelm both regulators and financial institutions. As currently practiced, efforts to counter terrorist finance should focus on terrorist organizations or infrastructure, platforms that could be used to launch multiple attacks. This seems like a simple point, but the current lexicon does not distinguish between these different types of threats, thereby running the risk of setting unrealistic goals and misallocating resources.[14]

The focus on groups, networks, and attack infrastructure will also help moderate the privacy considerations associated with integrating different information sources with financial data. It is perfectly reasonable for both financial institutions and intelligence agencies to use all publicly available information to assess threats and minimize risks. This includes social networking, videos, blog posts and the like. Things become infinitely more complicated with the possibility of integrating publicly available data with the proprietary, and ostensibly private, information on spending patterns that the financial institutions access.

These legitimate and serious privacy concerns will limit the ability to integrate data streams and build early warning platforms capable of finding radicalized individuals. It should not, however, prevent institutions from investigating whether funds are tied to illicit activities by any legal means at their disposal including automated and integrated platforms. In this regard, private institutions may actually have more latitude than the government, and in fact most of the social media tools, websites, and apps we use on a daily basis are already doing much more extensive mining on our individual activities than financial institutions and domestic law enforcement agencies. If expectations are appropriately set, there is ample room to develop new capacities while being mindful of privacy.

The relationship between the public and private sectors is another area with promise and limits. There is a steady and ever louder drum beat of public-private partnership, particularly in areas of counterterrorism and homeland security. While this buzz phrase will certainly be with us for some time to come, it evokes very different responses among the public and private sector participants. Many in the public sector believe that there are unique resources that private sector financial institutions can bring to bear on a host of issues. They are absolutely correct. Unfortunately, the concept often invokes skepticism or outright contempt as some on the private side see it as a way for the public sector to abdicate certain roles or pass responsibility to others without much support.

This is not a reason to abandon the notion of public-private partnership, or the more express goal of integrating the financial services industry into discussions of national security in a more robust way, but it does mean that it needs mending and tending. The private sector needs to believe they have a partner willing to bring tangible capabilities to the table and incentive structures that help them to help the public sector.

One method of signaling the commitment to change might focus on the bureaucracy itself. The array of government agencies and offices involved in suspicious transactions and countering terrorism finance is difficult to navigate to say the least. The Treasury Department has at least four offices involved in these efforts, the Departments of Justice and Homeland Security both play important roles, and banking regulators such as the FDIC and Federal Reserve are responsible for direct oversight. This patchwork of bureaucracy should be rationalized to help shift the burden of compliance and open space for different types of engagement.

Conclusions

Make no mistake: the last decade of counter threat finance is a story of success. It is one of the most efficient and effective tools in promoting security, and one that should gain increased attention and resources despite the constrained environment. At the same time, it is important to constructively focus on ways of building on that success to create a system that will confound our adversaries, from terrorists to smugglers to proliferators.

There are serious shortcomings in the current system, but there are some limitations that might be circumvented with some innovative thinking and constructive engagement. The hardest aspect will be aligning incentives in ways to maximize performance, first with the financial services industry and then with foreign partners and third parties. The capacity to effect serious change not only exists, but has already come to fruition. Building the will, among the private sector and foreign countries, to take on these issues despite the political and economic costs is difficult. Nonetheless, these issues should take front and center in planning for the next decade.

Dr. Scott Helfstein *is an HSPI Senior Fellow, and Director of Research at the Combating Terrorism Center of the United States Military Academy.*

The views expressed in this Issue Brief are the author's and do not necessarily reflect those of the Combating Terrorism Center, U.S. Military Academy, Department of Defense or U.S. government.

The author would like to thank Jeff Bardin, Lauren Burns, Sharon Cardash, Joseph Clark, Gary Howe, John Solomon, Jim Spencer, Janey Wright, and Elad Yoran for their helpful comments. All errors are my own.

Founded in 2003, The George Washington University Homeland Security Policy Institute (HSPI) is a nonpartisan "think and do" tank whose mission is to build bridges between theory and practice to advance homeland security through an interdisciplinary approach. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, HSPI creates innovative strategies and solutions to current and future threats to the nation. The opinions expressed in this Issue Brief are those of the author alone. Comments should be directed to hspi@gwu.edu.

---

[1] Tony Capaccio, "U.S. Military to Target Terror Finance Networks," *Bloomberg News*, December 8, 2008, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aWCdqrmv031g.
[2] Douglas Farah, "The Success of Counter-Terror Financial Measures," October 14, 2009, http://www.douglasfarah.com/article/509/the-success-of-counter-terror-financial-measures.com.
[3] Moises Naim, *Illicit: How Smugglers, Traffickers and Copycats are Hijacking the Global Economy* (Doubleday: New York, NY, 2005); Moises Naim, "It's the Illicit Economy, Stupid: How Big Business Taught Criminals to Go Global, *Foreign Policy*, November 9, 2005, http://www.foreignpolicy.com/articles/2005/11/09/its_the_illicit_economy_stupid.
[4] National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report," 1st ed.(New York: Norton, 2004).
[5] "Al Qaeda Members Hide in Brazil, Raise Money: Report," *Reuters*, April 2, 2011, http://www.reuters.com/article/2011/04/02/us-brazil-qaeda-idUSTRE7312LJ20110402.
[6] "Finance And Economics: The iceberg beneath the charity; Terrorist finance." *The Economist,* March 15, 2003: ABI/INFORM Global, ProQuest. Web. 29 Nov. 2010.
[7] Annie Sweeney, "Al-Qaida Operative Invested with Chicago Brokerage House in 2005," *Chicago Tribune,* June 21, 2011, http://articles.chicagotribune.com/2011-06-21/business/ct-met-terrorism-financing-20110621_1_al-qaida-qaida-al-ghamdi.
[8] Patrick Radden Keefe, "The Trafficker: The Decades-Long Battle to Catch an International Arms Broker," *The New Yorker*, February 8, 2010, http://www.newyorker.com/reporting/2010/02/08/100208fa_fact_keefe.
Read more http://www.newyorker.com/reporting/2010/02/08/100208fa_fact_keefe#ixzz1jDTcdBMD
[9] Laura K. Donohue, "Anti-Terrorist Finance In The United Kingdom And United States," *Michigan Journal of International Law* 27 (2006): 303-435.
[10] "Small-scale Attacks to Continue, Al Qaeda Group Says," *Reuters,* November 21, 2010, http://www.reuters.com/article/2010/11/21/yemen-qaeda-idUSLDE6AK01H20101121.
[11] Josh Barbanel, Andrew Grossman and Sumathi Reddy, "From New Citizen to Suspect in a Year," *Wall Street Journal*, May 5, 2010, http://online.wsj.com/article/SB10001424052748703866704575224451665380256.html.
James Gordon Meek, Judith Crosson, Rocco Parascandola and Larry Mcshane, "A Dozen On Constant Watch Including Najibullah Zazi In FBI's Terrorist Probe," September 18, 2009, http://articles.nydailynews.com/2009-09-18/news/17931114_1_najibullah-zazi-fbi-law-enforcement.

[13] The Financial Action Task Force Report, February 29, 2008, highlights the low costs associated with direct operation support.
[14] *Ibid.*, the Financial Action Task Force Report does draw the distinction in scale and scope.

Homeland Security Policy Institute • 2300 Eye Street, NW • Suite 721 • Washington, DC 20037
202-994-2437 • www.homelandsecurity.gwu.edu