The Future of Terrorist Financing: Fighting Terrorist Financing in the Digital Age

SEAN PAUL ASHLEY, PRINCETON UNIVERSITY

Abstract

The principal concerns of anti-terrorist financing (ATF) reforms thus far have been the seizure of al-Qaeda’s assets, increased regulation of financial institutions and the use of blacklists and sanctions against non-compliant states, terrorist groups and supporting financial entities. With the success of post-9/11 ATF reforms, al-Qaeda has increasingly moved away from traditional financial institutions to alternative financial networks. This includes the expanded use of digital networks as a source and means of circulating terrorist funds. Troublingly, online transfers, mobile banking and digital currencies et cetera challenge many post 9/11 ATF reforms. Simply put, the digital arena is not subject to the effective regulation of established financial institutions. Digital transactions and transfers are poorly regulated, highly anonymous and difficult to trace, making them resistant to seizure, sanctions and surveillance.

The central question is whether post-9/11 reforms are adequate to protect the United States from evolving digital means of terrorist financing, and how these reforms have been challenged. This paper will evaluate the challenges that digital transfers and transactions pose to post-9/11 anti-terrorist financing efforts and to discuss the need for initiatives targeting the digital networks that can be exploited by terrorist financing. Particular attention will be paid to the dangers posed by digital currencies such as BitCoin, the Younis Tsouli and Babar Ahmad cases of digital terrorist funding, and the global proliferation of mobile banking services. Finally, recommendations will be made to address the weaknesses in post-9/11 ATF reforms through expansion of legal instruments, international cooperation and technological innovation.

Sean Paul Ashley is a junior from Kingston, Jamaica. He is currently majoring in politics at Princeton University with a focus on international relations, as well as pursuing a certificate in African-American studies. He attended boarding school at Deerfield Academy. At present, he is researching the military stalemate in the Syrian uprising and is in the middle of writing commentary on strategy in the Indian Ocean and the KONY 2012 campaign. His academic interests include regime change, fragile states, and American primacy. Sean serves as a student commentator for the Lichtenstein Institute on Self-Determination, an editor of Voices of Africa magazine, a staff member of the Nassau Literary Review and a member of Whig-Clio. He enjoys his leisure time in revelry as a member of the Glorious Tiger Inn.
Introduction

“Money is the oxygen of terrorism”.

Former United States Secretary of State, Colin Powell

Terror isn’t cheap. On the face of it, the numbers say otherwise. The most ambitious of terror attacks, those of September 11, 2001, were estimated to only cost about 500,000 dollars. The 2002 Bali bombings cost a tenth of that, and the suicide attacks USS Cole bombings in October 2000, which killed 17 and injured 39, cost a mere 10,000 dollars (Prober 2005, 1). However, numbers notwithstanding, the idea of cheap terrorism is specious.

Actual execution of a terrorist attack is only the tip of the iceberg, with estimates of cost mostly focusing on admittedly cheap materiel. As such, gauging the costs of terrorism through terrorist attacks severely undervalues the underlying “substantial structural costs of maintaining [a terrorist] organization” (Miguel del Cid Gomez 2010, 2). Terrorist attacks are simply the overt physical product of an extensive, covert terrorist organizational infrastructure. Terrorism requires substantial funds for planning terrorist attacks, training and recruiting operatives, disseminating propaganda, providing transportation, preserving channels of communication, supporting satellite organizations and subsidizing living costs of terrorist operatives. In the case of al-Qaeda, these operations necessitated funds of roughly 30 million US dollars annually (Greenberg, Roth, and Wille). Further substantiating the financial scale of terrorism, economist Loretta Napoleoni estimates that “economic activity related to terrorism accounts for a staggering $1.5 trillion, or 5 percent of annual global output” (Cowell 2003). It has been estimated that of al-Qaeda’s income, “about 10% [is spent] on operational costs. The other 90% goes on the cost of administering and maintaining the organization” (Biersteker and Eckert 2008, 8).

In short, significant funds and the maintenance of a sound financial infrastructure are of vital importance in preserving a robust and effective terrorist organization. Accordingly, the effort to detect and disrupt terrorist financing is a critical campaign in the War on Terror. In recognition of this fact, a number of post-9/11 reforms were enacted to attack the terrorist financial infrastructure, using methods of bank regulation, asset seizure, sanctions and surveillance to this end. By several accounts, anti-terrorist financing (ATF) reforms have been effective. The 9/11 Commission “report card” issued ATF efforts an A-minus grade, and the Treasury claims to have effectively frozen 140 million dollars in assets post-9/11 (Kaplan 2006).

