Financial Action Task Force

Groupe d'action financière

TERRORIST FINANCING

29 FEBRUARY 2008

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Terrorist organisations vary widely, ranging from large, state-like organisations to small, decentralised and self-directed networks. Terrorists financing requirements reflect this diversity, varying greatly between organisations. Financing is required not just to fund specific terrorist operations, but to meet the broader organisational costs of developing and maintaining a terrorist organisation and to create an enabling environment necessary to sustain their activities.

The direct costs of mounting individual attacks have been low relative to the damage they can yield. However, maintaining a terrorist network, or a specific cell, to provide for recruitment, planning, and procurement between attacks represents a significant drain on resources. A significant infrastructure is required to sustain international terrorist networks and promote their goals over time. Organisations require significant funds to create and maintain an infrastructure of organisational support, to sustain an ideology of terrorism through propaganda, and to finance the ostensibly legitimate activities needed to provide a veil of legitimacy for terrorist organisations.

Terrorists have shown adaptability and opportunism in meeting their funding requirements. Terrorist organisations raise funding from legitimate sources, including the abuse of charitable entities or legitimate businesses or self-financing by the terrorists themselves. Terrorists also derive funding from a variety of criminal activities ranging in scale and sophistication from low-level crime to organised fraud or narcotics smuggling, or from state sponsors and activities in failed states and other safe havens.

Terrorists use a wide variety of methods to move money within and between organisations, including the financial sector, the physical movement of cash by couriers, and the movement of goods through the trade system. Charities and alternative remittance systems have also been used to disguise terrorist movement of funds. The adaptability and opportunism shown by terrorist organisations suggests that all the methods that exist to move money around the globe are to some extent at risk.

Disrupting funding flows creates a hostile environment for terrorism, constraining overall capabilities of terrorists and helping frustrate their ability to execute attacks. Disrupting terrorist financing involves both systemic safeguards, which protect the financial system from criminal abuse, and targeted economic sanctions informed by counter-terrorism intelligence. The study highlights the links between financial tools and wider counter-terrorist activity: the effectiveness of authorities at both detecting and investigating terrorist activity is significantly enhanced when counter-terrorist intelligence and financial information are used together.

Looking ahead the study identifies four areas which could be the focus of efforts to further strengthen counter-terrorist financing efforts: (1) action to address *jurisdictional issues* including safe havens and failed states, (2) *outreach to the private sector* to ensure the availability of information to detect terrorist financing, (3) *building a better understanding* across public and private sectors and (4) *enhanced financial intelligence* to exploit the value of financial investigation as a tool in fighting terrorism.

INTRODUCTION

With the conclusion of United Nations Security Council Resolution (UNSCR) 1373 in 2001, the international community put financial measures at the centre of its efforts to combat terrorism.

In October of the same year, the Financial Action Task Force (FATF) expanded its mandate beyond anti-money laundering to include countering the financing of terrorism and issued a set of special recommendations on terrorist financing to complement existing standards aimed at countering the laundering of the proceeds of crime.

Conclusions in the early work by the FATF focussed on the similarities between money laundering and terrorist financing. In particular, the similar objectives in money laundering and terrorist financing of masking financial resources and activities from the scrutiny of state authorities and occasional use of similar techniques resulted in the two activities' being examined with the same lens.

Since 2001, significant work has been undertaken to examine how financial measures applied by states, the private sector and the non-profit/charitable sectors, play a role in:

- *Deterring* terrorism.
- *Detecting* terrorism.
- *Disrupting* terrorism.

Although much has been learned about the financing activities used by terrorists in support of their activities, there has been limited success in developing specific indicators to assist financial institutions in the detection of these activities. It is appropriate to re-examine our understanding of terrorist financing and how information can most effectively be used to combat terrorism.

To inform these efforts, this typologies research project was initiated to provide a contemporary snapshot of the ways in which terrorists *raise*, *move* and *use* funds and the ways in which financial information and the implementation of the FATF's international anti-money laundering and combating the financing of terrorism (AML/CFT) standards are helping to hold those responsible to account. This report is organised into four distinct sections, covering in turn: (1) the ways terrorist organisations *use* funds, (2) the ways terrorists *raise* funds, (3) the tools used by terrorists to *move* funds and *iv)* the global response to terrorist financing.

The report begins by surveying the diverse funding requirements that terrorist organisations have in the first place. That is, this report explores what terrorists *need funds for* and what the practical implications are that flow from this need for funds. This initial section generally examines the requirement of terrorist organisations for funds by distinguishing between the financial demands of *direct operational support* and the financial needs of meeting *broader organisational requirements*.

The second section of the report addresses the ways terrorist organisations *raise* funds and obtain support – from legitimate sources (clean money) and from criminal activity. This section also describes the challenge posed by failed states, safe havens and state sponsorship which create an *enabling environment* for terrorist organisations to use funds in strengthening their supporting infrastructure and preparing for attacks.

The third section explores the ways that terrorist organisations *move* funds or support – using the formal financial system, alternative remittance services (ARS), cash couriers, trade, and charities or non-profit organisations (NPOs).

The fourth section describes the global response to terrorist financing. This section describes why financial information provided by financial institutions and intelligence provided to financial institutions are critical to the success of global counter-terrorism efforts. This section then broadly identifies and briefly describes relevant international standards designed to combat the various ways that terrorist organisations raise, move and use funds. This section points to the critical partnership that financial institutions and governments must develop as part of an integrated challenge to combat international terrorism.

Finally, this paper outlines policy implications which could be considered further by the FATF.

THE TERRORIST REQUIREMENT FOR FUNDS

The first step in identifying and forestalling the flow of funds to terrorists[1] is to understand the funding requirements of modern terrorist groups. The costs associated not only with conducting terrorist attacks but also with developing and maintaining a terrorist organisation and its ideology are significant. Funds are required to promote a militant ideology, pay operatives and their families, arrange for travel, train new members, forge documents, pay bribes, acquire weapons, and stage attacks. Often, a variety of higher-cost services, including propaganda and ostensibly legitimate social or charitable activities are needed to provide a veil of legitimacy for organisations that promote their objectives through terrorism.

The nature of funding for both operational and broader support activities will vary by the type of terrorist organisation, with traditional, hierarchical quasi-state-like terrorist organisations on one side of the spectrum and small, decentralised independently supported organisations on the other. At its extreme, this second category has involved small, ostensibly self-directed networks seeking to meet their own funding requirements through means that differ little from their everyday activity. Purchases – even when used to procure the precursors for attacks – are not conspicuous.

Terrorist financing requirements fall into two general areas: (1) funding specific terrorist operations, such as direct costs associated with specific operations and (2) broader organisational costs to develop and maintain an infrastructure of organisational support and to promote the ideology of a terrorist organisation.

DIRECT OPERATIONAL SUPPORT

18. While the funding requirements of terrorist organisations vary too widely to be described by any single typology, recent literature does suggest some common themes as to how terrorists actually use funds[2]. The demand-side of terrorist finance includes:

The direct costs of terrorist attacks and conflict

The precursor materials necessary to stage specific attacks are highly diverse and include, for example, vehicles, improvised bomb-making components, maps, surveillance material etc. These direct costs of terrorist attacks are often very low relative to the damage they can yield, as illustrated by the following estimates:

Table 1: The direct attack costs of a terrorist conspiracy

Attack	Date	Estimated cost[3]
London transport system	7 July 2005	GBP 8 000[4]
Madrid train bombings,	11 March 2004	USD 10 000
Istanbul truck bomb attacks,	15 & 20 November 2003	USD 40 000
Jakarta JW Marriot Hotel bombing	5 August 2003	USD 30 000
Bali bombings	12 October 2002	USD 50 000
USS Cole attack	12 October 2000	USD 10 000
East Africa embassy bombings,	7 August 1998	USD 50 000

1 Obligations set out chiefly in UNSCR 1373, 2001.

2 Including: Comras (2005), Kohlmann (2006), National Commission on Terrorist Attacks Upon the United States (2004) Williams (2005), Abuza (2005) and Prober (2005).

3 Unless otherwise noted, all estimates adapted from the August 2004 report of the UN Monitoring Team Report on al-Qaeda and the Taliban.

4 The United Kingdom Home Office (2006).

Terrorist organisations involved in geographical conflicts have a constant need of funds to support the organisation and their activities in territories they control or act in.

Salaries / subsistence and communications

Individual operatives need to cover their day-to-day expenses and perhaps also those of their dependents. A cell will also need to communicate with its members and perhaps the parent network. This will be a more significant commitment if there is no other source of income for the operatives (such as employment or welfare payments).

Training, travel, and logistics

Training of operatives continues to be an important investment for terrorists, both in terms of ideological indoctrination and practical skills. The financial facilitation of training and travel, which can include the procurement of false documentation, represents an important cost for many terrorist networks. Even in recent attacks where terrorist operatives were "home grown" and largely operationally independent of any overarching leadership structure, many operatives still travelled to receive training or other forms of indoctrination prior to the operational phase of a plot.

Shared funding

Where a cell is part of a network or shares a common goal or ideological or religious background with another cell or network, it may be called upon or feel compelled to provide financial support. An illustrative case study, where funds were collected to host extremist websites used by multiple terrorist networks, is discussed below.

BROAD ORGANISATIONAL REQUIREMENTS

Financially maintaining a terrorist network – or a specific cell – to provide for recruitment, planning and procurement between attacks represents the most significant drain on resources. Beyond the funds needed to finance terrorist attacks and provide direct operational support, terrorist organisations require funding to develop a supporting infrastructure, recruit members and promote their ideology. In addition, this infrastructure spending may go to support charitable organisations and media owned or controlled by the terrorist organisation.

Charities

Terror networks often use compromised or complicit charities and businesses to support their objectives. For example, some groups have links to charity branches in high-risk areas and/or under-developed parts of the world where the welfare provision available from the state is limited or non-existent. In this context, groups that use terrorism as a primary means to pursue their objectives can also utilise affiliated charities as a source of financing that may be diverted to fund terrorist attacks and terrorist recruitment by providing a veil of legitimacy over an organisation based on terrorism[5].

Mass Media Outlets

In addition to the civilian or social welfare function of organisations committed to paramilitary violence, there is often a sophisticated public relations and media operations component that sustains the ideology of terrorism.

