**UCLA Working Paper:**

**Terrorism and International Business: The Case of Banking**

October, 2009

Robert Grosse

Standard Bank of South Africa

[Robert.grosse@standardbank.co.za](mailto:Robert.grosse@standardbank.co.za)

Robert Spich

Anderson Graduate School of Management

UCLA

**Abstract**

This paper raises security issues to a strategic, rather than an operational level in international business. Banks (and other firms) need to deal with the issue of terrorist risk as a strategic concern, rather than as a simple cost in an operational context. We have identified and examined four general (universal) security risks facing banks, and presented empirical evidence from several countries to show the dimensions of the risks and a structured method for exploring and dealing with these risks. The specific cases of the 9/11 terrorist attack in New York, ATM bombings in South Africa, kidnapping of bank employees in Colombia, and laundering of terrorist money in the US are examined. We offer a security exposure classification system, to assist the strategic decision makers to make better sense of the security challenge they are facing, with a specific analytical model, the CRR model, to assess and compare relative terrorist events outcomes in banking.

**Section 1- Introduction**

**The terrorist and the target**

Terrorists are people with motives, missions and goals. They may be single individuals or they may be organized networks. Why they choose to “get their way in the world” by means of terror is a complex story and not easily subject to rational analysis. But once they do engage in acts of terrorism, identify and act on a target, they essentially enter into a complex game with their targets that is not intended to have a win-win outcome.

In contrast, the targets are usually organizations. Organizations are rationally structured relationships between people whose purpose is goal attainment, growth and sustainability. Of course, organizations are people too. Because they are gathering places for people, organizations are preferred targets. The payoff to a terrorist act holds more promise when the terror effects can be leveraged through organization structures, physical locations and networked communications processes.[[1]](#endnote-1) Once organizations are targets of a terrorist act, they too enter, voluntarily or otherwise, into a gaming relationship with terrorist.

The game is simple in theory: one group wants to damage, dislocate, disrupt and destroy; the other group defends, denies access and protects itself against danger. In practice, terrorism and anti-terrorism become an increasingly complex and costly challenge for both the perpetrator and the victim. Because of this, the management of security and risk has become a central concern for top management.[[2]](#endnote-2)

This paper then is about terrorism and its impacts on global organizations, specifically commercial and investment banks. Its main purpose is to articulate the terrorist challenge for banking, and to offer an analytic approach for banks to identify, assess and respond to terrorist threats, both active and passive. We begin with some observations about organizational vulnerability and the terror gambit. We then analyze the particular vulnerabilities of banks and the central role they play in the global economic system. The paper presents four cases of banking experience with terror and security management in several countries to show the complexities involved in security management. Using a specific framework, the CRR© model, the paper analyzes and assesses the cost, risk and revenue dimensions of the bank security challenge. The paper ends by presenting an analytic framework for classification of strategic security challenges in the banking industry.

**Organization vulnerability and the terror gambit**

The terror gambit has two interesting characteristics as a choice of strategy: It can be applied to any and every organization at least once; its utility has a severely decreasing marginal utility! Every industry can be a target for terror at least once because terrorism generally is not an expected event and the element of surprise has its highest value when there is little preparation in place to anticipate or defend against it. Thus, the first terrorist act can often succeed, almost spectacularly, as was the case in the 9/11 attack on New York. This vulnerability is especially true for organizations which are open to the public such as movie theatres, theme parks, transport stations, libraries, malls, universities, public buildings and of course, banks. By nature these places are ready-made and relatively easy targets because they are places of meeting and movements. They all require a high degree of openness (low barriers to entry, weak borders) because the maintenance of flow, access, interface and transactions are central to their purposes and function. Organizations of this type tend to be, by nature, fully open systems and follow all the “rules’ that systems theory indicates are necessary to function effectively. (Spich and Grosse, p. 461, 2005)

However, once a terrorist event occurs in any one of these sites, the defensive and proactive responses are usually immediate and strong. The introduction of screening devices, the identification of potential threats and targeted activities, profiling of potential suspects and introduction of membership fees and requirements serve to both increase the cost of entrance and provide barriers to entry and frictions to easy terror actions. The desired effect is to make the next terrorist act harder to achieve. [[3]](#endnote-3) Thus the ability to use that same tactic a second time with the same effectiveness dissipates quickly (e.g. has a steep curve of decreasing marginal utility), as the cost to overcome newly raised defenses of the target organization gets increasingly high (eg. screening at airports). In addition, this defensive reflex also has a network effect. Once a terror event enters into the collective consciousness of an industry, network effects (common communications, sharing, cooperation) take over to increase the awareness and relative vulnerability of others who then can take anticipatory proactive initiatives (eg invest in technology, join cooperative antiterrorist ventures) against potential terror attacks. Thus the overall vulnerability of an industry or a cluster of industries can collectively decrease as a result of the first attack. This in turn raises the stakes for the terrorist if he/she wants to continue in this game of terror.[[4]](#endnote-4)

This second feature of decreasing marginal utility is reflected in the old maxim that says, ”Fool me once, shame on you! Fool me twice, shame on me!” Few are the organizations fooled by the terrorist more than once. If they are, Darwinian selection processes usually intervene to decide their fate!