However, the successes of the War on Terror and ATF reforms have had an unintended consequence – the mutation of the organizational structure of terrorist organizations (Biersteker and Eckert 2008, 59). Al-Qaeda for one has proven to be extremely plastic in adapting to current efforts; with the fortification of formal
banking institutions, the decimation of their foregoing leadership, and the destruction of physical operational bases, al-Qaeda has become disaggregated, decentralized and deterritorialized. This, in conjunction with rapid global dissemination of technology and global access to digital networks, has allowed “terrorist groups to almost seamlessly transition from the battlefields of the Middle East and Northern Africa to the virtual [environment] of the Internet” (Landman 2009, 8). Such a fact poses a grave challenge to post-9/11 ATF reforms. Digital transactions and transfers prove highly resistant to traditional counter-money laundering (CML) tactics of seizure, sanctions, surveillance and regulation. The central question addressed herein is whether post-9/11 reforms are adequate to protect the US from evolving digital means of terrorist financing, and how these reforms have been challenged.

This paper thus analyzes the various threats posed by digital networks in facilitating terrorist financing, assesses the resulting vulnerability and limitations of current post-9/11 ATF reforms and proposes further reforms to mitigate the digital threat. First, the background of terrorist financing, prior to and immediately following 9/11 will be described, as will its role in shaping post-9/11 ATF responses. Second, the role of the War on Terror, and post-9/11 ATF reforms currently in effect in decentralizing terrorist financial and organizational structures will be explored. Then the convergence of digital networks and terrorist financing will be analyzed wherein specifically, two broad areas are identified: Internet use and mobile banking. The respective challenges both pose to current reforms will be addressed, and proposals for further reforms to address said challenges raised. Finally, possible challenges to the reforms proposed will be anticipated and explored, and concluding remarks given.

The Anatomy of Terrorist Financing

How does terrorist financing work? The anatomy of the terrorist financial infrastructure can be divided into two basic parts: the sources of terrorist funds and the mechanisms by which these funds are circulated and transferred. The main sources of terrorist funds, centrally that of al-Qaeda, are as follows:

1. Charities – The bulk of al-Qaeda’s wealth stems from its “continuous fund raising efforts” and vast charity network (Greenberg, Wechsler and Wolosky 2002, 1). Charities are both highly attractive and highly susceptible to terrorist exploitation. For one, the sheer number of charities in the Islamic world, tens of thousands, prohibits effective surveillance and regulation. Second, the veil of legitimacy conferred by the charitable façade allows terrorists to solicit funds from unsuspecting donors (Levitt and Jacobson 2008, 10). Third, the Islamic tradition of zakat – the donation of 2.5 percent of one’s yearly income to mosques and charities – ensures a steady influx of funds. With no official law requiring records of zakat, which usually takes the form of cash donation, corrupt officials and radical clerics may easily turn it to terrorist ends (Rudner 2006, 44). Finally, the presence of charities in high-risk
conflict zones deters law enforcement and allows terrorists to easily transfer arms and personnel into these areas (Levitt and Jacobson 2008, 10).

(2) Crime – Terrorists profit extensively from a diffuse array of criminal activities. The DEA definitively links “19 of the 43 designated foreign terrorist organizations, to the global drug trade.” With a 300 billion dollar global drug market, and suspected al-Qaeda investment in heroin production and trafficking via the Golden Crescent, crime is a deep financial well from which terrorism can draw (Levitt and Jacobson 2008, 9-10). Terrorists have also profited from credit card fraud, theft, smuggling and kidnapping (Bruno 2010).

(3) Legitimate businesses/wealthy financiers – Terrorists operate a network of legitimate businesses. From al-Qaeda owned honey shops in Yemen, to the allegedly vast Bin Laden business empire, legitimate business provide terrorists with a convincing cover and salary, generate revenue, and may be used to conceal the transportation of terrorist materiel, alongside legitimate goods (Kaplan 2006).

(4) State sponsorship – Though few terrorist organizations enjoy state sponsorship in the traditional sense, the importance of implicit, and occasionally explicit, state support cannot be discounted. Extensive Iranian sponsorship of Hamas and Hezbollah is well documented (Levitt and Jacobson 2008, 13). Even states providing physical safe havens, such as Sudan, Lebanon and Pakistan, provide access to lucrative and ill-regulated financial environments in which terrorist activity can proceed unchecked (Martin 2006, 38).

Further complicating the task of detecting and disrupting terrorist financing, are the means by which al-Qaeda circulates funds. The three main means of circulation are

(1) legitimate financial institutions,

(2) Hawala and other informal value transfer systems (IVTS's) and

(3) physical movement through cash smuggling and couriers.

The latter two both obfuscate the source of terrorist funds and bypass formal regulatory procedures. In summary, the infrastructure of terrorist financing has been and still continues to be global in scope, vast in scale, diverse in sources, and exploitative of vulnerable financial environments.

The post-9/11 ATF response to terrorist financing, however, was not privileged to the structural and financial workings outlined above. Rather, the lens through which terrorist financing was initially viewed was 9/11, which has effectively shaped the entirety of ATF reforms (Kaplan 2007). Second, 9/11, though an isolated incident, gave significant, though limited, insight into certain financial and organizational workings of al-Qaeda at the time: its core organizational structure was localized to Afghanistan; charities and wealthy financiers formed the backbone of al-Qaeda's wealth; and al-Qaeda's assets had extensively penetrated formal, legitimate financial
Institutions. In the case of 9/11, roughly 300,000 dollars of al-Qaeda’s 500,000 dollar budget had entered and circulated within the formal US financial system. The 9/11 terrorists used entirely mundane methods of asset transfer and circulation including wire transfers, cash and travelers checks and withdrawal using credit and debit cards (Greenberg, Roth and Wille, 3, 13).