Terrorist groups such as al-Qaeda have been especially adept at manipulating television through the release of videos. In addition, virtually every terrorist organisation has a website dedicated to recruitment and spreading the message of bloodshed. These major mass media tools emit powerful

5 Kohlmann (2006).

propaganda for violence, suicide bombing, and the killing of innocent civilians, posing a direct threat to international stability.[6]

Case study: Inciting terrorist violence via the Internet

Three British residents used illicit funds to pay for web sites promoting martyrdom through terrorist violence. The three men were sentenced in 2007 in the UK to jail terms ranging from six-and-a-half years to ten years. All three pleaded guilty to "inciting another person to commit an act of terrorism wholly or partly outside the United Kingdom which would, if committed in England and Wales, constitute murder." These are the first people to be convicted in the UK of inciting terrorist murder via the Internet. Two of the men registered dozens of Internet domains through Web hosting companies in the US and Europe. The sites facilitated communications among terrorists through online forums, hosted tutorials on computer hacking and bomb-making, and hosted videos of beheadings and suicide bombings in Iraq. The sites were paid for with funds stolen from "hacked" credit card accounts, with the money laundered through online gambling sites.

Commentary: This case demonstrates the full scope of terrorist exploitation of the Internet. The three men involved took advantage of the web's global reach and multimedia capability for terrorist recruitment, training, and tactical coordination. They also used the web for terrorist financing through online financial fraud and money laundering.

Source: United Kingdom.

Case study: Terrorist-funded television station

A satellite TV station based in Country A was broadcasting programmes into country B. The content of the broadcasts were pro terrorist and encouraged terrorist acts in country B.

The TV station required substantial funding to keep it operational (around GBP 1 million per annum for the satellite uplink alone). The funding for this came from terrorist group funds. Cash was given to a number of individuals who then made "donations" to the TV station. The TV company had its licence to broadcast in country A revoked and was closed but subsequently opened under another name in a third country.

Source: United Kingdom.

Case study: Terrorist-owned and operated television station

TV Station M is the official television station of Group A. With a stated purpose of waging "psychological warfare," Station M is a potent instrument that incites violence to viewers in the Middle East, Europe, and elsewhere. US Treasury designated Station M for serving as the media arm of Group A and facilitating terrorist activity. The EU has stated that Station M is in breach of Article 22 of the Television Without Frontiers Directive – the directive that governs all audio-visual law – which states that "*Member States shall ensure that broadcasts do not contain any incitement to hatred on grounds of race, sex, religion or nationality.*"[7]

Television employees are members of the organisation and engage in pre-operational surveillance for Group A operations under cover of employment by Station M. The station also supports fundraising and recruitment efforts. The station has broadcast bank account numbers calling for donations specifically for the terrorist organisation and incites viewers to commit acts of violence. The station has repeatedly called for disrupting the public order and peace by promoting suicide bombing and terror. It also broadcasts videos encouraging children to become suicide bombers.

Station M has been removed from ten satellite providers in France, the Netherlands, Spain, Australia, China, Brazil, and the United States. The station is still being broadcast in Europe and the Middle East by two satellite providers.

Source: United States.

---

[6] For al-Qaeda's use of the internet, see Weimann (2004). For material relating to Al-Manar TV, see Jorisch (2004).

[7] For a discussion led by the President of the European Parliament regarding an example of a breach of the *Television Without Frontiers Directive*, see "European Parliament Questions and Answers," 6 July 2005, available online at: www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20050706&secondRef=ITEM-029&language=EN#3-370

For an example of a designation of such an entity, see US Department of the Treasury (2006).

These diverse funding requirements indicate that although individual terrorist attacks can yield great damage at low financial cost, a significant infrastructure (even if relatively loosely organised) is required to sustain international terrorist networks and promote their goals over time.

This broad spectrum of activity is reflected in the financing of terrorist networks themselves. For example, according to the National Commission on Terrorist Attacks on the United States, al-Qaeda is believed to have spent some USD 30 million per year prior to the September 11 attacks on funding operations, maintaining its training and military apparatus, contributing to the Taliban and their high-level officials, and sporadically contributing to related terrorist organisations.[8]

Although the hierarchical, quasi-bureaucratic command and control structures for terrorist finance like pre-September 11 attacks, al-Qaeda may have metamorphosed into more fragmented and decentralised models, the requirements themselves have not necessarily changed over time.

[8] National Commission on Terrorist Attacks Upon the United States (2004).

RAISING TERRORIST FUNDS

In general, terrorist organisations may raise funds through: legitimate sources, including through abuse of charitable entities or legitimate businesses and self-financing, criminal activity, state sponsors and activities in failed states and other safe havens. The examples below principally focus on how terrorists raise funds, with some crossover on how they move funds. The movement of funds will, however, be explored in further detail in the following section.

These sources of terrorist financing can be divided into two general types: financing *from above*, in which large-scale financial support is aggregated centrally by states, companies, charities or permissive financial institutions; and financing *from below*, in which terrorists fundraising is small-scale and dispersed, for example based on self-financing by the terrorists themselves using employment or welfare payments. [9] A single terrorist organisation may use a number of different financing methods.

Raising funds from legitimate sources

Terrorist organisations receive considerable support and funding from and through legitimate sources including charities, businesses, and through self-funding by terrorists and their associates from employment, savings, and social welfare payments. This includes the phenomenon known as "black-washing" where legal funds, for example money stemming from collection by charities or governmental subsidies and social benefits, are diverted for purposes of radicalisation, recruitment or terrorism.

Charities

Charities or non-profit organisations possess characteristics that make them particularly attractive to terrorists or vulnerable to misuse for terrorist financing. They enjoy the public trust, have access to considerable sources of funds, and their activities are often cash-intensive. Furthermore, some charities have a global presence that provides a framework for national and international operations and financial transactions, often in or near areas most exposed to terrorist activity. Finally, charities are subject to significantly lighter regulatory requirements than financial institutions or publicly-held corporate entities, (for example, for starting capital, professional certification or background checks for staff and trustees at registration, or for ongoing record keeping, reporting and monitoring), depending on the country and legal form of the charity and reflecting their principally non-financial role.

In developing the key financial standards to combat terrorism, the FATF has found that "the misuse of non-profit organisations for the financing of terrorism is coming to be recognised as a crucial weak point in the global struggle to stop such funding at its source".[10]

Charities have different sets of risk profiles and thus vary in the types of unusual characteristics that may be detected and help to identify terrorist financing. Broadly speaking, there are three forms of abuse:

(1) Diversion of funds through fraud – for example, donors are told that they are donating money for orphans, and the charity then uses the funds to fund terrorists. This can occur alongside charitable work and within an otherwise legitimate charity.

---

9 Raufer (2007), pp. 17-21.

10 *FATF Best Practices paper on Special Recommendation VIII*.

(2) The use of an entirely bogus or sham organisation that poses as a legitimate charity as a front organisation for terror groups.

(3) Broad exploitation – for example, the charity raises money to feed orphans and actually does so but does it through a designated terrorist organisation.[11]

Diversion/Fraud within legitimate charities

In one case considered for this research, a legitimate charity was established and quickly raised large amounts of funds from the local community. A controller of the charity diverted a portion of these donations to terrorist training camps in Pakistan using a cash courier.

Case study: Exploitation of a legitimate charity

A suspicious transaction report (STR) was made following an attempt by Individual A, to deposit substantial amounts of cash into the account of a charity – over which he had power-of-attorney – with the instruction that it be transferred onward to a notary as an advance for the purchase of real estate.

The Investigation revealed that:

- Payments into the account consisted of multiple cash deposits (presumably donations) but also payments directly from the account of Individual A. In turn, A's personal account revealed multiple cash deposits that corresponded to donations from private individuals.
- The debit transactions consisted of transfers to the non-profit organisation (NPO) and international transfers to Individual B. Police sources revealed that A had links with individuals that were known for terrorist activities, including B.
- Law enforcement assessed that the charity, which continued to fulfil an important social function, was being exploited both as a "front' to raise funds and as a "means of transmission" to divert a portion of them to known terrorist associates of A.

Commentary: This case is indicative of the vulnerabilities to exploitation that arise with weak governance combined with high levels of cash deposits.

Source: Belgium.

Sham charities

While the funds of charities can, on occasion, be misappropriated by individuals with privileged access to them, cases have arisen in which the *entire charity* is used as the vehicle to perpetrate fraud against donors in order to raise funds for terrorism. Terrorist organisations use sham organisations to pose as legitimate charities to disguise terrorist financing activity and provide apparently legitimate explanations for links with terrorist groups.

Case study: Extremist-linked charity used as a vehicle for fraud

Charity X raised significant sums over 2 years by fraudulently obtaining grants from a Government agency.

Intelligence had associated the controllers of the charity with violent extremist groups in another country. Separately, there were indications - such as an unrealistic growth in the organisation's student numbers (and therefore its demands for funds) of possible fraud.

Source: United Kingdom.

[11] For more on this, see FATF (2004).

Case study: Charity embedded in terrorist finance laundering network

An NPO with an office in Russia came to the attention of the authorities through the submission of STRs by credit institutions on an apparent discrepancy between the stated objectives of the NPO and its actual expenditure. The NPO was also known to have a poor history of reporting to the authorities on tax issues.

An investigation revealed that funds were being transferred from the NPO to apparently fictitious or shell entities and then being withdrawn in cash for onward transmission to illegal armed militants.

Source: Russia.

Broad Exploitation

Another area of concern is the use of charitable organisations to raise funds for recipients in a third country who are part of an organisational structure that includes paramilitary violence – a case illustrated by the prosecution in 2000 of a major NPO in the United States. Establishing whether there are linkages between military and charitable aims of a charity can be difficult.

Funds destined to support the participation of terrorist and paramilitary groups in conflicts differ from other forms of terrorist exploitation of charities, giving law enforcement agencies greater opportunities to detect them. The scale of funding required is larger, and transfers are concentrated on specific locations with funds raised where the diaspora of the same ethnic group is living and transferred to the territories the terrorist organisation controls.

Case study: Charity passes funds to organisation engaged in terrorism

Foundation A acted as a charity, while its primary purpose was to support Terrorist Group H. In 2000, Foundation A raised USD 13 million. The US Government shut down four of its offices in the US in 2001.

Foundation A supported the activities of Terrorist Group H through direct fund transfers to its offices in the West Bank and Gaza that were affiliated with the group and transfers of funds to Islamic charity committees ("*zakat*[12] committees") and other charitable organisations that were part of the group or controlled by group members.

