Securitising money to counter terrorist finance: some unintended consequences for developing economies

Abstract

With its roots in the ‘war on drugs’ and the criminalisation of money laundering, the global initiative to combat the financing of terrorism (CFT) provides one strategy for preventing and pre-empting terrorist attacks. In public pronouncements terrorist finance was named the ‘lifeblood’ and ‘oxygen’ for terrorism itself, thus displaying an analogy suggesting that its mere removal could bring an end to terrorism. Following the theoretical perspective of the Copenhagen School of security studies this paper argues that national and international measures against terrorist finance constitutes the ‘securitisation’ of money. By situating money as the essential component to an existential threat it was possible to justify extraordinary measures to monitor financial transactions. These measures produced unintended consequences prompting resistance and an evolution of procedures to reduce those consequences. This paper considers two affected areas (migrant remittances and financial inclusion) and points to the potential use of financial surveillance against grand corruption.
Securitising money to counter terrorist finance: some unintended consequences for developing economies*

Introduction

This paper considers the global dissemination of procedures to identify and seize terrorist organisations’ existing financial assets and to prevent the further financing of terrorism. Grounded in the response of the United States to the terrorist attacks of 2001, mechanisms for financial surveillance initially designed for a formal retail banking system evolved and then were extended to a variety of other potential sources for terrorist financing. And due to the transnational nature of the terrorist threat targeted by these procedures they must, perforce, be implemented globally. The efforts made to achieve global cooperation encountered resistance at several levels, necessitating that ‘money’ itself be securitised. For the context of developed economies this securitisation process was necessary to overcome resistance against mandated practices of surveillance presented by financial firms (over cost and customer privacy concerns) and by civil libertarians (over citizens’ liberty, anonymity, and encroaching state power). The process is exemplified in the story of the USA PATRIOT Act, composed of measures rejected by the US Congress several years prior to 2001 (USA PATRIOT Act, 2001; Vlcek, 2008a). And as explored in the later sections of this paper, for the context of developing economies there was resistance not only because terrorism and terrorist finance was not viewed as a direct security threat, but also the implementation of the financial surveillance mechanisms produced a number of unintended consequences. For the case of the developing economy, however, resistance to securitisation is less about securitisation for the local context and is situated more against the transnational securitisation process implemented through international organisations.

The initial move made to securitise terrorist finance was to identify it as the ‘lifeblood’ or ‘oxygen’ of terrorism and therefore the argument was that if states could shut down the flow of money to terrorist organizations then they would be deprived of the means necessary to operate. This view was at the core of President George W. Bush’s statement at the Rose Garden signing ceremony held on 24 September 2001 for his Executive Order freezing the assets of 27 individuals and groups accused of financing terrorism. With that Executive Order the President established a ‘financial

* An earlier version was presented at the international workshop, ‘The civil society-security nexus – facing the challenges of international terrorism and domestic resistance’, Department of Political Science, Stockholm University, Stockholm, Sweden, 2 - 4 May 2012.
front’ to his war on terror, declaring that the US was launching ‘a strike on the financial foundations of the global terror network.’ (Bush, 2001) This discourse on the nature and location of terrorist finance within the campaign against transnational terrorism is central to the securitisation of money operationalised as a tool against terrorism. It is not the aim for this analysis to provide yet another case study in support of securitisation theory. Rather it is to apply securitisation as a concept with which to understand the nature for the emphasis placed on the financial and monetary features of a security threat, and to use that understanding to assess the implications arising from mechanisms constructed to protect against a threat that may not in fact exist for some states. That is, to evaluate the implications from imposing measures against illegal money in states that do not feel directly threatened by illegal money nor any terrorist violence that could be financed by it. The objective for this intervention is to highlight those unintended consequences from these practices on a developing economy, to explain in part the rationale behind the resistance and limited cooperation demonstrated by developing economies to satisfy the security concerns expressed by developed states.

The structure for the paper is first to provide an overview for the nature of the threat found in illegal money, followed by a section explaining how this illegal money was then ‘securitised’. The third section provides an overview for the tactics deployed against terrorist finance before coming to the central section for the paper, which addresses several of the consequences from these tactics for a developing economy. This section is composed of three sub-sections, considering in turn migrant remittances, financial exclusion and grand corruption. The concluding section reflects on the implications from the practices of developed states threatened by 21st century terrorism to securitise money for the developing economy.

Overview for a security threat

Early concerns with terrorist finance focused on state-sponsored terrorism, in which a state government (Libya was a favourite example) provided funds, equipment, and training to a terrorist group. This situation was more common during the Cold War in the 1970s and 1980s, and an early attempt was made in Europe to track the financing of terrorism when the Council of Europe published a Recommendation in 1980 that outlined “Measures Against the Transfer and Safekeeping of Funds of Criminal Origin” (Council of Europe, 1980). The objective for the Recommendation was to identify and confiscate the profits from crimes that were committed by the leftist terrorist groups operating in Europe in the 1970s—including the Red Army Faction (a.k.a. Baader-Meinhof Gang) in
West Germany and the Red Brigades in Italy. These groups engaged in bank robberies and kidnappings to raise money to support their political activities, including bombings and assassinations. Similarly, the Irish Republican Army (IRA) was involved in criminal activities like bank robbery and illegal drug dealing to finance its political agenda (Horgan and Taylor, 1999; Horgan and Taylor, 2003). But in general, the Council of Europe was ahead of its time in this area and failed to generate much support for the initiative, individual European governments continued to follow their existing domestic strategies to counter these forms of domestic terrorism.

