CHAPTER FOUR

Terrorist Organizations' Vulnerabilities and Inefficiencies

A Rational Choice Perspective

JACOB SHAPIRO

This chapter uses a rational choice approach to examine the political economy of terrorist financing. To date, much of the theoretical literature and almost all government-sponsored reports discuss terrorist organizations as though they are made up of ideologically driven purists who share a uniform commitment to the cause. This assumption is needed to explain how these organizations can both (1) efficiently distribute funds and (2) operate covertly without the checks and balances most organizations require. However, upon closer inspection, one often sees substantial differences in the preferences of key players in terrorist networks. Two selection processes explain why these differences exist, and a principal-agent framework shows how these differences lead to inefficiencies in terrorist financial systems. Terrorist organizations face a trade-off between enduring the inefficiency or employing corrective strategies that create vulnerabilities. Governments can undertake specific actions to make this trade-off more problematic.

Accountability

> With all due respect, this is not an accounting. It's a summary accounting. For example, you didn't write any dates, and many of the items are vague. The analysis of the summary shows the following:
>
> 1—You received a total of $22,301. Of course, you didn't mention the period over which this sum was received. Our activities only benefited from a negligible portion of the money. This means that you received and distributed the money as you please. . . .
>
> 2—Salaries amounted to $10,085—45 percent of the money. I had told you in my fax . . . that we've been receiving only half salaries for five months. What is your reaction or response to this?
>
> 3—Loans amounted to $2,190. Why did you give out loans? Didn't I give clear orders to Muhammad Saleh to . . . refer any loan requests to me? We have already had long discussions on this topic. . . .
>
> 4—Why have guesthouse expenses amounted to $1,573 when only Yunis is there, and he can be accommodated without the need for a guesthouse?
>
> —Ayman al Zawahiri, e-mail to Yemeni cell, February 11, 1999[1]

Standard accounts of terrorist financial and logistical systems stress the efficiency with which terrorist financial networks distribute funds while operating through a variety of covert channels. We are told that "Al Qaeda is notably and deliberately decentralized, compartmentalized, flexible, and diverse in its methods and targets. . . . Al Qaeda's financial network is characterized by layers and redundancies. It raises money from a variety of sources and moves money in a variety of manners."[2] Reports from the multinational Financial Action Task Force on Money Laundering,[3] the Asia/Pacific Group on Money Laundering,[4] and others provide a similar narrative.[5]

Because of the covert nature of their work, these networks must operate with fewer checks and balances than most financial organizations.[6] Indeed, the cellular structure of terrorist networks so often cited in the literature necessarily implies that leaders will be poorly informed about the actions of their subordinates.[7] If we assume that all members of the network are uniformly committed to the cause and all agree on how best to advance the group's political goals, then there is no inconsistency here. However, if lead-

ers, middlemen, and operational cadres have divergent preferences over spending, then information asymmetries created by the secretive nature of terrorist networks lead to myriad opportunities for spending money differently than leaders would like.

While the evidence is mixed regarding disagreements between key terrorist leaders, there is good reason to believe that the preferences of middlemen are not always aligned with those of leaders and operational elements. For example, mid-level managers of organizations such as Harakat ul-Mujahidin (HUM), a Pakistani militant group focused on Kashmir, often live luxurious lives far beyond what their followers can afford.[8] Captured Palestine Liberation Organization (PLO) documents show that those who plan attacks are paid eight times as much as the families of those who die carrying out the attacks.[9] People running criminal fund-raising operations in the United States for Hezbollah drive luxury cars and live in upper-middle-class neighborhoods.[10] During the Christian-Muslim violence in Poso, Indonesia, in late 2000, a relatively senior Jemaah Islamiyah (JI) member arranged for funds raised from oil company workers to be channeled through one local militia, KOMPAK-Solo, to JI and another local militia, Mujahidin KOMPAK. The workers were so concerned about the probity of these transfers that they appointed an auditor to oversee the funds.[11] Arguments betweens moderates and extremists over strategy frequently occur in organizations contemplating making peace with the government.[12]

RATIONAL CHOICE

Several academic studies have noted that such variations in motivation can cause difficulties for terrorist groups.[13] However, none have explored the challenges such heterogeneity pose for terrorist financial systems.[14] This chapter offers a rational choice perspective, using agency theory, for analyzing these issues. The rational choice approach is particularly attractive for dealing with this type of problem because it presents the strategic and organizational dilemmas faced by terrorist groups in the starkest possible contrast. Doing so can help explain otherwise puzzling patterns of behavior.[15]

Terrorist groups face two adverse selection problems. The first is that those likely to survive for long periods in terrorist networks tend to be less ideologically committed and less likely to volunteer for the most dangerous missions.[16] The second is that, because participation as a financier or logisti-

cian is less risky than participating as a local leader or operator, middlemen in terrorist organizations tend to be less committed.

