2005-01-01

Warning Indicators, Terrorist Finances, and Terrorist Adaptation; Strategic Insights, v. 6, issue 1 (January 2005)

Williams, Phil

Monterey, California. Naval Postgraduate School

Warning Indicators, Terrorist Finances, and Terrorist Adaptation[1]

Strategic Insights, Volume IV, Issue 1 (January 2005)

by Phil Williams

Strategic Insights is a monthly electronic journal produced by the Center for Contemporary Conflict at the Naval Postgraduate School in Monterey, California. The views expressed here are those of the author(s) and do not necessarily represent the views of NPS, the Department of Defense, or the U.S. Government.

For a PDF version of this article, click here.

Introduction

The attacks of September 11, 2001 on the World Trade Center and the Pentagon were seen initially as a “bolt from the blue," but were, in fact, in the planning stage from 1995 onwards. The plans themselves were carefully adapted and refined in ways designed to increase the prospects of success. They were also given a much higher level of funding than any other al-Qaeda attack. Indeed, it has been estimated that the cost of mounting the attacks for al-Qaeda was about $500,000. Although this is a trivial sum when compared to the death and destruction that were caused, the psychological impact which shattered United States illusions of invulnerability, and the impact on the economy of the United States which lost billions of dollars, it was nonetheless a significant investment, and one that involved the transfer of substantial sums of money to the hijackers prior to the attack.

Had law enforcement and intelligence agencies been focused on these money flows or sensitive to their potential significance, then the catastrophic surprise of September 11 might have been avoided. This is not to suggest that financial transfers were the only indicator. Indeed, there were several other indications of the impending attacks that could have provided some degree of warning for the United States, had there been better inter-agency coordination and intelligence sharing and greater receptivity to the possibility that civilian airliners might be used as weapons. At the same time it is important not to under-estimate the sheer difficulty of the intelligence process—which is less about finding a needle in a haystack than finding a particular needle in a stack of needles—by imposing what one management analyst has termed “retrospective coherence.”[2] For the most part, the signals were scattered, fragmentary, incomplete, indeterminate, and surrounded by noise.[3] The hijackers made mistakes, but the mistakes were not sufficient to alert authorities to the impending action. In the aftermath of the attacks, however, the United States formulated a comprehensive strategy against al-Qaeda that included an assault on the network’s finances as well as efforts to strengthen indicators and warnings of future terrorist attacks.

These two aspects of the United States response to al-Qaeda—developing better indicators and warning on the one side and trying to freeze and seize terrorists assets on the other—created

dilemmas that have not yet been resolved, required difficult and uncomfortable tradeoffs that have yet to be made. The decision to freeze and, where possible, seize terrorist assets was an important part of the effort to weaken al-Qaeda's capacity to carry out further attacks, but in some respects ran counter to the possibility that following the money trail might offer important insights into future terrorist operations. Frozen assets cannot be moved and therefore deprive intelligence and law enforcement agencies of opportunities to monitor the movement or transfer of funds that might be used for the next attack. The justification for freeze and seize, of course, is that the loss of monitoring opportunities is outweighed by denying terrorists access to funds. Yet, it is far from clear that the attack on terrorist finances has yielded to the kind of results initially anticipated. In fact, the global campaign aimed at terrorist assets is more accurately characterized as a dismal failure than a qualified success. Against this background, this paper sets out to:

- highlight some of the reasons why the freeze and seize strategy has not been more successful, and to consider if this lack of success is a result simply of inadequate policy or of more fundamental structural factors that are impossible to overcome.
- identify the various ways in which financial transactions of different kinds could provide indicators, both of a potential attack and of the ways in which terrorist organizations are not only reacting to the attacks on their financial base but also responding more generally to the pressure exerted on them by national governments and the international community.
- make recommendations about the optimum trade-off between freezing assets and following the money trail.

Attacking Terrorist Finances: A Failed Strategy?

In the months following the September 11 attacks the international community, led by the United States, was able to freeze approximately $100 million of terrorist funding. Subsequent efforts over the next three years, have failed to add much more than $40 million to the total of frozen or confiscated funds. Some of the reasons for this are traceable to the inherent inadequacies of global regimes designed to combat terrorist financing; others stem from the availability to terrorist networks of alternative methods of raising and moving money; and yet others reflect the agility, flexibility, adaptability, and sheer ingenuity of terrorist networks that are not burdened with the constraints of sovereignty, not confined to the use of formal financial institutions, and not dependent on state sponsorship for their income.

This third factor—the capacity of terrorist organizations to adapt quickly to new regulations by adopting novel methods of circumventing rules and restrictions—is a major part of the problem for the United States and the international community. Containing and constraining transnational networked adversaries who play by their own rules is a formidable undertaking. Indeed, if we use a complexity theory lens to consider the terrorist financing issue we can more readily see that some of our policies are likely to be not only limited in their impact but also counter-productive. In the final analysis, the attack on terrorist finances might simply make terrorist networks smarter than they would otherwise be.