Concurrent with early efforts against terrorist finance were the efforts to deal with other forms of illegal money in the context of the US government’s “war on drugs”. As we are regularly reminded by films and TV shows, it’s hard to prove that the big-time criminal is actually involved in criminal activities, instead they are insulated by subordinates that do all the dirty (illegal) work. Consequently US government officials decided on a strategy to go after drug bosses in much the same way the FBI finally convicted Al Capone, through the possession of illegal money. Capone was convicted in 1931 on tax evasion, the logic of the case was that even though his income was illegal it was still necessary to pay income tax. The strategy from the mid-1980s has been to charge the drug trafficker with either possessing the illegal profits from drugs trafficking or to with attempting to make illegal income appear to have legitimate and legal origins. This crime of “money laundering” was established in the United States in 1986; the story behind the name is that it originated in the practice of a gangster who owned a number of Laundromats (Blum et al., 1998). It is a believable etymology, a laundromat is a cash-only business and the only way for investigators to determine if the declared income exceeded what the laundromat actually earned would be to have someone sit there counting loads of laundry going through the machines all day.

Regardless for its origins, the definition for the act of money laundering is straightforward, it is to take an action or series of actions in order to disguise the origins or ownership of the money. The definition over time has been expanded beyond money as cash, to include any convertible asset, including gold, jewellery, casino chips, and prepaid debit cards (Financial Action Task Force, 2012: 19). However, to make money laundering a felony charge in the United States does no good if it can be circumvented simply by crossing the border, depositing the funds in a foreign bank account, and then repatriating it to the US from the foreign bank. The US bank has to trust the foreign bank and hence treats the transfer as a completely legitimate transaction; instantly the money is clean and the efforts of the US government defeated. Obviously the problem must be addressed by an international solution and in turn the internationalisation of money laundering has served as a case
study on the emergence of a global governance regime. For Rainier Hülße, it is more than simply the production of a global governance regime, it is first and foremost a case for the production of a transnational problem requiring a transnational remedy. As he describes it, the issue of money laundering was first ‘problematised’, that is the nature of money laundering activity was constructed as a transnational problem which then required the creation of a transnational solution (Hülße, 2007: 166 – 168). Operating through the G7, the United States promoted the establishment of an international organisation to determine the parameters of the money laundering problem and then to produce the mechanisms to deal with it. The Financial Action Task Force (FATF, or Groupe d’Action Financière, GAFI) was created in 1989 and directed to study the techniques used to launder money. With this knowledge it then created procedures to prevent or discover the presence of money laundering in a national economy. Since 2001 the responsibilities of the FATF have been expanded to include producing measures to counter the financing of terrorism, for which it has produced additional methods and procedures for identifying and preventing terrorist finance (Financial Action Task Force, 2012: 7 - 9).

Defining what activity actually constitutes terrorist finance, however, is more problematic than money laundering, for example, does it make any difference before the law if the money used for a terrorist act had a legal source, rather than an illegal source? Consequently, while money laundering is all about the money that comes from criminal activities, terrorist finance may come from such ordinary and legal sources as charitable contributions, for example, passing around a collection cup at the pub. The point here is that money laundering is all about money that is already considered to be illegal, because it is the result of some preceding, or predicate, criminal act. Terrorist financing, on the other hand, may involve money that is legal because it was not connected to a crime until it has been used to commit an act of terrorism. In other words, it is ex post facto illegal, after the terrorist event. Subsequent to the 2001 terrorist attacks some US government officials identified this activity as “reverse money laundering” because moving money from a legal source to the illegal terrorist activity while concealing (and thus protecting) the legitimate source of the money also should be treated as a criminal act (Cassella, 2002: 11).

This issue then creates a corollary to Hülße’s ‘problematisation’ of money laundering to produce a mode of global governance. How may we overcome the problem raised by the use of ‘legal’ money for the terrorist act when that money, in itself, does not become ‘illegal’ until after the terrorist event? From this viewpoint, the presence of legal money creates a barrier to pre-emptive action against the financing of planned terrorist acts of violence or the emergence of a new terrorist group.
By securitising the money itself that barrier is removed, consequently the definition for terrorist finance relies on the intentionality of the actor for the use of the money—that they know that the money will be used for a terrorist offense. Once the action (donation, financial transfer) of the individual is determined to be intended for the support of a terrorist organisation or activity, the financial actions are illegal because terrorism is illegal. This chain of logic also makes the financial assets of the individual or group involved illegal.

Acting on behalf of its membership the FATF produces/reproduces rules and guidelines for dealing with this illegal money. The Forty Recommendations of the FATF on money laundering initially were drafted to operate in the formal banking system with which the individual authorial participants were most familiar, and therefore the Recommendations are not an easy fit for the variations on formal banking and the informal banking and financial services (e.g. hawala) that operate beyond the limited presence of formal banking in a developing economy (Vlcek, 2010). Further, the increased awareness that these informal value transfer systems exist and operate in the vacant spaces left by the retail branch banks in developed economies (i.e., to transfer remittances to Somalia) serves to frustrate the security officials attempting to cut off the movement of money to terrorists, suspected terrorists and potential terrorists. This is a case where it is not the actor or activity that is securitised, but rather the means necessary to accomplish the activity, which itself is only a threat under specific defined circumstances. As a result, however, all instances of financial exchange must be observed, monitored and recorded in order to assess its potential status as representing a threat.