These two dynamics create a moral hazard problem for leaders. For security reasons, leaders (principals) have to delegate fund-raising and financial duties to middlemen (agents).[17] However, the agents can take advantage of the information asymmetries in the network to expropriate some funds, to shirk. Because the environment is noisy and security concerns prevent perfect monitoring, principals are uncertain whether the agents are passing on all the resources they bring in or are keeping a cut for themselves, a classic moral hazard problem. Leaders can solve this problem by providing enough money to middlemen so that, after the logisticians take their cut, the optimal amount still makes it to the operators. However, doing so is inefficient. Alternatively, leaders can try to reduce inefficiency.

Of course, the real-world division of labor is not always so stark. The level of specialization can vary over time and between groups. Al Qaeda and its affiliates used to have quite defined organizational roles with a strong distinction between support and operational roles.[18] However, since losing their refuge in Afghanistan, al Qaeda and its affiliates may have shifted to a less-hierarchical system. In Madrid and Casablanca, for example, the same members appear to have engaged in logistical tasks and conducted operations.[19] Moreover, the level of specialization can be a strategic choice. Resource-poor groups must be efficient to survive, while wealthy organizations may not be concerned with inefficiency so long as they can meet their political goals.

There are at least four inefficiency-reducing solutions to this moral hazard problem. First, leaders can engage in monitoring or auditing of their middlemen. Second, leaders can provide incentive-based compensation, withholding payment for services until they have observed a signal—a successful attack, for example—telling them the agent has performed as promised. Third, leaders can engage in punishment strategies when they have evidence of shirking. Fourth, leaders can encourage members to enter into relationships that raise the costs of getting caught expropriating funds.

Unfortunately for terrorist leaders, each of those strategies creates vulnerabilities. The first two demand that the group conduct additional communications and keep records, both of which violate operational security concerns. The third strategy is risky because it entails additional communications and because the punished individual may decide to compromise the network.[20] The fourth strategy creates additional interconnections, making

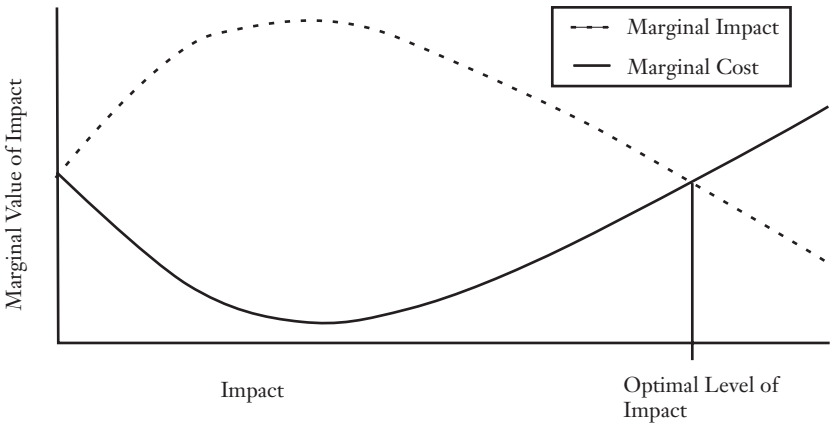

FIGURE 4.1. Value of Terrorist Attacks

the potential cost of any one compromise much greater. Thus, given the selection dynamics caused by government strategy, terrorists face an inherent trade-off between security and efficiency.

The Economic System of Terror

Decisions about spending are best understood in terms of the trade-off between achieving political impact and the fact that greater impact spurs greater government enforcement efforts. Figure 4.1 demonstrates this logic.[21] Leadership seeks a level of political impact where the marginal benefit of one more unit of impact matches the marginal cost in terms of government action.

