Terrorist financing in Southern Africa:
Are we making a mountain out of a molehill? [1]

Annette Hübschle

ISS Paper 132 • January 2007
Price: R15.00

Introduction

The detection of terror funds is a complicated undertaking due to the size and nature of the transactions involved. Contrary to popular belief, planning and committing a terrorist atrocity does not require much money. If banks are used, the transactions tend to involve small amounts and an uncomplicated layering of funds. The much-cited 9/11 atrocities in the United States provided a classic example. An examination of the hijackers' finances revealed that the individual transactions were small, falling below the reporting threshold for unusual cash transactions, and the funds involved added up to less than half a million US dollars. The 1998 US embassy bombings in East Africa were estimated to have amounted to an overall cost of less than US$10 000.

AML/CFT (anti-money laundering and combating the financing of terrorism) regimes have become the key tools in fighting terrorism in the post-9/11 world. The stakes, in what the Bush government in the United States has called a 'war on terrorism', have been raised on account of the inevitable friction between the trappings of development on the one hand and the imperative to maintain security on the other. The global and transnational nature and reach of financial institutions, the greater role of intermediaries and the uneven development, even divergence, of the world's economic systems combine to magnify the challenges of combating money laundering and terrorist financing. Mindful of the differences in banking and financial systems between the developed and developing world, this paper provides an overview of international instruments against terrorist financing, the evolving methods of detecting terrorist financing and the practical problems they are likely to encounter – and, in some cases, have already encountered.

Are the anti-terrorist financing mechanisms applied in the developed world appropriate and sufficient in Southern Africa? The region comprises Angola, Botswana, the Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe. These countries' human development index rankings suggest that they will accord priority to speeding up economic development. Considering the limited resources at their disposal, can they afford to implement anti-terrorist financing measures?

> With their limited resources, can Southern African countries afford to implement anti-terrorist financing measures?

Informal economic sectors account for a large number of financial and business transactions in Southern African countries. With the probable exception of South Africa and Mauritius, the informal economic sectors are far more economically active than the formal sectors. Also known as the 'parallel market', 'unrecorded trade' or the 'cash economy', these sectors provide for the livelihood of millions of Africans, although their magnitude is undetermined. Direct interaction between the informal sector and formal financial institutions is insignificant. In Tanzania, which has a vibrant informal economy, a mere 6% of the population use banks for depository purposes,[2] while only 4% of Malawians[3] and fewer than 1% of Congolese and Angolans are 'banked'. Figures in other countries are just as low.

This paper is based on findings from field trips in the region.

Definitions

US treasury agents trying to catch Al Capone coined the term 'money laundering' in the 1930s. The notorious mastermind of organised crime and his associates owned hundreds of clothing laundries

around Chicago. He disguised the illicit income from selling alcohol during the Prohibition as money honestly earned from operating these laundries (Mathers, 2004:22). In its modern incarnation, money laundering simply refers to "the process by which proceeds from criminal activity are disguised to conceal their illicit origins" (Schott, 2004:1).

The International Monetary Fund (IMF) has estimated that money laundering generates up to a staggering US$1.5 trillion per year (FATF, n.d.). It feeds on criminal activity. Money laundering investigations start off by determining the underlying criminal offence or the substantive offence. Traditionally, the substantive or predicate offence was linked to organised crime such as drug trafficking, fraud or theft (Bachus, 2004:835). In 1996, the international Financial Action Task Force (FATF) included 'ordinary' crimes against property, as well as corruption, illegal arms trading, gaming and trafficking in human beings, as predicate crimes (Pieth, 2002:120). Nonetheless, before 9/11, international anti-money laundering efforts were aimed primarily at the proceeds of transnational organised crime activities. In 2000, the United Nations adopted the United Nations Convention against Transnational Organised Crime (also known as the Palermo Convention) and its protocols dealing with trafficking in persons and the smuggling of migrants.

After 9/11, terrorism or planning to commit an act of terrorism was added as an additional substantive offence (Mathers, 2004:22). Thus, the focus of anti-money laundering has been broadened. Whereas funds attracted the interest of law enforcement before on account of a link to illegal sources, nowadays the international community also treats with suspicion funds whose purpose (e.g. the financing of terrorism) is or is likely to be illegitimate (Bachus, 2004:836). The wisdom of adding the financing of terrorism as a substantive money laundering offence will be examined in this paper.

How is terrorist financing defined? The financing of terrorism is easily explained as "the financial support, in any form, of terrorism or of those who encourage, plan or engage in terrorism" (Bachus, 2004:836). It is less simple to define 'terrorism', because of political, religious and national implications that differ significantly from country to country. An all-encompassing and globally applicable definition of terrorism remains elusive, not least in Africa. Legal drafters tend to avoid an outright definition of 'terrorism', but rather describe an 'act of terror' or 'terrorist activity'. Contrary to what one might expect, not many governments consider this disturbing – in fact some governments seem to benefit from the lack of a universally accepted definition, as it makes it easy for them to label organisations and individuals that are critical or problematic 'terrorist'. All liberation movements can attest to this kind of abuse: the African National Congress, the South West African People's Organisation and others were perceived as terrorist organisations. More recently, the Zimbabwean Movement for Democratic Change has been condemned as a terrorist organisation fronting for hostile foreign governments.

Most African scholars and researchers adopt the definition of 'terrorist act'[4] in the Organisation of African Unity Convention on the Prevention and Combating of Terrorism (Algiers Convention). The closest to a universally accepted definition is perhaps contained in United Nations General Assembly Resolution 54/110 of 9 December 1999, which states that terrorism comprises "criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes" (UN, 1999a).

The discourse of risk and globalisation is key to the anti-terrorist financing debate

International obligations and standards on combating terrorist financing

The discourse of risk and globalisation is key to the anti-terrorist financing debate. Due to the global reach of the international financial network, all countries are vulnerable to money laundering. If terrorist financing follows the same routes as money laundering, it follows that countries are equally vulnerable to terrorist financing.

The international community recognises financial controls as essential anti-terrorism tools. A series of measures at national, regional and international level have been introduced to deprive terrorists of the means to inflict serious damage. The main sources of international obligations in combating the financing of terrorism are the resolutions of the United Nations Security Council (UNSC), in particular Resolution 1373 of 2001 (referred to here as 'the Resolution'), the 1999 International Convention for the Suppression of the Financing of Terrorism (referred to here as 'the Convention') and the nine Special Recommendations on Terrorist Financing issued by the FATF (referred to here as 'the Special Recommendations').