Accordingly, the US ATF reforms took, broadly speaking, three main approaches: seizure, sanctions and surveillance. These approaches were largely consonant with the facts known above; they attempted to redress the regulatory failings of financial institutions, freeze known terrorist assets and attack charities and individuals suspected of financing terrorism. Critical reforms included the Executive order 13224 and IEEPA Emergency Powers Act, which both authorized the president to freeze funds, consonant with national security. The extensive use of Office of Foreign Assets Control (OFAC) sanctions against “specially designated nationals,” including charities and nonstate actors, provided the US with a broad charter to cut off diverse sources of terrorist funds (Greenburg, Roth and Wille, 8, 37). Moreover, increased use of US-backed blacklists leveraged pressure on noncompliant states and entities to emulate US financial reforms that fortified formal financial institutions, targeting fragile global banking practices – as indicated in the case of the American wing of the Arab Bank, which was charged with a 24 million dollar civil fine for failing to implement adequate regulatory mechanisms (Catan 2010).

In regards to banking reform, the United States has prosecuted the War on Terrorist Financing most aggressively, by instituting formal procedures for the surveillance, regulation and documentation of financial transactions. From Know Your Customer policies, to Article III of the USA PATRIOT Act of 2001— which includes “special measures” to strengthen the Bank Secrecy Act (BSA) — formal banking institutions have become the focal point of ATF efforts. The use of the BSA, originally an article of counter-money laundering (CML) legislation, was replicated in the adaptation of multiple CML legislative articles for purposes of ATF (Weiss 2005). Finally, in 2006, the US executed the Terrorist Finance Tracking Program. This included US clandestine surveillance of global financial institutions in the Society for Worldwide Interbank Financial Services (SWIFT) database, which resulted in the apprehension of Riduan Isamuddin, mastermind of the 2002 Bali bombings (Litchblau and Risen 2006). In short, the US used legislative, regulatory and executive reforms, as well as enterprising use of technology to prosecute the War on Terrorist Financing, particularly in the formal financial sector.

At face value, the statistical toll US ATF reforms have taken on terrorist financing is impressive. In both the strengthening of the BSA and adaptation of CML legislation, control and regulatory mechanisms crucial to identifying terrorist funds have been implemented. The National Commission on Terrorist Attacks Upon the United States asserts that “worldwide, more than $136 million, including $36 million in the
United States, has been frozen” (Greenburg, Roth and Wille, 45). OFAC sanctions have also had a telling effect. As of 2008, the US Treasury reports the blacklisting of 472 individuals and 44 businesses. Former US Director of National Intelligence, Admiral Michael McConnell claimed that post-911, “al-Qaeda has had difficulty in raising funds and sustaining themselves” (Jacobson and Levitt 2008, 40). It seems that current US ATF reforms have managed to both identify and neutralize terrorist capital within its borders, as well as significantly weaken al-Qaeda through disrupting its financial structure. The US Treasury Department asserts that al-Qaeda is in its worst financial position thus far (Miguel del Cid Gomez 2010, 4). Nevertheless, as satisfying as the triumph may seem over terrorist financing, it is both limited, and more disquietingly, fleeting.

While US ATF efforts have admittedly been effective in policing the licit economy and formal financial sector, and even compelling international compliance with US standards, this is quite possibly a Pyrrhic victory. If one considers the facts, one estimate places 140 million dollars of assets frozen as roughly 10 percent of al-Qaeda’s proceeds (Acharya 2009). If we assume that US formal banking regulations have identified a large portion of al-Qaeda’s assets circulating within banks, this indicates two things. First, that al-Qaeda’s assets, while damaged, are still considerable. Though secondly, this indicates that al-Qaeda has shifted towards using the means and mechanisms of the terrorist financial infrastructure that exist beyond the licit channels. US anti-terrorist financing efforts, while “closing channels to the legitimate international economy…only open up new ones to the illegal one” (Napoleoni 2005, 208). The gravity of this shift in al-Qaeda’s financial infrastructure cannot be underestimated. In fact of the matter, it indicates a larger, and extremely exigent threat: the evolution of al-Qaeda’s organizational structure.

