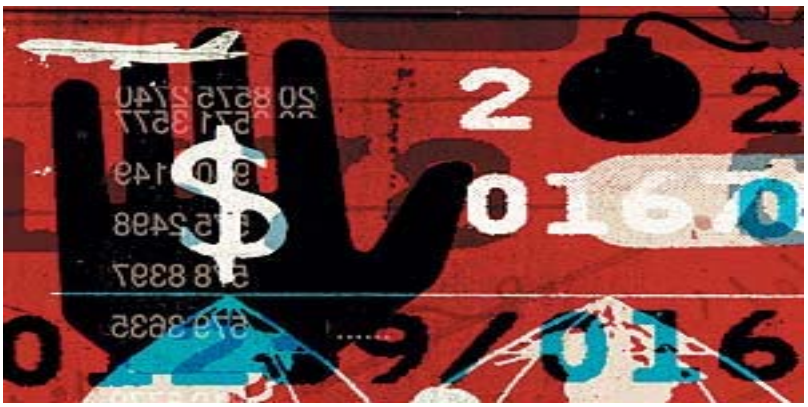
Financing terrorism

Looking in the wrong places

Oct 20th 2005 | DUBAI, LONDON AND SHARM EL-SHEIKH
From The Economist print edition



Hindering flows across international financial networks is costly and does not stop terrorists' primary activity

Get article background

UNDER the scorching sun in Egypt's inhospitable Sinai peninsula, security forces last month drew a tight cordon around terrorist suspects holed up in caves on Halal Mountain, hoping to starve them out. The authorities have been on high alert after several terror attacks, most recently in the Red Sea holiday town of Sharm el-Sheikh, where scores of tourists and locals were killed in July.

As the security forces waited, a more staid faction in the global fight against terror gathered in one of the resort's luxury hotels. Under the watchful eyes of officials from America's Treasury, nearly 200 grey-suited bankers from the Middle East and Africa spent two days discussing recommended financial safeguards to choke terrorist funding and money laundering, another crime that abuses the financial system. "This is about creating hostile environments," said Neil Bennett of Britain's National Terrorist Financial Investigation Unit. Last week an even bigger gathering took place in Paris, as officials from 32 jurisdictions and 16 international organisations debated the uneven pace of progress in reducing financial crime, including that linked to terrorism.

Four years after the attacks of September 11th 2001 put the "war on terror" at the top of George Bush's agenda, political pressure from America, Britain and, more recently, the United Nations, has resulted in this: scores of bankers, fund managers, accountants and solicitors on the lookout for terrorists around the world. "Money is the lifeblood of terrorist operations," declared Mr Bush: "We're asking the world to stop payment." Tony Blair has beaten the same drum more loudly since the attacks in London on July 7th. Governments from Australia to Bangladesh and Paraguay have ratcheted up their political rhetoric too. Yet deadly attacks keep coming—most recently in Bali, Indonesia on October 1st.

The private sector bears the major burden of the effort to choke off funding for terrorists. Banks and other financial institutions are scanning their customer accounts more carefully for

signs of suspicious people and transactions. Accounts have been frozen and foreign banks have been cut off from doing business in dollars if America is not satisfied that they are properly sharing information.

Millions of prospective and current customers are hampered by tougher compliance standards. To open an account or transfer money these days means numerous demands for identification—a passport or driver's licence with a photograph. Customers have grown used to delays in gaining access to their own money. There are growing requirements for disclosure of detailed information on business directors and funding sources. All this means additional fees. Expatriate executives, international-exchange students and low-wage workers wiring money to their families abroad have been most affected.

The compliance costs for financial institutions are substantial. Graham Dillon of KPMG, a consultancy, reckons it costs each mid-tier bank in Britain £3m-4m ($5m-6m) to implement a global screening programme that involves regularly checking customer names—and those of third parties involved in their transactions—against United Nations embargo and American sanctions lists for possible terrorist matches. He reckons multinational banks each spend another £2m-3m per year to oversee implementation in their far-flung operations (such institutions commonly have 70 to 100 different transaction systems). In addition, "tens of millions of pounds" are spent each year in London alone on data storage and retrieval to satisfy a requirement that banks' client and transaction data be kept for five to seven years. Similar rules exist in America, Singapore and other European countries.