The Convention, which opened for signature on 9 December 1999, stipulated the criminalisation of direct involvement or complicity in the financing or collection of funds for terrorist activity. Article 2(1) requires states to create an offence when a "person by

any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used" to commit an act that constitutes a terrorist offence (UN, 1999b). In Southern Africa it has been ratified by seven states: Botswana, Lesotho, Malawi, Mauritius, South Africa, Swaziland and Tanzania.[5]

The Resolution, adopted in the immediate aftermath of the 9/11 attacks, imposed unprecedented legal obligations on UN member states to comply with measures designed to counter terrorist financing, travel, recruitment and supply.[6] To monitor the enforcement of these and other anti-terrorism measures, the UNSC created the Counter-Terrorism Committee. In March 2004, the committee became the Counter-Terrorism Executive Directorate and it serves as a professional secretariat for the implementation of counterterrorism strategies.

The FATF adopted eight Special Recommendations on terrorist financing in October 2001. These included a call for the ratification and implementation of relevant international instruments, the freezing and confiscation of suspected terrorist assets, the reporting of suspicious transactions, the evaluation of alternative remittances and wire transfers and the revision of laws and regulations related to non-profit and charity organisations. An additional measure adopted late in October 2004 called on states to stop cross-border movements of currency and monetary instruments related to terrorist financing and money laundering and to confiscate such funds. The recommendation stipulates a limit (US$15,000) for undeclared cash that can be carried across borders. Furthermore, it proposes control over cash couriers through the intervention of national authorities on the basis of intelligence or police information.

Considerable overlap is noticeable among the various obligations and standards. The Convention, the Resolution and the Special Recommendations each deal with aspects of the freezing, seizure and confiscation of terrorist assets. The Special Recommendations deal with four topics not covered by the Resolution and the Convention: alternative remittance systems, wire transfers, non-profit organisations and cash couriers (IMF, 2003:4). These topics focus on financial systems other than the formalised banking and financial systems. On the face of it, the four recommendations were informed by conclusions made in respect of the financial sources of al-Qaeda before 9/11. It remains an open question whether the FATF recommendations are pertinent to vulnerabilities within the cash economy or informal sectors in Southern Africa.

Of further relevance to the region are anti-terrorist financing measures passed in the United States. On 14 September 2001, US President George W. Bush issued Executive Order 13224 entitled "Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism", which expanded the US list of designated terrorist organisations. Most importantly, the order acknowledges the global reach of terrorists by imposing extraterritorial financial sanctions against all "foreign persons that support or otherwise associate with these foreign terrorists" (US Department of State, 2001).

Another beacon in the US war on terrorist financing is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (also known as the USA PATRIOT Act). Major AML/CFT provisions that have a bearing on foreign jurisdictions include:

- US banks are prohibited from opening correspondent accounts for foreign banks with no physical presence, no employees or no regulatory supervision in the US; and
- informal money transmitting businesses have to be licensed and report suspicious transactions.

There is no obvious benefit in adopting the measures stipulated in the anti-terrorist financing instruments

Anti-terror measures pose significant dilemmas for developing countries in Southern Africa. They are under pressure to either comply with the international obligations or be blacklisted as non-co-operative and risk economic sanctions. There is no evidence that terrorism is considered a significant threat to many of these countries. There is, in consequence, no obvious benefit in adopting the measures stipulated in the anti-terrorist financing instruments. Michael Levi and William Gilmore suggest that transnational regulation involves the "persuasion" of "formally independent nation states to adopt similar measures even though there may be no obvious benefit to them in doing so" (2002:90) Terrorist networks and organised criminals threatening the US and other Western powers may be substantially different from those threatening countries in the developing world, so the 'one-size-fits-all' approach may well be inappropriate.

The sentiments of an implicit 'persuasion' have been echoed by political decision-makers, law enforcement officials and other bureaucrats assigned the task of implementing the AML/CFT regimes in the region. The political will is low and the perception of bullying is strong in the region.

The World Bank and other international financial institutions (IFIs) have assumed a critical role in

'persuading' developing countries to toe the line. Representing the most influential financial institutions in the world, the World Bank, the IMF and other IFIs control many billions of dollars in resources, including development aid and foreign direct investments, which are allocated for lending and capital projects around the world. These institutions each have multiple correspondent banking relationships and deposit funds for use in developing or recipient countries in central banks and commercial banks (Winer, 2002:38). The IFIs declare that they will only do business with commercial banks and other financial institutions that comply with anti-money laundering standards. This of course puts international banks and commercial banks with a large turnover at an unfair advantage. A small local bank in Malawi, Namibia or anywhere else in the region will struggle to comply with international standards, while its competitor with international ties, or the subsidiary of an international bank, has the capacity and financial backing to do so. Increasingly, smaller and local banks are stigmatised as financial backers to terror financiers, warlords, corrupt bureaucrats and organised criminals.[7]

Noteworthy in the context of the Southern African region is the stipulation in the USA PATRIOT Act that US banks are prohibited from opening correspondent accounts for foreign banks with no physical presence, no employees or no regulatory supervision in the US. This means that any financial institution wishing to enter into a trade or banking agreement with a US bank has to open an office on US territory. For small local banks in Southern Africa, such an obligation presents a serious financial burden. This and other AML/CFT obligations undermine the long-term goal of conducting business with the US. Small banks struggle to finance and staff such offices. Again, big, international banks or financial institutions command an unfair advantage. Perhaps the question is not how one complies with the international obligations, but who stands to benefit from the AML/CFT regime.

International financial institutions have assumed a critical role in 'persuading' developing countries to toe the line

Domestification of international instruments: Practical considerations

International bodies such as the UN and the FATF recommend some basic steps towards achieving a reliable AML/CFT regime. It should be noted that these steps implicit in the Resolution, Convention and Special Recommendations use as a point of departure the formalised banking and financial sectors of the developed world.

Domestic legislation

The three key instruments on terrorist financing suggest that domestic legislation should provide the general legal framework and establish the obligations of financial institutions and other providers of financial services. Such legislation should define and criminalise money laundering and terrorist financing, setting penalties. It should cover a wide set of predicate crimes and also define the responsibilities and powers of the various government agencies involved. Commercial banks should be obliged to be especially vigilant, given their role in the payment system (IMF, 2003).

Within the region, Mauritius and South Africa have domestic laws that specifically address terrorist financing. Mauritius lists as key laws in the fight against terrorist financing the International Convention for the Suppression of the Financing of Terrorism Act of 2003, the Anti-Money Laundering (Miscellaneous Provisions) Act of 2003 and the Financial Intelligence and Anti-Money Laundering Act of 2002.[8] The main statutes dealing with terrorist financing in South Africa are the Prevention of Organised Crime Act of 1998 (Poca) and the Financial Intelligence Centre Act of 2001 (Fica). With the enactment of the Protection of Constitutional Democracy against Terrorism and Related Activities Act of 2004, the Poca and Fica were amended to accommodate measures against terrorist financing (Hübschle, 2006:110–111). The Malawian parliament passed the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act of 2005 in August 2006 after many months of vigorous debate.