To ‘securitise’ the terrorists’ money

Securitisation is the process of constructing a new security threat; new as in identifying an activity or actor not previously identified as the source for an external threat and consequently society now requires protection from it. As a process, securitisation involves an actor identifying the referent object, declaring it to be threatened and convincing the necessary audience that it requires protection from the activity or actor determined to be the source of the threat. Furthermore, this threat is normally found to be ‘existential’, in other words the threat is deemed so great as to bring about the end of the referent object (Buzan and Wæver, 2003: 491; Fierke, 2007: 102 - 115). For example, one perspective on money laundering is that it represents a threat to the safety and stability of the national financial system and consequently measures must be taken to prevent and suppress this activity in order to defend banking from the ill effects of dirty money (Alldridge, 2008:...
In the late 1990s the failure of the initial measures to significantly reduce illegal drugs trafficking meant that stricter measures were proposed in the US. But the threat to the banking system was not seen as an existential threat, sufficient to overcome the privacy concerns raised by opponents to the proposed new anti-money laundering procedures. As a result the US Congress refused to expand the scope of existing legislation, and in particular it refused to impose ‘Know Your Customer’ requirements on the banking industry. Dramatically, the case for stricter measures to pursue illegal money was reinforced in 2001 by the claim that enhanced anti-money laundering (AML) procedures would be equally effective against terrorist finance. Terrorism provided the existential threat sufficient to overcome the privacy concerns raised by civil libertarians and the banking industry, bringing to an end the existence of anonymous accounts and establishing the requirement to collect and maintain detailed information attesting to the identity of each account holder (Eckert, 2008: 210-211, 213-214).

Consequently, transnational terrorism should be understood as the existential threat to liberal democracies which is central to the logic behind the campaign to combat the financing of terrorism (CFT). Discussions on the financial aspects for this existential threat frequently include a reference to President George W. Bush’s ‘Rose Garden speech’ for the introduction of language framing the US-led efforts against terrorist finance in September 2001. The event marked his signature on Executive Order 13224 (Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism) with his assertion that ‘a major thrust of our war on terrorism began with the stroke of a pen. Today, we have launched a strike on the financial foundation of the global terror network.’ (Bush, 2001) President Bush made the further claim in his remarks that ‘Money is the lifeblood of terrorist operations.’ (Bush, 2001) A later public statement on 7 November 2001 announced the addition of further suspected financial supporters for al Qaida to the list of individuals and organisations subjected to US sanctions (and subsequently UN sanctions), including the identification of the Somali remittance firm al Barakaat. This firm was named as the ‘quartermasters of terror’ by government officials and together with the phrase contextualising terrorist money as the ‘lifeblood of terrorism’ these terms were reproduced extensively in US and foreign media (Hall et al., 2001; see, e.g. Bronskill et al., 2001; Cambanis, 2002).

The discourse of terrorist finance as the ‘lifeblood’ or ‘oxygen’ of terrorism was extensively critiqued by Ibrahim Warde (2007), who noted the difficulty in separating facts from fiction when apparent facts make for good headlines, e.g. Osama bin Laden’s personal fortune of US$300 million as the
source for al Qaida’s funding (Warde, 2007: 6 - 9). Such facts-by-repetition become embedded in the discourse, notwithstanding the efforts by some authors and even the 9/11 Commission to reveal the exaggerated status for this claim (Tupman, 2009; Roth et al., 2004). The characterisation that situates the finance factor of terrorism as its ‘lifeblood’ is highly dependent on the early claims for ‘guesstimated illicit flows in the trillions dollars’, which should be discounted because in fact only millions in assets have been frozen (Levi, 2010: 254). Further, in light of the surge of terrorist attacks globally in 2002 it has been argued that the initial surge to freeze and seize terrorists’ financial assets in late 2001 did little to remove this ‘lifeblood’ and reduce the capacity of terrorist groups to commit acts of terrorism (Warde, 2007: 154).

Nevertheless, the US government responded to the terrorist attacks in New York City and Washington, DC by constructing terrorism as an existential threat to the United States. Subsequently it is designated the money used to finance terrorism as an existential threat because of a logic that determined that money to be essential to the operation and functioning of a terrorist organisation. Collectively this process has served to securitise any money that possesses the potential for financing terrorism. But as suggested elsewhere the international campaign against terrorist finance appears to be much more about “Protecting the West” from terrorism than it is about addressing the root causes motivating terrorist actions as a means for pre-empting terrorism (Vlcek, 2008b). The pursuit of terrorist finance is represented as “vital to the process of ‘connecting the dots’ of potential terrorists and plots before they strike.” (de Goede, 2008: 97) Those dots, however, exist for the most part in the financial systems of the terrorists’ target states in Australasia, Europe and North America. Financial surveillance systems designed for a retail banking sector in Europe were ill-suited for an environment where formal banks serve a very small part of domestic society and implementing them distracts governments from other, locally more relevant, development activities (De Koker, 2005). Nevertheless, measures against money laundering and terrorist finance are directed by United Nations Security Council Resolutions as much as by the International Convention for the Suppression of the Financing of Terrorism for global implementation. Before assessing some of the implications affecting the developing economy from these procedures, the next section reviews some of the tactics developed for use against terrorist finance.
The tactics used to combat terrorist financing