Foundation A was established in California in 1989 as a tax-exempt charity, not a religious organisation. It relocated to Richardson, Texas. It had offices in California, New Jersey, and Illinois, and individual representatives scattered throughout the United States, the West Bank, and Gaza.

Person A, a political leader of Terrorist Group H, provided substantial funds to Foundation A. In 1994, Person A (who was named a Specially Designated Terrorist by the US Department of the Treasury in 1995) designated Foundation A as the primary fund-raising entity for Terrorist Group H in the United States. In July 2004, the US charged Foundation A and seven of its officers with criminally conspiring to provide millions of dollars to Terrorist Group H and the families of suicide bombers. The criminal charges included conspiring to provide and providing material support to a foreign terrorist organisation, tax evasion and money laundering.

Source: United States.

Legitimate Business

The proceeds of legitimate businesses can be used as a source of funds to support terrorist activities. This is a particular risk in sectors which do not require formal qualifications (such as a master craftsman certificate) and where starting a business does not require substantial investments. The risk that a business will divert funds to support terrorist activity is greater where the relation between sales reported and actual sales is difficult to verify, as is the case with cash-intensive businesses.

[12] *Zakat* is a voluntary charitable tithe, normally of 1/40th of income, paid as a religious obligation.

Case study: Diversion of funds from legitimate business

The personal bank account of Person A (a restaurant manager) regularly received cheques drawn from wooden pallet Company B, as well as significant cash deposits. The account did not show any 'normal' financial activity such as payment for food, travel, etc. The bank account of Company B also showed significant cash withdrawals of between EUR 500000 and EUR 1 million.

The bank where A's account was held became suspicious because of the inconsistency between Person A's profession and the nature of Company B's business and submitted a suspicious transaction report to the financial intelligence unit. FIU analysis revealed that the individuals concerned were linked to Salafist movements, and the case was referred to prosecutors for wider investigation.

Source: France.

Case Study: Account monitoring reveals terrorist financing activity

Routine monitoring of the bank account of a locksmith company revealed large-scale flow of funds that was disproportionate to the normal business activity of this kind of company. The company had also issued cheques to individuals involved in organisations defending prisoners detained for terrorist offenses.

FIU analysis revealed links between the locksmith company and radical movements; with individuals sending money orders between themselves as well as to prisoners and to other individuals registered in police databases. This prompted wider investigation by judicial authorities.

Source: France.

Self-Funding

In some cases, terrorist groups have been funded from internal sources, including family and other non-criminal sources. The amounts of money needed to mount small attacks can be raised by individual terrorists and their support networks using savings, access to credit or the proceeds of businesses under their control. Terrorist organisations can be highly decentralised, and self-funding can include cases in which a relatively autonomous external financial facilitator who is not directly involved in planning or carrying out an attack nevertheless contributes funding.

Case study: A small, self-funded network launches major attack

The official report into the 7 July 2005 attacks on the London transport system stated that:

"Current indications are that the group was self-financed. There is no evidence of external sources of income. Our best estimate is that the overall cost is less than GBP 8 000."

"The bombs were homemade, and that the ingredients used were all readily commercially available and not particularly expensive".

"The group appears to have raised the necessary cash [for overseas trips, bomb making equipment, rent, car hire] by methods that would be extremely difficult to identify as related to terrorism or other serious criminality."

Terrorist A "*appears to have provided most of the funding. He had a reasonable credit rating, multiple bank accounts (each with just a small sum deposited for a protracted period), credit cards and a GBP 10 000 personal loan. He had 2 periods of intensive activity – firstly in October 2004 and then from March 2005 onwards. He defaulted on his personal loan repayments and was overdrawn on his accounts*."

Terrorist B "*made a number of purchases with cheques (which subsequently bounced) in the weeks before 7 July. Bank investigators visited his house on the day after the bombings*."

Commentary: Though Terrorist B was not specifically identified as a terrorist until after an attack took place, this case demonstrates that financial intelligence on its own was sufficiently accurate to prompt investigation by financial institutions.

Source: United Kingdom.

Case study: Small, self-funding network plans attack

In July 2006**,** rail employees found two unattended suitcases on two German regional trains. Improvised explosive and incendiary devices were discovered in each suitcase consisting of a propane tank, an alarm clock as a timer, batteries for energy supply, various detonating agents as well as a plastic bottle filled with petrol.
The instructions for building an explosive device were taken from an al-Qaeda-linked website, with components purchased in ordinary shops, costing no more than EUR 250.

No suspicious funding from abroad was required, and the suspect's primary source of funding during this period was from family members to pay for his education. The only transactions that appear to have been linked to the planned attack were for plastic bottles, which when filled with petrol and linked to propane tanks would have made an improvised explosive device.

Source: Germany.

Raising funds from criminal proceeds

In the past, some terrorist groups derived much of their funding and support from state sponsors of terrorism. With increased international pressure, many of these funding sources have become less reliable and, in some instances, have disappeared altogether. In addition, newer decentralised, independent cells often do not have the same level of access to foreign funding as traditional terrorist groups. As a result, terrorist groups have turned to alternative sources of financing, including criminal activities such as arms trafficking, kidnap-for-ransom, extortion, racketeering and drug trafficking.

Terrorist use of criminal activity to raise funds ranges from low-level fraud to involvement in serious and organised crime. It is often difficult to determine whether the funds raised from these activities are destined for terrorist activities or are simply the proceeds of general criminal activity. Described below are criminal activities terrorists are known to have engaged in, including selling narcotics, credit card fraud, cheque fraud and extortion. Each of these is discussed in turn.

Drug Trafficking

Drug Trafficking is an attractive source of funds for terrorist groups, enabling them to raise large sums of money. The degree of reliance on drug trafficking as a source of terrorist funding has grown with the decline in state sponsorship of terror groups. This trend has increasingly blurred the distinction between terrorist and drug trafficking organisations.

Both criminal organisations and terrorist groups continue to develop international networks and establish alliances of convenience. Globalisation has enabled both terror and crime organisations to expand and diversify their activities, taking advantage of the internationalisation of communications and banking systems, as well as the opening of borders to facilitate their activities.

Investigations and intelligence have revealed direct links between various terrorist and drug trafficking organisations that frequently work together out of necessity or convenience and mutual benefit. Some examples are detailed below:

Case study: Terrorist organisation raises money through drug trafficking

Since 1990, Person A led an international heroin-trafficking organisation (the "Organisation") responsible for manufacturing and distributing millions of dollars worth of heroin in Afghanistan and Pakistan. The Organisation then arranged for the heroin to be transported from Afghanistan and Pakistan into the United States, including New York City, hidden inside suitcases, clothing and containers. Once the heroin arrived in the United States, other members of the Organisation received the heroin and distributed the drugs. These co-conspirators then arranged for millions of dollars in heroin proceeds to be laundered back to Person A and other members of the Organisation in Afghanistan and Pakistan. To launder the funds, Person A used several import/export commercial enterprises to wire his funds. Funds were placed in the financial system as proceeds and/or expenses related to those diverse concerns and remitted under that cover.

The Organisation was closely aligned with the Taliban in Afghanistan. During the course of their cooperation, the Organisation provided financial support to the Taliban. More specifically, between 1994 and 2000, the Organisation collected heroin proceeds in the United States for the Taliban in Afghanistan. In exchange for financial support, the Taliban provided the Organisation protection for its opium crops, heroin laboratories, drug transportation routes, and members and associates.

Source: United States.

Case study: Terrorist organisation raises money through drug trafficking

Paramilitary organisation F currently supplies more than 50 % of the world's cocaine and more than 60% of the cocaine that enters the United States. Organisation F initially taxed other narcotics traffickers involved in the manufacture and distribution of cocaine in areas it controlled. Recognising the increased profits available, from the 1990s up to the present, Organisation F moved to become directly involved in the production and distribution of cocaine. Methods include, among other criminal activities, setting the prices to be paid to farmers across Colombia for cocaine paste, the raw material used to produce cocaine, and transporting cocaine paste to jungle laboratories under its control where it was converted into ton quantities of finished cocaine and then shipped out of Colombia to the United States and other countries.

Organisation F leaders allegedly ordered the murder of Colombian farmers who sold cocaine paste to external buyers or otherwise violated its strict cocaine policies. Colombian farmers who violated rules were allegedly shot, stabbed, or dismembered alive, and the bodies of murdered farmers were cut open, filled with rocks, and sunk in nearby rivers. Organisation F Leadership also allegedly ordered members to kidnap and murder US citizens to discourage the US government from disrupting its cocaine-trafficking activities. In July 2007 a senior leader was convicted of conspiring to commit hostage-taking. Organisation F leaders allegedly authorised their members to shoot down US fumigation planes and plotted to retaliate against US law enforcement officers who were conducting the investigation into the organisation's narcotics activities.

Recognising that cocaine was the lifeblood of Organisation F, its leaders allegedly collected millions of dollars in cocaine proceeds and used the money to purchase weapons for terrorist activities against the government and people of Colombia.

Source: United States.

Case study: Terrorist organisation financed using proceeds of drug trafficking

During a drugs investigation in relation to cocaine importation from South America to Europe, the FIU found out that the organisation involved in the drugs trafficking used money transfers to send funds from the Netherlands to Paraguay and Brazil to invest in drugs and profits to Lebanon. Police investigations indicated that the profits were used to fund a terrorist organisation.

Source: The Netherlands.

Case study: Exchange of narcotics for weaponry

Nine persons were involved in a conspiracy to procure USD 25 million of weaponry in exchange for cocaine and cash.

High-ranking members of the group were arrested in a sting operation in Costa Rica, while they were preparing to inspect a purported cache of weapons. Simultaneous with that operation, the weapons broker was arrested in the United States.

Commentary: This case is an example of an attempt by a terrorist group to finance its activities, including the purchase of weaponry, through the sale of illegal narcotics. Seven defendants pleaded guilty to both providing material support to terrorists and to drug conspiracies. Three defendants pleaded guilty to the material support conspiracy only.

Source: United States.

Case study: Terrorist organisation extorts money from drug traffickers

An investigation and prosecution carried out by Turkish authorities revealed that drug trafficking is the principal source of funds for a terrorist organisation. Drugs are grown in Pakistan, Afghanistan and Iran; and sent from there to Europe, both through known members of the organisation, and through their associates and other non-designated militants.

