The Latest Trends in Terrorist Financing: The Challenges of Detection

By Simon Dilloway

Introduction

Terrorist Financing (TF) is not the same as money laundering, but some of the behaviours are similar. Money Laundering (ML) is about disguising the money and bringing it back into circulation with justification. TF can be about raising cash, moving cash into or out of the country, moving it within a country, and using it to facilitate terrorism, not to get rich in the accepted sense. Resourcing of any description comes within the definition, so need not involve the movement of funds at all. The provision of premises for shelter or bomb-making equally constitutes the financing of terrorism, even though no actual *things* change hands. Any accumulative financial behaviour close to a terrorist suspect is likely to be some support mechanism for families of suicide bombers. Any transactions can be of any amount, so a holistic picture is essential to put the transaction into context.

No institutions are immune from being used by TF. The 2005 London bombings were inadvertently paid for by high street bank and credit card companies.

The State is a significant unwitting financier of domestic terrorism. Most domestic terrorists in the UK have been in receipt of welfare benefits, if not actively defrauding the system, and this is the subsistence that keeps them going during the crucial periods. It also means that there is less need for the importation of funds for day to day living expenses. Financial records, behaviours and associations are essential and invaluable in investigating terrorist suspects and incidents.

Most terrorists are financially unsophisticated – once they discover a reliable method for raising or moving money, they are likely to use it repeatedly, providing patterns for exploitation. Therefore, similar activity, such as specific loan raising, within a group of financially associated account holders with a risk profile should instigate a Suspicious Activity Report (SAR). This will also apply to new ways to abuse old systems, such as raising small sums through below the threshold motor insurance claims. Large sums are not essential.

Sometimes a lack of financial activity can be as suspicious as activity, for example changing from normal account activity to withdrawal of cash only is

a likely indicator of a desire to hide a financial footprint. So too is a tendency towards the use of alternative remittance systems, especially money service businesses. (MSB). The likely type of MSB for repeated use is the small independent business, often operated by those of the same ethnic group as the particular terrorists. The transactions will be easily hidden amongst the many thousands of similar ones being honestly conducted to get funds back from developed to underdeveloped countries for the support of family.

However, having said that most terrorists are financially unsophisticated, those whose primary role is the financing of terrorism are, on the contrary, extremely sophisticated. However much international organisations provide guidance typologies and analyses of incidents, these can by definition only describe those methods which have come to light. Despite a long standing refutation in some law-enforcement quarters of the involvement of dealers in counterfeit goods in terrorist funding, recent activity suggests that is an incorrect view. So, just because a method has not been *seen* to be utilised, it does not follow that is not going to be, now or in the future.

Emerging Technologies

New financial products must be rigorously examined for vulnerabilities. Most financing behaviour is *away from* developed countries *towards* the site of conflict. Sums need not be huge. Electronic purses and mobile phone banking provide ideal anonymity and scope to get money to where it is needed.

Reports have been made in national newspapers of concerns that terrorist suspects are showing an interest in 'virtual world' technology. In these 'worlds', the anonymity available, the lack of monitoring, and the facility to transfer and even to raise money 'in world', and then have it extracted anywhere in the real world by whatever means is desired, provides an ideal environment for terrorists, and for their financing activities.

Any indication of the use of the more expensive or technologically sophisticated methods of money transfer, such as the established transfer agents (Western Union, Moneygram *et al*), should also raise the temperature of the risk assessment undertaken in the course of the normal AML monitoring. A glance at the operating methods of those services that offer anonymity and/or ease of money movement reveals that such transfer methods are always at the forefront of payment behaviours. This includes all of the emerging technology based services, largely because a high proportion of involve online activity requiring some non-physical means of depositing funds.

Offshore accounts now routinely offer anonymous debit cards, and contrary to protestations that the amounts that can be loaded onto them are low, for a fee it is possible to easily obtain the facility to deposit many thousands of dollars onto such cards, untraceably usable worldwide under the established

card service providers' logos (see www.openoffshorebankaccountsfornonresidents.com/AnonymousDebitATMCardMaestro.htm or www.ssl-panama.offshorelegal.org for examples). To maintain the circle of anonymity, loading can be done by the above mentioned transfer agents, as well as via e-gold, and host of similar methods. This is not to suggest for one moment that there is anything dishonest or illegal about these facilities. However, any indication of the use of any of the aforementioned financial products should certainly exercise the interest of compliance officers, and make them reach for the risk assessment matrix, in the same way that it does law-enforcement investigators.

Mobile phone banking offers a lifeline to remote communities in third world countries, where banking facilities may be scarce and/or unreliable. In particular, the form that effectively turns a cellphone SIM card into a front loadable electronic purse is particularly attractive. The fact that the funds are not originating from a bank account means that the operator, *i.e* the telephone company, is performing the functions of a bank without being subject to the same financial regulation that banks must endure. This must be a worrying situation for those concerned with the transparency of money movements.
Even if facilities are put into place to perform customer due diligence checks on the phone subscriber, which is a difficult task in the target markets, who can say who has actual control of the phone. Furthermore, if the funds can be transferred by a telephone call, where, and with whom, will the funds end up? What facilities exist for reporting of suspicious activity in these circumstances?

The latest FATF reports on this subject note no observed cases of ML or TF using these methods. Given the obvious attraction of the facility, and the vulnerable areas in which they are being promulgated, how likely is it that is an accurate observation?

Challenges of detection

Much terrorist financing activity is beyond the capability of the regulated sector to discover, because it is far removed from the established financial world. The hiving off of part of a ship's cargo in a faraway port can provide more than ample funds to purchase weapons and explosives in areas of unrest. Cash couriers are never going to come anywhere near a financial institution, that is the whole point of them. The bulk of the effort, therefore, must be concentrated on the established means of moving funds.

There were no Suspicious Activity Reports made about any of the London bombers prior to the attack. Subsequent analysis of the finances of those involved produced a huge amount of material that was invaluable to the investigation, and in fact produced the bulk of the intelligence unearthed. Nevertheless, nothing was discovered that should have prompted such a report from any of the banks concerned. The activity was simply too mundane and low value to have caused any suspicion to arise. Had they been under investigation already, as was so in some subsequent cases, the financial activity, such as it was, would have been extremely useful, but they were not.

It is accepted that terrorists will go to great lengths to change their behaviour to avoid coming to notice. They know that security services have various means by which to monitor financial activity, and to obtain the valuable intelligence and evidence mentioned from the financial footprint that they leave behind them. Efforts to thwart such virtual surveillance have been evident for some time. As mentioned above, sometimes those efforts of themselves act as a useful indicator of suspicious activity, such as moving towards the use of cash in as may transactions as possible.

The challenge, therefore, is find a way, partly through more vigilant use of the tools already available in the regulated sector, to identify any behaviour which might indicate terrorist financing using the newly available facilities, as well as in the established systems. Awareness of the potential of innovative products to assist terrorists is vital. The availability of these ever more convenient and sophisticated ways to move funds, whilst making life easier for everyone in general, makes life easier for terrorist financiers in particular.