As for the rest of the region, most countries are at different stages of developing or implementing anti-money laundering laws. Most are aware that new enforcement agencies and other institutions not only constitute an additional financial burden, but also raise issues around capacity, training and maintenance. Some officials have suggested that anti-money laundering laws are drafted to satisfy minimum international obligations, but they pay little more than lip service to the international instruments, as their implementation is put on the back burner.

Banking regulation and supervision

For primary legislation to be operational, banking regulations and supervision need to be implemented. Ideally, financial institutions should be obliged to institute procedures to avoid dealing with criminal and terrorist elements.

'Know your customer'

Banks and other financial institutions should verify the identity and legitimacy of clients, especially new clients and those acting on behalf of others. The 'know your customer' (KYC) obligation may involve elaborate background checks.

The KYC obligation poses significant practical challenges to commercial banks in the region. For those banks that can tap into the know-how and financial networks of their foreign parent companies, the KYC obligation, on the face of it, can be implemented with relative ease. However, elaborate background checks involve confirmation of identity and proof of residence, traditionally in the form of utility bills (electricity, water, telephone, etc), and at this point, no matter how much foreign cash and expertise is available, all banks doing business in the developing countries of Southern Africa face certain challenges in this regard. The following are especially pertinent:

- the absence of systems of national identification;
- the absence of birth certificates;
- the minimal use of passports;
- the minimal availability of driving licences as a means of identification;
- the lack of employment credentials or 'job cards';
- unfixed or unmarked residential addresses in informal settlements, undemarcated townships and rural areas (a surprisingly large number of African metropoles and cities only have physical addresses in the city centre); and
- low levels of access to utilities, and hence to utility bills.[9]

When the Basel Committee on Banking Supervision wrote the Basel Statement of Principles and introduced the concept of KYC as a fundamental principle of banking supervision back in 1988 (Pieth, 2002:122), little thought appears to have been given to the limitations, in a different setting, of standards that may be viable in the developed world. However, central banks, bankers' associations and other stakeholders in the region have come up with creative and innovative approaches to circumvent the practical challenges of adhering to KYC obligations. In Tanzania, a bank can carry out a KYC on a customer by contacting two referees. Of great significance are letters of introduction by local authorities. The basic unit of civil administration in Tanzania is a cell, which consists of 10 houses or separate units, and the leader of such a cell may provide proof of identity. But these leaders, who are in a powerful position, are not always unbiased.[10]

The KYC obligation raises another dilemma. Compliance officers from a number of Southern African countries have argued that although KYC may lead to compliance with international obligations, in reality it discourages the great majority of 'unbanked' citizens of the region from entering the banking system. Uncomfortable questions and requests for documentation may put off prospective customers.[11] Banks may do business with international investors and multinational corporations, but the people sleep with their money under the mattress.

Of further concern in South Africa is that banks are reluctant to allow asylum seekers and refugees to open bank accounts. Upon arrival, asylum seekers are furnished with an asylum-seeker permit until they receive official refugee status. The processing of applications can take months, and the backlog is huge. In the meantime, banks will not allow asylum seekers to open bank accounts, as the temporary permits do not provide a 13-digit identity number as required by the Fica regulations. Increasingly, asylum seekers (especially the Somali community) have been targeted by criminals, as they are known to keep their money on their business premises or in their homes (Ismail, 2006).

Banks may do business with international investors and MNCs, but the people sleep with their money under the mattress

'Fit and proper'

The Convention calls for measures to ensure that criminals and terrorists do not set up or gain control of financial institutions. The question is how to do this effectively in a free market. Shareholders and senior managers in financial institutions should demonstrate that they are 'fit and proper' to hold these positions of control and oversight. This applies to the initial licensing stage, but regulators should also scrutinise management turnover and changes in shareholdings.

The Finance Bank in Malawi provides an excellent example of what can happen if no 'fit and proper' test of senior managers is conducted. The Finance Bank's banking licence was revoked on 27 January 2006, after several acts of operational malpractice and non-compliance with banking regulations were discovered. More specifically, senior managers had not complied with foreign exchange regulations and had created 'ghost accounts', apparently in order to externalise foreign currency. Furthermore, the

branch manager in Lilongwe had failed to provide the Anti-Corruption Bureau with information on clients who contravened the foreign currency transaction regulations. Corrupt government officials were found to have hidden their ill-gotten gains in accounts at the Finance Bank, while 12 bank employees had created an intricate net of transactions that effectively drained the bank's coffers of close to US$200,000 (Tambulasi, 2006).

Unusual transaction reporting

Financial institutions are advised to establish systems of identifying and reporting unusual transactions.

Bank officials have pointed out that what constitutes an unusual or suspicious transaction in one country may be perfectly 'normal' in another. Bank regulators may not bat an eyelid if an amount of US$20,000 is transferred in a developed country, but the same amount transferred in a developing nation could constitute an unusually large amount.[12] The unusual transaction threshold may be linked to the KYC obligation. Thus it would be unusual, for example, if a civil servant transferred amounts in excess of his/her monthly income.[13]

What constitutes an unusual or suspicious transaction in one country may be perfectly 'normal' in another

Record-keeping

Linked to KYC and the reporting of unusual transactions is the need for adequate record-keeping. When a suspicious transaction is investigated, a financial institution needs to be able to help authorities establish an audit trail going as far back as five years. The laundering of funds controlled by General Sani Abacha of Nigeria demonstrated the need for financial institutions to focus more attention on the 'layering stage', where laundered funds or terror finances are already in the system and the audit trail is disguised, often with numerous transactions used to move funds around (Fitzsimons & Lewis, 2002).

An anti-money laundering officer for one of the big banks in Tanzania remarked cynically that even though banks were keeping records of transactions, tracing them was still problematic. Finding the record of a specific transaction in a storeroom was like looking for a needle in a haystack.[14] Paperless and computerised transaction record-keeping is not that well established. In this regard, local subsidiaries of banks and financial institutions in developed countries may have an edge over smaller indigenous banks.

Establishment of a supervisory institution

Linked with banking regulation and supervision is the need for government to establish a supervisory institution to ensure that commercial enterprises comply with the laws and regulations and that suspected cases of money laundering or terrorist financing can be monitored. Typically such financial sector regulators are responsible for supervising AML/CTF procedures followed by financial institutions and for checking that their managers, owners and shareholders meet the 'fit and proper' test. Many countries have also set up specialised FIUs.

