Preceeds of crime: fighting the financing of terrorism

Michael Levi tracks moves to prevent the financing of 'terrorist' activities.

From the perspective of the authorities and (usually) the majority of citizens in the West, fighting terrorism preferably involves stopping 'terrorism' before it strikes. Zedner (2007) writes of the shift of anti-terrorism policy to prevention 'in which the possibility of forestalling risks competes with and even takes precedence over responding to wrongs done', and where 'the post-crime orientation of criminal justice is increasingly overshadowed by the pre-crime logic of security'. However, the pre-crime activities may not reflect a shift in anti-terrorism policy so much as a shift in the importance of anti-terrorism policy as part of the fabric of crime control. One large rhetorical plank of the struggle against (no longer 'war on') terrorism is the attempt to reduce the financing of terror, which has been extended to the control of 'proliferation finance', mainly to try to isolate Iran and North Korea. The social costs of measures against financing terror are less visible than stops and searches, which occur in public space, to the Western public. This is because they are a back-office extension to existing anti-money laundering regulations – first begun in 1986 as part of the 'War on Drugs' – which affect everyone who tries to open a new account or send money anywhere. 'Islamic terrorism' (sic!) has developed a control focus on moving money via charities and via money service businesses (like Western Union and MoneyGram) and informal value transfers (Passas, 2003, 2006) – sometimes termed 'hawala banking'. The latter preceded formal banking and are cheaper and more efficient than banks in getting money to most developing countries.

Within this context, there is a disputed debate over what the category of terrorist finance constitutes. Operationally, little money is needed. '9/11' cost less than $500,000 to organise; and the London and Madrid bombings cost less than £10,000: the equivalent of fewer than 10 credit card frauds. However, if by 'terrorist finance' one includes the cost of recruitment and preparation, and even broader ideological indoctrination, the sums involved are much larger. Whichever definition is used, it is an extremely ambitious task to cut off the financial lifeblood of terrorism: what I have termed here 'preceeds' as contrasted with 'proceeds' of crime. Those interested in promoting violent extremism obtain funds from:

- Wholly licit sources (which can include 'rogue states' as well as wealthy sympathisers)
- Contraband (like smuggled alcohol, fuel, and tobacco)
- Wholly illicit 'market offences' (e.g. drugs)
- Property crimes which have losers (fraud, robbery, and theft)

Proceeds of crime controls deal with last three categories only. Controls also have to deal with displacement risks. Terrorists prefer licit-source money on pragmatic grounds, bringing less risk of victim/law enforcement action against them before they have achieved their objectives. But if controls cut these sources off, displacement may occur to the easiest frauds (such as payment card frauds) or other crimes *within terrorist skill/contact sets*.

To effect these controls, the banks have been 'responsibilised', i.e. forced to try to spot funds that are destined to aid terrorism or the development of nuclear and other weapons of mass destruction. It is this that brings about the major element of pre-crime analysis. The hope of the authorities is that the prospect of being identified (a) puts potential donors on notice that they may lose their liberty and their assets for assisting terrorism or the purchase of components for proliferation; and (b) deters them from participation or (c) leads to their apprehension and prosecution *pour décourager les autres*. However, in the UK the Charities Commission has monitored not-for-profits for weakness in internal controls and 'evidence' that funds have leaked to terrorist groups. Controls were established in Italy in the late 1970s and in Ireland from the late 1980s to try to cut off the flow of funds to terrorists and paramilitaries. However, post-2001, pre-crime financial monitoring took on a step change of transparency to the state. After the attacks, the UN Security Council unanimously adopted Resolution 1373 (2001) and the EU followed: whereas the normal aim of proceeds-of-crime legislation is to confiscate assets and return them to the community (and/or law enforcement), the aim here was to put the funds beyond terrorist use by freezing them. Usama Bin La¯den, the Taliban (currently under review in 2010), and those associated with 'the Al-Qa¯'idah network' were included in a list developed by a special committee of the UN (Biersteker and Eckert, 2008): even less clear were the criteria for getting *off* the list. There are 539 specially designated global terrorists, including 45 foreign terrorist organizations (OFAC, 2009). Asset freezing following up the attempts to create a financial panopticon has run up against some due process rulings in the European courts.