In order to better understand the impact and consequences from the securitisation of money for the developing economy it is first necessary to situate the tactics and methods used in developed economies, because it is the nature of their fear of terrorism that permits and accepts the extensive surveillance assemblage created to make money safe (Haggerty and Ericson, 2000). The widespread recognition for the increased levels of government surveillance in society for over a decade has produced several modes of response. Obviously there is resistance to this surveillance as much as there has been grudging acceptance for the official government argument that more surveillance is necessary in order to defend society from criminals and terrorists. The unease found with the myriad forms of surveillance increasingly present in society may be seen in media representations for the possible danger from the misuse of surveillance technologies, including, for example, the American films *Enemy of the State* (1998) and *Eagle Eye* (2008). At the same time, there has been an almost exuberant embrace for the opportunity to provide open scrutiny of one’s personal life as represented by social networking websites like Facebook and LinkedIn, along with the persistent intrusion of personal minutiae possible through the medium of Twitter and Instagram. More relevant to a discussion on the use of surveillance as a defence against the terrorist is the experience of the conceptual artist Hassan Elahi. He responded to the persistent multiple interrogations by US officials that followed any of his post-2001 foreign trips by first informing the FBI of pending foreign travel and then simply announcing it to the world at large via the internet, now available at <http://elahi.org> (Lerer, 2006).

The topic of financial surveillance brings to the fore several problematic and possibly unintended consequences from the specific tactics deployed to identify illegal money. There are two main approaches in this financial war on terror as initiated by the US (Taylor, 2007: 12, 18). One approach is the imposition of targeted financial sanctions against known and suspected terrorists, their supporters and any person (natural and legal) who might provide funds to a terrorist organisation (de Goede, 2011; Heupel, forthcoming). The financial surveillance approach looks for suspicious transactions in order to bring the transacting parties to the attention of law enforcement and security services for closer inspection in order to determine if these transactions were intended to finance terrorism (Amicelle and Favarel-Garrigues, 2012). The mechanisms used were developed originally to identify criminal money and track down drug traffickers, now they are used to identify the money associated with any number of predicate crimes beyond illegal drugs and terrorism. The FATF released the first version of the Forty Recommendations on Money Laundering in 1990, outlining practices and procedures that should be implemented in national law in order to prevent...
and punish money laundering as a criminal activity. These criteria to combat money laundering were joined in 2001 by the Nine Special Recommendations to Combat the Financing of Terrorism. More recently, the Recommendations of the FATF were revised and reorganised into a document consolidating the special recommendations on terrorist finance with the previous forty recommendations targeting money laundering, The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (Financial Action Task Force, 2012).

Globally, the strategy is achieved by situating the FATF at the centre of a global network of ‘FATF-Style Regional Bodies’ (FSRBs) that are similarly ‘committed to combating money laundering and terrorist financing’ (see e.g. Financial Action Task Force, 2005). This approach has created a set of regional groups (now recognised as ‘associate members’ of the FATF) for mutual support as well as creating local peer pressure against money laundering beyond the membership of the FATF itself (Financial Action Task Force, 2006a: 4 - 5). Representative FSRBs include the Asia/Pacific Group on Money Laundering (APG), the Caribbean Financial Action Task Force (CFATF), and the Middle East and North Africa Financial Action Task Force (MENAFATF). As with the FATF, they promote anti-money laundering policies and facilitate co-operation among their member jurisdictions to identify and eliminate money laundering and terrorist financing operations. In essence, it was through this process that the Recommendations created by the FATF for its members in the early 1990s were reproduced over the past two decades as an international regime applicable to countries that are not members of the core FATF group. Illegal money, whether from criminal activity or intended for future terrorist activity, is re-produced as a problem or threat to be dealt with by everyone, everywhere. And in this fashion a securitisation process initiated in the United States has been reproduced globally.

More recently the FATF released a series of guidance documents presenting a risk-based approach to combat money laundering and terrorist finance in a number of business sectors. Starting from a document providing high-level principles and procedures on implementing a risk-based approach more specific documents were developed in cooperation with representatives from the affected industry (Financial Action Task Force, 2007; Financial Action Task Force, 2008; Financial Action Task Force, 2009). Areas covered include: legal professionals; accountants; trust and company service providers; casinos; dealers in precious metals and stones; and real estate agents. The risk-based strategy has been implemented through methods and controls more appropriate to the perceived level of risk within a particular population of customers/potential customers. In other words, rather
than treating everyone as a suspicious potential criminal/terrorist, each individual is measured for membership in a population already evaluated for its risk potential and the surveillance mechanisms are applied to an appropriate extent. Examples for this strategy in the context of developing economies are outlined in the next section.