The inadequacies of global financial regimes

In some respects, the effort to target terrorist financial assets was doomed to failure from the outset. The approach simply extended the existing global anti-money laundering regime to include efforts to combat terrorist finances. The problem was that this regime—which had been developed in the 1990s to combat drug traffickers and transnational criminal organizations—had serious shortcomings. The key player in the regime was the Financial Action Task Force created by the G-7 in 1989. The FATF enunciated 40 recommendations that:

- emphasized the need for legislative measures to enable authorities to identify, trace, evaluate and confiscate laundered money or property of corresponding value;
- highlighted the need for financial transparency which required measures to obtain information about the true identity of persons on whose behalf an account was opened or a transaction conducted; and
- provided a bench-mark against which national efforts to combat money laundering could be assessed. Indeed the 40 Recommendations can be understood as an attempt to establish an anti-money laundering regime with two broad components: a domestic regulatory regime that encompassed monitoring and reporting of cash transactions above a certain amount ($10,000 in the United States), the reporting of suspicious transactions, and know your customer and due diligence requirements; and a regime for international cooperation against money laundering that embodied mutual legal assistance treaties (MLATS) extradition, cooperative investigations, the sharing of information, and greater responsiveness to "on-request" information exchanges in response to suspicious transactions, and to requests by foreign countries to identify, freeze, seize and confiscate proceeds.

Although the FATF did not develop a formal convention, implementing the 40 recommendations became a crucial requirement for the member states (the 26 original members and those which joined subsequently) and provided the basis on which the FATF has subsequently developed a three-fold role:

- monitoring the progress of the member-states in implementing measures to counter money laundering through annual self-assessments and more detailed mutual evaluations; this was done though review processes that provided opportunities to put considerable moral and political pressure on governments that were not in compliance with the recommendations and, therefore, not meeting their obligations. Under pressure from the FATF, for example, Austria grudgingly agreed to eliminate anonymous savings accounts that ran against FATF notions of transparency and accountability.
- reviewing money laundering trends, techniques and counter-measures and their implications for the forty recommendations—and sharing this information among the members so as to enhance their capacity to counter innovations or new trends in laundering. This has resulted in annual meetings and reports on money laundering typologies. In recent reports, the FATF members have focused attention on specific money laundering mechanisms such as trade-related schemes, informal remittance systems, internet banking, and the role of company-formation agents.
- extending the adoption and implementation of the FATF recommendations in an attempt to build a global anti-money laundering network. This process has two separate but complementary components: broadening membership to include new countries such as Brazil, Mexico and Argentina; and the creation of regional groupings with a similar mandate to the FATF itself. The Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) created in August 1999 is an example of the second variant.

In effect, the FATF has sought to extend the scope of anti-money laundering measures geographically, sectorally and functionally. In 1996 it recommended that money laundering crimes be extended beyond the predicate offense of drug trafficking and that consideration be given to imposing restrictions on the use of new technologies to conduct financial transactions that were remote, anonymous, and outside traditional institutions. Not surprisingly, these proposals were accompanied by the recommendation that the same laws and regulations that had been developed for the banking sector be extended to non-bank financial institutions. More recently, the FATF gave teeth to its efforts by developing and publishing criteria for identifying "non-cooperative jurisdictions," and actually naming those states which fell into this category. This marked a new stage in the effort to establish an effective global anti-money laundering regime. It was based on the recognition by the FATF that "continued mobilization at the international level to

deepen and widen the fight against money laundering" remained essential in the second decade of the organization's existence.

The FATF has some real achievements: in particular the promotion of international information exchanges on recent trends and developments in money laundering is extremely valuable. FATF also placed the money laundering issue on the international agenda to a degree that was difficult to imagine in the late 1980s. Moreover, the "name and shame" campaign had some success in forcing a number of jurisdictions to meet international norms and standards by creating greater financial transparency, imposing reporting requirements for both cash transactions and suspicious transactions, and establishing Financial Intelligence Units to monitor the financial system. It was not surprising, therefore, that in the aftermath of the September 11 attacks, the FATF extended its mandate to terrorist finances. If the FATF has rightly obtained major plaudits for imposing an anti-money laundering regime, however, the congratulatory rhetoric hides a reality that is more complex and somewhat disappointing. In spite of its successes, the FATF has suffered from several flaws:

1. The first major deficiency is the emphasis on procedural norms rather than the creation of substantive norms with substantial impact. International cooperation against money laundering became a goal in its own right rather than simply a means to an end. Even more important, the cooperative venture became fundamentally flawed by elevating form over substance. The FATF established a set of standards and practices that require considerable effort but that do not yield commensurate results. The FATF has imposed procedural requirements that states adopt certain forms of regulation designed to inhibit or detect and prosecute money laundering. Although this has probably had some impact in obstructing and displacing money laundering, in substantive terms the achievements have been disappointing. This is not surprising: cash transaction reports and suspicious transaction reports are enormously time-consuming and yield vast amounts of information, but very few successful prosecutions. The United States and the states of the European Union have far more elaborate and formalized rules against money laundering than any other countries—yet they remain probably the largest laundries in the world. This suggests that the FATF's approach to combating money laundering results in the wrong questions being asked. The focus is on whether or not the participating states meet FATF standards, rather than on whether or not the measures which have been introduced by states are effective in combating money laundering. The result is an impression that far more is being achieved than is actually the case. Until the FATF not only develops measures of effectiveness that reflect real rather than ostensible results but also addresses the substantive effectiveness of procedural norms in combating money laundering, some states will manage to be simultaneously wonderful launderettes and in good international standing.
2. In spite of the broadening of its membership and the expansion of its geographic reach the FATF still remains circumscribed geographically. As a result, its impact is not to halt money laundering but merely displace it to locations where the risks are lower. A partial regime in the money laundering field creates balloon effects in the global financial system similar to those created by enforcement in the "war on drugs" at the local level.
3. The third problem is that of covert defection from the regime. Governments play games and will increasingly do so in relation to the anti-money laundering regime and its offspring, the regime to combat terrorism finances. States such as Russia have created new laws and score highly in terms of international cooperation—but have not been nearly so effective at implementation. Since the problem of defection can take many forms, a much more sophisticated approach to notions of conformity with the regime is essential. The levels of conformity that need to be examined include not only the legal framework, but the capacity for

implementation, the number of indictments, the number of prosecutions, and the number of convictions. Without this much more rigorous approach, some governments at least will continue to engage in cosmetic conformity, ostensibly performing to the standards demanded but doing very little in practice to meet these standards.