The mandate of FIUs includes investigating, analysing and passing on to the appropriate authorities financial and related information concerning suspected proceeds of crime or terror funds. A key component of an FIU's mandate is to share information about suspicious transactions across borders. The Egmont Group, set up in 1995, serves as an association of FIUs and promotes best practice among its members. International co-operation between FIUs in terrorist financing or money laundering cases is encouraged and based on mutual trust. Part of the mandate of FIUs is to ensure that national legal standards and privacy laws are not formulated in a way that inhibits the exchange of information. Thus, FIUs should be able to exchange information freely on the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and requesting parties.

Here again the recommendation raises concerns for some countries. It is not only a costly exercise to establish an FIU, but competent staff have to be recruited and trained. Mauritius, South Africa and Zimbabwe are the only countries in the region with FIUs in place.

The Financial Intelligence Bill before the Namibian parliament will, if passed, allow the central bank, the Bank of Namibia, to collect, access and analyse financial intelligence data and to freeze and seize the assets of suspicious institutions under investigation.[15] This initiative exemplifies a bone of contention as regards the independence of FIUs. Ideally, an FIU should be a stand-alone institution, because links with the regulator (the central bank), a law enforcement agency (a general or specialized police agency) or the line ministry (finance) may constitute a conflict of interests. Yet such a conflict of interests may be preferable to not creating an FIU at all. Considering the financial and developmental

status of most countries in the region, this may be the lesser of two evils. At least the central bank, the police agency or the line ministry may be able to provide financial resources, equipment, staff and institutional memory to undertake financial intelligence work.[16]

The FIU in Mauritius and South Africa's Financial Intelligence Centre (FIC) have received thousands of suspicious transaction reports. Data on how many of the reported cases have led to successful prosecutions is not available. Furthermore it remains unknown whether there have been cases involving terrorist financing, as there have been no prosecutions for financing terrorism.

Sources of terror finances

The previous section set out some practical considerations in the implementation of a domestic AML/CTF regime. Before looking at emerging global trends and methods of detection, it is necessary to examine sources of terrorist financing.

Criminal activities such as bank robberies, kidnapping for ransom, extortion, smuggling and drug trafficking

Loretta Napoleoni, an expert on terrorist financing, has declared the illicit drug trade the single largest source of terrorist income (2005:143-182). Afghanistan's poppy crops, responsible for as much as 86% of the world's opium supply, are widely believed to be a major contributor to terrorist coffers. In 2002, US Drug Enforcement Agency officials broke up a methamphetamine ring operating in a dozen US cities which had allegedly been funnelling its proceeds to Hezbollah. The Revolutionary Armed Forces of Colombia have long used the cocaine trade to finance their operations (Kaplan, 2006).

Donations from local and foreign supporters, including emigrants and charitable organisations, and cash infusions from wealthy individuals or organisations

Donations originating from charities, NGOs and wealthy individuals were once the largest source of terrorist financing. Charitable organisations are still believed to play a role in the financing and operations of terrorist groupings (Napoleoni, 2005:143-182), and religious charities have come under increasing scrutiny and severe restriction since the 9/11 attacks, with many Muslim charities being closed down or banned. It is important to recognise, however, that there have only been a few instances of NGOs or charitable organisations being positively linked to terrorist financing.

Assistance from foreign sympathetic states

Quite a few countries, predominantly in the developing world, have provided support to terrorist organisations for political and military reasons. The US State Department updates its list of 'state sponsors of terrorism' annually. The government of Sudan and the former Taliban government of Afghanistan not only supplied funds to al-Qaeda, but also provided financial services and integrated state and terrorist financial services. Such activities do not break domestic laws. When terrorist organisations have the full range of state-controlled financial services at their disposal, large sums of money can be integrated into the international financial system, whether the state or some other legal or illicit source is the funding agency (Navias, 2002:68).

Some terrorist organisations have legitimate business operations that generate profits and can also be used as fronts for money laundering

Revenues from legitimate business operations

Some terrorist organisations operate legitimate business operations which generate their own profits and can also be used as a front for money laundering. Ties to terrorism have been identified in the livestock, fish and leather trades. Those behind the 1998 US embassy bombs in East Africa had moved to the region in the early 1990s, engaging in small business deals such as the transporting of clothing between Dar es Salaam and the Kenyan port city of Mombasa (Mlowola, 2003). In 2001, the *New York Times* reported that Osama Bin Laden was operating a string of retail honey shops throughout the Middle East and Pakistan. Not only did the honey generate revenue, but it also was used to conceal shipments of money and weapons (Kaplan, 2006).

Is there evidence of terrorist financing in Southern Africa?

Most financial experts agree that the financing of terrorism can occur in any country in the world, whether or not it has complex financial systems. Since complex international transactions can be abused to facilitate terrorist financing and the laundering of money, the different stages of money laundering (placement, layering and integration) may occur in a host of different countries (Schott, 2004:18).

Despite the region's apparent vulnerability to terrorist financing, evidence of terrorist funding within or from Southern Africa is scanty and mostly anecdotal. Southern Africa has very rich mineral resources, such as gold, diamonds, uranium and gemstones. Following 9/11, there were allegations that diamonds and gold were being used to support the al-Qaeda terror network.

Clandestine business arrangements involving the diamond trade date back to the days of the cold war, when the superpowers used African nations as pawns in their geopolitical conflicts. They funnelled weapons to what were termed 'local proxies'. After the end of the cold war, the superpowers lost interest in Africa, and arms and ammunition became less readily available through direct channels. It was at this stage that the trade in illicit diamonds escalated. Warring factions and even a few governments became reliant on the illegal trade in 'conflict diamonds' and 'blood diamonds'. Notably, the civil war in Angola was prolonged by both the covert support of the UN and the sale of diamonds by the Unita (National Union for the Total Independence of Angola) terrorist movement (Fletcher, 2003).

African militaries and paramilitary factions may have used diamonds, gold and other mineral resources to finance their operations, but this would have been impossible without backing from multinational corporations, the international diamond industry and retail outlets selling 'blood diamonds' (Fletcher, 2003). There is no evidence of a link between the diamond trade or illicit diamond smuggling and al-Qaeda or other terrorist groupings in Southern Africa . Furthermore, the Kimberley Certification Process has established a system of warranties guaranteeing that diamonds are mined and exported legally.

The tanzanite scandal spun by two *Wall Street Journal* reporters has become notorious for its adverse effects on the Tanzanian gemstone industry.[17] The reporters suggested that al-Qaeda controlled a sizeable chunk of the trade in the rare blue gemstone mined from a 13km^2 patch of graphite rock in north-eastern Tanzania. Tanzanian investigators could find no evidence of such a connection. However, the publication of the allegations led to major US retailers dropping tanzanite from their sale offerings (Elvin, 2002). In February 2002, a Tanzanian delegation assured dealers at a major gem trade show in Tucson, Arizona, that no terrorist group was profiting from the sale of tanzanite. The Tucson Tanzanite Protocol originates from that meeting. Like the Kimberly Certification Process, it established a system of warranties guaranteeing that the gems were mined and exported legally. The United Republic of Tanzania declared the mining site a controlled area where no visitors were allowed without a dealer's license and other identification (Gomelsky, n.d.).