An exhaustive, one-time process known as "remediation", in which institutions painstakingly go through their databases of existing customers to verify personal information and check names against sanctions lists, can cost a large multinational bank between £20m and £30m, KPMG estimates. There is increasing emphasis on this process in America. In Britain, though, regulators scrapped the requirement as too costly after several retail banks had undergone the process; it has been downgraded to a recommendation.

A costly pursuit

The total cost of complying with anti-terror financing regulations is difficult to determine partly because many institutions (private and governmental) tackle the issue in tandem with money laundering, a separate financial crime. The British Bankers' Association (BBA) estimates that banks in Britain spend about £250m each year to comply with regulations on the two sorts of crime. According to a global study of about 200 banks last year by KPMG, those interviewed increased investments on anti-money-laundering activities by an average of 61% in the prior three years.

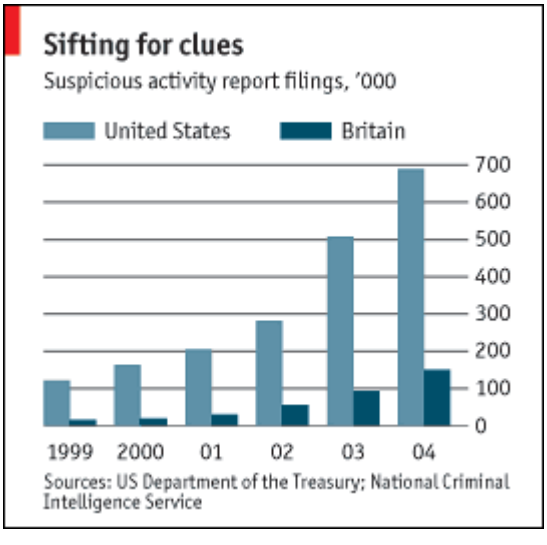
But Mr Dillon says anti-money-laundering technology is focused on identifying suspicious transactions that bear little resemblance to those typically used by terrorists. He contends that current technology could be reconfigured to check for things that better fit the profile of terrorist financing—liquidating accounts, for instance (what one might expect of a suicide-bomber) or purchasing high-risk materials. But he is not aware of institutions doing this now. "There's a high probability that institutions have not learned from Madrid, 9/11 or the London bombings in relation to re-enhancing their systems against terrorist attacks," he says.

Meanwhile, the compliance staffing and services industries are booming. Compliance officers' salaries have climbed. Software vendors tout programs that can quickly scan millions of transaction records (big banks typically have more than 150m customer accounts and might have upwards of 20,000 staff). Specialist training programmes are designed to teach bank staff the latest in behavioural analysis. Private firms offer vast databases that allow banks to do background checks on new and existing clients. One such firm, World-Check, offers banks and governments profiles of more than 300,000 people who may present a "heightened risk" to financial institutions.

The result has been a veritable flood of data on customer transactions deemed suspicious. In America, institutions file reports on about 13m cash transactions over $10,000 every day. The total number of "suspicious activity reports" filed nationwide more than tripled between 2001 and 2004, surpassing 685,000 that year. In Britain, about 250,000 such reports will be filed this year, about three-fifths of them from banks. The BBA estimates only 3-4% of the suspicious activity reports filed in Britain involve terror financing.

Ironically, the welter of paper has prompted some authorities to ask financial institutions to file fewer, better quality reports. Without sufficient resources to process the reports, backlogs mount and many cases are never carefully reviewed. In developing countries, law enforcement is too corrupt or inefficient to process them all. Banks also gripe about poor feedback from the authorities. A report commissioned by Britain's government and police chiefs and released on September 29th finds many flaws in the system of handling suspicious activity reports in money-laundering cases. It contends that the reports are under-utilised by most law-enforcement agencies, which simply lack the resources to analyse and act on the information in them.