**The case of banks**

If we apply the above thinking to banks, we see that the challenge to banking to protect themselves and others from the intentions and effects of terrorist groups is a staggering task, perhaps more difficult than any other industry because of the nature of the finance function. If you add the dimension of globality to their activities the complexity of the management task is multiplied

In any market system, the free and constant flow of funds is fundamental to the success of that market, growth and development. Without this flow, structured and delivered in the form of services such as payments, deposits, credits, swaps, collateral, hedges, and insurance, the ability to engage in transactions and exchanges, and the ultimate creation of wealth, is severely bounded. . As one astute observer wrote recently during the financial collapse of investment banking in the US in 2008, “Finance is the web of intermediation binding economic agents to one another across space and time. Without it, no modern economy can survive.”[[5]](#endnote-5)

The critical role of the finance function is readily seen in the ongoing global financial crisis of 2008. In this case, the banking credit system has essentially frozen because of a compromised trust caused by an obfuscating complexity in transactions instruments (particularly derivatives), excessive risk taking and an absence of strong accountability practices. The U.S. government bailout is essentially a blood bank operation infusing liquidity into the rapidly drying and clogging global financial markets. [[6]](#endnote-6)

Global banking, as an industry, thus requires regular stable and protected flows of international funds to support international transactions of all kinds. Banks are called on now to provide access to it services for all customers on a 7/24 basis (eg ATM cash services in multiple currencies), to serve as a central interface for all financial exchanges (eg foreign exchange markets), to provide expertise and special services for global customers and to make money for their stockholders on all of these transactions. The more transactions that occur, the more opportunities there are to offer services and products to a wider variety of customers. This in turn leads to growth and additional possibilities for profit. But as international opportunities increase, so do business risks and threats to security. This growth/risk conundrum is a strategic challenge for all companies that globalize their business. For these reasons, security and risk in the banking industry is increasingly a strategic issue with large scale implications.

**Banks and security risk**

Given their functional importance and central role in facilitating transactions, banks’ positions in business networks would seem to be particularly vulnerable to disruption and damage because of the very nature of the business. Banks depend on extensive networks of correspondent and other cooperative relationships with other banks and financial institutions in order to keep the flows of funds in movement. At the same time there is a need for a constant free flow of current data and information between these network players for decision making. The present global reach of banking has presented dangers of overextension and increased exposure to risk not experienced in local business environments. Secondly, though required to be discreet and secretive in their handling of financial transactions, banks, at the same time, are open to doing business with all kinds of clients, legitimate, legal, moral and otherwise. This exposes them to two problems: the potential increased scrutiny of local authorities seeking law breakers and illegal funds flows; and increased regulation to forestall security breaches and dis-incentivize transactions with identified security risk organizations.[[7]](#endnote-7)

Thirdly, because banks are in the business of making “money with money”, they do not prefer to discriminate against the sources of monies even though this might open them up to actions from the government or the courts. Guilt by association with, and/or by serving terrorist organizations, remains a possible hazard in this business. Further complications come with being open to business with clients who could be either target companies or terrorists, all under the same roof!

Lastly, in facilitating transactions, a bank’s location in the center of a web of transactions (e.g. financing a complex M&A deal) makes them a more attractive single target for terror that seeks to disrupt and make these transactions and exchanges more risky and costly. A recent car bomb in the Basque region was exploded next to a regional bank’s headquarters in Vitoria. (LAT 9-22-08 pA6 ) “Taking out” the center of a network out of operations disrupts whole systems. That in part was the hope of Al Qa’ida in its attack on New York City. Their belief was that the Twin Towers were the heart and brains of the global financial system. The fact that this did not happen, even with all of the direct and collateral damage to the financial system, leaves us to speculate about the real vulnerability of global banking to terrorist actions. Possible reasons for this lie in the fundamental transaction and conduit role that banks play in the global economy. In this case the financing of activities, the transfer of monies, the payment of bills, the provision of investment and savings facilities of banks actually serve the interests of everyone, both terrorists and their targets. All parties have an interest in banking systems that function effectively.

**Section 2 -- The Nature of the Business Security Challenge**

To talk about the challenge of business security, we need to clarify how a business works with respect to security and risk, and to understand how terrorists seek to achieve their goals.

**Some assumptions about the firm as target**

There are four elements that make the firm sensitive to the issues of risk and security.

1) Capitalist business firms work and thrive in open market places. They are opportunity-seeking entities, sanctioned by society, and are driven largely by private motives for gain. Opportunity is the purposeful pursuit of risk for some expected gains. At the same time that firms seek opportunity for gain, they have an aversion to losses. However, because they work in open markets, firms must take the risk of free association with business partners, for better or for worse. But since they cannot know the future outcome of transactions with any business partner fully, they engage in multiple transactions with a range of risks with calculated losses and gains so as to balance their portfolio of transactions ending hopefully with a positive final balance. Since terrorist organizations are free to work these same markets, there is the additional risk of doing business which has potential political and societal implications. These in turn can lead to direct and indirect costs to doing business. So while firms have a natural sensitivity to economic risks of the marketplace, they now must include security risks, both direct and indirect, into their risk calculations.

2) Businesses constantly monitor environments for both opportunities and threats. They do not exist in a vacuum. Environments represent a complex and dynamic set of situations, conditions, institutions and contexts that help shape the strategy and tactics of the business firm. In order to take advantage of opportunity or deal with a threat, firms must develop a business intelligence and forecasting function that constantly scans the environment for changes in conditions. This suggests that the successful firm practice “intelligent vigilance”: it develops capabilities, technologies and relationships for better intelligence about markets, competitors, public policy and now security. They are not, therefore, easy targets.

3) Businesses are goal-seeking entities that seek to optimize the use of resources to achieve important goals over defined time periods. The general management mandate is to create a business that is stable and seeks goals of growth, productivity and performance. In contemporary times these goals now include firm sustainability, security and longevity. Because resources are limited for most firms, management takes different time/action perspectives and decisions to maximize and minimize resource use within different time frames (short term, midterm and long term). This creates a tension within the various firm stakeholders who may have different time horizons and expectation for economic results and profit outcomes. With these tensions, the firm may then alter its risk security profile and engage in more risky ventures which expose them to the inevitable tradeoff decision of risk versus return. This can create a vulnerability, because it opens opportunities for outsiders to enter the system. This is in part what has contributed to the recent failure of several Wall Street firms.