**Consequences in developing states**

The impact for a developing economy, with its constrained resources and capabilities, to accomplish the full raft of regulations came to be recognised in time by the FATF as a problem for transferring its AML/CFT agenda to developing economies (Vlaanderen, 2009). One approach for overcoming the difficulty was outlined in the FATF document, ‘Guidance on Capacity Building for Mutual Evaluations and Implementation of the FATF Standards within Low Capacity Countries’ (FATF, 2008). The most beneficial feature for the developing economy in recent FATF guidance, however, may be the introduction of the ‘risk-based’ approach permitting the low-capacity jurisdiction to scale its implementation and enforcement efforts to fit the level of the perceived risk present in any particular market sector or with any particular financial product (De Koker, 2009b). The focus in many of the measures created to deal with money laundering and terrorist finance are firmly grounded on ‘knowing the customer’ (De Koker, 2005). Such knowledge comprises details about the person (natural and legal), their origins, source of income and destinations of payments, which serve to produce a ‘data double’ (Haggerty and Ericson, 2000). The knowledge also produces a network structure connecting the person to other persons that can provide traceability of financial flows to and from the known terrorist to the potentially unknown terrorist while also producing a pattern that may be compared to the already identified pattern (or profile if you wish) of a money launderer or terrorist financier. Consequently, this knowledge, collected through the process of ‘customer due diligence’, is a critical element for the procedures to combat terrorist finance (Financial Action Task Force, 2012: 14 - 16). The demand for information about a customer becomes a problem, however, when the transaction request is made of a person without the necessary identity documents, while the expectation for data collection and recording by informal businesses is similarly problematic. In particular this situation is a challenge for regulating migrant remittances, which in the past was largely via informal methods, and a challenge for efforts to promote financial inclusion when the persons currently ‘unbanked’ are also ‘undocumented’ (Shehu, 2012). These two issues are outlined in the next two subsections, followed by a subsection presenting a case that has been made for the beneficial use of AML surveillance and laws for investigations of bribery and corruption by government officials.
Facilitating remittances

One method accused of terrorist financing that received particular attention in the media, in part because it is so ubiquitous, is the use of an informal value transfer system to send money consisting for the most part of migrant remittances from a developed state to a developing state. For example, hawala, which is an ancient practice for informal transfer that operates through a series of trust relationships to transfer value across borders in the modern context (Vlcek, 2010: 436 - 439).

Informal methods of money transfer remain popular over the past decade even with the efforts directed by the FATF to formalise them, partly due to cultural familiarity since they frequently exist and operate within ethnic communities and also partly because they are able to reach remote destinations that lack local banking facilities. And as with many things in life the cost of the transaction also is important because remittances are commonly small amounts which make the use of a bank or a money transfer business, as a percentage of the amount of money transferred, fairly expensive. Consequently, adding a money transfer service to your small business could be a profitable side venture, if, for example, you are a travel agent specialising in travel to one of the leading destination countries for remittances (e.g. Pakistan, Philippines, India or China).

Nevertheless, it can be deduced from the data on migrant remittances flows provided in World Bank Development reports that there has been some success in the FATF-directed international effort to replace the use of unsupervised informal transfer methods with one that is monitored and tracked. There is a spike in reported remittances data in 2003 and significant annual increases in subsequent years that are not easily explained by economic causes; reported remittances for 2001 were US$ 96 billion, in 2003 there were US$ 145 billion, in 2005 US$193 billion, in 2007 US$ 278 billion, and for 2009 US$ 307 billion (World Bank, 2007: 54; World Bank, 2011: 17). And while this shift away from unsupervised informal transfer methods may have succeeded in making it more difficult for terrorists and money launderers to move money without the knowledge of law enforcement agencies, at the same time it represents a net cost increase for migrants to send money home. In turn the cost increase for the migrant from these measures leads to reduced welfare in the destination countries because more money is consumed in transfer fees paid to banks and money transfer businesses rather than going to support the migrant’s family and home community (Department for International Development, 2005).

Technological advances that have emerged in the past decade also provide new means and methods for migrant remittances (and potentially money laundering and terrorist finance) that can be more
cost-effective than using a bank wire transfer. The FATF is aware of the potential mis-use of new payment technologies, and released its first report on “New Payment Methods’ in 2006, considering internet and electronic payment systems operating outside of the traditional banking system and prepaid cards, which while replacing cash may remain just as anonymous as cash (Financial Action Task Force, 2006b). The specific measure directing the formalisation of informal value transfer, FATF Recommendation 14 (formerly Special Recommendation VI) is applicable for these new payment methods and it directs states to enact legislation to regulate informal (as in any non-financial institution) method used to transfer money or value (Financial Action Task Force, 2012: 17). The new technological method of interest here results from the expansion of mobile phone technology around the globe and the innovative uses achieved with mobile phones. Mobile money (m-money) involves the use of the mobile phone service provider to transfer money from one user’s mobile phone account to a second user’s mobile phone account. Appropriately for migrant remittances, the m-money service is structured to support small amounts, and the second user may be other than a family member, including for example shops, schools (for tuition fees), transportation providers (bus or taxi fares), utility companies and even local government offices (to receive welfare benefits as well as for paying local taxes). The emergence of m-money services as a low-cost method for migrant remittances and the incorporation of regulations against money laundering and terrorist finance for regulating these systems in the cases of Kenya and the Philippines is discussed in more detail elsewhere (Vlcek, 2011). The relevant aspects for this discussion concern the risk mitigation features intended to reduce, if not completely prevent, the use of the m-money service to transfer illegal money. Those risk mitigation features include a requirement for face-to-face contact with a service provider’s agent when establishing an m-money account, which includes the presentation of a government-issued form of identification, and the operation of low account limits for the size and frequency of transactions. These limits are scaled such that they are sufficient to the purposes of migrant remittances and the needs of low-waged (generally unbanked) customers while at the same time they hamper the use of an m-money account for money laundering and the requirement for positive identification serves to hamper their use by known and potential terrorist suspects.