**The War on Terror and Decentralization of al-Qaeda’s Financial Structure**

In terms of both organizational and financial structure, al-Qaeda has mutated in three main fashions:

1. First, it has become massively decentralized, having suffered the destruction of its hierarchical structure, as well as its capacity to control financial operations. The War on Terror has inflicted massive casualties on al-Qaeda’s organizational structure. In one respect, terrorists have been severely deprived of territorial sanctuary. Military action has largely neutralized Afghanistan as al-Qaeda’s operational base. Moreover, core al-Qaeda leadership has been decimated. With over 80 percent of its operational membership having been killed or captured, al-Qaeda has abandoned almost entirely a commander-cadre structure (Biersteker and Eckert 2008, 55). Deprived of physical havens, especially in Afghanistan, al-Qaeda can no longer operate its training camps, political partnerships and local funding networks with ease. This, in conjunction with the physical destruction of its hierarchical structure, has inhibited al-Qaeda’s “central’s oversight of affiliated networks such as al-Qaeda
in Iraq, al-Qaeda in the Islamic Maghreb, and al-Qaeda in the Arabian Peninsula.” Financially, this has had impact. Once, al-Qaeda “directly funded and controlled operations from its base in Afghanistan” (Bruno 2010). Now, central command no longer funds terrorist operations as it did previously.

(2) Second, as a result of this physical dismantling of central command structure, al-Qaeda has disaggregated and has adopted a “cellular” structure spanning the globe. Both its inner circle and vertical chain of command have been destroyed, correspondingly reducing its ability to exercise control over satellite groups. Despite these losses, al-Qaeda is not dead – quite the reverse. According to Head of the International Centre for Political Violence and Terrorism Research, Rohan Gunaratna, terrorism has entered a new chapter in its lifecycle: that of global jihad (Bruno 2010, 47). Many cells, such as those responsible for the Madrid bombings, though ideologically affiliated with al-Qaeda, are operationally discrete. The al-Qaeda of 2001 has fragmented into a diffuse jihadist movement.

(3) Thus, finally, and most disquietingly, we arrive at the de-territorialization of terror. The necessity of maintaining global jihad in the absence of physical refuge has caused terrorism not only to metastasize, but also, to become virtualized.

The former two mutations, as well as US ATF reforms, have correspondingly altered the terrorist financial infrastructure. Critically, there has been a move by terrorists away from the use of formal banking institutions and towards nontraditional, illicit methods of obtaining and circulating finances. Terrorist groups have become increasingly fissile, self-sustaining and criminally adept. In contrast to the direct funding approach that financed the 1989 and 2011 al-Qaeda attacks, the 2005 London bus bombings were entirely self-financed through criminal activity (Jacobson and Levitt 2008, 13). Matthew Jacobson reports that since the crackdown on banks, there has been “a shift away from banks to terrorists using cash, to terrorists using cash couriers, to terrorists using Hawala” an informal remittance system common in the Middle East where funds are provided to an operator in one country, and disbursed by another abroad, “…and other informal financial-transfer mechanisms” (2008). The increasing use of the unregulated sector of the economy helps explain the steep decline in the seizure of al-Qaeda’s assets, the bulk of which “took place in the first two years after 9/11” (Solomon 2007). In Yemen and Somalia, terrorists have turned to “petty theft, credit card fraud, and narcotrafficking” to generate and circulate cash (Bruno 2010). More ambitious efforts, such as the suggested al-Qaeda attempt to “transfer its traceable assets into non-traceable conflict diamonds from Charles Taylor’s Liberia to the polished diamond market in Antwerp,” further corroborate this trend (Solomon, 2007).

More and more, terrorists are frustrating US ATF reforms with the simplest tactic: avoiding banks. US ATF reforms, combined with lack of core al-Qaeda support and the disruption physical sanctuary in which charity diversions can be
conducted with impunity, obliges terror groups to avoid banks and use crime in order to assume financial autonomy.

The two phenomena, the physical devolution of terror, and the shift to illicit methods of financing, pose a critical threat when one considers how the two function in conjunction with the global dispersion of modern technology. As digital technology penetrates thinly policed corners of the globe, digital methods of terrorist financing promise to make current US ATF reforms obsolete.

**The Convergence of Digital Networks and Terrorist Financing**

In a 2005 letter to late Iraqi al-Qaeda leader Abu Musab al-Zarqawi, Ayman al-Zawahiri wrote, “We are in a battle, and more than half of this battle is taking place in the battlefield of the media” (Theohary and Rollins 2011, 3). Zawahiri is correct: the Internet has become a critical asset to terrorists in training, recruitment, dissemination of propaganda and creating channels of communication. Stephen Landman cites a study that claims that “by 2000, virtually all terrorist groups had established their presence on the Internet” (Landman 2009, 11). Internet chat rooms have become breeding grounds for radicalization and the exportation of jihadist ideology. In the virtual marketplace of ideas, the influence of al-Qaeda extends far beyond its original physical reach. The global proliferation of Internet access has been extensively used as a conduit to bypass international boundaries. This has ominous consequences for the War on Terrorist Financing.

If the theater of the War on Terror has shifted significantly onto “the battlefield of the media,” the same ought to be expected of the War on Terrorist Financing. In the same way that the Internet has allowed information to move across boundaries, digital technology has transformed the way money moves across borders (Solomon, 2007). As a 2006 National Intelligence Estimate warned, “groups of all stripes will increasingly use the Internet to obtain logistical and financial support” (Jacobson 2010, 355). With terrorists possessing growing Internet access and aptitude, compounded with the constant exigency of raising and circulating funds, the integration of digital networks and terrorist financial infrastructure must be recognized as a leading threat to the War on Terrorist Financing.

