Trends in Terror Finance

Part 1: The Unregulated Sector

by John Solomon - World-Check Terrorism & Insurgency Unit

Six years since 9/11, securing the financial front remains central to the fight against al-Qaeda, its affiliates and associated cells. US-led initiatives to combat the financing of terrorism are often cited as the most effective weapons in the counter-terrorism arsenal. In its December 2005 report, for example, the 9/11 Commission rated US and partner governments' progress in countering the financing of terrorism (CFT) higher than any of the other 41 areas assessed. To date, the US and its allies have frozen or seized some $200 million of terrorists' assets. In this new kind of war, where measurable progress is often an elusive concept, the fight to secure the financial front has achieved tangible results. Indeed, a substantial sum of terrorist money has been taken out of circulation, and much praise is due to the global financial community for undertaking a greater role in complying with additional CFT requirements. Yet, it is remarkable that the overwhelming majority of asset freezes and seizures took place in the first two years after 9/11. Since 2003, the money trail has largely dried up. What explains this steep decline?

AL-QAEDA USES THE UNREGULATED SECTOR

Since the crackdown targeted the regulated financial sector, terrorist groups such as al-Qaeda have probably turned to the unregulated sector to raise, move and store their money since 9/11.

Although al-Qaeda paid for the 9/11 attacks – estimated to cost $500,000 – via the regulated, formal financial sector using US and Western financial institutions, it is quite likely that the organization reduced its financial exposure after 9/11 by converting its traceable assets into untraceable forms of value.

Al-Qaeda exhibits a "lose and learn doctrine" in which the organization distills lessons from past mistakes and applies those lessons systematically in order to avoid future problems.[1] 11 September wasn't the only incident that precipitated US measures targeting al-Qaeda's finances.

In the aftermath of the August 1998 Al-Qaeda attacks on US embassies in Kenya and Tanzania, the Clinton Administration froze a significant amount of money held by al-Qaeda and the Taliban in Western banks, most of it in the form of gold reserves on deposit with the US Federal Reserve.

This likely sensitized al-Qaeda to the risk of holding assets in the Western financial system in the immediate aftermath of an attack.

There is significant information to indicate that al-Qaeda has increasingly used the unregulated financial sector in the period leading up to 9/11 through to the present.

From January 2001 through September 2001, US State Department and Belgian federal police reports strongly suggest that al-Qaeda was involved in a rapid, large-scale operation to transfer its traceable assets into non-traceable conflict diamonds from Charles Taylor's Liberia to the polished diamond market in Antwerp.[2]

On 20 September 2007, the US Department of Justice, together with a number of other federal agencies and international partners, released an indictment that named individuals involved in a scheme to remit $5 million to al-Qaeda and other criminals using *hawala*, an informal value transfer system (IVTS) popular in the Middle East and South Asia.

[1] Rohan Gunaratna, 'Al Qaeda's Lose and Learn Doctrine: The Trajectory from Oplan Bojinka to 9/11', in Teaching Terror: Strategic and Tactical Learning in the Terrorist World, ed., James JF Forest, pp. 171-188, Rowman & Littlefield Publishers, Inc.,2006.

[2] Douglas Farah, 'Al Qaeda and the Gemstone Trade', in Countering the Financing of Terrorism, eds., Thomas J. Biersteker and Sue E. Eckert, p. 199, Routledge, 2007.

INTERNATIONAL RESPONSES TO ARS

Governments and international bodies responsible for suppressing the financing of terrorism immediately recognized the dangers associated with unregulated financial systems post-9/11. In response to this need, government regulators and security services have acted swiftly and aggressively to supervise IVTS that parallel the formal banking sector.

The Financial Action Task Force (FATF) issued its Special Recommendations on Terrorist Financing in October 2001 and October 2004 in order to create an international standard on the issue. Special Recommendation VI applies to alternative remittance systems such as hawala, which requires governments to license these money service businesses in the same manner governments would license a bank.

On this front, significant challenges have been overcome in the Middle East, South Asia and Africa, where hawala has predated the Western-dominated banking system, and is firmly entrenched culturally, legally and economically.

The United Arab Emirates, a hub of both hawala and terrorist financing, for example, has moved towards compliance with the FATF terrorist financing standard by requesting that hawaladars register with the central bank. Indeed, steps have been taken in the right direction, but much more progress is needed.