4) Managers are rational actors. They seek to maximize gains, minimize losses and optimize holistically. Since reality challenges ideals, managers tend also to be pragmatic, realistic and practical in their decisions. Management seeks a balance between change and steady states (dynamism versus stasis). Firms actively seek opportunity in order to grow. They understand the role of innovation and creativity in competitive markets. Change, especially growth-induced change, always involves some risk because the future is unknown. Therefore management seeks to constantly “predict and prepare for the future”. It does this in a number of ways: by creating an intelligence capability that scans the environment for opportunities and threats; by identifying the parameters of uncertainty in a risk situation; by establishing sensible risk/reward relationships; by getting good estimates of probability (a range of possible future events and their probability of occurrence); by having plans, options, resources and skills to respond to both opportunity and threat. Therefore as rational actors, managers can be expected to respond to terrorism in a more calculated manner which is less emotional and strongly practical.

The above four assumptions of a market based system then suggest that firms, as private and self motivated entities will not make necessarily make for easy targets. Their resiliency is a proven fact and their ability to undertake proactive business system defense is known. (Yossi Sheffi 2007)

**Some assumptions about terror and terrorism**

To balance out the adversary assumptions between target and terrorist, we now look at some assumptions about terror and the agents who use terror to achieve goals.

1. Terror is an outcome and not a cause. It is an induced state in a target audience. Its purpose is to “disrupt, damage, dismantle or destroy” (Spich and Grosse, 2006, p. 468) an individual’s and/or an organization’s ability to function normally. The state of terror is a stimulated emotional state where the targeted person begins to think, feel and act abnormally and with a high degree of emotionality. Fears and concerns (real and imagined) tend to take the upper hand in behavior, and the outcomes of decisions may begin to appear irrational, counter productive and self-defeating. The objective is to wear down the target’s ability to resist and force the target to change its own strategies and course of action. An apocalyptic finale may not be the real final purpose of a terror strategy, and terror is not necessarily violent or extreme. The degree of violence and extreme tactics will vary as in all strategic and tactical decisions. Like in past conquests, the focus may not be to destroy but rather to gain control at a minimal cost.[[8]](#endnote-8)
2. Terrorists are rational enemies. They are quite like managers in that they are goal seeking, have purpose and strategies, create organization, seek to be successful and perform well. Terrorists must “manage” scarce resources and their application in terror tactics. The better managed they are, the more likely the terrorists will be successful. The view of terrorists as irrational, unintelligent, random and subject to uncontrollable emotions (i.e., to be totally unpredictable) is both inaccurate and risky. (Simon 2001)
3. Terrorism and anti-terrorism are engaged in a strategic game. The game can be large as in a war for control or small as in an act of personal vengeance. Games can be well structured with rules for combatants, arenas for games, scores, referees and a definition of winning. Or they can be quite unstructured and full of uncertainty, have changing “rules” that may be random, free from moral constraints and have a definition of winning that has no parameters! In either case, there is gaming going on, the seeking of advantage for self. To gain advantage therefore, the terrorist has choices of weapons technology, location and type of engagement, timing, degree of force used, stealth, deception and target vulnerability. This makes the terror game a difficult one to both play and win!
4. Terrorists choose terror as a strategy when others means of effecting change are not available, unknown, not seen as valid or relevant, and/or are not understood. Thus diplomacy may be shunned in favor of violence because it may achieve a tactical gain and has less risk to the terrorist.
5. The terrorist may be a single individual acting on their own or they may be a formal organization. The former case is seen in the recent anthrax case where a trusted scientist, Bruce Ivins, used his position to induce terror in government offices for particular gains. (<http://www.fbi.gov/anthrax/amerithraxlinks.htm>) We consider individual terrorists as less common events. In the latter case, we see the long term case of the New York mafia and now Mexican drug lords using terror as an organizational tactic. Governments themselves may be deemed as terrorist states, as in the case where the U.S. has declared Iran as a terrorist state, or where the U.S. itself is subject to the same charge in its extralegal activities in its Guantanamo Bay war prison. Organization-based terror has more momentum and is of a continuing and self- supporting nature.[[9]](#endnote-9)

There are a number of more complex issues regarding terrorism and its effects on business strategies and operations that are more completely handled in other sources. (Alexander 2004; Yossi Sheffi 2005; Ganor 2005). Our purpose is to highlight some key aspects of both a target business system and terror organizations so that we can begin to understand the choices that banks have in developing their business security strategies.

**The business of business security**

Business security can be defined as “a defensive strategy and state of organizational readiness to assure and protect (but not guarantee) the functional integrity of the organization’s operational systems against purposeful, willful and intentional attempts by agents (inside or outside) to disrupt, damage, dismantle or destroy them” (Spich and Grosse, 2006, p. 468).

A security strategy seeks to weaken or neutralize an enemy’s ability to reduce an organization’s defensive capabilities and responsiveness to terror. The focus of a security strategy is to maintain the functional integrity of an organization’s key people, information, assets and organization while experiencing a “terror attack”. Thus the business firm seeks to show the terrorist that it has strong capabilities to respond effectively to terror threats. Under the rubric of business continuity, management seeks to reduce and control uncertainties about its commitments and willingness to maintain its operations or to use it resources and competencies effectively to continue functioning effectively in a marketplace. This definition makes no assumptions about the source, identity, purpose or effectiveness of a security threat. While external threats are the more common ones, given the increased complexity and vulnerability of open systems that most businesses work in, internal threats (intentional or accidental) can be just as serious. Lastly, a business security strategy assumes that threats are ubiquitous, unpredictable (but assessable) and constant and that it is the job of management to prepare the organization for this challenge. A result of this heightened sensitivity to security issues is that business security issues are now raised to a strategic level of concern and not just an operations issue.