In 2007, more than 10 members of the organisation terrorist group were arrested and large amounts of money seized. Investigation and testimony by these members revealed that the organisation extorts money from smugglers at points of entry in the North of Iraq in the form of 'taxes' worth around 7% of the value of smuggled items. The groups also collect money for each person or each car crossing their 'customs points'. One such 'customs point' earns USD 20,000 — 30 000 per week. One member of the group stated that the most important income for the group is the money collected from drug traffickers as 'taxation'.

Source: Turkey.

Credit card fraud

The methods of making dishonest purchases through the use of someone else's credit card details are many – but one of the easiest ways to do so is to buy goods using the internet or by phone (carding). The two cases studies in this report related to credit card fraud shows the vulnerability of credit cards to misuse for terrorist financing purposes and other illegal activities.

There is a market for illegally obtained personal details, including credit card account numbers, as well as personal information such as the card holder's full name, billing address, telephone number, start and expiry dates, the security number on the rear of the card, etc.

Case study: Stolen card details purchased online

Person A frequented criminal Internet sites that specifically bought and sold credit card information (including shadowcrew.com, investigated by the United States Secret Service in 2003). Stolen credit card numbers were passed to Associate B, and then on to C, a computer expert specialising in facilitating the creation and management of websites that provided forums for extremists and downloads of highly violent material intended to incite attacks.

The associates were later found to be linked, via telephone and e-mail records to a terrorist cell in Bosnia, and were arrested on the brink of launching an attack.

Commentary: The case illustrates how terrorists' need for funds can go far beyond those required to launch specific attacks. In this case, terrorist facilitators fully exploited the opportunities of new technology to acquire funds illicitly and anonymously – extending the distance between their identity and their actions. The case also highlighted how sophisticated forensic skills can be needed to recover financial data. Note that the case study "Inciting terrorist violence via the Internet" (see above) describes how terrorists made use of the money raised through the methods described in the current case.

Source: United Kingdom.

Case study: Credit card fraud

A North African terrorist funding group accumulated details of nearly 200 stolen cards and raised more than GBP 200 000 to fund the al-Qaeda terrorist network through international credit card fraud. Twenty to thirty 'runners' collected the names and credit card details of almost 200 different bank accounts from contacts working in service industries such as restaurants. These details were not used in their country of origin (the UK) but sent on to associates in Spain and the Netherlands. These associates used the cards to fraudulently collect more than GBP 200 000 for al-Qaeda cells around Europe.

Commentary: The case illustrates that the high returns achievable from credit card fraud are not lost on terrorists and that sophisticated arrangements can be put in place to operate a fraud ring linked to terrorism.

Source: United Kingdom.

Cheque fraud

Several cases have been identified in which a basic model of bank fraud has been applied to generate funds for terrorism. These cases involved bank accounts being opened using false identity documents and fraudulent deposits. Cheque books are then stockpiled; and when a large number have been accumulated, they are used to purchase goods from department stores costing under the amount that would trigger verification to ensure sufficient funds were available in the account. The goods are returned for a cash refund. This activity can be carried out by organised individuals, who draw on cheques from the same account simultaneously in several locations.

Chequebook fraud, which has figured in a number of terrorist finance cases, allows terrorists to raise and move significant amounts of cash quickly. There are often limited preventative measures in place to obviate what appears to be an "ordinary" crime, rather than terrorist finance. It can be perpetrated alone or in concert with others to maximise the amount taken.

Case study: Cheque fraud

A network of North African terrorists used organised, low-level bank fraud against a number of UK banks to raise funds in support of terrorist activity. Using in excess of 50 individuals the group raised at least GBP 550,000 within 12 months. Once raised this money was used to support terrorist training, procurement, travel and subsistence costs incurred by terrorists and extremists across Europe.

Source: United Kingdom.

Extortion

Supporters of terrorist and paramilitary groups exploit their presence within expatriate or diaspora communities to raise funds through extortion. A terrorist organisation would make use of its contacts to tax the diaspora on their earnings and savings. The extortion is generally targeted against their own communities where there is a high level of fear of retribution should anyone report anything to the authorities. They may also threaten harm to the relatives – located in the country of origin – of the victim, further frustrating any law enforcement action.

Extortion from diaspora communities can be a significant and consistent source of funds. Estimates state that before 2001 one terrorist group collected up to USD 1 million a month from expatriates in Canada, Britain, Switzerland and Australia, making it among the most well-funded terrorist groups in the world.[13] One report outlines how extortion demands were made on expatriate businesses of up to CAD 100 000 and GBP 100 000 in Canada and the UK respectively, with equally high demands made in France and Norway.[14]

13 Kurth Cronin (2004).

14 Human Rights Watch (2006).

Case study: Extortion of a commercial organisation

In September 2007, Company C was sentenced to pay a USD 25 million criminal fine, placed on five years of corporate probation and ordered to implement and maintain an effective compliance and ethics program. Earlier in the year, Company C pleaded guilty to one count of engaging in transactions with a Specially Designated Global Terrorist (SDGT) in that, from 1997 through 2004, the company made payments to a terrorist group. The payments, demanded by the group, were made nearly every month and totalled over USD 1.7 million. The group was designated as a Foreign Terrorist Organisation in September 2001, and listed as an SDGT in October 2001.

Source: United States.

Multiple types of criminal activity

The opportunism of terrorist financiers is particularly illustrated by cases where suspects move fluidly from one kind of crime to another. One group considered in this research was found to be responsible for burglary, identity theft and credit card fraud in its drive for funds.

Case study: Use of multiple types of criminal activity

A terrorist financier was a member of an enterprise that created a complex cigarette smuggling scheme in the US. This financier would purchase low-taxed cigarettes from one US State; apply forged 'tax stamps' to the goods; and then smuggle the untaxed cigarettes into Michigan (where State cigarette taxes are considerably higher) for resale.

In parallel with this exercise, the organisation defrauded retail and wholesale merchants with counterfeit credit cards. The cash garnered from these unlawful activities would then be laundered by members of the enterprise by purchasing businesses, buying additional cigarettes, and obtaining additional fraudulent credit cards.

The enterprise also committed acts of arson and attempted to engage in insurance fraud by burning down a cigarette shop that it owned on an Indian reservation in New York, and then attempted to recover on their fire insurance policy.

The terrorist financier used the profits from these activities to provide material support to a designated terrorist organisation.

Commentary: This case demonstrates the wide range of fraudulent activities that terrorist supporters will engage in, such as trading in illegal contraband, and tax, credit card and insurance fraud, to generate funds to support terrorist groups.

Source: United States.

The role of Safe Havens, Failed States, and State Sponsors

Whether through the absence of effective jurisdictional control, tolerance of terrorist organisations and their activities, or active support to terrorist organisations, safe havens, failed states and state sponsors create enabling environments or otherwise provide support to terrorist organisations.

Safe havens, failed states and state sponsors continue to represent crucial sources of support for terrorist organisations today, including from territories in Somalia, Iraq, and the Pakistan-Afghanistan border.

Safe havens and wider cases of weak jurisdictional control, state tolerance or support of terrorist organisations are also important in how terrorists *move* and *use* finance, in addition to their role in raising terrorist funds. The wider issues of how jurisdictional factors can enable terrorists to move funds are discussed in the next section.

Case study: State sponsorship of terrorism by the Taliban regime in Afghanistan

When the Taliban regime swept to power in Afghanistan in late 1996, it became a critical safe haven and source of support for Osama bin Laden and al-Qaeda until it was removed from power by international coalition forces following the terrorist attacks against the United States on 11 September 2001.

On 15 October 1999, the United Nations Security Council unanimously adopted Security Council Resolution (UNSCR) 1267 against the Taliban regime in Afghanistan in response to the Taliban's continuing support for terrorist organisations and activity, including providing sanctuary to Osama bin Laden and al-Qaeda. In particular, UNSCR 1267 cited the continuing use of Afghan territory, especially areas controlled by the Taliban, for the sheltering and training of terrorists and planning of terrorist acts, and the safe haven provided by the Taliban to Osama bin Laden and al-Qaeda to allow the continued operation of terrorist training camps from Taliban-controlled territory and the use of Afghanistan as a base from which to sponsor international terrorist operations.

UNSCR 1267 also noted the indictment of Osama bin Laden and his associates by the United States for, *inter alia*, the 7 August 1998 bombings of the United States embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania and for conspiring to kill American nationals outside the United States, and the continued refusal of the Taliban to surrender them for trial,

Finally, as noted in UNSCR 1267, the Taliban facilitated the largest production of opium in the world as a means of financing their activities and providing further support for international terrorism and a war effort that devastated the humanitarian conditions of the people of Afghanistan.

Source: United States.

MOVING TERRORIST FUNDS

There are three main methods by which terrorists move money or transfer value. The first is through the use of the financial system, the second involves the physical movement of money (for example, through the use of cash couriers) and the third is through the international trade system. Often, terrorist organisations will abuse alternative remittance systems (ARS) [15], charities, or other captive entities to disguise their use of these three methods to transfer value. Terrorist organisations use all three methods to maintain ongoing operation of the terrorist organisation and undertake specific terrorist activities. All of these methods are discussed in turn below.

The multiplicity of organisational structures employed by terror networks, the continuing evolution of techniques in response to international measures and the opportunistic nature of terrorist financing all make it difficult to identify a favoured or most common method of transmission. Regular funding to maintain a group's capacity is best facilitated via the conventional banking system – as money sent from one country to another can be disguised behind false name accounts, charities or businesses to disguise the ultimate recipient; but other ways to move money are used for specific purposes, or to disguise terrorist financial trails.

The literature on terrorist finance developed since 2001 has emphasised the great adaptability and opportunism[16] that terrorists deploy in meeting their funding requirements. Indeed, the breadth of cases outlined below suggests that the answer to the question: "How do terrorists raise and move funds?" is:"Any way they can."

Cases highlight how in many situations, the raising, moving and using of funds for terrorism can be especially challenging and almost indistinguishable from the financial activity associated with everyday life. The identification and the disruption of terrorist finance are naturally harder when authorities are confronted by "informal" support networks that do not operate as part of well structured organisations with clear roles and lines of accountability. In such circumstances, the links between financial activity and *terrorist* activity become more opaque and the targets for disruption harder to identify.