While hawala and other low-tech IVTS are critical in CFT, the financial community must also take a proactive approach in addressing the terrorist financing risks associated with emerging high-tech remittance systems such as mobile banking and virtual currencies.

The convergence of the banking and telecommunications industries promises to transform the way money and value is moved both within and across borders; thus creating gaping holes for terrorists such as al-Qaeda to exploit.

THE EVOLUTION OF THE UNREGULATED SECTOR

The ability to transfer money instantaneously and anonymously is a key element in sustaining the structural and operational needs of terrorist organizations. Today, technological innovation provides new types of international payment systems using the internet and mobile phone networks that can bypass the conventional banking and money transfer system; thereby making it easier for terrorists to move money and more difficult for regulators and counter-terrorist financing institutions to identify and trace their transactions. In particular, the convergence of the financial services and telecommunications industries has opened a new corridor for the threat and risk of terrorist financing.

Through transforming almost any mobile phone into a banking device that is capable of remitting, receiving and storing funds across borders, this emerging technology holds tremendous potential for terrorist financing purposes.

Known as mobile banking (or m-banking), the technology provides a quick, cheap and anonymous way for terrorists to move and store money that can be used to bolster their infrastructures and to fund attacks.

How does m-banking work? There are several models operating today but the Philippine telecom provider Globe and its innovative program, G-Cash, offers a good example. Users of the service can purchase a prepaid stored value card from any authorized G-Cash outlet, which includes G-Cash ATMs. Similarly, they can cash out their stored value cards at any G-Cash outlet or ATM.

Globe states that it aims to facilitate and capitalize on the considerable number of overseas Filipino workers (OFWs) who have remitted about $12 billion or 10.5% of the country's GDP in 2007 alone.

With over 1 million OFWs in the Gulf Arab states where there is an established pattern of OFWs adopting Jihadist tendencies and acting as money couriers for extremist causes originating abroad, there is reason to worry. It must be remembered that it was Saudi national, Mohammed Jamal Khalifa, that used OFW such as Abu Sayyaf Group founder, Abdulrajak Janjalani, to help spread extremism and violence in the Phillipines.

A more recent example of the migrant worker-terrorism nexus includes the Rajah Solaiman Movement, an affiliated terrorist group comprised and led by Catholic OFWs that converted to Salafi-Jihadist Islam in Saudi Arabia.

The group took responsibility for the terrorist attack on the Superferry 14 cruise ship in February 2004, killing 116 people. In regions where terrorist and extremist activities are significant, there is good reason to be concerned about m-banking and other emerging technologies that could facilitate cross-border financial transfers among these groups.

There are reliable indications that m-banking services will become increasingly global. Six months ago, the GSM Association (GSMA), representing over 700 GSM mobile phone operators across 218 countries of the world, announced its intention to enable the world's 200 million international migrant workers to easily send remittances home using their mobile phones. The m-banking service would enable them to make global person-to-person payments without more than minimum oversight even if the individuals have no bank accounts and are located in regions proximate to known terrorist groups and their supporters.

Initiated by 19 leading telecommunications firms, with networks in over 100 countries and representing over 600 million customers, and MasterCard Worldwide, this pilot program seeks to double the number of recipients of international remittances to more than 1.5 billion while at the same time quadrupling the size of the remittance market to over $1 trillion by 2012. While there is certainly vast potential for the under-banked poor, the unmitigated risk of increased terrorist financing may be too high a cost to pay.

Considering that about 1 billion people have bank accounts and nearly 3 billion own mobile phones, nearly half of these residing in the developing world, it does not take much imagination to foresee the radical transformation that will take place when the number of people gaining access to financial services for the first time doubles, triples or even quadruples.

Will the financial community be able to keep up with the exponential growth in financial traffic and transactions while at the same time doing its part to keep terrorists out of the financial system?

M-banking represents the anonymity and speed of hawala coupled with the reach of Mastercard and a regulatory standard dependent on the resources and political will of nations with limited resources, where it will tend to be most dominant. Conceivably, the money for the next terrorist attack could be only an SMS away.

Don't miss the next issue of the T-Brief for Part 2 of John Solomon's fascinating series on the inner workings of terrorist financing in the unregulated financial sector – it's a must-read for compliance professionals!