Allegations of the abuse of charities to fund terrorism turned out to be unfounded in a case in Malawi. In June 2003 US and Malawian officials arrested five foreign nationals on suspicion of funnelling funds to al-Qaeda through various Islamic charities and schools (Tambulasi, 2006). Not only were the arrest and deportation of the suspects in stark contravention of the country's constitutional principles, but the allegations turned out to be false (Banda, Katz & Hübschle, 2002). No evidence was found that money had been channelled to the terror network.

The region's long, porous and uncontrolled border are a cause for concern

Another cause for concern is the region's long, porous and unpatrolled borders. Police forces from several member countries have encountered, and at times arrested, suspects attempting to export huge amounts of US dollars from the region. The apprehension by Mozambican police of four Pakistani nationals on suspicion of attempting to smuggle close to a quarter of a million US dollars out of the country is a case in point ("Mozambique detains Pakistani nationals", 2005). A few months before 9/11, two South African nationals were arrested attempting to cross the border between South Africa and Swaziland with more than half a million US dollars stuffed into their underwear. Investigators found that the couple had travelled from the South African port of Durban through Swaziland to neighbouring Mozambique more than 150 times over an 18-month period. Links emerged between the suspects, an exchange bureau in the Mozambican capital of Maputo and gold dealers in Dubai (Block, 2002). Investigators speculated on a possible connection to al-Qaeda. Despite this suggested link, most cases that involve the illegal smuggling of currency across national borders are attempts to bypass or flout tough foreign exchange and currency regulations.

Alternative remittance systems take the form of non-bank institutions that transfer funds on behalf of clients through their own networks. Many of their transactions are paperless. Unregistered lenders in at least two countries move money across borders with no written record. Part of the attraction of this system lies in the fact that there is no proper trail to the source of the funds. It has been alleged that al-Qaeda has exploited the global *hawala* network by using it to transfer funds around the world. The proceeds of drug trafficking were

channelled through the network operating between London, the Punjab and Kashmir to support Sikh and Kashmiri secessionists (Navias, 2002:61). As for Southern Africa, *hawala* operations are said to take place in Malawi, Mozambique and Tanzania.[18] Marc-Antoine Pérouse de Montclos (2005) argues that it is more common for diaspora communities to collect money in the developed world and send it to their poorer brothers and sisters in Africa. There are variants of *hawala* used by the Zimbabwean diaspora in South Africa, Botswana and Malawi. However, there has been no evidence of links to terrorism. Indeed, African countries are usually at the receiving, not the donating, end of remittances.

State sponsorship of terrorism in the region probably reached its high-water mark during the apartheid era, when South Africa perpetrated acts of terrorism against its own citizens and those of neighbouring countries such as Namibia and Mozambique. It also sponsored proxy terrorist organisations in Angola, Namibia and Mozambique over a long period of time. Currently Zimbabwean President Robert Mugabe and his associates are being accused of using the state machinery to commit acts of terrorism against ordinary citizens (Goredema, 2005).

As the international community, with its various protocols, starts cracking down on the trade in conflict diamonds and other mineral resources tainted with innocent blood, a window of opportunity may be opened for warlords and organised criminals to collude with terrorist elements in the largely unknown and unregulated terrain of the informal sector.

Detection of terrorist financing

Many analysts agree that terrorist financing mimics the techniques of money laundering, so many of the countermeasures are similar. Furthermore, some terrorist organisations are known to finance their activities out of the proceeds of crime. Nonetheless, terrorist financing differs from money laundering in several ways:

- terrorist financing is mostly directed at future action, so the only offence that may have been committed when the financing takes place is conspiracy to commit a terrorist act; and
- the amounts needed to finance terrorism are relatively small: as mentioned above, the 1998 US embassy bombings in East Africa are estimated to have cost less than US$10,000 to mount, and 9/11 less than half a million US dollars (Roth, Greenburg & Wille, n.d.:52).

The date of 9/11 is regarded as a defining moment in international concern around money laundering. Since that point it has no longer been perceived as just the sanitising of criminal proceeds, but also as the means by which terrorists hide their revenue-generating processes and gain access to funds. Difficulties arise when applying money laundering legislation that relies on the assumption of an implied or specific predicate offence. Terrorism may or may not derive financial reward, but it will ultimately use funds obtained from legitimate or illegitimate sources. A further conclusion is that terrorists are ad hoc clients of the global financial network. Their use of the financial system may be limited to having funds available when needed, while using a laundering process to separate financial backers from acts of terror (Johnson, 2002).

Most strategies aimed at curbing the threat of terrorism are *ex post facto* in nature; in other words, strategies are developed once an act of terrorism has occurred. Policymakers and legislators perceive regulations aimed at curbing terrorist financing as serving to prevent terrorists from carrying out their deeds in the first place. The impact of 9/11 and the introduction of various pieces of anti-terrorism legislation have focused attention on the traditional money laundering model. Ideally, suspected money laundering and terrorist financing would both be reported to the banking sector regulator or other financial supervisory authority, although the processes of identifying them may differ. In money laundering, the proceeds of crime are converted into ostensibly clean funds. Terrorist financing, on the other hand, involves either illegal or legitimate funds being paid to a party associated with terrorism. The guidance issued by the FATF suggests that the way to identify terrorist financing is by reporting suspicions of money laundering. The underlying assumption is that terrorist financing will involve a type of money laundering. However, this excludes cases where the money used to finance terrorist activities originates from legitimate sources. Obviously, where there is a link between terrorist financing and money laundering, the identification of terror finances is easier.

Identifying terror finances is obviously easier where there is a link between it and money laundering

Significant practical issues confront institutions trying to implement anti-terrorist financing measures. These stem partially from the problems inherent in identifying terrorist monies. Anti-money laundering techniques rely, partly at least, upon the identification of suspicious transactions, patterns of transactions and the handling of large amounts of cash, the presence of which cannot be easily explained in the light of what is known about the customer. Terrorist funds

which are generated in a legitimate manner, on the other hand, only become tainted once they are transmitted to a terrorist cause or a terrorist organisation. One can thus assume that this type of terrorist funding does not move around the financial system like dirty money. Rather, it behaves like "ordinary money doing ordinary things and so is impossible to identify" ("The law: an overview", 2003). The US Central Intelligence Agency estimates that it costs al-Qaeda about US$30 million per year to sustain its activities, an amount that, before 9/11, was raised almost entirely from donations. In the aftermath of the attacks on the US, it is believed that donations from charitable organisations fund at least some of al-Qaeda's activities, but there are largely unconfirmed allegations that the organisation is increasingly funding its activities by illegitimate means, such as the drug trade, conflict diamonds and state support (Roth, Greenburg & Wille, n.d.:52).