As scholar Michael Judy notes, for terrorists the digital arena can easily be thought of as the virtual parallel to physical safe havens. Judy defines these “virtual havens” as “those non-physical areas which constitute a threat to the U.S. national security interests whereby terrorists are able to organize, plan, raise funds, communicate, recruit, train and operate in relative security … through physically diffuse networks consisting of local and wide area computer networks, mobile phone systems, media communications outlets, informal transaction and banking, and various forms of information dissemination” (Judy 2011, 35-6). This characterization indicates that, by virtue of its extensive global diffusion and lack of central oversight, the Internet is
the structural analogue and natural ally of terrorist financial networks. The proceeding discussion of the possible convergence of digital networks and terrorist finance divides the digital threat furthermore into two main categories: exploitation of the Internet and mobile banking. The particular challenges each poses to current ATF reforms will be discussed, and finally a final assessment of US ATF capabilities, in view of the digital TF threat, will be given.

**The Convergence of Digital Networks and Terrorist Financing: the Internet**

Exploitation of the most obvious digital avenue for terrorist funds – direct solicitation through websites – had already begun pre-9/11. In 1997, Babar Ahmad, a British terrorist ran the website Azzam.com, with the explicit purpose of financing terror. Babar, seeking support for the Chechen Mujahidin and Afghan Taliban, claimed that the “first and most important thing that Muslims can do in the West is to donate money and to raise it amongst their families, friends and others .... [F]or someone who is not able to fight at this moment in time due to a valid excuse they can start by the collection and donation of funds” (Jacobson 2009, 18).

Though Babar’s use of the Internet in 1997 was both crude and unconcealed, it remains an effective TF strategy. For one, no reforms were passed following the discovery of Ahmad’s websites, leaving channels of direct Internet solicitation open to exploitation. Indeed, charities, which have played a crucial role in funding terror, have employed the Internet to this end using this very same method. The Global Relief Foundation and Al-Haramain Islamic Foundation, both of which have been blacklisted by the US, operated websites that actively solicited donations, with donors able to pay through credit and debit card, and wire transfers, among other means (Jacobson 2010, 356). The hazard this poses to US ATF efforts is better illustrated by the case of the Internet presence of the Union of Good, hosted by UK-based organization, Interpal. Despite both being blacklisted by the US, the UK has not designated the two as terrorist threats. Thus, both currently operate. With the Internet placing terrorist assets outside US jurisdiction, US blacklists no longer have teeth. Furthermore, just as physical charities can be shut down and then later reopened, their websites can be hosted and operated from an infinite number of locations, and by any number of people (Jacobson 2009, 18).

Nevertheless, websites soliciting direct payment have two exploitable weaknesses, although the increasing use of crime to self-fund terror cells lends itself to evading detection by such means. Namely, both IP addresses and the use of credit or debit cards can provide substantial ownership information. Credit card fraud and identity theft have often been used to escape detection through such means. In the case of Younis Tsouli, for example, stolen credit card numbers were acquired through the Web, the money from which was then laundered through upwards of forty gambling websites (Jacobson 2009, 355). At the time of his arrest, Tsouli, with his partner, Tariq al-Daour, made more than 3.5 million dollars in charges. It is Tsouli’s motive
as much as his method that is of interest; he needed to purchase larger bandwidth for the maintenance and construction of websites disseminating al-Qaeda in Iraq (AQI) propaganda. This indicates the Internet is beginning to serve as an instrument of terrorist funding as well as recruitment, training and communication.

Moreover, the Tsouli case is emblematic of how the current “cellular” model of global jihad complicates the War on Terrorist Financing. Tsouli maintained ideological rather than economic connections to core al-Qaeda, necessitating the use of crime. The growth of criminal funding among terrorists is compounded by increasing Internet aptitude, which logically lends itself to criminal use. The absence of Internet regulatory mechanisms makes for easy execution of credit card fraud and money laundering. As evidenced in the fact that Tsouli never met his co-conspirator, al-Daour, in person, it is furthermore important to note that global jihad increasingly substitutes the Internet for face-to-face contact. The anonymity afforded by use of digital networks is anathema to current ATF reforms. Fortification of the formal financial sector has, in large part required the implementation of Know-Your-Customer policies, as well as required offshore institutions to keep detailed financial records of account ownership. However, with the Internet removing face-to-face interaction, or the need for identity verification, these policies, while effective in formal institutions, have no teeth in the digital arena.

The proliferation of “virtual worlds” on the Internet illustrates the ease with which terrorists might exploit the absence of face-to-face interaction. According to Steven Landman (2009), virtual worlds are “computer based simulated environments where millions of users can interact with each other on a daily basis” (17). Usually in the form of popular games, such as World of Warcraft, Farmville and Second Life, these virtual worlds are completely anonymous, requiring usually only an email address to access. Disquietingly, virtual worlds also possess robust virtual economies in which virtual currencies can be used to purchase in-game, and real world items.