This customer due diligence requirement to present an identification document to an agent for the m-money service provider was readily implemented in the Philippines and Kenya because of the widespread provision of government-issued forms of identification in these countries. Similar m-money services may not be as readily secured against money-laundering or terrorist finance in other jurisdictions where a similar level of formal documentation may not already be in place. For example, the limited dissemination of such documents in Tanzania served to constrain the expansion
of Kenya’s m-money service provider in Tanzania, because it attempted to maintain its ‘know your customer’ due diligence requirements.

**Overcoming financial exclusion**

While financial exclusion may arise from a number of causes, here the concern is for the barrier to financial services that is created by customer due diligence obligations. In other words, financial exclusion is a spill-over effect or unintended consequence produced by the ‘Know Your Customer’ requirements that are intended to identify possible terrorists, money launderers, and other likely criminal conduct. At the same time, requirements for identity documents, proof of residence and proof of employment mean that anyone unable to provide these documents will be denied service. In a developed economy this group denied access to financial services will include the undocumented migrant, unemployed and/or homeless citizen, and the transient university student. Meanwhile in the developing economy the excluded may consist of a larger segment of the population that includes people who did not previously need an identity document, those working in the informal economy, and those living in unofficial and informal residences. The objective behind financial inclusion, on the other hand, is to counter these effects and to promote access and use of financial services (Shehu, 2012: 308). A bank account is understood generally to provide a safer means to save money than an envelope under the mattress and access to more secure ways of transferring money than handing cash to an acquaintance to deliver to a family member back home. At the same time, financial inclusion anticipates the availability of access, that is a bank branch, post office or ATM; which is where the widespread access to mobile phones now offers new opportunities to increase financial inclusion.

In conjunction with its risk-based approach mentioned above the FATF produced a guidance paper to support ‘countries and their financial institutions in designing AML/CFT measures that meet the national goal of financial inclusion, without compromising the measures that exist for the purpose of combating crime.’ (Financial Action Task Force, 2011: 6) While this statement is supportive for these measures to facilitate financial inclusion in the context of the FATF Recommendations, the overriding concern for the organisation (and its more powerful member states) remains focused on security and the establishment and enforcement for a rigorous system to prevent money laundering and terrorist finance.

The Guidance is based on the important assumption that financially excluded and underserved groups, in both developing and developed countries should not be
automatically classified as presenting a lower risk for ML/TF, but could be lower risk depending on the various risk factors. (Financial Action Task Force, 2011: 6)

Recognition for the need to consider the implications from financial exclusion is present in the FATF view that ‘financial exclusion works against effective AML/CFT policies.’ In other words, financial exclusion motivates and maintains the informal and unregulated cash-based economy that is seen as producing ‘significant money laundering and terrorist financing risks’ as well as limiting the effectiveness of financial surveillance systems that rely on knowing the customer and tracking the customer’s transactions (Financial Action Task Force, 2011: 15). The goal remains the maintenance of measures against potential terrorist financing, rather than promoting economic development through financial inclusion.

Beyond possessing a government-approved form of identification, the ‘know your customer’ requirement for proof of address becomes difficult when the nature of one’s residence may not include a utility bill of any form. The experience of South Africa may be instructive as it represents one example for where a large number of people live in informal residences around the periphery of urban areas, and these people are also the intended customer group for a basic bank account in South Africa’s promotion of financial inclusion. The solution was to offer an exemption for this type of bank account on the customer due diligence requirement while at the same time keeping the services provided by the account limited in order to minimise the risk for money laundering through it. When a customer’s banking requirements later exceed those account limits, further identification verification is completed. This solution to the customer due diligence requirements in South Africa is an example for an implementation of the risk-based approach to AML/CFT measures (De Koker, 2009). At the same time, a study for the World Bank argues that financial inclusion is hindered by other barriers with more substance than AML/CFT documentation requirements. The report’s authors point to the fact that poverty itself is a more relevant reason for not having a bank account, along with a distrust of banks, the high cost to maintain an account, and the simple fact of living in a predominantly cash-based society. Hence they conclude, in line with the desires of the FATF, that ‘financial inclusion and AML are complementary … because the widespread use of cash reduces the effectiveness of the AML system.’ (Yikona et al., 2011: 87) Notwithstanding this conclusion and acknowledging that there are other barriers to financial services in developing economies, nevertheless, as Louis de Koker observes, the FATF ‘should not unnecessarily exacerbate existing barriers or construct new ones.’ (De Koker, 2011: 363)
**AML against corruption and bribery**