Forensic auditors agree that identifying terrorist funding that originates from apparently legitimate sources will continue to pose a challenge. Beyond the FATF guidelines and related regulations, they recommend that transactions be subjected to additional scrutiny, when:

- a dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals; and
- several persons have 'signature authority' on an account, despite their appearing to have no obvious relation to each other (Fitzsimons & Lewis, 2002).

In addition, the US State Department has produced the following list of potential indicators of terrorist financing:

- the use of multiple personal and business accounts to collect and funnel funds to a small number of foreign beneficiaries;
- deposits followed within a short period of time by wire transfers of funds;
- beneficiaries located in a problematic foreign jurisdiction;
- the structuring of cash deposits in small amounts in an apparent attempt to circumvent foreign currency transaction report requirements;
- the mixing of cash deposits and monetary instruments;
- deposits of a combination of monetary instruments atypical of legitimate business activity (business checks, payroll checks etc);
- stated occupations of those engaging in transactions that are not commensurate with the level of activity (e.g. student, unemployed, self-employed);
- large currency withdrawals from a business account not normally associated with cash transactions;
- movement of funds through a FATF-listed "non-cooperative country or territory"; and
- the involvement of multiple individuals from the same country or community (Rosenoer, 2002).

Methods and systems to detect money laundering have been around for several years. Initially they were rules-based, but now they have evolved into more analytical systems that employ techniques such as anomaly detection (profiling and peer grouping) and predictive modelling (neural networks and decision trees). Despite the continuous progress made in the field of money laundering detection techniques, extending them to terrorist financing has proven problematic due its unique characteristics.

It is hard for financial institutions to set thresholds that discriminate between terrorist financing activities and legal transactions

Mark Moorman (2005) observes that **rules-based systems** are designed to uncover specific transactions or patterns that are often associated with criminal financial activity. However, there are few clear patterns with regard to terrorist financing. Furthermore, terrorist financing tends to occur in much smaller transaction amounts than traditional money laundering. It thus becomes difficult for financial institutions to set thresholds that discriminate between terrorist financing activities and legal transactions. In studying the funding of 9/11, it was discovered that the terrorists sometimes funnelled money through charities. To detect this kind of funding, a rules-based approach would have to flag all charitable funds that receive international wire transfers or have foreign nationals sitting on their boards, and this could lead to the blacklisting of many innocent charities. The inability to define clear indicia of terrorist fund-raising efforts creates the risk of financial institutions relying on religious, geographic or ethnic profiling to find criteria to identify instances of terrorist financing.

The FATF has recommended an **anomaly-based approach**, which requires programmes to detect money laundering and/or terrorist financing that look out for unusual transactions or activities. Various methods can be used to define 'normal', which may include the building of profiles based on past account activity or creating peer groups of accounts that should "behave in a similar manner" (Moorman, 2005). Once 'normal' has been delineated, an anomaly-based approach can identify those activities that do not fall within the normal range, using descriptive statistical measures such as standard

deviations or variances. Again Moorman cites the example of the 9/11 terrorists to demonstrate this approach. Having entered the US on student visas, the 9/11 terrorists had bank accounts with large sums of money moving in and out via wire transfers. This is not typical of student bank accounts.

A drawback of the anomaly-based approach is that there could be valid or legal reasons for such transactions (Moorman, 2005). Similarly, creating a profile for terrorist fund-raising groups may prove a tricky endeavour. A faith-based charity that collects funds from small donors, pools the funds, and then sends large monthly wire transfers to Chechnya, Somalia, Sudan, Afghanistan, Kashmir or the West Bank might be supporting terrorist groupings, but is more likely to be contributing to humanitarian operations in those war-torn regions (Roth, Greenburg & Wille, n.d.:57).

Using historical information on known suspicious and unsuspicious activities, analysts can apply the **predictive modelling approach**. Decision trees, regression analysis and neural networks are used to develop models that score any new activity on its likelihood of being suspicious. This approach has proved successful in fraud detection. However, its downfall is the need for historical data, which is lacking in most cases of terrorist financing (Roth, Greenburg & Wille, n.d.:57). Again, financial institutions find it difficult to discriminate between bona fide charitable transactions and terrorist financing operations.

Although all of the above approaches have shown some success in detecting criminal financial activities in the developed world, none can capture a broad range of activities (including terrorist financing). Another difficulty in tracking down terrorist financiers is that terrorist networks are well aware of global efforts to stymie their projects and adjust their activities accordingly. A general concern is that while effective AML/CTF laws are seen as essential means to combat the phenomena, they may push such illegal activities outside of the formally regulated sector. Napoleoni suggests that terrorist financing "mutates continuously" (quoted in Kaplan, 2006), which keeps it a few steps ahead of global law enforcement agencies. Increasingly, terrorists rely on illegal activities like counterfeiting and smuggling, which are difficult to trace through the financial system.

A further dilemma arises from the fact that launching a terrorist attack costs very little money, yet the introduction of anti-terrorist financing measures is a rather expensive enterprise. With little or no evidence of terrorist financing, it is understandable that politicians are reluctant to introduce such measures. In the absence of anti-terrorist financing laws and corporate computerised banking regimes, the various detection methods are useless. Again one needs to ask whether such complicated and often inappropriate methods serve any purpose in countries where cash transactions are the order of the day.

Conclusion

This paper has highlighted some of the difficulties of complying with international obligations against terrorist financing in Southern Africa. The countries of the region have large informal sectors with millions of unbanked people. While the international community sets about keeping terrorist funds out of the formal financial sectors, there may be opportunities for such funds to be passed around in parallel, informal or shadow economies.[19]

Strict banking regulations have the undesired side effect of encouraging people to remain unbanked

Should countries in Southern Africa implement anti-terrorist financing measures costing a lot of money that could otherwise be used for development purposes?

As mentioned above, foreign development assistance is often tied to compliance with AML/CFT obligations. Although intended as an incentive for developing countries to establish anti-money laundering regimes, the growing need for financial transparency may also work to the advantage of those countries. Not only can suspicious transactions by 'terrorist' or criminal elements be scrutinised, but the malpractices of multinational corporations, corrupt officials and others may be uncovered.

This paper submits that African governments should support initiatives that take account of African realities. International regulations against money laundering and terrorist financing fall short when it comes to addressing the Southern African reality of cash economies. Strict banking regulations have the undesired side effect of encouraging people to remain unbanked. While countries continue to make strides in implementing anti-money laundering mechanisms, an effort should be made to give the unbanked opportunities to become banked without red tape and exorbitant banking fees.