4. The fourth problem is that, more often than not, money laundering is transnational and multinational in scope. Not only do the launderers operate on the basis of jurisdictional arbitrage, but they also exploit jurisdictional voids and deliberately create jurisdictional confusion which makes it difficult to follow the money. Indeed, only if international cooperation is truly genuine, sustained, and systematic will there be real successes in prosecuting transnational money laundering cases.

In short, the anti-money laundering regime has some fundamental flaws that limited its impact even on the initial target set. These deficiencies are even more telling when the targets become not profit-seeking groups (where removing the money flow and thereby reducing the profits challenges the raison d'etre of the organizations) but groups or networks where money is no more than a means to achieve political objectives. Terrorist are less concerned about laundering dirty money than using clean money to further the cause—which includes carrying out additional attacks. Moreover, the way in which al-Qaeda has beaten the U.S. government in winning the "battle of the story"[4] suggests that cosmetic conformity and tacit defection is likely to be the norm in a large part of the Islamic world.

Operations are cheap

A second major problem with the extension of strategies initially designed to attack the profits of organized crime, is that the success level has to be much higher when dealing with terrorists even though the target profile is so much smaller. Indeed, the inherent advantage lies with the terrorists simply because most terrorist attacks can be carried out without large expenditures of money. The Madrid bombings of March 11, 2004 for example, are generally believed to have cost no more than about $10,000. Even though for this figure might be somewhat on the low side—and a $20,000 to $30,000 estimate might be more accurate—even this larger assessment is still a relatively modest amount of money. Other terrorist attacks such as the Bali nightclub bombing, the attack on the JW Marriott Hotel in Jakarta, the Cole bombing, and the thwarted strike against the U.S. Embassy in Paris in the summer of 2001, have been carried out for between 20,000 and $75,000. The implication, of course, is that unless efforts to constrict the flow of finances to operational cells are extremely successful they are unlikely to degrade the capacity of terrorist networks to carry out new attacks.

Alternative means of raising and moving money

A third difficulty for the United States and the international community in attacking the financial basis of terrorist organizations is that both terrorist organizations and their financial support structures are not static targets. This is evident in two distinct phenomena. The first is that although the focus on financial support for terrorism from Islamic charities has led to the closure of some of these charities, the charities have adapted in a variety of ways. In some cases the head office has closed but branch operations continue to operate unhindered; in others the charities have simply re-registered and re-opened under new names but with the old infrastructure intact. A third approach has been to support terrorists less through direct contributions than through logistic support (such as employment in a charity branch office.)[5] The essential point is that some of the prime targets of the effort to combat terrorist finances have displayed a degree of resilience and a capacity for morphing and adapting that have neutralized a very precise and well-planned strategy by the United States and its allies.

This is not to suggest that the strategy has had no impact. Clearly the financing of terrorist organizations is much more problematic than it was: funds from the charities are neither as plentiful nor as easily moved as in the past. Terrorist organizations have compensated for this, however, with their own form of adaptability and emergent behavior. This is reflected in terrorist appropriation of organized crime activities which are increasingly used to make up the shortfalls in funding from the charities. Kidnapping, extortion, drug trafficking, other forms of smuggling, credit card theft and fraud, document fraud, and robbery have become staple features of the terrorist fund-raising repertoire. Such activities have been evident in locations as diverse as Colombia, the Philippines, Central Asia and Western Europe. This is not surprising: most organized crime activities do not have a steep learning curve; nor do they require significant upfront investments. Given the low entry costs on the one side and the gains that can be made on the other, the exploitation of organized crime methods by terrorist organizations and networks is a natural and foreseeable (if unstoppable) development. What is surprising, however, is the extent to which different terrorist organizations operating with diverse political agendas in various parts of the world have engaged in the same forms of adaptive behavior—and in so doing have neutralized the "global" effort to undermine terrorist finances.