Banks comply with the rules for two primary reasons: fear of sanctions, and worry about their reputations. Should they fail to toe the line, the Patriot Act essentially cuts off foreign institutions from business relations with America. That provision "scared the living daylights out of the rest of the world", says a security consultant. "They realised that without dollar accounts they were sitting ducks." For those institutions that fail to comply with the regulations, there is a price to pay: the American unit of Arab Bank, for example, was recently slapped with a $24m civil fine for having inadequate financial controls in place. It faces other suits for allegedly funnelling money to Palestinian extremists.



In more zealous places like America and Britain, the dragnet requires the filing of suspicious activity reports by lawyers, accountants and insurance companies as well. Las Vegas casinos are screening high rollers. Even yacht brokers and jewellers have been told to report buyers who try to pay with big rolls of cash.

Yet all this effort has yielded depressingly few tangible results. America's Treasury says more than 1,000 grand-jury subpoenas and more than 150 indictments have been handed down, although there has been nothing like that many convictions. In July, an American court sentenced a Yemeni cleric to 75 years in prison for conspiracy to support al-Qaeda and Hamas. In Yemen, "they call me the father of needy people," he told the court, proclaiming his innocence.

Such cases are rare, though. Many experts, both in government and the private sector, admit that the chances of detecting terrorists' funds in a bank sufficiently far in advance of a planned attack that it can be prevented are incredibly small. "In my view, it's hardly worth the effort," says one banking industry official in Europe.

Critics note that a number of terror attacks have occurred this year—in Saudi Arabia, Jordan, Russia, Egypt, Britain, Bali (again), not to mention Iraq—and they often seem to involve very little money. The young men who tried but failed to detonate home-made bombs on London's transport system on July 21st packed explosives into cheap plastic containers of the kind that are sold in Indian shops, the sort of things that housewives use to store left-over curry. Even the most devastating terror attacks cost relatively little to pull off. Estimates vary, but western officials say al-Qaeda operatives spent $350,000 to $500,000 to plan and carry out the September 11th attacks. The Madrid bombings cost about $15,000, the earlier Bali bombings $15,000 to $35,000.

Identification of terrorist funds is complicated by the increasingly fragmented nature of terror groups, says Rohan Gunaratna, a Singapore-based expert on al-Qaeda. "Targeting the known financial infrastructure will give you no guarantee that the threat has been diminished because some cells won't ever come on your radar screen."

Keeping bad company

The effort to choke off terrorists' financing has been slow to adapt. Initially, programmes were designed as if al-Qaeda was a big multinational corporation with Osama bin Laden at the helm. "The crackdown on terrorist financing didn't amount to much, for it soon became clear that al-Qaeda was not some accounting trick that could be uncovered and righted by regulators willing to spend a few weeks in Grand Cayman," writes William Brittain-Catlin, a journalist and security consultant, in a new book on financial crime*. Rather, he argues, al-Qaeda was a disjointed, fragmentary organism operating at street level in western cities, where disillusioned young men formed small groups and engaged in small-scale financial fraud, stole identities and credit-card data, communicated through the internet and cell phones, typically using multiple identities to escape capture and detection.

Indeed, the terrorists have shown an ability to keep changing their money flows. "The bad guys are definitely getting smarter," says a European expert on financial crime. "The banking system is so well patrolled they're resorting to more primitive means." Counter-terror experts say some groups have simply switched to using more cash, slipping across borders undetected. Authorities say they recognise the changing money flows, but cutting them off is no simple matter, particularly in cash-based economies with loose border controls.

The cash nexus

A controversial area of focus for counter-terror experts is the global network of informal money-transfer systems (known in some countries as *hawalas*), which have long been popular with overseas workers sending home remittances. They have come under particular scrutiny since September 11th, but have not been banned in most countries. Experts say *hawalas* are extremely hard to regulate and still offer one of the cheapest ways for poor people to send money abroad. Nikos Passas, an expert on financial crime at Northeastern University in Boston, says *hawalas* have had too much attention, given the wide range of fund-raising and transfer methods used by terrorists.