The vulnerability of such a system is glaring and dangerous. Through use of credit, debit, or prepaid cards — which as the Tsouli case demonstrated, are easily obtainable through crime — users may purchase virtual currency, and exchange this currency with other users. This currency can be then converted back to real capital. With no oversight, no regulation, no limits to the amounts transferred or converted, and no documentation of the transaction and completely opaque ownership structures, assembling critical information concerning the sender, recipient and amount of funds is as difficult as money laundering is easy. Further, as in the case of the Union of Good website, the international nature of these networks call into question the extent of US legal jurisdiction, and whether counter-money laundering or ATF measures can be implemented (Jacobson 2010, 356).

Finally, the expansion of virtual currencies outside virtual worlds further opens up avenues for terrorist exploitation through digital crime. Currencies such as
BitCoin and eGold are used solely for financial transactions. A DEA report puts it bluntly, “Digital currencies provide an ideal money laundering instrument because they facilitate international payments without the transmittal services of traditional financial institutions” (Department of Justice 2008). The same issues accompanying virtual currency use inside virtual worlds arise in transaction-oriented digital currency programs. They are unregulated and undocumented, and allow unlimited sums to be exchanged. Uncertainty about the reach of US legal jurisdiction allows these programs to claim exemption from US regulation and oversight. The international nature of digital currencies highlights another possible threat. Digital currencies “[enable] standardized international financial transactions” which, combined with speed and anonymity, is attractive for money launderers. Considering the fact that terrorism is increasingly funded by the proceeds of crime, virtual currencies are ripe for terrorist exploitation. Additionally, anonymity is a central attraction of digital currency networks. Digital currency accounts “can…be funded with varying degrees of anonymity by mail and over the Internet, using electronic money orders (EMOs), checks, and online banking transfers” (Department of Justice 2008).

**The Convergence of Digital Networks and Terrorist Financing: Mobile Banking**

Exacerbating the digital TF threat posed by the Internet is the rapid global proliferation of mobile banking technology. Similar to digital financial networks on the Internet, mobile banking, or m-banking is largely lacking regulatory mechanisms. However, the danger unique to m-banking is its escalating popularity in the global South. Unlike many of the e-payment systems discussed previously, m-banking is perceived to be “a much more significant driver of development and economic growth in the developing world” With companies such as Kenya-based Safaricom and Vodafone, as well as the GSM Association (GSMA)— an organization “representing over 700 GSM mobile phone operators across 218 countries of the world”— expecting to extend m-banking services to hundreds of millions of users in the Global South in the near future, the mobile remittance market may approach 1 trillion dollars within the span of years m-banking, as it currently functions within the global South, is hugely problematic for the War on Terrorist Financing. Critically, the diffusion of m-banking across the fragile states and the global South allows for small and diffuse cross-border transactions to be conducted in areas “where terrorist and extremist activities are significant” (Solomon 2007). M-banking, as will be explored below, exacerbates the vulnerability of said areas to terrorist exploitation and criminal activity.

First, M-PESA, Vodafone’s m-banking service, “allows its users to load money on their mobile devices by making deposits with M-Pesa agents residing in rural and remote areas with limited or no banking facilities” (Villasenor and Monk 2011, 11). The use of local agents and intermediaries in lieu of formal banking, and indeed
in lieu of even possessing a bank account, allows for unscrupulous falsification of documentation. This lack of formal oversight may allow funds of all sums to pass unnoticed. Second, the sheer scope of predicted m-banking remittances assures the presence of criminal funds. Without the regulatory mechanisms to detect and deter criminal funds, m-banking becomes attractive to criminal, possibly terrorist, actors (Villasenor and Monk 2011, 12).

Additionally, with some of these m-banking providers located in the global South, even formal regulatory mechanisms, after which m-banking regulation could be modeled, would likely be less strict than US standards. On a related note, considering the poverty of its targeted market and the expanse of the m-banking network, funds are both small and diffuse, both of which make tracking difficult. Finally, the global South, with its burgeoning Islamic population, poverty and absence of social welfare, is a breeding ground for radicalization. Considering that terrorist organizations have often gained legitimacy through the provision of social service, the presence of both weak states, and substantial Muslim populations in East and North Africa, makes m-banking particularly susceptible to terrorist exploitation.

As demonstrated, the spread of m-banking, assures that “the network of devices available for possible use in illicit financial transactions includes not only every Internet-connected laptop computer, but almost every mobile telephone as well.” With its appeal within the global South, combined with its international scope, and its near-total absence of regulatory mechanisms, m-banking has transformed every mobile device into a potential instrument of terrorist funding.