Indeed, experience suggests that *all* of the mechanisms that exist to move money around the globe are to some extent at risk. This is illustrated by the list of known and historical techniques provided below that are drawn from earlier research.[17] A challenge common to them all is that the connections between funds and terrorism can be extremely difficult to determine in the country of origin, when the terrorist-related activity itself takes place elsewhere.

Formal financial sector

Financial institutions and other regulated financial service providers represent the formal financial sector and serve as the principal gateway through which retail and commercial transactions flow. Additionally, the services and products available through the formal financial sector serve as vehicles for moving funds that support terrorist organisations and fund acts of terrorism. The speed and ease with which funds can be moved within the international financial system allow terrorists to move funds efficiently and effectively and often without detection between and within jurisdictions.

---

[15] Alternative remittance systems are addressed by the FATF Recommendations (see *FATF Special Recommendation VI*).

[16] See Williams (2005) and National Commission on Terrorist Attacks Upon the United States (2004).

[17] Examples include Comras (2005), Kohlmann (2006). National Commission on Terrorist Attacks Upon the United States (2004), The United Kingdom Home Office (2007) and Abuza (2003).

Combined with other mechanisms such as offshore corporate entities, formal financial institutions can provide terrorists with the cover they need to conduct transactions and launder proceeds of crime when such activity goes undetected.

Money and value transfer (MVT) mechanisms have proven to be particularly attractive to terrorists for funding their activities, as demonstrated by the cases below. MVT operations range from the large-scale and regulated funds transfer mechanisms available in the formal financial sector, to small-scale alternative remittance systems (discussed separately below). Funds transfers refer to any financial transaction carried out for a person through a financial institution by electronic means with a view to making an amount of money available to a person at another financial institution. It was this use of wire transfers that the FATF was addressing when it issued Special Recommendation VII in October 2001 which requires that full originator information accompany any such transfer.

Analysis of a number of terrorism cases has revealed that radical groups as well as persons related to terrorist organisations have used the network of the registered and world-wide operating money transfer companies to send or receive money. These transactions enabled authorities to develop a wider understanding of the main contacts of these people and the extent of their networks. By creating a public–private partnership with the money transfer organisations, it has been possible to gain a valuable source of financial intelligence on the operations of networks worldwide. Money transfer offices are obliged to register identity-data of the person who sends the money from Country A and the person who receives the money in Country B - in line with FATF Special Recommendation VII. These data have proved to be excellent input for network analysis in regard to terrorist financing.

Case study: Terrorist organisation uses MVT mechanisms to move money

Person D, a leader of a terrorist organisation based in Country C and once a resident in Country A, was in hiding in Country B. The FIU in Country A found out though investigations that persons in Country A were sending money through money transfers to D's friends in Country B to financially support him. The money flow was detected because the transfers were made by nationals of Country C – which was unusual in Country A. Person D was later arrested in Country B on suspicion of terrorism. Money transfers from Country A to Country B were presented in court as supporting evidence of terrorist financing.

Source: The Netherlands.

Advances in payment system technology have had a twofold impact on the potential abuse by terrorist financiers and money launderers of such systems. Electronic payment systems allow law enforcement an increased ability to trace individual transactions through electronic records that may be automatically generated, maintained and/or transmitted with the transaction. However, these advances also create characteristics that may be attractive to a potential terrorist or money launderer. For instance, the increased rapidity and volume of funds transfers, in the absence of the consistent implementation of standards – such as SR VII – for recording key information on such transactions, maintaining records, and transmitting necessary information with the transactions, could serve as an obstacle to ensuring traceability by investigative authorities of individual transactions.

Case study: Terrorist organisation uses wire transfers to move money across borders

A terrorist organisation in Country X was observed using bank wire transfers to move money in Country Y that was eventually used for paying rent for safe houses, buying and selling vehicles, and purchasing electronic components with which to construct explosive devices. The organisation used “bridge” or “conduit” accounts in Country X as a means of moving funds between countries. The accounts at both ends were opened in the names of people with no apparent association with the structure of terrorist organisation but who were linked to one another by kinship or similar ties. There were thus the apparent family connections that could provide a justification for the transfers between them if necessary.

Funds, mainly in the form of cash deposits by the terrorist organisation were deposited into bank accounts from which the transfers are made. Once the money was received at the destination, the holder either left it on deposit or invested it in mutual funds where it remained hidden and available for the organisation’s future needs. Alternatively, the money was transferred to other bank accounts managed by the organisation’s correspondent financial manager, from where it was distributed to pay for the purchase of equipment and material or to cover other ad hoc expenses incurred by the organisation in its clandestine activities.

Source: FATF Typologies Report 2003-4.[18]

[18] FATF (2004).

Trade Sector

The international trade system is subject to a wide range of risks and vulnerabilities which provide terrorist organisations the opportunity to transfer value and goods through seemingly legitimate trade flows. In recent decades, international trade has grown significantly: global merchandise trade now exceeds USD 9 trillion a year and global trade in services accounts for a further USD 2 trillion.[19] The specific methods and techniques used to launder money through the trade system were described in the 2006 FATF Typology Report on trade-based money laundering,[20] although terrorist financing was not a focus of that work. Further examination of the specific methods and techniques used to exploit the trade system for terrorist financing purposes could assist in the development of measures to identify and combat such activity.

Case Study: Terrorist use of the trade sector to move funds

An FIU received disclosures from several banks concerning account holders: Persons A and B and Company C, all active in the diamond trade. In the space of a few months, A, B and C's accounts saw a large number of fund transfers to and from foreign countries. Moreover, soon after the opening of his account, person B received several bank cheques large amounts in US dollars.

Financial information collected by the FIU showed that Company C was received large US dollar transfers, originating from companies active in the diamond industry and debited by several transfers to the Middle East in favour of Person A, a European citizen born in Africa and residing in the Middle East. One of the directors of Company C, a Belgian citizen residing in Africa, held an account at a bank in Belgium through which transfers took place to and from other countries in Europe, Africa, North America, and the Middle East. Inward transfers from foreign countries mainly took place in US dollars. These were then converted to EUR and used to make transfers to foreign countries and to accounts in Belgium belonging to Person B and his wife.

Police information collected by the FIU showed that the prosecutor had opened a file related to trafficking in diamonds originating in Africa. The largest transfers of funds by the company trading in diamonds were mainly destined to the same person, A, residing in the Middle East. Police sources revealed that both Person A and Person B were suspected of having bought diamonds from the rebel army of an African country and of smuggling them into Belgium for the benefit of a terrorist organisation.

Moreover, it appeared that certain persons and companies linked with Persons A and B had already been referred to prosecutors by the FIU in other cases for money laundering derived from organised crime.

Source: Belgium.

Cash couriers

The physical movement of cash is one way terrorists can move funds without encountering the AML/CFT safeguards established in financial institutions. It has been suggested[21] that some groups have converted cash into high-value and hard-to-trace commodities such as gold or precious stones in order to move assets outside of the financial system.

Counter-terrorist operations have shown that cash couriers have transferred funds to a number of countries within the Middle East and South Asia. Direct flight routings are used for simple transfers; however, indirect flight routings using multiple cash couriers and changes in currencies take place within more sophisticated schemes.

The movement of cash across borders is prevalent in countries where the electronic banking system remains embryonic or is little used by the populace. Large parts of Africa and the Middle East have predominantly cash-based societies, and this naturally lends itself to cash flows using alternative remittance systems or by courier. Analysis of a number of terrorism cases has shown that money couriers are active even within Europe and between countries with a well functioning financial system. In most cases couriers are involved in moving funds generated outside the financial system and kept out of the financial system to avoid detection.

19 World Trade Organisation (2005).

20 FATF (2006).

21 *Ibid.*

Case Study: Terrorist financing using cash couriers

The activities of Terrorist Organisation A in Southeast Asia clearly show the critical role of cash couriers in support of their terrorist operations. Organisation A avoided using the conventional banking system in order to evade safeguards and to avoid leaving an audit trail for law enforcement. The funding for the Bali bombings that took place in October 2002 were provided by Al-Qaeda's chief of operations to Person H, Organisation A's head of operations, who was hiding in Thailand in 2002. Person H passed USD 30 000 to the perpetrators of the Bali bombings in two batches using several cash couriers. The couriers took several weeks to complete the runs. The funding for the JW Marriott Hotel bombing in Jakarta was also provided by Person H from Thailand. Again, a total of USD 30 000 of Al-Qaeda's funds was sent to Indonesia in April 2003 through a string of couriers.

Source: Asia Pacific Group (APG) Annual Typologies Report 2003-2004.

Moving money using cash couriers may be expensive relative to wire transfers. As legitimate financial institutions tighten their due diligence practices, it has become an attractive method of transferring funds without leaving an audit trail. When cross border remittance of cash is interdicted, the origin and the end use of cash can be unclear. Cash raised and moved for terrorist purposes can be at very low levels – making detection and interdiction difficult.

Case study: Terrorists use Gold to Move Value

During the invasion of Afghanistan in 2001, it was widely reported that the Taliban and members of al-Qaeda smuggled their money out of the country via Pakistan using couriers that handled bars of gold. In Karachi, couriers and hawala dealers transferred the money to the Gulf Region, where once again it was converted to gold bullion. It has been estimated that during one three-week period in late November to early December 2001, al-Qaeda transferred USD 10 million in cash and gold out of Afghanistan.[22] An al-Qaeda manual found by British forces in Afghanistan in December 2001 included not only chapters on how to build explosives and clean weapons, but on how to smuggle gold on small boats or conceal it on the body.[23]

Gold is often used by hawala brokers to balance their books.[24] Hawala dealers also routinely have gold, rather than currency, placed around the globe. Terrorists may store their assets in gold because its value is easy to determine and remains relatively consistent over time. There is always a market for gold given its cultural significance in many areas of the world, such as Southeast Asia, South and Central Asia, the Arabian Peninsula, and North Africa.

Source: United States.

Use of Alternative Remittance Systems (ARS)

Alternative remittance systems (ARS) are used by terrorist organisations for convenience and access. ARS have the additional attraction of weaker and/or less opaque record-keeping and in many locations may be subject to generally less stringent regulatory oversight. Although FATF standards call for significantly strengthened controls over such service providers, the level of anonymity and the rapidity that such systems offer have served to make them a favoured mechanism for terrorists. For some networks there are also cultural and pragmatic reasons for using these services: many have their origins or control structures in areas where the banking infrastructure is weak or practically non-existent. The role of ARS in terrorist financing may be primarily an "end-user" gateway; *i.e.* the means by which new or stored funds are passed to operational cells.