Stopping the flow of money to the sharp end of terrorist networks is impossible. Consequently, a reappraisal of the efforts to combat the financing of terrorism is essential. With the rationale for the freeze and seize campaign undermined by a continued lack of effectiveness, the tradeoff issue between freezing and following the money should be resolved in favor of the latter option. The argument in favor of this is even more compelling because the attempt to freeze terrorist funds has not only failed, it has actually been counter-productive. This can be explained most clearly in terms of two components of complexity theory: the notion of co-evolution and the idea of a fitness landscape. The coevolution concept recognizes that the United States government and al-Qaeda are in a highly interdependent relationship. Within this interdependence, however, al-Qaeda as the weaker entity has to exhibit greater sensitivity to United States initiatives than vice versa. If it is to survive, al-Qaeda has to evolve quickly in response to environmental shaping measures initiated by the United States. It can do so partly because of its reliance on network structures and partly because of its learning capacity. Indeed, al-Qaeda and other terrorist groups are adept at organizational learning and this enables them to mutate into unfamiliar forms, adopt novel and unexpected methods of operation, and generally confound measures designed to constrain them. In this connection, the notion of a fitness landscape is particularly pertinent. Because of the coevolution of competing systems or organizations, the outcome of the competition will be determined largely by which one evolves most rapidly and effectively to the challenges posed by the other. Thinking in terms of the fitness landscape, the danger is that governments will compel terrorists to move to new fitness peaks in the landscape yet fail to move to higher peaks themselves. The effort to freeze terrorist assets has created precisely this outcome. Efforts by the United States and the international community to combat terrorist finances through freeze and seize have compelled Islamic charities and al-Qaeda to move to higher fitness peaks, but it is not clear that the institutions in the forefront of the international effort to combat terrorist finances can do the same. Indeed, it is arguable that one of the major consequences of the freeze and seize strategy has been to make it even more difficult to follow the money and use money as a critical warning indicator.

Even before this occurred, however, following the money was a formidable task. Nevertheless, it is clear that the financial dimensions of terrorist activity offers opportunities for intelligence collection and analysis that might be important in providing warning of impending attacks. This theme must now be elaborated.

Financial Transactions as Warning Indicators

There are several ways in which financial transactions could provide indicators of a possible or impending attack. In only very few cases, however, will the financial transaction provide the critical indicator. In most cases, the transaction will simply become part of a broader picture and

add a piece to the overall understanding and assessment of what is going on. In some instances, this can be the critical piece in illuminating and crystallizing what had hitherto been uncertain; in other cases, it is merely one part of a broader picture that remains murky and diffuse. With this caveat in mind there are several dimensions of financial transactions that need to be considered:

- Financial movements and expenditures as a critical component of attack preparations.
- Money as a connection between a known part of the terrorist network and an unknown part.
- Changes in the predominant patterns of financial transactions within and by a terrorist network, perhaps signaling an extension of terrorist activities and a focus on a new set of targets.
- Criminal activities of a terrorist cell that are either designed to fund terrorist action by the cell itself or to provide support for a cell that is planning an attack.
- Suspicious financial transactions (i.e. financial transfers, deposits or withdrawals of whatever amount that either appear to have no economic rationale or that, for whatever reason arouse the suspicions of banking personnel).

There is clearly some overlap among these various indicators. Criminal activities at the cell level to provide operational funding, for example, are very closely connected to financial expenditures as a critical component of attack preparations. Nevertheless, it is worth distinguishing between these indicators, recognizing that in practice, the greater the concentration of indicators, the more confident the judgments and warnings that are based on them. With this in mind each of the possible indicators must now be explored.

1. Financial Expenditures as a Critical Component of Attack Preparations.

As suggested above, terrorist attacks are relatively inexpensive, as one would expect from what is often considered as a form of asymmetric warfare, and a weapon of the weak against the strong. In the case of the projected al-Qaeda suicide bombings on the United States embassy in Paris and the Consulate in Marseilles in the summer of 2001, Jamal Beghal, the leader of those involved, was to go to Morocco to pick up $50,000 for the operation. The cost of the abortive attack on the Christmas market in Strasbourg in December 2000 was probably somewhere between $20,000 and $30,000.[6] Although the costs will depend in crucial ways on the precise nature of the operation, it seems likely that they fall into several categories:

- *Subsistence for the perpetrators as they prepare for their actions.* The day to day living expenses are not trivial even if the terrorists live a very frugal lifestyle. If they try to blend in through frequenting social events and clubs, their expenditures will increase. The costs will also vary depending on the location of the targets, and the proximity of the terrorists to these targets. The costs of operations in the United States or Western Europe will obviously be considerably greater than operations in countries such as Tanzania, Kenya and Yemen.
- *The cost of special training and the development of expertise that is critical to the successful completion of the mission*. Although many of the skills necessary for an operation will have been developed at terrorist training camps, some of the more specialized requirements can only be met through more legitimate and more costly avenues such as attendance at flight schools.
- *The purchase of any weapons or explosive materials that are to be used in the attack.* The September 11 hijackers were relatively unusual in that they were so lightly armed. In other cases, however, the acquisition of explosives or weapons is more costly—especially if combined with efforts to disguise the activities. Ahmed Ressam, the LAX bomber reportedly spent about $7,000 in Vancouver on the purchase of explosives prior to his attempt to enter the United States to implement the millennium plot. In the case of the terrorists in Frankfurt planning an attack in Strasbourg, the cost of the raw materials

was increased because they traveled extensively and bought small amounts in an attempt to avoid suspicion—although they also used stolen credit cards for the purchases.

- *The cost of travel for meetings related to the plan.* In most cases of planned or actual attacks by terrorist networks operating in the United States and Western Europe, there was considerable travel prior to the event itself. The reasons for this can include meetings among the conspirators, meetings with senior people in the network, or meetings with members of the network providing some kind of support services. Mohammed Atta's trip to Spain, for example, in July 2001 could well have included meetings with the Spanish cell that had been providing support to Atta and his group while they were in Hamburg.
- *The cost of communications among those involved.* Communication costs, of course, have declined enormously with cell phones, pre-paid telephone cards and e-mails (often from public libraries and Internet cafes). Nevertheless, these costs still have to be included in the overall cost of the mission. Moreover, even though cell phones and pre-paid telephone calls are relatively cheap, the tendency to use them and quickly dispose of them in order to maintain operational security can add to the costs.