**The Nature of Protection: managing the positives and negatives.**

Security strategies have two foci: to increase the defensive capability of the organization and its ability to respond, or, to reduce the enemy’s effectiveness and will to engage in terror. The strategic purpose is to increase the positives and reduce the negatives of security for self while doing the opposite for the enemy. The enemy of course is following a similar strategy. These two aspects are closely linked in a zero-sum type game: my gain is your loss. Thus one central aspect of a business security strategy is to “make life difficult for the enemy” by increasing the negatives or reducing the positives of a terrorist’s strategy. We tend to feel more protected therefore when we can increase the costs of a terror operation, increase the required effort and complexity to be effective, increase the probability of failure, increase the negative lagged and side effects (collateral damage), increase the pain, insecurity and exposure of the terrorist, and increase the illusion of invulnerability of the target. At the same time we simultaneously pursue strategies to reduce the payoff (positives) for the risk taken by the terrorist.

One difference in this contest with terrorists though is that there are often unequal valuations of the payoffs and risks taken. This unequal valuation occurs because either the terrorist ignores or distorts the valuation of actual risk (sees it as low cost) or because “losing” is actually seen as a positive gain. That is the case of the Muslim martyr bombers who destroy themselves, an ultimate sacrifice to a Western person, because of the supposed gains in a promised life hereafter or real gains of payments to their families in exchange for martyrdom. All of these tactics have the same effect: they increase the challenge for the “terrorist manager” to be effective and achieve his terror goals.

**Section 3 -- Four Cases of Terrorist Risk in Banking**

In the follow subsections we review four kinds of terrorist incidents for their impact specifically on the banking sector. We begin with the “mother of all attacks”, the 9/11 attack on New York.

**The 9/11 Attacks**

International terrorism appeared to have an enormous effect on the banking industry as a result of the 9/11 attacks. Many major US commercial and investment banks were visibly hit by the attack on the World Trade Center, as shown in television and newspaper accounts, and they lost personnel as well as property. What exactly were the ultimate effects on these firms? First of all, there was the destruction of close to $US 20 billion of property and killing of 2,800 people[[10]](#endnote-10). Then there was the fact that banks had to move some of their business activities to alternative locations, uptown in Manhattan, into New Jersey, and further afield. The destruction and loss of life were extensive and heartbreaking.[[11]](#endnote-11) The chaotic conditions in the Wall Street area lasted for weeks, as damage was assessed and rubble was removed. The clean-up and reconstruction of the site took well more than a year[[12]](#endnote-12).

As far as losses of money or losses of information in the banking system are concerned, no major problems were uncovered after the event. Assuming that the banks had protected their physical facilities with property insurance, they did not suffer major losses on that score (though of course the insurance companies did[[13]](#endnote-13).) Financial records appear to have been preserved in all cases, though undoubtedly there were some non-trivial costs of operating through alternative facilities and utilizing back-up data systems. In the end, however, the cost in terms of lost financial information was very small.

If we consider the impact of 9/11 on the banks, it was far more damaging in terms of lost business, due to the economic downturn in the United States that followed the attacks. The stock market dropped from 11,000 to 8,000 in the month after the attacks, and to 7,200 by one year later. The US economy grew at a -1.4% annual rate in the third quarter of 2001, following growth of 1.0% in the twelve months before that[[14]](#endnote-14). The overall economy’s growth was already slowed by the dot-com crisis that hit toward the end of 2000, so it is difficult to separate out the 9/11 impact on growth. Nevertheless, it is clear that the economy slowed immediately after the attacks, and that therefore banks found their business activity reduced and their profitability affected.

What can be concluded about banks and terrorism from this, the most serious terrorist attack on the United States in the history of the country? Clearly, the impact on banks was not greater than on other sectors of the economy, despite the fact that the attack was aimed at the financial heart of the country. Clearly, the banks were affected by the attacks, most importantly due to the downturn in business overall due to the business slowdown in the US.

What could banks do to deal with this terrorist event and future threats of this kind? Probably very little, in a direct manner, since the impact on their physical facilities and people was relatively small and, in the case of the facilities, fairly easy to repair or replace. On the facilities side, back-up computer systems are the central element needed to respond to attacks, and these were solidly in place during the 9/11 crisis, and are still available now. Further testing and probing these systems is desirable, to try to avoid the possibility that a future attack could derail this crucial information and data storage capability.

Since human resources are the key to a bank’s ability to compete, the lesson is to avoid congregating the bank’s key people in close proximity to each other, in the event that an attack could hit that location. This is the same issue that banks should be concerned about for natural disaster risk, fire risk, and other physical damages that could occur and that could affect the key members of the bank’s ‘brain trust’. Thus, there is no specific need for further response to the terrorism threat in this context, other than to make sure that the issue is analyzed and a clear strategy and working plan for dealing with the risk is in place.

**Example b. Bombing ATMs in South Africa**

While this activity is far less striking than the 9/11 attacks, the bombing of automatic teller machines (ATMs) in South Africa has become a serious terrorist problem in that country. This phenomenon appears to have started in the early 2000s, with a handful of attacks primarily in the Johannesburg area. By 2007 the problem had become a true national crisis, with almost 400 bombings during that year, leaving 12 people dead, 20 wounded, and more than R 14.3 million ($US 2 million) stolen in the attacks.