He and other experts contend that terrorist networks today are more likely to use money-laundering methods (such as falsified trade documents) for funds transfers. "Trade is not transparent," according to Mr Passas, making it an attractive outlet for terrorist groups. Other experts agree, pointing, for example, to the falsification of documents by terrorist groups to launder money in Africa.

Nonetheless, one of the things that distinguishes Islamic terrorists from earlier groups—including the Irish Republican Army and Basque separatists—is their use of significant funds from legitimate (as opposed to criminal) sources. Much of the money for the September 11th attacks came from charities and wealthy individuals in the Persian Gulf region, especially Saudi Arabia. While the Saudis have passed a number of laws to crack down on regulation of charities since then, enforcement is uneven. America's Treasury has frozen the assets of 41 aid organisations globally for alleged links to terror groups. But Islam's obligation of *zakat*, or giving a portion of one's income to the poor, means that law enforcement's efforts have ruffled feathers among governments in Muslim-dominated countries.

Credit-card fraud, welfare fraud and smuggling are some of the other known sources of funds for terrorist activities in the West. Mr Gunaratna has pointed to Spain and Belgium as two centres for such activities. Funds from cigarette smuggling in America (packs are shipped from one state and resold at higher prices in another) have supported Hizbollah's operations in the

past.

Given the mutating nature of terrorist financing, international regulators keep layering on new laws and recommendations in an effort to keep pace. The result is what Mr Passas calls a "regulatory tsunami". The multilateral effort is based on the notion that terrorists will exploit the weakest links in the global financial system. It got a boost in July when the United Nations passed Resolution 1617, which clears the way for governments to cut off support networks of al-Qaeda and the Taliban around the world. The resolution calls on states to freeze the assets, cut off financial access and block foreign travel of anyone supporting these groups.

Specific recommendations for governments (which have the final say in enacting national laws regulating financial services) come from the unimaginatively named Financial Action Task Force (FATF), an international body based in Paris. It has developed nine recommendations, including the regulation of wire transfers, remittance systems (*hawalas*) and non-profit organisations, to complement 40 already in place to fight money laundering. So far 151 countries have committed to implementing the recommendations, but a recent report from the IMF and World Bank says countries' action on the anti-terror recommendations lags efforts to fight money laundering.

Part of the challenge is a lack of teeth. The FATF contends its main source of leverage is a blacklist of countries that have failed to adopt or implement adequate laws. The list contained 15 countries in 2000, including places like the Cayman Islands and Lebanon. Today only Nigeria and Myanmar remain on the blacklist (the Pacific island nation of Nauru was removed last week), but no one believes they are the only trouble spots. Indeed, sceptics question how some countries—Russia, Indonesia and Israel among them—have managed to avoid the list of shame. Passing laws, of course, is no guarantee of vigorous enforcement. "The gap between rhetoric and reality is not only in the developing world," says a World Bank official. "It exists in the West too."

Networks apart

Most problematic of all may be the 41 countries that do not even pretend to follow the FATF process. China is in the process of joining, and India has started discussions with the group. But Libya, Sudan, Vietnam and Venezuela remain outside the organisation. Africa is a particular concern. "Many countries in north and west Africa have not even reached step one—political commitment," says Alain Damais, head of the FATF.

For all the finger-pointing, though, experts admit that big financial centres such as London and New York—by virtue of the huge money flows going through them—are probably still major hubs for laundered funds and terror financing. Nick Kochan, author of another recent book on financial crime**, says Britain's government has failed to invest in sufficiently skilled law enforcement personnel or regulators to police its large financial sector.

For now the burden of implementation appears likely to rest with the private sector. "Banks are going to have to start behaving like the FBI and CIA," contends David Porter of Detica, a Britain-based consultancy with expertise in financial crime. "They need to start connecting the dots." This "risk-based" approach—concentrating time and energy on checking a smaller number of individuals or businesses based upon their transaction histories, sources of funding and other factors—is gaining wider acceptance.

For KPMG's Mr Dillon, the resources already spent on the effort have handed a victory to the terrorists. "The cost to our global economy is so large, they've already had the effect they wanted," he says. "The increasing costs of compliance and technology are a form of terrorism. We're damaging ourselves."