In other words, certain kinds of expenditures have to be met—and therefore have to be funded either by those directly involved in the operation or by their supporters. In some cases, the payments for the purchases (whether material or services such as training) can be an indicator. In others, the transfer or raising of money to fund purchases and meet other costs for the terrorists can also help to reveal attack preparations.

2. Money as a Connection between Known and Unknown Parts of Terrorist Networks

Terrorist organizations that use network structures pose difficult problems for law enforcement and intelligence agencies. Mapping the network is an enormously difficult and complex task for several reasons: the inherent dynamism and expansionism of the network as it draws in new recruits; the fact that although parts of the network might be well known, other loosely coupled components will be at some distance from the core of the network, both geographically and in social network terms, and therefore inherently difficult to trace or identify; and the fact that deliberate efforts are being made by the terrorists to maintain anonymity and a low profile. One of the responses to this is to monitor the communications of known members in the hope that this will provide additional clues about unknown members of the network. Although terrorists sometimes limit their communications in a deliberate effort to avoid detection, in some circumstances, communication becomes essential. Indeed, one reason for communication is to ensure there is adequate funding for a planned operation. Monitoring such communications can provide missing pieces of the puzzle and allow law enforcement and intelligence agencies to connect components of a terrorist network in ways that allow them to take decisive action in forestalling an attack. Perhaps the best example of this concerns the Meliani terrorist cell in Frankfurt that, in December 2000, was planning an attack on the Strasbourg Christmas market and Cathedral. Members of the cell were under surveillance by German law enforcement. Although their actions were suspicious, however, it was not clear what they were planning and there was no obvious reason for apprehending them. The group had bought chemicals for making explosives with stolen credit cards supplied to them by a support group in Milan. Moreover, they still had "almost $14,000 (£9,675) in cash—some of it …raised by drug dealing on the streets of Frankfurt."[7] Nevertheless, "the cell members needed more money. They went back to their paymasters. It was the mistake that destroyed the mission."[8] A member of the Frankfurt cell called a key al-Qaeda operative in Britain known as Abu Doha or "the Doctor," asking for more money and informing him that the operation would be carried out before the end of the year. British intelligence agents had Doha under surveillance and monitored the call. They then informed the German authorities, providing a critical piece of information that enabled the Germans to act preemptively and forestall the planned attack. In this case, not only was an additional segment of the network identified, but the information was so good that it facilitated action preventing the planned attack from coming to fruition.

In effect a puzzle was solved when a secret was uncovered. Actions that had earlier been difficult to explain or understand now became part of a recognized pattern of attack preparation. Although critical tactical intelligence about the target of the attack was still missing, enough indicators had been uncovered to justify decisive action. This case might have been exceptional in that the payoff in terms of attack prevention was so high. Nevertheless, the importance of money as a link or connector between the known and the unknown segments of the network transcends this particular case. At the very least, following money flows can assist in mapping the network and identifying previously obscured or unknown nodes and connections.

3. Changes in the predominant patterns of financial transactions by terrorist networks

As more details have been uncovered about Islamic terrorist finances in general and al-Qaeda finances in particular, it has become clear that one important and recurring pattern has been the use of charities for both raising money and moving money. This is an important pattern that facilitates careful monitoring and the potential acquisition of good tactical intelligence. Changes in financial flows within terrorist networks, for example, might suggest that new targets have been identified or there is a shift of priorities on the part of the terrorist network and its leadership. Channeling of funds in a direction that they have not hitherto gone can be a clue to an impending operation, usually in an area where it is otherwise unexpected. When known or reconstituted Islamic charities suspected of being covers for terrorist networks appear in countries where previously they had no presence this is an important indicator that new targets are either under consideration or have already been selected. If the charities are already present, then serious shifts in funding levels and a surge of funds into the charity in general, or the country office in particular, can be another important indicator. Sudden surges might be particularly revealing, but even more gradual surges could offer a degree of warning and, at the very least, impel much closer scrutiny.

The speculation after September 11 about al-Qaeda owned stock being sold prior to the attacks on Washington and New York was inconclusive. Nevertheless, the idea behind the speculation was very sound: what occurred seemed to have been some kind of deviation from an established pattern of investment, possibly caused by prior knowledge. As such, it clearly merited attention. Moreover, it again suggests that in the financial world surge activity of one kind or another might require careful scrutiny. The problem, of course, is that such surges of activity are ubiquitous. They are often caused by rumor or by some shift in the political or economic context. Nevertheless, this is another area where close human scrutiny combined with innovative data-mining techniques might uncover indicators that would otherwise be missed.