These are seen as terrorist attacks, because the style of the events. Attackers generally strike at night, in locations that are not well guarded, and they generally have no concern for safety of anyone near the attacks. When confronted by police or bank guards, the bombers often resort to automatic weapon responses. While the intent of the attacks is presumably to steal money from the ATMs, the terror caused by the bombings is far greater than the amounts of money that are taken. Often money is destroyed in the explosions, or it is marked by dye when explosions occur, so that it cannot easily be used once removed by the bombers.

The ATM bombings are a different kind of terrorist attack from the World Trade Center attacks for a number of reasons. Most obviously, they are far smaller in scope, with far fewer deaths caused. The amount of terror generated, however, may well be higher with the ATM bombings, since citizens throughout the country are fearful about getting near the machines when these attacks are possible. And the attacks continue to terrorize the community to this day, since police and bank security responses have not reduced the level of intensity of attacks.

The attacks are frequent and have relatively low-level impact on the banks. In fact, it can be estimated what the average cost is for replacing a bombed ATM in South Africa, along with the expected number of bombings for the year. In 2008, for example, the projected number of bombings for the whole year is approximately 633, with a loss of R 32.1 million in cash stolen, and a replacement cost for each ATM of approximately R 82,162. This is almost an actuarial problem, in the sense that the probabilities can be estimated beforehand, and banks can plan for replacing machines and cash. Nevertheless, one of the authors can assure you that the attacks are terrorist phenomena, affecting anyone in the vicinity with potentially fatal consequences.

How can banks deal with this terror risk? In simplest terms, they largely deal with it as a cost of doing business. They are planning to replace bombed machines, looking for ways to make the machines more bomb-resistant, and placing machines in more defensible locations. The banks plan for the expected number of lost machines and replacement costs in their annual budgeting, and generally look at the issue as one of a cost of doing business rather than a terrorist threat.

**Example c. Kidnappings in Colombia**

Another terrorist activity that affects banks around the world is kidnapping of bank executives and managers. This may happen when a branch manager is kidnapped in order to get access to the vault in the branch to steal cash. It may happen to top executives of a bank, to hold the person for ransom. And in principle, it may occur when a terrorist group wants to make a statement against a particular bank or against a particular country that the bank represents.

Colombia has been a source of an inordinate number of kidnappings during the 1970s up until today, and thus may serve as an example of this kind of terrorist event. The kidnappings began largely as a tactic of the leftist guerilla groups, FARC and ELN. They kidnapped government leaders and police officers, to demonstrate their ability to disrupt society. They also kidnapped businesspeople, including bankers, to obtain ransom payments and help finance their insurgencies. Banks were not specific targets of this terrorist activity, but bankers are known to have wealth, and thus were/are good targets for ransom demands.

The violent nature of the kidnappings has led to deaths of numerous captives, along with many who have been released as well. Thus, the cost to a bank from having an executive or manager kidnapped range from ransom payments to the loss of a key person in the organization. The numbers are truly striking: an average of 1700 people were kidnapped each year during 1996-2003, while happily this terrorist activity has declined under the leadership of President Alvaro Uribe to a low of less than 600 kidnappings in 2007.[[15]](#endnote-15) During the 1996-2003 period, the Colombian government estimates that $US 260 million was spent on ransom ($57 million), loss of income ($93 million), and government spending ($110 million) on intelligence, policing, jails and technology.

**Example d. Money Laundering of Terrorist Funds (illustrated by the US)**

Money laundering has evolved from a practice that was long known and largely disregarded in banking circles, until the major US anti-drug campaign that began in the 1980s. While the US government did enact the Bank Secrecy Act in 1970, including sections making money laundering a civil offense and specifying penalties for banks and bankers who failed to report large cash and money instrument transactions of clients, this initial legislation did not produce much prosecution of money launderers or money laundering activity. The requirement for banks to file reports on cash transactions and on currency and monetary instrument transfers into and out of the United States[[16]](#endnote-16) took several years to implement in terms of specific reporting requirements, and responses to challenges from the commercial banks that were facing the burden of these reports.[[17]](#endnote-17)

The US moved to make money laundering a criminal offense in 1986, with the Money Laundering Control Act. This legislation required banks to file not only cash transaction reports, but also Suspicious Activity Reports, SARs, to identify possible money laundering activity based on unusual client activities. Without debating the appropriateness of using the banks to pursue law enforcement in this area, the cost to banks of creating, filing, and maintaining these reports is not trivial. In the mid-2000s the US Government was considering some modifications of the filing requirements, to reduce the burden on banks somewhat and to eliminate some categories of clients from the required reporting list.

In addition to drug proceeds, terrorist funds are another target of anti-money laundering efforts by governments. Terrorist activities require financing, and funds can be traced and forfeited if law enforcement can uncover them. The amounts of money involved in this activity are small relative to narcotics trafficking proceeds, estimated at over $US 200 billion annually in recent years. But particularly in response to the 9/11 attacks, anti-money laundering efforts have been increased in the US to pursue this kind of transactions.

**Section 4 – A Framework for Analyzing Terrorism Effects on Banking**

**Analyzing the security risk**

In this section we will present the CRR© analytic framework and demonstrate how it can be applied to the terrorism challenges that were described above. We begin with a general model of strategic risk management for banks that identifies four broad categories of response to risk events: risk transfer; risk adaptation; risk diversification; and speculation. Figure 1 shows this set of response categories. (Spich and Grosse 2005)

•

**Futures**

•

**Options**

•

**By operating in**

**several countries**

•

**By denominating in**

**different currencies**

•

**If a competitive**

**advantage exists**

**for managing it**

**Run the Risk**

**(Speculate)**

**Figure 1**

•

**Select office locations**

**and inputs**

•

**Use flexible contracts**

•

**Choose timing of**

**investment**

•

**Select alternative**

**organizational forms**

**(joint**

**-**

**venture;**

**alliance)**

•

**Make a pre**

**-**

**emptive**

**attack**

**INTERNAL**

**EXTERNAL**

•

**Swaps**

•

**Insurance**

**Diversify**

**Transfer**

**(Hedge)**

**Adapt**

**4**

**Methods to**

**Manage**

**Risk**

**Risk transfer** is the most commonly-discussed strategy for dealing with terrorist risk or any other business risk. The idea is to find a third party to take on the risk, for a price. This would be an insurance company, to insure a building or to provide kidnapping insurance. Or it could be a futures market to ensure the price of a key commodity or an interest rate. This strategy uses the external market to obtain protection against such risks.