22 For sources relating to al-Qaeda's abuse of the gold sector see the following sources: US Government Accountability Office (2003), Farah (2002), British Broadcasting Corporation(2002) and Shahzad (2002). In addition, for a detailed study of al-Qaeda's use of diamonds and gold, see Global Witness (2003). More generally, in FATF (2003), there is a section that details the use of gold and diamonds in money laundering.

23 US Government Accountability Office (2003) and Global Witness (2003).

24 Commonwealth Secretariat (1998).

Case study: Alternative remittance system used for terrorist financing

An African national, residing in Africa, held an account with a bank in European Country B. This account had been credited with significant sums transferred from companies that had their registered offices mostly in Western Europe. Shortly afterwards the client issued an order to transfer a large sum in favour of a company in the Middle East which held an account with a bank located there.

Analysis by the FIU revealed the following elements:

- According to police information, it appeared that the beneficiary bank, located in the Middle East, was suspected of maintaining financial links with a terrorist group.
- According to the security services in Country B, this bank had collaborated with another bank in making transfers of funds on behalf of hawala operators. This latter bank was suspected of having links with an organisation with ties to a terrorist group.
- Analysis further revealed that the account of the African national, who had no known connections with Country B, was being used as a transit account for large funds transfers originating primarily with a European company involved in the sale of chemical products and destined for a company in the Middle East. There was no apparent reason why operations should be performed via an account in country B.

Source: Belgium.

Use of Charities and Non-Profit Organisations

Charities are attractive to terrorist networks as a means to move funds. Many thousands of legitimate charitable organisations exist all over the world that serve the interests of all societies, and often transmit funds to and from highly distressed parts of the globe. Terrorist abuses of the charitable sector have included using legitimate transactions to disguise terrorist cash travelling to the same destination; and broad exploitation of the charitable sector by charities affiliated with terrorist organisations. The sheer volume of funds and other assets held by the charitable sector means that the diversion of even a very small percentage of these funds to support terrorism constitutes a grave problem.

Case study: Use of non-profit organisation for terrorist recruitment

A bank checked its customer database for matches with lists relating to terrorism; and found that a non-profit organisation which held an account with it, with its registered office in European Country B, was named on a terrorism list. The Bank submitted a STR based on this match.

The organisation's account had been opened a few years before and had seen low activity, then suddenly experienced a particularly intense bout of activity starting on 1 January 2002. The transactions on this account consisted of multiple cash deposits made by several different people for a large total amount. These funds were then withdrawn in cash.

Analysis by the FIU revealed the following elements:

- Based on information requested from the state security services in Country B, the FIU concluded that this non-profit body was one of a number of contact points in Country B established with the aim of recruiting and sending people to fight in the Middle East.
- It also transpired that two or three of the signature authorities for the account of this organisation were linked to a terrorist group.

This case is the subject of an ongoing judicial investigation.

Source: Belgium.

Case study: Charity embedded in terrorist finance laundering network

FIU analysis of STRs identified substantial transfers of funds between an apparently small company and a charity working in the North Caucasus region.

Further investigation revealed that the company had itself received significant transfers from other charities, ostensibly for consultancy services received from the company. The company had also received funds from an individual based in a region with a high level of activity by extremist groups. The company appeared to be accumulating the income from these sources and then passing it on to the charity in the North Caucasus region.

Further concern arose from the discovery that the charity had another source of funding: a foreign citizen living in Russia, who routinely received transfers of funds of small amounts of cash below the statutory monitoring threshold which were then transferred in bulk to the charity. These small transfers originated from a region with a high level of activity by extremist groups.

The investigation of the charity's expenditures showed that funds were used in a variety of ways, including: cash withdrawal and couriering to the North Caucasus region; direct transfers to a "welfare unit" within a known illegal militant organisation; and onward transfers to apparently legitimate charitable organisations in the North Caucasus region. As a result of the investigation, the authorities discontinued the activities of the charity concerned.

Commentary: This case study serves to highlight the role that captive and compromised charities and businesses can play in providing conduits for multiple donors to operational cells, and in obfuscating the financial trail between financiers and terrorists.

Source: Russia.

INTERNATIONAL RESPONSE TO TERRORIST FINANCING

This section of the report briefly describes how the global response specifically addresses the characteristics of terrorist financing as described in Part II of this report. This section begins by explaining the logic of disrupting terrorist financing and then describes how the international community has developed and applied international standards to combat the various sources, conduits and uses of terrorist financing. Finally, this section concludes with a discussion of the use of financial information to identify and combat terrorist financing and terrorism more broadly. In general, this section highlights the importance and relevance of certain international standards in combating terrorist financing and identifies vulnerabilities where the global response to particular aspects of terrorist financing may need to be strengthened.

The logic of disrupting terrorist finance

Disrupting and dismantling terrorist financing networks is essential to combat terrorism. Terrorist organisations' diverse requirement for financing creates a strong logic for seeking to disrupt terrorism by choking off funding flows to all terrorist-linked activities. Interdicting these flows can degrade the capability of terrorist groups over time, limiting their ability to launch attacks, increasing their operational costs and injecting risk and uncertainty into their operations, which can have tactical benefits, such as:

- Damaging morale, leadership and legitimacy within a network.
- Forcing terrorist groups to shift activity into areas where they are more vulnerable, including areas that they would otherwise avoid.[25]

The disruption of specific attacks through the interdiction of specific transactions appears highly challenging. Recent attacks demonstrate that they can be orchestrated at low cost using legitimate funds and often without suspicious financial behaviour.

Nevertheless, direct attack costs are only a fraction of terrorist organisations' demand for funds. Disrupting financial flows to terrorist organisations limits the resources available for propaganda, recruitment, facilitation, et cetera, in ways that frustrate terrorists' ability to promote and execute attacks over time.

In large measure, terrorists require funds to create an *enabling environment* necessary to sustain their activities – not simply to stage specific attacks. *Disrupting terrorist-linked funds creates a hostile environment for terrorism.* Even the best efforts of authorities may fail to prevent specific attacks. Nevertheless, when funds available to terrorists are constrained, their overall capabilities decline, limiting their reach and effect.

Case study: Financial disruption of terrorist activity

A national of Country A was identified leaving the UK in possession of USD 340 000 in cash. Intelligence linked this individual to the support of extremist groups in Country A. Evidence also linked him to criminal offences in Country A. As a result of this information the cash was seized under legal provisions in the UK.

Full investigation subsequently identified that the cash had been given to him so that it could be passed on to terrorists in Country B, where it would be used to finance a planned attack on a senior official of Country B. The seizure of the funds frustrated the intentions of the terrorists, denying them the ability to carry out the intended attack.

Source: United Kingdom.

[25] HM Treasury (2007).

Preventing Terrorists from Raising, Moving, and Using Funds

Previous sections of this report explored the diversity of ways in which terrorist funds are raised, moved and used. Terrorists use legitimate and criminal methods to finance their organisational and operational activities. The international response addresses each of these methods in a focused manner.

Detecting terrorist involvement in otherwise legitimate financial activity requires financial institutions to implement the FATF standards through strong application of the "know your customer" principle and of customer due diligence (CDD) policies and procedures. These are also fundamental to the reporting of suspicious transactions which may indicate criminal activity supporting terrorism.

To assist financial institutions in combating terrorist financing, jurisdictions must adopt certain measures. These include implementing targeted financial sanctions programmes, protecting vulnerable sectors including the charitable sector and money-service businesses, and encouraging effective reporting of suspicious activity.

Targeted Financial Sanctions

FATF Special Recommendation III (SRIII) calls on countries to develop and implement targeted financial sanctions regimes that identify, freeze the assets of, and prohibit making funds available to designated terrorists and their support networks without delay. These requirements are necessary to deprive terrorists and terrorist networks of the means to conduct future terrorist activity and maintain their infrastructure and operations. The preventive intent of SRIII requires countries to designate the elements of terrorist support networks pursuant to an evidentiary standard of reasonableness.[26]

Protecting Vulnerable Sectors

Formal Financial Sector

Jurisdictions have an obligation to protect their financial sectors from money laundering and terrorism finance. In particular, *FATF Special Recommendation VII* was developed with the objective of preventing terrorists and other criminals from having unchallenged access to wire transfers for moving their funds and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator of wire transfers is immediately available to: (1) appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists or other criminals; (2) financial intelligence units for analysing suspicious or unusual activity and disseminating it as necessary; and (3) to beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions.

Charitable Sector

FATF Special Recommendation VIII lays out a framework that aims to protect the non-profit organisation / charitable sector by ensuring it is not misused by terrorist organisations that: (1) pose as legitimate entities; (2) exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (3) conceal or obscure the clandestine diversion of funds intended for legitimate purposes but are diverted for terrorist purposes.

Toward this aim, FATF has developed an effective four-prong approach to identifying, preventing and combating terrorist misuse of charities that focuses on: (1) outreach to the charitable sector; (2) supervision or monitoring of the sector; (3) information gathering and investigation of

[26] *Interpretive Note to Special Recommendation III*, paragraph 2.

terrorists and their networks that abuse the charitable sector; and (4) international engagement to protect the sector globally.[27]

Cash Couriers

FATF Special Recommendation IX was developed with the objective of ensuring that terrorists and other criminals cannot evade financial market controls through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures to: (1) detect the physical cross-border transportation of currency and bearer negotiable instruments, (2) stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, (3) stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed, (4) apply appropriate sanctions for making a false declaration or disclosure and (5) to enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering consistent with FATF Recommendation 3 and Special Recommendation III.

Suspicious Transaction Reporting

Financial information – including that gathered from suspicious transaction reporting (STR) [28] has a central role in identifying terrorist financing and the movement of terrorist funds through the financial system.

Efforts are ongoing to examine the operational experience of counter-terrorism agencies and establish general "alerts" or "indicators" that suggests a particular transaction presents a risk of terrorist finance. The diversity and multifaceted nature of terrorists' financial activity makes this challenging.

Despite the challenge in developing generic indicators of terrorist financing activity, financial institutions may nevertheless identify unusual characteristics about a transaction that should prompt the filing of a suspicious transaction report. Although it may not be immediately apparent to financial institutions, reporting of large cash, electronic transfers, and cross-border currency transactions could provide law enforcement with information on terrorist activity.