4. Criminal activities to fund terrorist action

As suggested above, what might be termed “do it yourself organized crime” by terrorist networks has become an important and almost ubiquitous tool for terrorists. This has been evident in organizations ranging from the IRA to the Tamil Tigers. It has also been apparent in al-Qaeda and other Islamic terrorist organizations. In some instances, criminal activities are used at a strategic level as part of the overall funding mechanism for the terrorist organization. Hezbollah supporters or members involved in cross-state cigarette smuggling in the United States, for example, have sent the proceeds to the home organization. Similarly, Tamils in Canada who have been involved in such diverse crimes as drug trafficking and credit card fraud have sent a significant part of the profits back to Sri Lanka for the LTTE. In other cases, however, criminal activities are undertaken at the tactical or cell level, where they are used to fund specific terrorist activities. In the al-Qaeda network, despite the presumed wealth of the organization and of Bin Laden in particular, cells planning terrorist operations have received very little money from the leadership. Instead they have been compelled to engage in petty crime and minor forms of organized crime to acquire the necessary funding. Ahmed Ressam, for example, robbed hotels and unsuccessfully attempted to hold up a currency exchange office. His request for more money from al-Qaeda was turned down and as a result, he opened a store in Montreal where he

collected credit card information that was then passed to associates for fraud.[9] Similarly, the cell in Frankfurt engaged in drug pushing as a source of sustenance while planning the Strasbourg attack. Yet other groups engaged in selling false identities as a means of raising money. From this perspective, the criminal activities of a terrorist cell that are designed to maintain the cell and provide operational funding can be an indicator that the cell is preparing for action.

Yet there is an additional twist. In the European al-Qaeda network of 2000 to 2002 there appeared to be a division of labor among the cells, with some clearly designated as operational and others providing a financial support role. The cell in Milan under Ben Khemais, for example, stole credit card that were subsequently used by the Frankfurt group to purchase chemicals for explosives. In other words, criminal activities of one cell can be part of the support structure for another cell. This division of labor within a small matrix generally results in a one-way flow of money. This can provide indicators of which cell is actually planning an operation. Moreover, in some cases, the criminal activity leaves a trail that enables investigators and intelligence analysts to connect the dots and obtain a more accurate picture of at least one segment of the overall terrorist network.

5. Suspicious Financial Transactions

In its effort to combat drug trafficking and organized crime by making it more difficult to launder money through the financial system, the United States government, in effect, coopted the banks. Regulations were established to ensure that all cash deposits of $10,000 or more were accompanied by a cash transaction report (CTR) – which the bank subsequently had to submit to the Treasury Department's Financial Crimes Enforcement Network (FinCEN). In addition, any transaction that aroused the suspicion of bank employees—irrespective of the amount involved—had to be passed to law enforcement in a suspicious activity report (SAR). While some critics suggest that the effort involved especially in CTRs but also in SARs does not yield commensurate payoffs, the SAR mechanism in particular offers a way of identifying activities that are worth investigating further. Although this mechanism was initially designed to assist in combating drug-related money laundering it has broader application. The suspicion can come from the person (or persons) involved in the transaction, from the fact that there is no obvious commercial or financial basis for the transaction, from concern about the country or city of origin, or a variety of other considerations Indeed, the requirement to report suspicious activities or transactions has become a standard not only for the United States but for most countries with well-developed, sophisticated financial systems. When accompanied by provisions for due diligence and know your customer requirements, the SAR system provides opportunities for warning about criminal activity.

Such a system has some relevance to terrorist activity. The difficulty is that terrorist financial transactions cannot simply be equated with money laundering—in spite of the tendency of many commentators to make such an equation. In fact, the two phenomena, although occasionally converging, are mostly very different. Money laundering takes dirty money, hides its origins and ownership, and makes it appear to be the proceeds of legitimate economic activity. In essence it is about taking dirty money and making it clean so that it can be enjoyed. Terrorist operational financing, in contrast, takes money and simply uses it for terrorist attacks and their preparations. More often than not this is clean money that is being used for nefarious purposes. Although terrorism financing might encompass money laundering when the money involves the proceeds of crime, even then much of the money is simply spent rather than put through an elaborate laundering process. For the most part, therefore, terrorists do not actually launder much money. This is not to deny that terrorist networks want to move their money covertly and with the same lack of attention from the authorities that criminals seek when they move the proceeds of crime. In this sense, some terrorist financial activities clearly involve the "functional equivalent of money laundering" and employ many of the same mechanisms and modalities for moving money as do transnational criminal organizations. In some respects, terrorists have even added to the repertoire of options for moving money by supplementing or even supplanting front companies with charities. Al-Qaeda has also made extensive use of underground banking such as the

hawala system to move money without leaving a significant paper trail. Yet al-Qaeda also uses the normal banking system where its transactions are very hard to distinguish from legitimate business activities and financial transfers.

There are occasions, when the SAR system can trigger a warning that might be linked to terrorist activity. In the aftermath of the September 11 attacks, as investigators sought to discover the activities and movements of the hijackers, it was learned that a money transfer from the United Arab Emirates to SunTrust Bank in South Florida that had provided crucial funding support to several of the hijackers had also prompted a suspicious activity report. Unfortunately the report had not been followed up with a further investigation. Nevertheless, it does reveal that because the SAR system is designed to flag all suspicious transactions and is not limited to those involving money laundering it can, on occasion, provide an indicator of money transfer linked directly to support of terrorist operations.