On the other side of the cost-benefit calculation behind implementing AML/CFT legislation is the cost incurred by a government to create the institutions and legal structures necessary for the surveillance and monitoring its national financial system. This is an expense where arguably the money could be better used by the government of a developing state for something advancing local welfare as opposed to being used to satisfy the fears of Americans and Europeans about criminal money and terrorist finance. Even for the small developing economy with an offshore financial centre (OFC) for which a good reputation in compliance and enforcement of AML/CFT regulations is clearly ‘value-added’, the cost to establish and maintain the necessary institutions still exceed the economic benefits accruing from the operation of a successful OFC (Sharman and Mistry, 2008). The creation of a system nonetheless indicates to the rest of the world the determination of the developing state to be viewed as a good global citizen in these efforts to counter illegal money, even if it does not gain any significant discernible direct benefit. Beyond the representation of good global citizenship at the same time it may be possible to produce a positive if unintended consequence from the establishment of an AML/CFT regime for a developing economy’s financial sector. A case has been advanced arguing that a developing state can deploy these methods and laws for the benefit of society as a whole, specifically as a tool for use against practices of bribery and corruption. In this fashion, the unintended negative consequences arising from the cost of establishing and maintaining an AML/CFT regime may be utilised in a positive manner to counter a major problem in some developing economies. As Sharman and Chaikin describe it, the information gathered by the government’s financial intelligence unit as part of its AML/CFT compliance process could be used as evidence against cases of grand corruption. They make the very good point that government leaders accepting bribes have to conceal the source of this illegal income, therefore they must by definition ‘launder’ the money in order for it to appear as legal income. Consequently, even if it is the case that these corrupt leaders seem to be impervious to other criminal charges, if they possess more money than is reasonable based on their salaries, other acknowledged legal sources of income and any assets owned before becoming an elected politician or government official, then they have to be able to prove that it is not illegal income and that they have not been involved in money laundering. Moreover, Sharman and Chaikin point out that money laundering charges may be filed against the individual in the country where the money is located and not necessarily in the home country, in other words in Europe or North America where the proceeds of grand corruption are often used to purchase property or are otherwise invested in other financial assets (Sharman and Chaikin, 2009).
Central to the analysis of Sharman and Chaikin is the application of customer due diligence obligations by financial institutions and designated non-financial businesses or professions (DNFBPs, i.e. accountants, casinos, lawyers) to the domestic ‘politically exposed person’ (PEP) as well as the foreign PEP. The 2003 edition of the FATF Forty Recommendations focused the PEP requirement only on foreign individuals, that is

‘individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves.’ (Financial Action Task Force, 2003: 14)

It should be noted that the interpretive note to accompany Recommendation 6 at the time did state ‘Countries are encouraged to extend the requirements of Recommendation 6 to individuals who hold prominent public functions in their own country.’ (Financial Action Task Force, 2003: Annex, p. 5) The Recommendation, however, is clearly written from the perspective of the developed state members of the FATF, confident in the belief that their domestic legal systems are sufficient to the task of identifying any incidence of corruption amongst their political elite but wanting to make sure that the financial system is suitably observant for the foreign PEP that may investing the proceeds of corruption with a domestic firm. In the United States, for example, there was the case of Raul Salinas, brother of the former President of Mexico Carlos Salinas and therefore a PEP, who was found to have transferred US$ 90 - 100 million (now believed to be the proceeds of corruption) between 1992 and 1994 through a collection of Citibank subsidiaries with the complicity of bank employees (General Accounting Office, 1998; Truell, 1996).

With the 2012 edition of the FATF Recommendations the coverage for additional customer due diligence has been extended and the Recommendation also now reads,

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation.

(Financial Action Task Force, 2012: 16)

As this change to the text of the Recommendation makes its way into national legislation there is the potential that the benefit from an AML/CFT enforcement regime identified by Sharman and Chaikin for a developing country can be realised. But again it need not wait that long, consider, for example, the resolution to a case settled at Southwark Crown Court in London. James Ibori had been the
governor of Nigeria’s Delta state from 1999 to 2007, during which time he amassed a fortune of nearly £50 million (though the Metropolitan Police estimated that Ibori had embezzled closer to £157 million from the public purse). He pled guilty to several money laundering and money laundering-related charges, marking the culmination of a seven year investigation by the Metropolitan Police, which had previously obtained a court order in 2007 to freeze his UK-based assets. For his guilty plea Ibori received a thirteen year sentence, while his wife, sister, mistress and former lawyer in London all had been convicted on money laundering charges in 2010 for their involvement in his money laundering activity. Nigeria’s Economic and Financial Crimes Commission had charged Ibori with 170 charges of corruption after he left office in 2007. But those charges were dropped in 2009 when a Nigerian federal court ruled there was insufficient evidence to support them (Tran, 2012; BBC News, 2009; BBC News, 2012a). The challenge confronting any effort to prosecute politically powerful individuals in their home state is revealed by this case in Nigeria.