**Risk adaptation** is a second option for dealing with terrorist risk. The bank can adapt its business, from placing key executives in different locations, to putting back-up systems into place, to hiding information through encryption or other means, to diversifying activities into additional countries. Added security measures also fall into this category of risk management. And the bank can even try to avoid placing activities that are viewed as high-risk[[18]](#endnote-18). All of these steps constitute adaptations of the business to try to reduce the potential negative impact of a terrorist event.

**Diversification** is a third possibility for dealing with terrorist risk. Just as with the selection of multiple investments to reduce the risk of negative outcomes with any one investment, the bank can diversify its business geographically and even across different business activities, to reduce the risk on the overall firm that a terrorist event could cause major damage to any one business or location.

And finally, **speculation** is the choice to run a risk without protection from internal or external sources. This includes, for example, self insurance of physical properties. If a bank has hundreds of branches, it may make sense to not use insurance policies on each one, but rather to run the risk of insurable losses, because the cost of the insurance premiums may be higher than the expected cost of fires, floods, or in this case terrorist attacks. Speculation is a justifiable strategy if the bank believes that it understands the risk in question better than outside parties, and can manage that risk without resort to protection mechanisms.

While the above strategies focus on the risk element of security management, there are generic strategies available to banks to manage the cost side of terrorist threats. Returning to the idea of terrorism as a strategic game between terrorist and target, these strategies (see Table 1) represent “cost imposition moves” in the terror game. In this case, they are options a bank has to increase the costs of a terrorist act to the perpetrator, reducing the ROR of the terrorist act to a point where a rational actor would consider abandoning or altering an act of terror.

**Table 1**

**Business Security/Continuity Strategies**

1. Redundancy- creating parallel and or establishing backup systems so that the failure of one system will be automatically taken up by the redundant or backup system.
2. Secrecy and subterfuge- the hiding, obscuring or distortion of information to reduce the effectiveness of an enemy’s intelligence. The undisclosed placement of armed security officers on planes is an example. The requirements of codes to enter, use or leave a system are entrance and exit barriers. Codes represent a cost and friction to a smooth and quick operation. The offering of fake or false leads wastes resources and time. Related to this is randomizing standard activities so that habits and repeat activities do not have a probability of 1 of occurrence.
3. Distancing targets- the more spread out and distant related targets are, the harder it is for an enemy to put a system out of commission in a single blow. The placement of key personnel in separate locations is an example. This strategy has the opposite purpose from a portfolio strategy which seeks to spread risk over distance instead of increasing it (for the enemy) This tactic increases the need for more resources on both sides which in the case of unequal resources, gives advantage to the side with more resources.
4. Insurance- obtaining a guaranteed coverage for losses. There are many forms of risk transfer, for which insurance contracts and hedging with financial derivatives are two of the most important forms.
5. Cooperation- working jointly with industry, government and others to increase the effectiveness of strategies via leveraging, supplementing , or getting access to new approaches at low or no cost (free riding on positive externalities created by others).
6. Increase investment in the anticipation of events, such as spending on technology for surveillance and intelligence, increased training and whatever increases capabilities of “guessing” the actions of the enemy.
7. Exit- the choice to leave a business activity which is a likely target for terrorism. Dropping a client or a service that is used by a terror network or supporting organization.
8. Cooptation of allies and friends of the enemy. This depends on turning the old wisdom of “a friend of my enemy is my enemy” to one’s advantage via engaging in friendly activities with “friends of the enemy” which help to disengage and breakup the enemy’s support network. The recent strategy in Iraq to work with the sheiks against Al Qa’ida is an example of this.
9. Persuasion and public relations- using media strategies to influence and change perceptions of vulnerability, willingness and ability to bear future costs and the like.
10. Attack- taking the initiative to attack, be proactive, force exposure, put the enemy off balance. This follows the advice that the best defense is an offense. Banks could be proactive with clients in identifying terrorist risks and creating insurance products to cover that risk. They could actively lobby government to put more funding into securing national IT systems. They could provide information to internet bloggers to force the exposure of terrorist indicator events or actions.

This list of business security strategies and tactics is neither complete nor new. Many companies and no small number of consultants offer products and services that use combinations of these security strategies and tactics. But the fact that there are a relatively large number of security management options suggests that the targeting of banks may have a lower payoff for a terrorist than originally thought.

**The CRR**© **Framework**

We now turn to the CRR© framework. As originally developed, this framework was intended to capture the interplay of three critical dimensions of competitiveness and how they would be affected by homeland security policy and practice. It is a short step to apply it to the main source of homeland security concern, international terrorism. The three dimensions of the framework are: **C**osts, **R**evenues, and **R**isks. They are the three types of impact that need to be evaluated in assessing the potential impact of terrorism on business.

***Costs***

We find that terrorism creates two kinds of **costs** for banking firms in their efforts to remain competitive. First, there are *micro* costs, which banks must pay to protect their people and their facilities, beyond normal insurance costs. These include such things as increased costs of shipping documents and other items between offices, protecting physical assets, and moving people. And second, there are *macro* costs, that all firms or banks operating in a particular jurisdiction or location are subject to. These include greater costs of doing business because of security precautions (in US Customs, for example), along with greater costs of compliance with anti-terrorism money laundering regulations. They also include infrastructure adaptations for greater security, costs of protecting against macro events such as biological warfare, and lost sales in that firms identified as being from the U.S. or Israel or some other specific country may lose customer appeal, because of their country of origin, which may be more terrorist-prone.