Unlike in traditional economic organizations, this optimal point is not always determined by a spending constraint. Terrorist groups rely on five distinct sources of funding: (1) direct contributions from individuals; (2) intentional donations from charitable foundations; (3) state sponsorship; (4) profits from legitimate businesses—including tithing by the membership; and (5) profits from criminal enterprises—including skimming funds from legitimate organizations and extortion from individuals. Production decisions, choices about how many attacks to undertake or how much to spend

providing social services, influence the first three sources. In general, the more attacks or social services a group provides, the more funds it can raise from individuals, charities, or state sponsors.[22] However, the last two sources enable some groups to produce at this goal-optimal level even if their financial system is inefficient.[23]

Whatever impact the leader desires, the financial system has three basic tasks. First, it must generate resources through fund-raising, taxing criminal activities, fraud, or some other source. Second, the system must preserve these resources and protect them from seizure. Finally, it must distribute money to operational cells. There are opportunities for middlemen to appropriate resources at each step in this chain.

SELECTION DYNAMICS AND DIVERGENT PREFERENCES

One of the most striking patterns to emerge from a close examination of terrorist organizations is that financial network members face dramatically lower risks than local leaders and tactical operatives. Beyond not being asked to participate in risky or inherently fatal ventures, they are less likely to be targeted by government forces. When targeted, they are less likely to be killed; when arrested, they face more lenient treatment.

Using Sageman's sample of 366 participants in the "global Salafi jihad"—al Qaeda, affiliated groups, and some individuals operating outside of formal organizations—I assessed the risks of participating at different levels. Using open-source material, I collected data on individuals' operational roles, when they left the jihad, and how they left.[24] According to these data, between 1997 and 2003, financiers were rarely killed, and their chances of being arrested were 10–20 percent lower than that of tactical operators, with 2002 being the only exception.

Even when governments succeed in capturing logisticians and other support network members, the members face dramatically lesser consequences than operators. Of the 33 financiers and logisticians removed from the global Salafi jihad between January 2001 and December 2003, only 1 was killed. While roughly 40 percent of the captured local operational leaders in the sample received life in prison or a death sentence, only 8 percent of support personnel received such sentences. A particularly telling example is the Jemaah Islamiyah (JI) cell broken up in Singapore in late 2001. The cell provided fund-raising services to JI and was making logistical arrangements for

an al Qaeda attack in Singapore. Of the 30-plus people arrested, the 13 engaged in direct logistical support each received two years in prison. Those engaged in fund-raising activities were released but not permitted to leave the country.[25] This dramatic difference in risks leads to divergent preferences in terrorist organizations.

In our rationalist approach, individuals join terrorist organizations when the utility of doing so is at least as good as that provided by their next best option.[26] Utility is composed of two components. First, individuals get utility out of doing what they believe is right, in this case out of the impact of their actions in furthering the group's goals.[27] Second, individuals get utility out of monetary compensation. Each individual places a weight on these two components such that the sum of the weights is 1. The utility of an action is the probability it yields an impact, *I*, times the weight placed on impact plus the probability it yields wages, *W*, times the weight placed on wages.[28] We can then describe the population of potential members by the distribution of weights in the population. At the extremes are individuals who are purely motivated by impact, suicide bombers perhaps, and those motivated purely by money.

Within this framework, consider a hierarchical organization where individuals come up through the ranks, starting out in subordinate roles and moving into management roles as local leaders, financial facilitators, or logisticians.[29] Throughout their careers, these individuals will have opportunities to volunteer for risky missions.[30] Those most likely to do so will be those who place the greatest weight on impact. Thus, the longer individuals remain in the organization, and the further they move up in the management structure, the more likely they are to place a heavy weight on monetary rewards.[31] Of course, there is a countervailing dynamic. Assuming constant wages, those who are less committed will receive lower total utility from participating and will thus be more likely to quit the group.[32] Where the value of participating is only marginally greater than the value of the next best option, quitting should mitigate this particular adverse selection process.

Even without this adverse selection process, there is reason to expect divergence. The lenient treatment observed for support network members means that the threshold level of risk acceptance and commitment required for participation in support activities is much lower than for participation in tactical roles. Recall that there is a distribution of weights in the population of potential members. Thus, given set wages for different activities, individuals placing a certain weight on economic considerations might participate

in support activities while balking at other roles within the organization. Seeking to maximize operational capability, a rational organization would concentrate such individuals in support roles, freeing up the true believers for riskier operational duties. These personnel decisions would then lead to consistent variance between levels of the organization.