The evidence of terrorist financing in the region is unconvincing. For that reason, it seems more practicable to strengthen the existing banking and financial network in both the formal and informal arena. Development should be the region's top priority, not combating terror financiers with complicated new measures that lack applicability to developing nations or their development goals.

Endotes

1 This paper was first presented at the Seminar on Money Laundering in Botswana organised by the Directorate on Corruption and Economic Crime and the ISS on 24 and 25 April 2006 at the Gaborone Sun Hotel, Gaborone, Botswana.

2 Interview with Mr Lila Hemedi Mkila, Head of Compliance, Bank of Tanzania.

3 Interview with banking and money laundering experts in Blantyre, Malawi, in August 2005.

4 'Terrorist act' means:

(a) any act which is a violation of the criminal laws of a State Party and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to, any person, any number or group of persons or causes or may cause damage to public or private property, natural resources, environmental or cultural heritage and is calculated or intended to:

(i) intimidate, put in fear, force, coerce or induce any government, body, institution, the general public or any segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular standpoint, or to act according to certain principles; or

(ii) disrupt any public service, the delivery of any essential service to the public or to create a public emergency; or

(iii) create general insurrection in a State.

(b) any promotion, sponsoring, contribution to, command, aid, incitement, encouragement, attempt, threat, conspiracy, organizing, or procurement of any person, with the intent to commit any act referred to in paragraph (a) (i) to (iii). (OAU, 1999).

5 Refer to the United Nations website (http://www.un.org) for the status of ratification of the various anti-terrorism instruments.

6 Concerning the financing of terrorism, the Resolution states:

…all States shall:

(a) Prevent and suppress the financing of terrorist acts;

(b) Criminalize the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts;

(c) Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities;

(d) Prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons … (UN, 2001).

7 Interviews with bank officials in Malawi, Namibia and Tanzania during field trips in 2005 and 2006.

8 Interviews with officials from the Financial Intelligence Unit (FIU), Port Louis, Mauritius, February 2005.

9 Interviews with bank officials and other stakeholders during field trips to Botswana, Namibia, Malawi, Mozambique, South Africa, Tanzania and Zambia, November 2004 to July 2006.

10 Interviews with bank officials in Dar es Salaam, Tanzania in November 2004 and March 2006.

11 Interviews with compliance officers in Malawi, Namibia, Tanzania and Zambia, May and July 2005.

12 Interviews with representatives of the respective central banks, Namibia, Malawi and Tanzania, August 2005 and March 2006.

13 Interview with Vekuii Rukoro, CEO, First National Bank Namibia, August 2005.

14 Interview with an anti-money laundering official, Dar es Salaam, Tanzania, March 2006.

15 Interview with a senior official from the Ministry of Finance, Windhoek, Namibia, September 2006.

16 For more information on the viability of FIUs in Eastern and Southern Africa, see Gwintsa (2006:39–54).

17 For a detailed case study, refer to Hübschle (2004).

18 Interview with central bank officials in Malawi, Mozambique and Tanzania in August 2005, July 2006 and March 2006 respectively.

19 A forthcoming ISS monograph will study vulnerabilities of informal sectors in Southern Africa to terrorist financing.

References

Bachus, A.S. 2004. From drugs to terrorism: the focus shifts in the international fight against money laundering after September 11, 2001. *Arizona Journal of International and Comparative Law*, 21(3):834–872.

Banda, J., Katz, A. & Hübschle, A. 2005. Rights versus justice: issues around extradition and deportation in transnational terrorist cases. *African Security Review*, 4(4):59–61.

Block, R. 2002. Terrorists may be setting up shop in South Africa. *The Wall Street Journal*: 11 December.

Elvin, J. 2002. Gem dealers face war-on-terror backlash. *Insight on the News,* 18(25).

FATF. n.d. *Basic facts about money laundering*. Financial Action Task Force on Money Laundering. [Online]. Available: http://www.fatf-gafi.org/MLaundering_en/money_laundering.html [24 October 2006]

Fitzsimons, C. & Lewis, S. 2002. Money laundering: issues for building societies and regional banks. *Financial Services Brief*, 25 (September). [Online]. Available: http://www.ey.com/global/download.nsf/UK/FS_Brief_-_Sep_2002_Issue_25/$file/EY_FS_Brief_09_2002_issue_ 25.pdf [15 December 2005]

Fletcher, B., Jr. 2003. Deadly trade: diamonds are an African's worst friend. *Charleston Gazette*: 16 February.

Gomelsky, V. n.d. Tanzanite business recovering. *National Jeweler*, 96(13).

Goredema, C. 2005. *Organised crime and terrorism: observations from Southern Africa*. ISS Occasional Paper 101, March. Pretoria: Institute for Security Studies.

Gwintsa, M.N. 2006. Challenges of establishing financial intelligence units. (*In* C Goredema (ed.), *Money laundering experiences: a survey*. ISS monograph series, No. 124, June. pp. 39–54. Pretoria: Institute for Security Studies.)

Hübschle, A. 2004. *Unholy alliance? Assessing the links between organised criminals and terrorists in Southern Africa*. ISS Occasional Paper 93, October. Pretoria: Institute for Security Studies.

Hübschle, A. 2006. Flogging a dead horse: the incongruity of measures against terrorist financing in southern Africa. (*In* C Goredema (ed.), *Money laundering experiences: a survey*. ISS monograph series, No. 124, June. pp. 91–120. Pretoria: Institute for Security Studies.)

IMF. 2003. *Suppressing the financing of terrorism*, Washington D.C.: Legal Department, International Monetary Fund.

Ismail, S. 2006. Somalis live in fear in South Africa. *Mail & Guardian online*: 3 October 2006. [Online]. Available: http://www.mg.co.za/articlePage.aspx?articleid=285540&area=/insight/insight__national/ [6 December 2006]

Johnson, J. 2002. 11th September, 2001: will it make a difference to the global anti-money laundering movement? *Journal of Money Laundering Control,* 6(1):10.

Kaplan, E. 2006. *Tracking down terrorist financing*. Council on Foreign Relations, 4 April. [Online]. Available: http://www.cfr.org/publication/10356/tracking_down_terrorist_financing.html [6 December 2006]

Levi, M. & Gilmore, W. 2002. Terrorist finance, money laundering and the rise of mutual evaluation: a new paradigm for crime control? (*In* Pieth, M. (ed.), *Financing terrorism*. Dordrecht: Kluwer Academic Publishers. pp. 87–114.)

Mathers, C. 2004. *Crime school: money laundering*. New York: Firefly Books.

Mlowola, V. 2003. *Terrorism in Tanzania*. Paper delivered at a seminar on terrorism in Southern Africa, Pretoria, 18–19 September.