**Micro and Macro Scale *Costs* to Banks from Security against Terrorism**1

|  |  |
| --- | --- |
| ***Micro*** | ***Macro*** |
| 1. protection of offices and other facilities | 1. biological attacks that affect businesses in general |
| 2. protection of people | 2. computer network attacks that affect multiple businesses |
| 3. inability to get foreign nationals approved for technical or management jobs | 3. regulatory response that imposes costs of compliance to all industry members |
| 4. computer viruses and attacks; data theft | 4. potential industry reputation and good will losses because of poor management of security issues |

Costs can be classified by other categories: time frame, direct and indirect, degree of control. For this paper we will only focus on the scale of costs.

In applying the CRR© framework, the **9/11 attacks** represent a clear type of event that fits into the cost-revenue-risk analysis. The event has largely been seen in the ***cost*** context, with enormous costs to physical facilities and people. This is no doubt true, as we have noted. But the impact on banks was not unduly problematic, given the existing insurance contracts in place for their physical facilities. The loss of people could have been much more severe, but it turned out that major banks did not lose many of their key employees (as contrasted with the bond trading firm, Cantor, Fitzgerald, that lost 658 people, or 60% of their executives and managers). So, the overall cost impact of this terrorist event on the money center banks was not overwhelming.

The costs associated with the **ATM bombings** are largely the costs of increasing the defenses of the ATMs to avoid being bombed and to avoid losing cash when they are bombed. These costs include equipment (viz., the ATM machines themselves), people (i.e., guards), and money (including the dye to destroy bombed cash).

The cost to a bank of dealing with a **kidnapping** of one of its employees includes the effort to deal with the kidnapping, the lost work of the employee, and the ransom paid to obtain his/her return. In Colombia during 1996-2003, the average ransom paid per person kidnapped was just under $US 3,000.00. Added to these costs are the costs of protecting the bank’s personnel from potential kidnapping in terms of security measures that are put in place.

***Risks***

Banks face a variety of risks that affect their competitiveness. Parallel to the perspective on costs, there are *micro* risks at the individual firm level that will affect individual banks, especially those involved in risk sensitive industries (e.g., oil; airlines; real estate). There are also *macro* risks, or industry level risks that all banks based in a particular country, or banks operating in that country, may be more likely targets for terrorist acts (e.g., Pakistan, Colombia, the US after 9/11).

**Micro and Macro *Risks* to Banks from Security against Terrorism**1

|  |  |
| --- | --- |
| ***Micro*** | ***Macro*** |
| 1. risk of a terrorist event occurring, which could consequently damage the value of the bank | 1. opportunity risk of operating in the U.S. versus other countries (less risky sites not chosen) |
| 2. risk of being a symbol of the United States, and thus a target for terrorist attacks | 2. risk of negative impacts from government’s implementation of security policies |
| 3. risk to specific corporate assets from the threat of terrorist activity | 3. network serial interdependencies where the failure of one bank sets off a chain of events in network related banks. |

Risks can be further classified by time frame, whether they are direct or indirect, and their controllability.

As far as *risk* is concerned, after **9/11** banks in New York initially seemed to believe that they needed to spread out their geographic locations outside of Manhattan, to reduce the physical risk of being too concentrated there. Several years later it appears that the banks did not actually make major adjustments in their facilities locations, though perhaps shifting more business permanently to mid-town Manhattan after being dislocated from the Wall Street area for several months. The attractiveness of keeping people in close proximity for meetings and other interactions seems to have outweighed the concern for catastrophic risk that could imperil those people when grouped closely together. The decision to move more back-office functions away from the banking center of lower Manhattan to locations such as neighboring New Jersey and Connecticut did occur, though this was a trend that had been underway for many years before 9/11.

The *risk* impact of the **ATM bombings** is related to the probability of these events and their impact on bank costs (again, assuming low impact on revenues). And according to the information presented above, the risk of a single ATM bombing in 2008 in South Africa was a negative cash flow of R 167,980. The expected number of occurrences for a particular bank in a year would be: (total number of ATMs \* the bank’s percentage of this total\* cost/ATM.

With respect to *risks* in the **kidnapping** context, there is certainly an impact on risk management, that is noted above as a cost. That is, banks spend more on protecting their staff members against the risk of kidnapping. There may be a resultant decrease in the probability of a kidnapping taking place, but no evidence was available to support or reject this hypothesis. Additionally, there is the risk of lost ability of the bank to make specific decisions or carry out specific transactions, if a person key to the deal is kidnapped.

Given that the present financial crisis of 2008 is popularly seen as the work of greedy and “corrupt” bankers, one can speculate that bank officers could in fact become more tempting targets in the future. This could happen because such attacks might inherently possess a “Robin Hood” rationale that justifies such attacks in the public mind and achieve the dual outcome of comeuppance for the bankers and robbery from the rich. This potential change in public good will and trust in banking would suggest that bankers may need to be more vigilant in this area in the future.

***Revenues***

Revenues are the third focus of CRR analysis. Revenues are particularly important to protect because they are money flows that determine the economic viability of a business activity. When revenue flow is disrupted, slowed or stopped, all business transactions are affected. This is amply demonstrated in the global banking systems coordinated bailout of banks in October 2008. Because they are a flow phenomenon as opposed to one that is stationary and fixed, they can be readily disrupted because flows tend to have long and complex chains of interconnectedness. In addition, there are many entry points into a flow that need protecting. Terrorist threats can thus have serious impacts on new and future revenue streams.