A reasonable objection to the preceding logic is that groups would not engage in such centrally directed personnel movements because they create connections between cells. Because of this security consideration, terrorist organizations may actually recruit directly into specific positions with little opportunity for movement. Suppose that the organization in question filled these roles using a strategy of recruitment through existing social ties.[33] Any member tasked with the recruitment and early ideological training of potential members will have access to a limited population. From this population, they will need to fill various spots. If we make the reasonable assumption that belief in a group's ideology follows a bell-shaped distribution—the purely ideological or purely venal types are rarer than those who place moderate weight on both pecuniary rewards and impact—it will be harder for the recruiter to find potential tactical operatives than logisticians. Unless the recruiter knows a surfeit of potential members, he will place individuals in the riskiest position they will accept. Thus, individuals will rarely be more ideologically motivated than is necessary given the risk level of their occupation, leading to variance across levels.

A second, more significant, objection to the above logic is that if middlemen have scarce skills, their next best option will be much more valuable. Thus, their involvement in terrorism may actually suggest they are *more* committed than the foot soldiers who have no other employment options.[34]

Two responses are worth noting here. The first is that the modal profile of an operational terrorist is someone with better prospects than the average person in his society.[35] Moreover, that skills are rare among potential terrorist recruits does not necessarily imply that they are equally rare in the population, and it is the value of skills to the organization that drives the logic above. The second response is that the evidence from some conflicts is that middlemen do quite well. Middlemen in the PLO are paid relatively well compared to those who fight, and many middlemen in the Kashmiri jihad live relatively ostentatious lifestyles.[36] If these individuals were, in fact, more committed than those who fight and die, one would expect them to reject such large payments out of devotion to the cause.

Different levels of risk faced by those filling different roles will translate into different preferences within groups under three different sets of assumptions about how terrorist organizations make staffing decisions. This diversity of preferences, combined with the covert nature of terrorist organizations, creates a problem for terrorist leaders.

MORAL HAZARD IN COVERT ORGANIZATIONS

The relationship between terrorist leaders and their financial networks can be understood in terms of a principal-agent relationship wherein the principals, i.e., terrorist leaders, need to delegate certain tasks—raising funds and distributing them to operational elements—to their agents, the financial network. This delegation entails a risk. If the agents' preferences differ from those of the principal, the agents will not carry out their tasks exactly as the principal would like; they may "shirk." The moral hazard is that the agent can undertake actions that reduce the principal's utility, but the principal can neither perfectly monitor nor punish the agent with certainty.[37]

Traditional organizations use three general strategies to deal with this type of problem. First, they audit their employees, accepting monitoring costs to prevent shirking. Second, they create wage schemes that are attractive only to agents whose preferences are aligned with those of the principals. Third, they provide incentive pay or salary conditional on performance. There are many possible screening mechanisms and incentive-based contracts, but all involve making full payment conditional on not deviating too far from the principals' desires.

Both principals and agents hold five pieces of information. Principals know the amount passed to leaders through fund-raising activities, and each agent knows how much she has passed on. Likewise, principals know the amount given to financial network members to pass on to operational elements while each agent only knows how much she was given. Both principals and agents are able to observe the operational impact of their actions. They also share common beliefs about the amount of impact they can achieve given spending levels and the likelihood of achieving that amount.[38] Finally, both are able to observe how risky it is to fulfill certain roles.

There are three critical pieces of information known only to the agents, information that can be considered their "private information." Only they know the percentage of funds raised that is actually passed up to the leader-

ship. Similarly, only they know the amount passed down to the operational elements.[39] Finally, only the agents know how much weight they place on impact. Impact dominates the leader's decisions, but he is not so myopic as to spend an infinite amount to achieve his ideal level of impact.