Moorman, M. 2005. Cutting off the money. [Online]. 30 May. Available: http://www.gtnews.com/article/5956.cfm [18 April 2006]

Mozambique detains Pakistani nationals with huge stash of cash. 2005. *African Terrorism Bulletin*, 4 (September). Pretoria: Institute for Security Studies. [Online]. Available: http://www.iss.co.za/pubs/Newsletters/Terrorism/0405.htm [6 December 2006]

Napoleoni, L. 2005. *Terror incorporated: tracing the dollars behind the terror networks*. New York: Seven Stories Press.

Navias, M.S. 2002. Finance warfare as a response to international terrorism. *The Political Quarterly*, 73(s1):57–79.

OAU. 1999. Convention on the Prevention and Combating of Terrorism. Organisation of African Unity.

Pérouse de Montclos, M-A. 2005. *Diasporas, remittances and Africa south of the Sahara*. ISS monograph series, No. 112, March. Pretoria: Institute for Security Studies

Pieth, M. 2002. Financing of terrorism: following the money. (*In* Pieth, M. (ed.), *Financing terrorism*. Dordrecht: Kluwer Academic Publishers. pp. 115–126.)

Rosenoer, J. 2002. A brief look at anti-money laundering and anti-terrorist financing & the USA PATRIOT Act. [Online]. Available: http://www.cyberlaw.com/aml.html [18 April 2006]

Roth, J., Greenburg, D. & Wille, S. n.d. *Monograph on terrorist financing: staff report to the com-*

mission. National Commission on Terrorist Attacks Upon the United States.

Schott, P. A. 2004. *Reference guide to anti-money laundering and combating the financing of terrorism*. 2nd ed. Washington, DC: World Bank. [Online]. Available: http://www1.worldbank.org/finance/html/amlcft/docs/Ref_Guide_EN/v2/01-Ch01_EN_v2.pdf [6 December 2006]

Tambulasi, R. 2006. Research report on the vulnerabilities of NGOs, charities and schools to terrorist financing in Malawi. July. Unpublished.

The law: an overview. 2003. *Journal of Money Laundering Control*, 6(3):217–232.

UN. 1999a. United Nations General Assembly Resolution 54/110, 9 December. [Online]. Available: http://daccessdds.un.org/doc/UNDOC/GEN/N00/251/34/PDF/N0025134.pdf?OpenElement [6 December 2006]

UN. 1999b. *International Convention for the Suppression of the Financing of Terrorism*, United Nations General Assembly Resolution 54/109, 9 December 1999. [Online]. Available: http://daccessdds.un.org/doc/UNDOC/GEN/N00/251/28/PDF/N0025128.pdf?OpenElement [6 December 2006]

UN. 2001. United Nations Security Council Resolution 1373 (2001), 28 September. [Online]. Available: http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement [6 December 2006]

US Department of State. 2001. *Executive Order 13224*, 14 September. Washington D.C.: Office of International Information Program, Department of State.

Winer, J.M. 2002. Globalisation, terrorist finance, and global conflict: time for a white list? (*In* Pieth, M. (ed.), *Financing terrorism*. Dordrecht: Kluwer Academic Publishers. pp. 5–40.)

Subscription to ISS Papers

If you would like to subscribe to ISS Paper series, please complete the form below and return it to the ISS with a cheque, or a postal/money order for the correct amount, made payable to the **Institute for Security Studies** (marked not transferable).

Please note that credit card payments are also welcome. You can also deposit your payment into the following bank account, quoting the invoice number and the following reference: PUBSPAY.

ISS bank details: ABSA, Brooklyn Court, Branch Code: 634156, Account number: 405 749 8921

Please mail or fax:
ISS Publication Subscriptions, PO Box 1787, Brooklyn Square, 0075, Pretoria, South Africa
ISS contact details: (Tel) +27 12 346 9500, (Fax) +27 12 460 0998; Email: pubs@issafrica.org
Website: www.issafrica.org

Title		Surname		Initials	
Organisation					
Position					
Postal address					
		Postal Code			
Country					
Tel		Fax		E-mail	

ISS PAPERS SUBSCRIPTION 2007 – MIN 8 PER YEAR		
South Africa	African countries*	International
R150.00	US$ 30.00	US$ 40.00

* Angola, Botswana, Burundi, Comores, Congo-Brazzaville, Democratic Republic of the Congo, Gabon, Kenya, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Reunion, Rwanda, Seychelles, Swaziland, Tanzania, Uganda, Zambia, Zimbabwe (formerly African Postal Union countries)

Details of subscription rates for the African Security Review, ISS Monographs, SA Crime Quarterly or other ISS publications are available from:

ISS Publication Subscriptions, PO Box 1787, Brooklyn Square, 0075, Pretoria, South Africa
Tel: +27-12-346-9500/2 • Fax: +27-12-460-0998 • Email: pubs@issafrica.org • www.issafrica.org/pubs.html

The ISS mission

The vision of the Institute for Security Studies is one of a stable and peaceful Africa characterised by human rights, the rule of law, democracy and collaborative security. As an applied policy research institute with a mission to conceptualise, inform and enhance the security debate in Africa, the Institute supports this vision statement by undertaking independent applied research and analysis, facilitating and supporting policy formulation; raising the awareness of decision makers and the public; monitoring trends and policy implementation; collecting, interpreting and disseminating information; networking on national, regional and international levels; and capacity-building.

About this paper

Tough anti-money laundering and terrorist financing regimes have become the key tools in fighting terrorism in the post 9/11 world. The stakes in what the Bush government in the United States has called a 'war on terrorism', have been raised on account of the inevitable friction between the trappings of development, on one hand, and the imperative to maintain security, on the other. Mindful of the differences in banking and financial systems between the developed and developing world, this paper provides an overview of international instruments against terrorist financing, the evolving methods of detecting terrorist financing and the practical problems that are likely to be encountered – and, in some cases, have already been encountered. Informal economic sectors account for a large number of financial and business transactions in Southern African countries. The underlying research question was whether anti-terrorist financing mechanisms applied in the developed world were appropriate and sufficient in Southern Africa. The paper further explores whether Southern African countries can afford to implement anti-terrorist financing measures.

About the author

Annette Hübschle has been with the Cape Town offices of the Institute for Security Studies since 2002. She is a researcher in the Organised Crime and Money Laundering Programme.

Funder

The research was made possible by the generous funding from the Royal Norwegian government.

Published by the Institute for Security Studies • P O Box 1787 • Brooklyn Square • 0075 • Pretoria • SOUTH AFRICA
Tel: +27-12-346-9500/2 • Fax: +27-12-460-0998
Email: iss@issafrica.org • http://www.issafrica.org
67 Roeland Square • Drury Lane • Gardens • Cape Town • 8001 • SOUTH AFRICA
Tel: +27-21-461-7211 • Fax: +27-21-461-7213
Email: issct@issafrica.org