National authorities can assist the financial sector in its efforts to identify and prevent terrorist financing by sharing intelligence. *Financial information* alone may not be sufficient to identify terrorist financing activity. However, when combined with *counter-terrorist intelligence* drawn from surveillance of the range of terrorist activities and networks, financial information can be leveraged to provide financial institutions with a concrete indication of possible terrorist activity, whether these use legitimate or criminal sources of funds. More widely, effective information exchange between the public and private sector has been identified by the FATF as one of the five high-level principles for creating a risk-based approach to money laundering and terrorist financing[29].

---

27 *Interpretive Note to Special Recommendation VIII*, paragraph 6.

28 Also known in some jurisdictions as "suspicious activity reports" or "SARs".

29 *FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*; paragraph 2.17ff.

Case study: Additional financial information enriches STR reporting

Counter terrorist officers were tasked with the financial investigation into suspected terrorists based in the UK and Middle East intending to attack high profile targets. The FIU was engaged at an early stage with the development of STRs from the reporting financial sector.

As this investigation progressed, in partnership with counter-terrorist agencies, the FIU analysed the methodologies which were being used by the suspects and was able to enhance and share this information with financial sector STR reporters, particularly with identified vulnerable sectors. This process included meetings with various financial institutions and the dissemination of indicators relating to these activities. The methods used by the terrorists included identity theft, credit card fraud and mortgage fraud.

As a result of this interface between the FIU and the reporting sector, subsequent STRs submitted to the FIU were important in the development of the overall investigation.

Source: United Kingdom.

Modern financial standards require that financial institutions remain vigilant to the warning signs of financial abuse and report that suspicious activity to a financial intelligence unit. In turn, the FIU integrates the financial information gathered from financial institutions with law enforcement and intelligence inputs. It is therefore possible for an FIU to identify terrorist financing activity even though it is generally not possible for financial institutions themselves to draw the link between the suspicious activity and terrorism.

Case study: FIU finds STR to be linked to terrorist network

Individual X's account was credited with considerable cash deposits. On enquiry, he explained that these were his wages, paid by an employer in the Middle East. This was suspicious, as was a large cash deposit made by X to secure the rental of a building. STRs were submitted.

X also owned Company A, which owned Company B in North Africa. The account of Company A was credited with substantial amounts from the Middle East.

Enquiries showed that a manager of Company B (Person Y) had been convicted of terrorism. Further information revealed that X and Y were linked to each other and that Company A was known for an investigation regarding a terrorist organisation.

The cash deposits in X's personal account were linked to terrorism financing.

Source: Belgium.

Case study: Suspicious transaction matches counter-terrorism target

A foreign national residing in Belgium performed significant foreign exchange transactions shortly after officially establishing himself in Belgium. There was no obvious economic rationale for these transactions, which in any case were at a level that was at odds with his financial profile.

An STR was submitted, which – following enquiries by judicial authorities to an exchange house – was followed by a further disclosure which indicated that funds were routed to an individual in Asia, whom police sources suspected of being part of a terrorist organisation seeking to procure weapons.

Source: Belgium.

The analytic function of FIUs to identify terrorist financing activity has been strengthened by combining financial information with terrorist-related intelligence obtained from law enforcement and intelligence. In addition, FIUs have played a key role in disclosing financial information to intelligence organisations. Reports not linked to suspicious activity have therefore been useful in creating links when combined with other terrorist-related intelligence.

One FIU conducted a review of all STRs associated with its terrorist financing cases for a given year and found that, although the STRs may not have related specifically to suspicions of terrorist financing, the information they contained proved significant in identifying additional accounts and

individuals that were linked to subjects of ongoing terrorist financing cases. The FIU was able to conduct further analysis of the transactions involving these additional accounts and in turn, provide law enforcement and intelligence agencies with an expanded network of individuals and accounts that the FIU suspected would be relevant to ongoing terrorist financing investigations. The following table sets out the types of activities that were most frequently reported as suspicious and the indicators that factored into the FIU's Terrorist Financing case disclosures:

Most Frequently Reported Suspicious Activity

- Unusual business activity
- Unable to ascertain source of funds
- Multiple deposits at different branches
- Third party deposits in US cash
- Wire transfers following cash deposits
- Wires to specific location/account on regular basis
- Large cash deposits

Source: Canada

Most Frequently Used Indicators in TF Case Disclosures

- Sending or receiving funds by international transfers from and/or to locations of specific concern
- Atypical business/account behaviour
- Charity/Relief organisation linked to transactions
- Large scale cash transactions
- Media coverage of account holder's activities

Source: Canada

Financial information

The application of the FATF 40 Recommendations and 9 Special Recommendations provides a solid basis upon which to gather financial information. Leveraging this financial information with wider information on counterterrorism, including intelligence, at a national level may prove to be the most effective use of financial information in identifying terrorist activity.

Financial information has come to be one of the most powerful investigative and intelligence tools available. As money moves through the financial system, it leaves a verifiable trail that can in many cases indicate illicit activity, identify those responsible, and locate the proceeds of criminality that can then be recovered. Through the development of internationally recognised AML and CFT standards, financial institutions and other designated non-financial entities have taken steps to know their customers and keep records. The value of financial information in counter-terrorist investigations has increased dramatically in recent years.

Cases above show the investigative value of STRs submitted to FIUs – including those not initially linked to terrorist financing. Investigations draw on information about past transactions and from ongoing monitoring of suspect accounts. Other types of financial reports (including large cash transactions, wire transfers, and cross-border currency movements) can significantly increase the pool of financial information available to investigators.

Financial information is now used as part of the evidential case to hold criminals and terrorists to account. It also has a key intelligence role – for example by allowing law enforcement to:

- *Look backwards*, by piecing together how a criminal or terrorist conspiracy was developed and the timelines involved.

- *Look sideways*, by identifying or confirming associations between individuals and activities linked to conspiracies, even if overseas – often opening up new avenues for enquiry.
- *Look forward*, by identifying the warning signs of criminal or terrorist activity in preparation.

Financial information is particularly suited to these tasks in that it is relatively unambiguous, can be processed easily using technology, and easily accessed with little intrusion on the provider.

Looking Backward: Financial investigation following terrorist acts

Exploiting the 'financial footprint' left behind by terrorists often gives investigators details of how, when and where terrorist attacks were conceived, planned, and executed. Financial information has proved to be a reliable source of historical intelligence, available to investigators even when all the terrorists have died during the commission of their attacks.

Case study: Analysing preparations for an attack

Following a series of suicide attacks investigators were able to exploit financial intelligence which identified vehicle hire, accommodation at hotels, procurement and overseas travel. This assisted in identifying the timescale for the planning and preparation for the attacks. Other investigative techniques we then used to exploit the financial intelligence and establish a comprehensive picture of the lead-up to the terrorist attacks.

Source: United Kingdom.

Looking Sideways: The role of financial intelligence in counter-terrorism enquiries

Conventional investigative techniques have come to rely heavily on identifying telecommunications contacts to establish where there are links between individuals and groups. Following the money can produce similar information: Financial intelligence can be used to identify a terrorist's activity and be used directly to trace links with other individuals and groups, or indirectly to compare methods and approaches. Exploiting this additional intelligence can identify those who may otherwise go undetected. This reduces the chances of successful terrorist attacks.

Case study: Financial investigation jump-starts a post-attack enquiry

The identity of one of four perpetrators of a multiple suicide attack across a city was identified from two credit cards bearing the same name, but found at two different bomb scenes establishing an association between both of them. He was identified with an address that was used as the bomb factory.

Transaction analysis of associated accounts helped to establish the individual's activities in the months preceding the attack and the milestones in the attack-planning exercise, including the purchase of camping equipment associated with a pre-attack training event.

Interviews with shop staff revealed that these purchases had been preceded by others minutes beforehand, made by another person but for exactly the same amount. This was the first time that an association between two individuals, later confirmed as attackers, had been identified.

Commentary: The case is symbolic of the integrated role that forensic financial analysis plays in a counter-terrorism investigation. Financial intelligence, recovered from forensic examination of a bomb scene, provided a leap forward for the investigative team's efforts to establish the identity of the attackers and the nature of the conspiracy, in the immediate aftermath of the attack.

Source: United Kingdom.

Case study: Tactical intelligence sharing as basis for financial investigation

Group G operated a network of cells engaged directly in attack planning and the in the wider facilitation of terrorism. This latter activity included the transmission of funds to Country X to pay for the development of false documentation. In related cases, passport documents were stolen in armed robberies in Europe which were later found in the possession of several Group members in the UK, Germany and France.

With the serial numbers of many of these stolen and falsified documents established, and intelligence connecting these to a terrorist organisation, the FIU of country Y made these systematically available to financial institutions to enable them to cross reference against their 'know your customer' checks. In Country Y, 81 STRs were submitted in response relating to money transfers alone.

Source: The Netherlands.

Looking Forward: Identifying indicators of future attacks

It is challenging to identify a terrorist conspiracy in preparation solely from financial activity. Nevertheless, timely detection of financial factors can play a critical role in identifying indicators of future terrorist activity. The following case study highlights how financial intelligence has been essential in building the evidence suggesting a conspiracy was underway.

Case study: Identifying attack indicators

An individual suspected of involvement with Al-Qaeda used multiple accounts held in multiple identities to fund the supply of bomb components for use in another country. The conspiracy was revealed through extensive and forensic financial investigation, which allowed law enforcement to establish that:

- Travel patterns, crossing multiple jurisdictions to disguise their ultimate destination, all ultimately arrived at the same target country.
- Small items, ostensibly innocent components for improvised explosives, were sent to the same country by international courier over many months.
- Multiple transactions had been made to accounts which, on inspection, were controlled by an associate of the suspect - pointing to a wider conspiracy.

Commentary: The new suspect's financial affairs were deliberately structured to hide the audit trail. Transaction by transaction, it was established that this new target had been operating in close concert with the first, by sending money to the same third country, through third parties in multiple countries. The growing intelligence package now pointed to both suspect components and funds being moved to the same country. In partnership with law enforcement agencies overseas, the original suspect was arrested in a third country in a makeshift bomb factory.

Source: United Kingdom.