In summary, US ATF efforts are massively underequipped to protect the US from penetration from digital means of terrorist financing. Both Internet-based financial networks and m-banking pose a laundry list of debilitating problems. They facilitate opaque financial transfers involving highly anonymous, unverified parties with a lack of face-to-face interaction. Nonexistent regulatory oversight is compounded by the absence of documentation. With the transnational scale of digital methods possibly placing them outside the jurisdiction of US regulations, there are legal obstacles to implementing potentially useful US ATF legislation. Finally, the integration of crime, specifically narcotics trafficking, money laundering operations, and credit card fraud, with digital transfer systems provides a convenient environment in which the crime-terror nexus can be exploited and surveillance avoided. Finally, with the sheer speed of transactions allowing for monetary transfer of possibly unlimited sums, terrorist funds can change hands across countries instantaneously.

Proposed ATF Reforms

The fact of the matter is that the digital evolution of TF is rapidly outpacing an increasingly obsolescent TF campaign that has yet to adapt in tactics and strategy to the digital frontier. The emergence and proliferation of new technologies is
outpacing regulatory mechanisms to protect them against financial exploitation. For the War on Terrorist Financing to remain effective in detecting, deterring and disrupting terrorist financing, a number of approaches must be taken. Common to all is a cognizance of the exigent threat posed by both the virtualization and the globalization of terrorism. By implication, new ATF reforms extend beyond the legislative and domestic seizure, sanctions and surveillance strategy. Though these policies may be adapted to combat the digital threat, fighting the War on Terrorist Financing at the digital frontier warrants a global response and technological innovation. The United States must employ the legal instruments at its disposal, chiefly the BSA and Patriot Act to their fullest extent. Further the United States must strive to compel external powers, by virtue of “naming and shaming” and financial penalties, to adopt stricter standards of banking regulation. Closer to home, the state ought to collaborate with the private sector in innovating and implementing digital regulatory safeguards that both detect and defend against terrorist financing.

First, in order to negate the threat of websites soliciting terrorist finance, the US government may work in tandem with Internet service providers. Leveraging of government pressure against service providers who host said websites may be undertaken under “18 U.S.C. Section 2339B, [which] makes it a crime to provide “material support or resources to a foreign terrorist organization” (Greenburg, Roth, Wille, 31). Expansion of this legislation to include a provision regarding the aiding and abetting of material support to or resources to a foreign terrorist organization may go a long way in compelling internet providers to rigorously police websites they host, or pull the plug on suspicious websites. The US has to date used an effective, more amiable approach: simply asking Internet service providers to shut down suspicious websites (Jacobson 2010, 359). The two approaches would be even more effective if used in tandem.

In addition, the threat of websites soliciting terrorist financing can be negated by forcing online gambling sites, such as the ones exploited by Tsouli, to register as Money Services Businesses. Under the PATRIOT ACT Title III expansion of Banking Secrecy Act powers, “all individuals or entities that transfer money, no matter how formal or informal, must comply with all anti-money laundering and counter terrorist financing regulations” (Landman 2009, 41). Thus, as Landman notes, BSA legislation can be effectively used to compel US standards of regulation for all digital networks facilitating financial transactions, thereby including online gambling and virtual worlds, and virtual currency networks, three critically vulnerable areas identified above. BSA provisions would require these MSB’s to undergo Treasury registration, verification of customer identity, and preserve documentation “for transfers of more than $3,000” (Landman, 42).

While the remaining jurisdictional problems posed by virtual currencies and m-banking may not present themselves to legislative resolution, more aggressive
use of the OFAC “Specially Designated Nationals” list may compel international compliance with US interests. US blacklists have global weight by means of the “naming and shaming” of suspected terrorist-related financial entities discourages economic relationships with them. Even lesser-used and potentially very effective tools lay within the “special measures” section of the Patriot Act, and sections of the IEEPA “which empower the United States “to cut off foreign countries from U.S. capital markets” (Basile 2004, 180). This power may be especially effective in combating the m-banking threat from the global South. These countries, largely dependent upon trade with the US, may be compelled to crack down on irresponsible regulatory practices of m-banking service providers to which their country plays host. Even the drastic notion of conditional aid, contingent upon regulatory reform of m-banking services, may be an appropriate, albeit aggressive tool in mitigating the m-banking risk.

For virtual worlds, further proposed reforms are preemptive in nature. With the clear and present danger of terrorist exploitation, the US can act decisively in protecting virtual economies from terrorist finance. While bringing virtual worlds under BSA supervision is the first step in creating anti-money laundering regulatory mechanisms, extension and adaptation can only go so far. By fostering a culture of self-regulation, the US may accomplish informally what it currently lacks the technological means to do, that is regulating transactions within virtual worlds. By encouraging creators and players within Second Life and other virtual worlds to adhere to Know-Your-Customer policies when undertaking large transactions or when buying real-world items using virtual currency, the US may avoid financial abuse until more permanent technological solutions are found.

The ability to find permanent technological solutions requires governmental collaboration with the private sector (Villasenor and Monk 2011, 15). It stands to reason that those best equipped to implement regulatory safeguards are the creators of the online payment systems in question. Building relationships with the designers of PayPal et al. can only but assist US ATF efforts in understanding and possibly altering digital payment networks.