Given who knows what, there are three ways financial network members can take advantage of their private information. First, they can misrepresent their preferences over money and impact to pad their salary. Essentially, they can mislead the principal into thinking that he has to offer more compensation than he actually does. This problem will be ameliorated to the extent that there is a market for terrorist financial services.[40]

Second, the agent can appropriate some of the money from fund-raising activities. Because the environment is noisy and the network is covert, the principal will be poorly informed about the actual amount raised. Depending on the principal's beliefs about how accurately he can anticipate fund-raising levels, the agent will be able to get away with appropriating some amount without arousing suspicion. How large an amount will depend on the accuracy of the principal's beliefs, which depends in turn on where the funds are coming from. When money from legitimate enterprises is passed through the group to operational cells, the process can be relatively overt. Because the organization is putting good money to ambiguous purposes—at least until the cell commits an attack—the transactions are essentially indistinguishable from legitimate transfers.[41] As such, the principal will be better informed about the likely success of fund-raising efforts, and the agent will not be able to appropriate as large a percentage. However, when the organization is using money from illicit purposes to fund operations, some kind of laundering will be needed to prevent investigators who are tracking the original crime from finding out about impending operations. This is a riskier proposition, involving more financial machinations and a greater need for secrecy. Hence, the principal will be less well-informed about his returns from fund-raising. As such, the financiers will be able to appropriate a larger percentage without arousing suspicion.[42]

Third, the agent can appropriate money intended for operational cells. Whether these appropriations lead to underfunding of specific operations depends on the nature of the command and control structure.[43] Consider the case where the leaders decide how many attacks to carry out and allocate funds to each attack based on their beliefs about how to equate the marginal returns to impact with marginal costs.[44] Because the principal's ability to

observe the impact to cost relationship is imperfect, members of the financial network can skim some of the money intended for operations and blame the reduction in observed impact on the noisy environment.

If opportunities for shirking exist in terrorist organizations, the next question is to ask whether financial agents will take advantage of these opportunities. Consider the case of an agent who is participating because her utility from wages and impact are better than her next best option. This agent knows she can appropriate some funds and get away with it, thereby increasing her utility.[45] Now, consider the leader. He has some optimal level of impact that we assume to be below the maximum he could achieve if he spent all his funds.[46] He is uncertain whether he is dealing with a good agent who will pass everything on or a bad one who will appropriate as much as she can get away with. Since the leader's utility function is heavily weighted towards impact, and since he can spend above the point of diminishing marginal returns, he is willing to provide some extra wages to the agent. He knows the agent will appropriate these funds, but he takes the efficiency loss because the agent will then pass the ideal amount on to the operational group. Thus, the leader should pay what he needs to for his optimal impact plus the minimum amount that can be appropriated without his becoming suspicious. The agent then appropriates this amount and passes the optimal amount of funds on to the operators. The leader remains unable to tell whether he is dealing with a good or a bad agent and the system moves on. In a more formal presentation, this would be the "shirking" equilibrium.[47]

In the terrorist leader's ideal world, where the agents share the leader's preferences exactly, all the money raised would be passed to the organization and all the money intended for operations would be used as desired. However, selection dynamics mean there is likely to be a difference between the weights placed on impact and wages at different levels of the organization. This difference can lead the agents in the financial network to shirk by appropriating some funds for personal use, introducing inefficiency into the financial system. A security trade-off arises from each strategy leaders use to deal with these problems.

CREATING VULNERABILITIES

Terrorist leaders can undertake a number of strategies to minimize inefficiency due to shirking. However, each of these strategies creates specific vulnerabilities. This section looks briefly at six of those strategies and dis-

cusses the security-efficiency trade-off in more detail. The first two strategies, auditing and providing funds on a need-to-have basis, apply primarily to the process of moving money to operators. The remaining four strategies apply more generally.

Auditing strategies, such as those apparently employed by Ayman al Zawahiri, require the agents to provide periodic, detailed reports on their spending. Such reports provide the leadership with more detailed information about how their money is being spent. This additional information effectively reduces the noisiness of the environment, narrowing the scope of cheating available to the agent. But this additional efficiency comes at the cost of additional communications. Because each communication entails a specific risk of compromise, these strategies effectively raise the marginal cost curve, reducing the total impact a group will desire. Thus, we should not expect groups who have a surplus of funds to employ such strategies.[48]

Providing funds only on a need-to-have basis is another way in which principals can inhibit cheating by their agents. By increasing the frequency of transfers and reducing their size, leaders build up better knowledge about the nature of the spending-impact relationship.[49] This reduces the size of appropriations the agents can get away with. However, because each additional transfer entails communications, the previous security trade-off applies and, again, leaders who have a surplus of funds are unlikely to employ this strategy.