POLICY IMPLICATIONS

As this report details, terrorists' need for funds can be significant. Some recent attacks have been orchestrated at low cost, but in addition to the direct costs of mounting attacks, modern terrorist groups require funds for the wide range of activities involved in developing and maintaining an organisation and its ideology. Identifying and disrupting terrorist financing creates a hostile environment for terrorism, helping to limit terrorists' overall capability. Terrorists raise and move funds using distinct methodologies; each of which can be addressed using different tools.

In general, terrorist organisations may raise funds through: legitimate sources, including through abuse of charitable entities; criminal activity; or state sponsors, and activities in failed states or other safe havens.

Legitimate Sources: Terrorist organisations receive considerable support and funding from and through legitimate sources including charities, businesses, and in many cases through self-funding from employment, savings, and social welfare payments – methods that would not otherwise raise concerns because they appear legitimate. Case studies highlight the value of intelligence in determining whether seemingly legitimate activity is being used to fund terrorism.

Criminal Activity: Terrorist groups are increasingly turning to alternative sources of financing, including criminal activities such as arms trafficking, money laundering, kidnap-for-ransom, extortion, racketeering, and drug trafficking. Terrorist use of criminal activity to raise funds ranges from low-level fraud to serious organised crime.

State Sponsors: Safe havens, failed states and state sponsors continue to represent crucial sources of support for terrorist organisations today. Safe havens and wider cases of weak jurisdictional control, state tolerance or support of terrorist organisations are also important in how terrorists move and use finance, in addition to their role in raising terrorist funds

There are three main methods by which to move money or transfer value: through the use of the financial system, through the physical movement of money (for example, through the use of cash couriers) and through the international trade system. Terrorist organisations use all three methods to move money for the purpose of disguising its origins and integrating it into the formal economy. Often, terrorist organisations will abuse alternative remittance systems (ARS), charities, or other captive entities to disguise their use of these three methods to transfer value. Each of these areas has been considered by the FATF, though the FATF does not currently have a recommendation addressing the misuse of trade for money laundering and terrorist financing.

Early work by the FATF on terrorist financing focussed on the similarities of the methods used in money laundering and terrorist financing. In particular, the approach emphasised the similar needs of money laundering and terrorist financing to mask financial resources and activities from the scrutiny of state authorities and occasional use of similar techniques. Since 2001, experience and study within the FATF and the intelligence community has demonstrated that money laundering and terrorist financing are distinct activities and that the measures which have been successfully applied in the identification and prevention of money laundering are by themselves less effective in the prevention of terrorist financing unless supplemented with additional information.

The application of the FATF's 40 Recommendations and 9 Special Recommendations provide a solid basis upon which to gather financial information. Leveraging this financial information with wider information on counter-terrorism, including intelligence, at a national level proves more effective in identifying terrorist activity.

This report shows the need for continued strong commitment to the FATF standards. The *FATF Special Recommendations* are a key tool in gathering financial information potentially linked to terrorist activity and acting to disrupt it. In order to identify, deter, and disrupt terrorist financing, there are a number of specific actions countries must take in order to establish successful CFT regimes in accordance with the FATF international standards.

Issues for Further Consideration

In addition, this report highlights several steps that could be considered to strengthen the capacity of countries to identify and respond to terrorist activity:

- **Jurisdictional Issues**: There are concerns about the terrorist financing vulnerabilities associated with safe havens, failed states or state sponsors that create enabling environments or otherwise provide active support to terrorist organisations. Through the International Cooperation Review Group (ICRG), the FATF has developed a process to identify and address jurisdictions of AML/CFT concern. The FATF should continue to strengthen and refine this process as a means of identifying and addressing terrorist financing vulnerabilities.

- **Outreach to the private sector**: Financial institutions have clearly identified their needs for better understanding of terrorist financing, including indicators and other targeted information that could be used to identify potential terrorist financing activity. Countries could consider ways to ensure counter-terrorist information (such as high risk locations, activities, and individuals of concern) can be incorporated by financial institutions into their procedures and risk models designed to identify terrorist financing.

- **Build Better Understanding**: Creating an understanding of terrorist financing that is distinct from money laundering is critical. Participation of the whole counter-terrorist community could greatly contribute to the development of a better understanding of terrorist financing. It would ensure a common understanding of financing needs and methods of terrorists and provide insight into the value of financial information when combined with counter-terrorist intelligence.

- **Enhanced Financial Intelligence**: Financial information alone is not sufficient to effectively combat terrorism. However, when combined with counter-terrorist intelligence, financial information can greatly enhance a country's ability to identify and intercept terrorist activity. Because of its predictive value, gathering and sharing financial intelligence is a high priority. Countries could be encouraged to make financial investigation an automatic component of all Counter-Terrorist investigations.

BIBLIOGRAPHY

Abuza, Zachary (2003), *Funding Terrorism in Southeast Asia: The Financial Network of Al Qaeda and Jemaah Islamiyah*, The National Bureau of Asian Research, Seattle, *www.nbr.org/publications/analysis/pdf/vol14no5.pdf*.

Abuza, Zachary (2005), *Balik Terrorism: The Return of the Abu Sayyaf*, US War College, Carlisle, Pennsylvania.

British Broadcasting Corporation (2002), "Al-Qaeda gold moved to Sudan," web site article dated 4 September 2002, BBC, London, *http://news.bbc.co.uk/1/hi/world/middle_east/2233989.stm*.

Commonwealth Secretariat (1998), "Money Laundering: Special Problems of Parallel Economies", paper presented at the Joint Meeting of Commonwealth Finance and Law Officials on Money Laundering, London, 1-2 June.

Comras, Victor (2005), "Al Qaeda Finances and Funding to Affiliated Groups," *Strategic Insights*, Vol. IV, No. 1, US Naval Postgraduate School, Monterey, California, *www.ccc.nps.navy.mil/si/2005/Jan/comrasJan05.asp*.

European Parliament (2005), *Oral Questions for Question Time at the part-session in July 2005 pursuant to Rule 109 of the Rules of Procedure* (6 July 2005), European Parliament, Strasbourg, *www.europarl.europa.eu*.

Farah, Douglas (2002), "Al Qaeda's Road Paved with Gold," *The Washington Post*, 17 February 2002.

FATF (2002), *Best Practices paper on Special Recommendation VIII*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2003), *Typologies Report 2002-2003*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2004), *Typologies Report 2003-2004*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2006), *Trade Based Money Laundering: Typologies Report*, FATF, Paris. *www.fatf-gafi.org*.

FATF (2007), *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*, FATF, Paris. *www.fatf-gafi.org*.

The *FATF Interpretive Notes to Special Recommendation III* and *Special Recommendation VIII*, as well as *Special Recommendation VI* are available through the FATF web site*: www.fatf-gafi-org*.

Global Witness (2003), *For a Few Dollars More: How al-Qaeda Moved into the Diamond Trade*, Global Witness, London, *http://www.globalwitness.org*.

HM Treasury (2007), *The Financial Challenge to Crime and Terrorism*, HM Treasury, London, *www.hm-treasury.gov.uk*.

Human Rights Watch (2006), *Funding the "Final War" – LTTE Intimidation and Extortion in the Tamil Diaspora*, Human Rights Watch, New York, *www.hrw.org*.

Jorisch, Avi (2004), *Beacon of Hatred: Inside Hizballah's Al-Manar Television*, The Washington Institute for Near East Policy, Washington DC.

Kohlmann, Evan F. (2006), *The role of Islamic charities in international terrorist recruitment and financing*, DIIS Working Paper No. 2006/7, Danish Institute for International Studies, Copenhagen, *www.diis.dk.*

Kurth Cronin, Audrey, *et al*. (2004), *Foreign Terrorist Organisations: CRS Report for Congress*, Congressional Research Service, Washington DC, www.fas.org/irp/crs/RL32223.pdf.

National Commission on Terrorist Attacks Upon the United States (2004), *Monograph on Terrorist Financing*, Staff Report to the Commission, Washington DC, *www.9-11commission.gov/staff_statements/index.htm*.

Prober, Joshua (2005), "Accounting for Terror: Debunking the Paradigm of Inexpensive Terrorism," *Policy Watch*, No. 1041, Washington Institute for Near East Policy, Washington DC.

Raufer, Xavier, Alain Chouet, Anne-Line Didier, Richard Labévière (2007), *Atlas de l'Islam radical*, CNRS Editions, Paris.

Shahzad, Syed Saleem (2002), "From the al-Qaeda puzzle, a picture emerges," *Asia Times*; Hong Kong, China; 11 September 2002, *www.atimes.com/atimes/South_Asia/DI11Df02.html*.

United Kingdom Home Office (2006), *Report of the Official Account of the Bombings in London on 7th July 2005*, London, *www.homeoffice.gov.uk/documents/7-july-report?version=1*.

United Kingdom Home Office (2007), *Review of Safeguards to Protect the Charitable Sector (England and Wales) from Terrorist Abuse*, *www.homeoffice.gov.uk/documents/cons-2007-protecting-charities/*.

United Nations (2001), *UN Security Council Resolution 1373 (2001)* [*Threats to international peace and security caused by terrorist acts*], New York, *www.un.org/Docs/scres/2001/sc2001.htm*.

United Nations (2004), *First Report of the [UN] Monitoring Team pursuant to resolution 1526 Report on al-Qaeda and the Taliban*, S/2004/679, UN Security Council Committee established pursuant to Resolution 1267 (1999), United Nations, New York, *www.un.org/Docs/sc/committees/1267/1267mg.htm*.

United States Department of the Treasury (2006), "US Designates Al-Manar as a Specially Designated Global Terrorist Entity Television Station is Arm of Hizballah Terrorist Network," 23 March 2006, *www.ustreas.gov/press/releases/js4134.htm*.

United States Government Accountability Office (2003), *Terrorist Financing: US. Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms*, US GAO, Washington DC, *www.gao.gov/new.items/d04163.pdf*.

Weimann, Gabriel (2004), *www.terror.net: How Modern Terrorism Uses the Internet*, United States Institute of Peace, Washington DC, *www.usip.org/pubs/specialreports/sr116.pdf*.

Williams, Phil (2005), "Warning Indicators, Terrorist Finances, and Terrorist Adaptation," *Strategic Insights*, Vol. IV, No. 1; US Naval Postgraduate School, Monterey, California; *www.ccc.nps.navy.mil/si/2005/Jan/williamsJan05.asp*.

World Trade Organisation (2005), *International Trade Statistics 2005*, World Trade Organisation, Geneva, *www.wto.org*.