The US also ought not to hesitate in enlisting another technological agency in the private sector that has already been used to ATF ends: the Society for Worldwide Interbank Financial Services (SWIFT). In the 2001 Terrorist Finance Tracking Program, the Belgian-based SWIFT, which “provides electronic messaging services that direct financial transactions worth trillions of dollars a day…throughout the world” (Lormel 2006) granted the FBI, Treasury, and CIA access to its database. The information obtained, according to then-head of OFAC, Richard Newcomb, “identified the key leaders, fundraisers, businessmen, recruiters, companies, charities, mosques and schools that were part of the [al-Qaeda affiliate, Jemaal Islamiyah] support network,” leading to both capture and sanctions against several agents
responsible (Bender 2006). Direct access to SWIFT’s “communications platform [used] by more than 9,000 banking organizations in more than 200 countries” is of proven value and global reach (Bender 2006, 16). Further, SWIFT officials possess extensive experience in implementing regulatory safeguards for traditional financial institutions worldwide. SWIFT can thus be of critical aid by supplying personnel and technological assistance in addressing the digital TF threat.

Withal, the impact of intelligence reform cannot be underestimated. Intelligence is a critical tool in the ATF toolbox. Upgrades in both funding and technology to critical intelligence agencies, such as the NSA, will better signals intelligence. With al-Qaeda become increasingly adept at using tools of encryption to conceal illicit digital activity, maintaining cutting-edge SIGINT capabilities is imperative in keeping pace (Conway 2006, 9-30). The NSA, FBI, and DOJ all have various responsibilities in Internet surveillance and rendering terrorism-related websites inaccessible (Theohary and Rollins 2011, 7). In order to strengthen intelligence capabilities, there should be increased exchange between these offices, and the office of Terrorism and Financial Intelligence (TFI). In short, more cooperation is needed between the Treasury and other members of the intelligence community if financial intelligence “follow the money” strategies are to be effectively deployed against digital TF. Financial intelligence has proven useful thus far in detecting terrorist funds and disrupting the groups that aim to use them, and therefore further use of financial intelligence is desirable in the digital chapter of the War on Terrorist Financing (Rudner 2006, 50).

Most broadly, the US must level its attentions at the pursuit of a global campaign against terrorist financing. Acting in concert with global financial institutions, such as the IMF, UN and FATF, and partnering with other intelligence and law enforcement organizations, such as INTERPOL, and UK agencies (which apprehended both Babar and Tsouli), will shape the global response necessary to counter global jihad. Coordination of OFAC blacklists with those of the FATF and UN give greater global clout to all, impelling greater international compliance. Likewise, diplomatic initiatives as well as intelligence and personnel sharing will allow for a quicker, more standardized response to terrorist financing and shrink the global lacuna in the War on Terror. This global approach is far from being realized, though its realization would be a boon to the War on Terror at large, and a blow to global jihad.

Caveats of Proposed Reforms

Two main concerns are anticipated with regards to the reforms proposed above. First, privacy considerations militate against Internet censorship and aggressive legislative reform to that end. The introduction of S. 3480, the Protection of Cyberspace as a National Asset Act, in the 111th Congress raises questions as to the extent of appropriate governmental regulation of the Internet. Shutting down terror-related websites, chat rooms and forums to preempt potential financial transfers may
contravene first amendment rights. Certainly, a balance must be struck between individual rights and national interests, and yet, when potential terrorist funds can be transferred rapidly and anonymously through deregulated networks, it may be better to err on the side of caution rather than civil liberties. Further, it must be noted that web pages are the private property of Internet service providers and any decision on their part to censor or pull the plug on said websites, regardless of government encouragement, is perfectly legal.

Secondly, forced implementation of digital regulatory mechanisms, and the de-anonymizing of digital payment networks may broadly disrupt licit digital networks. Indeed, restrictions on m-banking may be seen as inhibiting the fiscal opportunities of the global South. However, the exigency of digital terrorist financing and existing counter-money laundering precedents make the situation clear: the cost incurred is well worth the benefits. Forcing regulation of digital economies and payment networks will benefit US interests, as well as set down precedents and technological solutions that lend themselves to responsible practices in digital transaction.

In conclusion, current ATF efforts thus far are in severe need of further reform. These reforms must seek to emulate and outpace the growth of terror, both globally, and into the digital world. With al-Qaeda adopting a cellular structure, terrorist financing is increasingly mobile, diffuse, and--without core-command and hierarchical organizational structures-- cheap. The resilience and plasticity of al-Qaeda’s financial techniques requires constant technological innovation, extensive digital regulation and the international extension of US policies and practices to their fullest extent. Only in this way can the War on Terrorist Finance be won.

References


Catan, Thomas. “Jordan Intervenes in U.S. Terror-Funding Suits.” The Wall Street


Miguel del Cid Gomez, Juan. “A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates.” Perspectives on Terrorism 4, no. 4 (2010).