Nigerian anti-corruption efforts were obstructed when Ibori successfully had his case transferred to a federal court on which a sympathetic cousin sat as a judge. Further, he had previously attempted to get the Economic and Financial Crimes Commission to drop all charges with the offer to its boss of a US$15 million cash bribe, and successfully got a court order to block the efforts of the Metropolitan Police to investigate and gather evidence in Nigeria’s Delta state for use in the UK prosecution (Shirbon, 2012). Consequently, those countries with significant financial centres where the suspicious assets of developing state PEPs are invested have the capacity to act now, it is simply a matter of resolve to collect the evidence and to pursue the charges.⁸

Concluding observations

The goal for the preceding text was to identify the tension between the securitisation moves of developed states against terrorist finance and the resulting consequences in developing states, particularly the impact for development itself. Mechanisms crafted for the banking and financial system evolved in the developed states imposed constraints in the developing economy with a less comprehensive financial architecture. Moreover, widespread cash-based transactions are immune to surveillance practices grounded in documentation and automation procedures missing in much of the economy found in developing states. And for many areas in the developing world the concern with transnational, Islamist-motivated terrorist violence is a concern resident in distant places and lacking locally. Rather, there are more immediate sources for violence, whose source of finance may be resilient to any locally reproduced ‘Know Your Customer’ due diligence procedures. Instead of proposing an innovative solution to an intractable problem, the intention here was been simply to
promote a consideration for consequences and an understanding for a resistance to foreign practices that are unsuitable to local context.

Money, in its cash form is anonymous, untraceable and fungible and it represents the risky potential of illegality and a threat for facilitating terrorist trauma. Beyond the securitising language of the Bush Administration in the US to prevent terrorism by preventing its finance, the FATF focus on cash money frames it as a vehicle preventing the reproduction of a safe, crime- and violence-free society where all financial activity is seen and measured, monitored for probity and evaluated for potential misconduct. This assessment is further reinforced by the fact that the latest version of the FATF Recommendations demonstrates a re-invigorated effort at securitisation, including a new recommendation against the financing associated with the proliferation of weapons of mass destruction (#7), and the introduction of corruption/bribery and ‘tax crimes’ to the list of ‘designated categories of offences’ (Financial Action Task Force, 2012: 13, 112 - 113). As noted by the authors of *Ill-Gotten Money and the Economy*, corruption and tax evasion were the two leading sources for ‘ill-gotten’ money in the two states they analysed (Malawi and Namibia), which they then extrapolate to represent the condition for ‘many developing countries’. Consequently, ‘a cash-based economy with a large informal sector is able to absorb large volumes of cash’ that in turn circumvents all efforts to use an AML regime against the proceeds of all forms of criminality (Yikona et al., 2011: 83, 85 - 86). The solution, to eliminate the use of cash in the economy, is neither novel nor new, this argument has been made by other commentators (i.e., The future of money: A cash call, 2007). But to achieve this goal in a developing economy will not only require that everyone have a bank account, but also it requires the government to provide for all the prerequisites for a bank account, e.g. universal government-approved identity documentation. It will be, in other words, a significant institutional challenge for the developing economy while also providing benefits beyond simply establishing financial surveillance.⁹

New payment methods, such as mobile money, open up a variety of development opportunities beyond migrant remittances. And the widespread availability for mobile phone service highlights further economic development opportunities beyond payment systems (e.g. connecting buyers and sellers). Nonetheless, AML/CFT regulations present a barrier to its use as a payment system if risk-based measures appropriate to its usage are not applied. The consequences emerging from financial surveillance and the securitisation of money, as experienced in a developed economy as compared to the developing economy may be different. Yet constraining legitimate financial transactions in pursuit of the minority of illicit transactions (claimed to represent 2 - 5 percent of global GDP) by
securitising money may not be the most efficacious means to deal with terrorism or other forms of illegality in the spaces beyond the developed state economy.

Endnotes

1 See <www.fatf-gafi.org>.

2 For a list of the ‘Designated categories of offences’ considered as potential predicate offences, see (Financial Action Task Force, 2012: 112 - 113).

3 The definitional dilemma was addressed in Article 2 of the United Nations Convention for the Suppression of the Financing of Terrorism (United Nations, 1999). This definition is replicated throughout the signatory states of the Convention, for example, the following clause in the European Union’s Third Money Laundering Directive.

   For the purposes of this Directive, ‘terrorist financing’ means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part in order to carry out any of the offences [defined as terrorism in the preceding paragraphs of the Directive]. (European Parliament and Council of the European Union, 2005)

4 See, e.g. (Biersteker and Eckert, 2008; Gardner, 2007; Heng and McDonagh, 2008).

5 For the complete list of FSRBs and FATF Observers, see < www.fatf-gafi.org/membership>, accessed 28 March 2012.

6 This process is different from mobile banking services, which involves an application on the mobile phone providing access to an already existing account with a traditional bank or with a payment system such as PayPal.

7 It should also be noted that the FATF initiative was undertaken in the wider context of a move for financial inclusion, which was highlighted in the G20 Leaders’ Communiqué at the Seoul Summit of 2010 (Financial Action Task Force, 2011: 8, 54 - 55).

8 Similar action was taken against Teodorin Obiang, son of Equatorial Guinea’s President and serving as the country’s Agriculture Minister. His lavish lifestyle in Europe and the United States, in terms of residences, expensive automobiles, and other luxury items, far exceeds the salary of a government minister (Chrisafis, 2012; Hinshaw and Landauro, 2012; BBC News, 2012b).

9 See, for example, the project to get every citizen counted and documented in India (India's UID scheme: Reform by numbers, 2012).
References


------ (2008b) 'Money, Terror and Protecting the West', The Round Table 97(395): 305 - 311.