This is not to suggest that following the money is a magic bullet that invariably leads to early detection and warning. As with all other aspects of counter-terrorism intelligence, attempts to use the movement and disbursement of money as a warning indicator will involve false leads, false positives, and false alarms. At the same time, leads that could offer warning indicators might appear so innocuous that they are overlooked or discounted. In this area, as in any part of the intelligence domain, signals and noise are often only distinguishable in retrospect. Moreover, there is a serious problem with efforts to link finances to operational planning and attacks by terrorists—the relatively small part of terrorist financial resources that are devoted to operations as opposed to recruitment and training. In other words, the financial signals themselves are intrinsically quiet, modest, and a very small part of the overall financing effort. A third difficulty is that many if not most financial transactions are neutral in the sense of setting off alarms. They take on real significance only when they are carried out by or involve people who are themselves regarded as an actual or potential threat—either because they are known or suspected terrorists or because they have strong associations with terrorists. It is the marrying of the person or persons and the transaction that is critical, rather than the transaction itself. If this is enough to suggest that there are limits to the use of financial flows and financial transactions as warning indicators, however, it does not mean that this dimension of activity can or should be ignored. In combating terrorism, financial scrutiny is a key component of a much broader process that also has to include network analysis, travel and telephone toll analysis, as well as fusion of open sources and covert intelligence such as electronic intercepts and information from defectors.

In delineating possible indicators of an embryonic, fully planned, or impending terrorist attack, it is necessary to consider several aspects of the intelligence process including the frequently made distinction between puzzles and secrets, the importance of both patterns and anomalies, and the need for both strategic and tactical forms of warning.

Many analysts have observed that the intelligence challenge in the post Cold war era is often a matter of solving puzzles rather than discovering secrets. The puzzles themselves are generally complex and multi-layered, requiring comprehensive efforts to solve them. Yet the distinction between puzzles and secrets is not clean and neat. Those who are part of the puzzle, for example, often take precautions to ensure that many of their activities are secret or covert. Terrorists and criminal networks, in particular, operate in the shadows, shielding their activities from intelligence and law enforcement scrutiny in an effort at risk minimization. Avoiding surprise, therefore, requires both solving puzzles and uncovering secrets. In this context focusing on the financial dimension of terrorism is essential. Such a focus can help both to uncover secrets and to solve puzzles. Obtaining knowledge about the financial flows of terrorist networks, for example, can help to assess the scope of the network and the thrust of its activities. Such knowledge can also provide insights into flows of money (including small amounts) that might be precursors to a terrorist attack. In this sense, following the money trail can be a critical element in uncovering secrets. As such it is crucial to efforts to avoid surprise

Part of the intelligence process can be understood in terms of both pattern detection and anomaly detection. Identification or detection of patterns is a central component of intelligence analysis and contemporary data mining, which is "concerned with uncovering patterns, associations, changes, anomalies, and statistically significant structures and events in data."[10] Even within this search for patterns, however, there are two complementary but distinct activities that can occur in the mining and analysis process: pattern discovery when there is no prior knowledge of the patterns, and pattern matching when a pattern that is identified in the data is identical with a pattern that is already known. In addition, patterns of either kind, also make it possible to identify deviations. A clear and recurring pattern that appears to be well-established provides a baseline from which it is possible to detect and assess changes, departures, or deviations. Such changes either provide indicators of an anomaly that needs to be further examined or of something that is recognizable and understood as a transition from one pattern of behavior to another. The anomaly itself is: either indicative of change to another pattern that is familiar and understood as such (pattern recognition); or a blip or aberration that is not indicative of a new pattern (true anomaly); or a development, the significance of which is uncertain, but that requires further scrutiny because of the possibility that it represents a new pattern (uncertain anomaly); or indicative of a change to a new pattern the purpose, meaning and significance of which is not yet understood (pattern discovery). In other words, the recognition of an anomaly sets off a search for meaning that can result in:

- a changed assessment of what is going on;
- a determination that although things have changed, the significance of the change is uncertain but requires continued monitoring and assessment;
- the dismissal of the anomaly as simply an unusual or unique incident that is unlikely to be repeated.

Whatever, the conclusion, though, it is clear that patterns provide a sense of order and establish baselines from which it is possible to discern deviations or anomalies that also help to strengthen understanding. In this connection, it is important to understand patterns of terrorist financing—how they typically raise money, move money and spend money. With this baseline established, changes in the patterns can be better understood. In some cases, these changes—especially as they relate to disbursement—will be potential indicators of terrorist attacks.

In terms of levels of warning, part of the challenge for counter-terrorism intelligence is that it is relatively easy to obtain strategic warning—Osama bin Laden himself made very clear that he was declaring war on the United States several years prior to the September 11 attacks—that some kind of attack is likely to occur. The difficulty, however, is going from the general to the specific, or from strategic warning to tactical warning. As a recent analysis of intelligence analysis and assessments prior to the September 11 attacks noted, "Tactical warning enables policymakers and government decision-makers to direct preventive action against specific individuals who may be involved in the planned attack and to implement appropriate protective action for specific targets."[11] Unfortunately, tactical warning regarding the time, target or method and the perpetrators of an impending attack is far more difficult to obtain—particularly where the terrorists have managed to obtain operational security. The challenge, therefore, is to link financial indicators to this tactical level of warning.

Conclusions

The implication of all this is that terrorist financial transactions can be an important—if elusive—indicator of a planned or impending attack. For the most part, however, such indicators need to be combined with other intelligence as part of a comprehensive assessment. While financial transactions alone are unlikely to provide definite and unequivocal warning, sometimes these indicators will spark a search for other parts of the puzzle, providing a stimulus for a tighter focus or simply a heuristic for a shift in direction. If their value as indicators is to be maximized, however,

then there are several other things that need to be done as part of the intelligence process. Some of these occurred as part of the immediate response to September 11, but need to become standard operational procedures.