However, a broader issue is what does and should generate suspicion? If bankers and other regulated bodies are to act against terrorist finance, they have to know names and/or behavioural characteristics to look for, preferably electronically, since there are billions of cross-border transactions daily and manual

scrutiny is impossible. There is an inherent difficulty about the publication of advice on *modi operandi* of terrorism finance (and on the laundering of other forms of crime), since this inevitably gives rise to leakage to some sympathisers. The UK, but not other countries, has created small 'vetted groups' of money laundering reporting officers (MLROs) with formal security clearance, but general publication of suspects beyond the lists is impracticable. After 9/11, substantial effort went on within the private sector to try to develop profiles for terrorist finance. This was notwithstanding early findings from analysis of the financial background to the 9/11 plotters and operations, which showed that they were unpredictable and largely 'normal' (Roth et al., 2004), a view which applies to much (though not all) other terrorism financing. A substantial profitable industry has sprung up to supply automated checks on names on the various sanctions lists, which can be an expensive problem where names are capable of multiple English spellings (especially where the origins are in Arabic) and are (reasonably) presumed to be willing to engage 'fronts' to act for them. Third party firms operate only on government and court-decision-generated datasets, but will electronically check against lists of designated terrorists and politically exposed persons (public officials and their immediate families) as a paid-for service. However, there are many false positives for common names, whether Islamic or not.

In 2006, it was revealed that the global inter-bank financial messaging system SWIFT was supplying all its data to the US' Terrorist Finance Tracking program (TFT), held in a secure facility, not mixed with any other data, and accessed only when a TFT analyst can demonstrate (to supervisors) a previously documented nexus between the subject of a search and suspected terrorist activity. The internal regulations state that there must be no generalised 'data mining' or algorithm manipulations, and a source stated that over 1,500 leads from these SWIFT data were shared with European partners, though their impact is unavailable. The US and EU are currently negotiating a formal agreement over the use of these data, though the European Parliament has rejected the proposals to date.

Although much counter-terrorist control behaviour is inaccessible and/or unpublishable, controlling 'threat finance' is in practice a modest element in the risk policing of terrorism rather than being its core: although financial institutions have every incentive to identify terrorist financiers, the task of building profiles without many false positives or false negatives is simply too difficult. In the case of financing through crime, most of the offences in the West – payment card fraud, selling counterfeit goods, etc. – would not normally be considered a priority by either reactive or intelligence-led policing, and is not plausibly preventable.

In the light of this, it is difficult to know where the financial component of the 'War on Terrorism' will end. Money is embedded in so many components of the obtaining and use of instruments of terror that the search for terrorist funds does have the capacity to create a claim for total transparency. Yet at the same time, so many arenas of commercial dealing lack that transparency, and the US has taken little action against its own states, such as Delaware, that have quite profound corporate secrecy rules. Both wealthy tax avoiders/evaders and terrorist financiers may have an interest in preserving financial secrecy.

Terrorist finance is not clogging up the courts or prisons. The number prosecuted in England and Wales was seven (in two cases in 2007 and 2008) (House of Lords, 2009). As of January 2009, about £632,000 of suspected terrorist funds has been frozen under the Al-Qaida and Taliban Order and Terrorism Order. Following cash seizures, 13 people were referred to the Metropolitan Police for suspected terrorist financing (House of Lords, 2009): but what that means in practice is unclear. However these are not the only yields. *After the event*, the pursuit of financial records enables linkages to be made; and controls may have a chilling effect on charitable donations by the wealthy, who may fear incrimination.

In reality, the best that can probably be achieved by 'follow-the-money' methods in countering terrorist finance is some intelligence that allows for interventions to make arrests, build up a broader picture of terrorist linkages, permit physical observations, and prevent particular individuals and groups from obtaining the funds for particular projects beyond the trivial amounts needed for suicide bombings at the local level – or make them run higher risks in the search for funding. Past and potential sources of major finance may also be deterred from funding larger attacks by fear of publicity and of financial and penal sanctions. However, there are less visible effects in raising the costs of money remittances to poor relatives in developing countries as a result of the administrative costs of anti-laundering measures, and in chilling charitable donations because of fears of being labelled a terrorist financier. ■

Michael Levi is Professor of Criminology at the Cardiff School of Social Sciences at Cardiff University.

References

Biersteker, T. and Eckert, S. (eds.) (2008), Countering the Financing of Terrorism, Routledge.

House of Lords (2009), Money Laundering and the Financing of Terrorism. 19th Report, 2008–09, HL Paper 132–II.

John Howell and Co. Ltd. (2007), The EU's Efforts in the Fight Against Terrorist Financing - Final Report, European Commission.

Passas, N. (2003), Informal Value Transfer Systems, Money Laundering and Terrorism, US National Institute of Justice.

Passas, N. (2006), 'Fighting terror with error: the counter-productive regulation of informal value transfers', Crime, Law and Social Change, 45 (4-5): pp. 315-336.

Roth, J., Greenburg, D. and Wille, S. (2004), Monograph on Terrorist Financing, National Commission on Terrorist Attacks Upon the United States.

Zedner, L. (2007), 'Pre-crime and post-criminology?' Theoretical Criminology, 11: 261-81.'