Punishment strategies depend on the principal's ability to catch and credibly punish shirking. Getting the information needed to increase the probability of catching shirking has a clear security cost, so the focus here is on the second requirement, credible punishment. Punishment can be as simple as excluding the agent from future transactions. The agent then loses the difference between the future value of participation and that of her second-best option. Where economic opportunity is low, this difference could be quite substantial, so such a strategy may be sufficient. Because such a strategy is built into the shirking equilibrium, the principal may want to use the threat of additional violent punishment, a punitive strategy.

A punitive strategy is harder to implement because the agent in a covert system holds an inherent threat over the organization. If she is sufficiently incensed by her punishment, she can go to the authorities. For example, Jamal Ahmed Al Fadl, who testified in the African Embassy bombing trial, stole money from al Qaeda, got caught, went on the run, and approached the U.S. government in an attempt to save himself and his family. Because agents have exactly this option, the organization should employ punitive strategies

only when it can wield a credible threat of violence over the agent. Financial agents operating in foreign countries, such as the Yemeni recipient of al Zawahiri's e-mail, will be less susceptible to this strategy. That agent responded to being called out by quitting the network, illustrating the difficulties transnational groups face in using punishment strategies.[50]

One common way to discourage shirking is to encourage members to enter into trust-inducing relationships such as marriage.[51] The logic is that those who have entered into such relationships will face a larger cost if they are caught cheating. Not only do they lose a future income stream, but they lose familial and community connections as well. For example, such a strategy is central to the success of the *hawala* funds transfer system.[52] Of course, if a member embedded in a dense network of strong ties is captured, myriad opportunities for compromise are created. Historically, governments have only worked aggressively through terrorists' non-operational relationships, targeting terrorists' friends and family, when the impact of a terrorist campaign is very large.[53] Thus, this strategy raises the slope of the marginal cost curve only at high levels of impact, where further attacks will trigger very aggressive government action. Think of this as bending the right side of the cost curve upwards. This is what happened to al Qaeda's cost curve following the September 11 attacks. If the optimal level of political impact is low—that is, if the curves cross where the marginal cost curve is not steep—then such a strategy will not reduce the acceptable impact, as it only affects the cost curve above the level of impact the terrorists seek.

However, when the cost curves intersect at higher levels of impact, the results are more conditional. In the first case, suppose that the curves intersect at high levels of impact when the slope of the cost curve is already quite steep. This would be the case where government enforcement is quite stringent but the political benefits to more attacks are still substantial. Here, requiring dense ties will not shift the equilibrium very much to the left since the cost curve is already steep. In the second case, suppose that the marginal political gains to attacks are rapidly decreasing. This could be because the group's supporters have gotten fed up with violence, or because the target population becomes inured to it.[54] In this situation, the cost curve has a small slope at high impact, and increasing that slope can shift the intersection dramatically to the left. This would yield a substantial decrease in the equilibrium level of impact. Only under this last condition would we not expect the strategy of trust-inducing relationships to be used.[55]

Incentive-based contracts offer another way for principals to reduce shirking. In the terrorism context, such an agreement could entail several different arrangements. One is that payments might be made only after successful attacks or other impact-producing activities.[56] Another strategy might entail allowing financiers a set wage once they raise a specific amount. This wage has to be greater than the expected utility of appropriations given the amount raised. Because the appropriation entails some risk of being caught, the incentive can be less than the amount the agent could appropriate. Thus, principals should prefer this strategy to overpaying to account for shirking. While these strategies do entail additional communications, they require fewer than the first two strategies. Thus, incentive-based contracts raise the cost curve less, and principals should employ them more often.

Finally, terrorist leaders may seek to screen their recruits for ideological purity, to ensure that they all place a very high weight on impact. Some accounts suggest that the training program in Afghanistan served as such a screening process for al Qaeda.[57] The lengthy ideological debates that form an essential part of the recruiting process in European Islamic expatriate communities also fulfill such a function. While this strategy does not generate additional risks, it does reduce the pool of potential participants. For groups recruiting from a limited recruiting population, this may be problematic. The best financiers are unlikely to be religious or ideological purists, as such individuals rarely spend time developing expertise in money laundering and covertly moving funds. This strategy, therefore, entails an efficiency loss. This loss may drop the feasible level of impact below that which could be achieved with less impact-driven agents.