- Establish a base-line of understanding about terrorist finances that encompasses knowledge of established patterns and sensitivity to deviations, anomalies, and the possible emergence of new patterns. The deeper the knowledge base and the greater the level of understanding of terrorist finances, the greater the chance of detecting activities or shifts in activities that provide warning indicators.

- Bring together combinations of expertise from disparate fields. In examining financial transactions, national security intelligence personnel and even law enforcement agents need accountants and banking and financial experts who are familiar with the often arcane practices of the financial world and adept at following money trails and identifying anomalies.

- Recognize that analysis is as important as collection. If the information has been reported but not analyzed the result is the same as if it had not been reported in the first place. This has been particularly the case with SARs. The analysis of SARs needs to be expedited and the results shared with the wider intelligence community on a timely basis.

- Information needs to be pooled, shared and widely examined in the intelligence community to ensure that financial indicators are seen in a broader context and considered along with other possible indicators of a forthcoming attack. In attempting to combat terrorist networks, government itself needs to operate as a network, transcending the bureaucratic turf wars and obstacles to information sharing that characterized the intelligence process prior to September 11. Information is not a resource to be guarded but one to be shared as widely as possible within the bounds of an intelligence community that goes well beyond the traditional agencies.

- Information needs to be widely diffused not only within the Federal government but also at the state and local level—albeit with sensitivity to security concerns. As a study of the ecology of warning carried out by Global Futures Partnership at CIA noted, the consumers for warning go well beyond the traditional national security community. This is particularly the case now that terrorist organizations are engaging in do-it-yourself organized crime since the people best placed to detect specific examples of this are in local law enforcement. The broadening of the customer base can have a positive feedback effect where specific warnings provoke a further search for indicators that can augment and refine the whole process.

None of these measures is a palliative. Nor are they a guarantee that financial indicators will always be identified and understood as such. Much of the time the intelligence task is an attempt to know the unknowable. And sometimes even when something is known its significance is not always fully understood or appreciated. Nevertheless, these kinds of changes—which are really about attitude, procedure, and bureaucratic norms and practices rather than about bureaucratic structures—are essential to ensure that financial indicators become an integral part of the indicator and warning process and a part that can have significant payoffs in terms of early warning.

The other thing that needs to be done—and this can be tacit rather than explicit—is to back away from the effort to freeze terrorist assets. This might be politically difficult given that frozen funds provide a tangible measure of effectiveness. Nevertheless, it should be borne in mind that such figures are usually endowed with more significance than they deserve, obscure more than they reveal, and give a misleading impression of the success of the counter-terrorism strategy.

Moreover, the unintended consequence of the freeze strategy is to make terrorist networks such as al-Qaeda even better at hiding their money—and thereby making it more difficult to follow the money and perhaps obtain the level of warning that is necessary. The tacit abandonment of the freeze strategy, therefore, might be an important contribution to the detection of financial indicators that would otherwise be elusive and the achievement of a degree of warning that would otherwise be unobtainable. Although such a conclusion is counter-intuitive, it is also inescapable.

About the Author

Dr. Phil Williams is Professor of International Security at the Graduate School of Public and International Affairs at the University of Pittsburgh. He was previously the Director of the University's Matthew B. Ridgway Center for International Security Studies. Dr. Williams has published extensively in the field of international security including *Crisis Management, The Senate and U.S. Troops in Europe*, and (with Mike Bowker) *Superpower Detente: A Reappraisal*. During the last decade, his research has focused primarily on transnational organized crime, and he has written articles on various aspects of this subject in Survival, Washington Quarterly, The Bulletin on Narcotics, Temps Strategique, Scientific American, Criminal Organizations, and Cross Border Control. He has been a consultant to both the UN and U.S. government agencies on organized crime and has given congressional testimony on the subject. Recently, he has focused on alliances among criminal organizations, global and national efforts to combat money laundering, and trends and development in cyber-crime.

References

1. The author would like to thank John Picarelli for his assistance in the preparation of this paper, and Paul N. Woessner and Shannon Horihan for their comments on an earlier draft. He also benefited from discussing some of the issues raised here with Professor Davis Bobrow and Dennis Gormley.

2. See David Snowden, "Complex Acts of Knowing: Paradox and Descriptive Self-Awareness," *Journal of Knowledge Management*, Vol. 6. No. 2 (May 2002)

3. For the distinction between signals and noise see the classic study by Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962).

4. See John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica: Rand, 2001).

5. See Matthew Levitt, "Charitable Organizations and Terrorist Financing: A War on Terror Status-Check," draft paper presented at the *University of Pittsburgh Workshop on the Dimensions of Terrorist Financing*, March 19-20, 2004 for a fuller and very incisive analysis.

6. All these figures are based on estimates in the public domain.

7. Paul Harris, Burhan Wazir, and Kate Connolly, "Al-Qaeda's bombers used Britain to plot slaughter" *The Observer,* April 21, 2002.

8. *Ibid.*

9. See "Attack on Terrorism – Inside al-Qaeda," *Financial Times,* November 28, 2001.

10. R.L. Grossman, et al, "Data Mining: Opportunities and Challenges for Data Mining During the Next Decade," January 21, 1998. Quoted on *SANS Institute Resources, Intrusion Detection FAQ*.

11. Eleanor Hill, *Joint Inquiry Staff Statement*, Part 1, September 18, 2002.