Of the six strategies outlined above, all entail some cost for the groups. In five of the six, there was a specific security-efficiency trade-off. Only demanding ideological purity did not have a clear security cost. However, in the realm of terrorist financing the necessary expertise may not be available from highly ideological individuals.

Conclusion and Recommendations

In a principal-agent framework, leaders are considered the principals who delegate three stages of financial activity to their agents. These agents raise funds, store them for future use, and transfer them to operational elements.

Two selection processes cause those agents to have divergent preferences from the principals. First, terrorist organizations face an inherent adverse selection problem because those individuals who are less committed are likely to survive longer and rise into the mid-level positions. Second, because terrorist financiers face significantly lower risks than other members of their organizations, recruiting efforts will place more risk-averse, less committed individuals into financial roles.

Because of the information asymmetries inherent in covert networks, these individuals have opportunities to "shirk" by skimming money at all three stages. So long as terrorist financiers face lower risks than other members of terrorist organizations, these groups will suffer from a moral hazard problem. "Shirking" by the agents creates inefficiency in the financial system. Like any organization, terrorist groups can use a variety of strategies to control the moral hazard problem. But all these strategies come at a cost. In five of the six strategies examined, there was a specific security-efficiency trade-off. Strategies that reduce the moral hazard problem create operational vulnerabilities.

Terrorist leaders thus face an unpalatable choice. Where funding constraints do not bite, terrorists can make the trade-off in favor of security. Where funding constraints do bite, government can undertake some specific actions to make this trade-off even more problematic.[58]

This analysis leads to three distinct recommendations. First, governments should not publicize the freezing of funds. If funds are frozen without public statement, then financiers must explain how the money was lost. The organization will then achieve a lower impact. Seeing this, the principal will suspect the agent of shirking. If the freezing is made public, the agent has an excuse. If it is not, she has two choices: she can make up the frozen amount, or she can get blamed and forego the future value of her relationship with the organization.

Second, governments can make engaging in trust-inducing relationships riskier. Publicly targeting relatives and extended families for surveillance would increase terrorists' assessment of the probability that such relationships would lead to compromise. Government can achieve the same end by publicizing counter-terrorism successes based on tracing such relationships.

Third, government may actually reduce tensions within terrorist organizations by engaging in economic development activities. Greater development in recruiting areas effectively increases the value of an individual's second-best option. Thus, the wages terrorist principals need to pay to induce

participation in terrorism will be higher. While this may make recruiting more difficult, the moral hazard problem becomes less problematic from the principals' perspective. Because the difference between the wage they must pay and the feasible appropriations—which depend only on the noisiness of the environment and the desired number of attacks—is smaller, the relative value of the inefficiency is reduced. Under this scenario, the group is less likely to engage in the inefficiency-reducing strategies that create vulnerabilities, making government's job more difficult.

Consider the following thought experiment. Suppose that for political reasons a leader wants to have two successful attacks. Given the success probabilities and economies of conducting an attack, the leader chooses to fund three attempts with $90 and pay someone $10 to serve as a middleman. To avoid detection as a shirker, the middleman must allocate $70 to the attacks, leaving a feasible appropriation of $20. Thus the boss pays $100 and gets $70 worth of attacks. Now suppose there is some economic development and the middleman's outside option increases in value to $20, but the boss still pays $100. The middleman must still devote $70 to attacks, so he captures only $10 in rents. Before development, the bad agent captured 20 percent of the expenditures in rents. After development, he is only able to capture 10 percent. Thus, the difference between a good and bad agent is smaller, and inefficiency is reduced. With this reduction, the leader has less incentive to engage in inefficiency-reducing behaviors. Whether this trade-off—difficulty recruiting but fewer security violations—is favorable to a government will depend on local conditions.

Each of these strategies impinges on other areas of counter-terrorism and cuts in several directions. For example, publicizing methods and causes of compromise may prevent terrorists from dealing with inefficiencies in their financial system, but it may also aid terrorists' efforts to improve operational security. This dilemma and others discussed above apply only when funds are restricted.

Based on this framework, clamping down on finances can have a host of benefits. So long as groups have excess funds, they do not need to face the trade-offs outlined above. However, when funding becomes scarce, terrorist leaders face a security-efficiency trade-off. Choosing efficiency-enhancing strategies creates vulnerabilities that governments can exploit. Choosing security means fewer operations and therefore less impact. In either case, government wins when funds are restricted.