For example, there are lost revenues by banks whose products/services are viewed as less attractive because of their country of origin. This may be due to opposition to U.S. policies by foreign citizens, who then react by shunning (some) U.S. services, and it may also be due to fears of doing business with U.S. entities because of the security threat. There are also direct revenue impacts of a terrorist attack, which may decrease overall demand for a period of time, and may disrupt the market’s functioning and thus reduce sales. In addition, a change in revenue flows changes the whole calculation of economic profitability of a venture. This can lead to increased interest rate charges or even cessation of activity, if a venture is seen as no longer viable because the cash flows do not meet client expectations.

In the *revenue* context, **9/11** had a more serious impact on the banks in New York. The US economic downturn that resulted from the attacks definitely caused a reduction in bank earnings, which was generalized across the economy. Banks were not affected as severely as, for example, airlines and insurance companies, but they did suffer reduced business activity and thus reduced earnings from the downturn. If we estimate that a bank’s earnings generally track the rate of growth of the economy, then earnings were reduced by about 1% during the year after the terrorist attacks of 9/11 due to this event. If we look at specific banks’ earnings, the three largest US banks experienced the results shown in Table 2 below.

**Table 2**

**Earnings of Citigroup, JP Morgan- Chase, and Bank of America**

(full-year net income in current $US billion)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Bank / earnings** | **1999** | **2000** | **2001** | **2002** | **2003** |
| Citigroup | 11.24 | 13.52 | 14.13 | 15.28 | 17.85 |
| JP Morgan-Chase | 7.50 | 5.73\* | 1.69 | 1.66 | 6.72 |
| Bank of America | 7.88 | 7.52 | 6.79 | 9.25 | 10.81 |

\* Chase Manhattan Bank merged with JP Morgan in 2000, approximately doubling in size.

These earnings show a slight decline in 2001 for Bank of America, which presumably resulted from both the dot-com bust (that actually started on March 10, 2000) and the 9/11 terrorist attacks. Citibank’s annual earnings actually rose through the whole period, and JP Morgan-Chase showed a huge drop in earnings after these two events, plus the merger of JP Morgan and Chase in 2000. So, one could only conclude that there may have been a partial reduction in earnings that counterfactually would have risen by 1% more in 2001 if not for the 9/11 attacks.

The *revenue* impacts on the banks from **ATM bombings** are probably fairly low, since all of the banks use ATMs, and none of them are immune or less subject to the attacks. It is conceivable that people will use ATMs less frequently, and therefore switch to internet banking, telephone banking, or to visits to bank branches. Given that the most frequent use of ATMs is to obtain cash, the physical delivery of cash will require physical facilities of some kind, and the banks all use ATMs and branches, so there probably will be very little impact on bank revenues from this problem.

With respect to *revenues*, the impact of a **kidnapping** has very little spillover into the bank’s revenues, given the lack of a link to the bank’s clients or business in such terrorist attacks. The clear impact is on the cost of dealing with kidnappings and potential kidnappings; since the risk is similar across banks, and none are more or less prone to such events, the impact on bank revenues is insignificant.

As far as **money laundering** is concerned, the impacts are not really related to terrorist acts on the banks themselves, but rather to the banks being used as channels for terrorist financing. So, in the CRR© framework, there are really no cost or revenue impacts of “terrorist money laundering attacks”. Rather, there are impacts of the banks trying to avoid being used for terrorist financing. In the CRR© framework the banks incur non-trivial costs of training employees to deal with potential money laundering activities, and of filing the various reports of cash and other potentially-suspicious transactions. Revenue impacts are minimal, unless a bank were to choose to participate in terrorist money laundering, in which case it could conceivably build up a significant revenue for offering the service[[19]](#endnote-19). Risk impacts are potentially large, because a bank found guilty of criminal money laundering may face fines and even the ultimate revocation of its license to operate.

CRR Inter-action Model

In Figure 1 below, we demonstrate the interaction of the cost, risk and revenue variables in a three-sided figure. This space can be looked at as a strategic security domain where each of the CRR© dimensions is given a numeric score by a decision maker. Given a firm’s particular preferences for cost bearing, risk taking or revenue flow needs, the decision maker must assign a low to high score for each dimension. The joint projection of these scores in the three dimensional space places a business activity (e.g. ATM) in a relative space that allow for comparisons with other activities. This gives the decision maker a way to see how business activities cluster or are spread within this security domain. And it means that tradeoffs between activities, relative to their security implications, can be more easily understood. This allows the firm to adjust its total security exposure position by adjusting its various preferences for CRR©.

For example, a bank seeking to do business with an American oil firm in Venezuela might assign this transaction with a high cost score, a medium risk score but a low revenue flow needs score. This allows for a strategic assessment of a portfolio of business activities simultaneously in three dimensions and allows comparisons between different projects and transactions based on composite security score. Depending on either clustering or spreading effects, the decision maker can see where relative security CRR© scores place a transaction and thus helps identify where and when, how much and in what form security resources might be needed to protect the bank’s business.



Thus, in the CRR© framework, the impact of 9/11 on major international banks was primarily on the macro, revenue side, and as a potential devastating risk, without major cost implications. If we consider the 9/11 attacks in the 3-dimensional space of our model, it appears as a tall, thin triangle, projecting from medium cost up to high revenue and risk impacts. The ATM bombings appear as a flatter triangle, projected from the middle of the risk side of the figure toward the low ends of the other two sides. The size of the area of the space and the overlap of triangles may give another indication of where tradeoffs and strategic focus may lie.

To better structure thinking about the four general types of terrorist events,( and others that may arise), Table 3 compares them on CRR and two other key dimensions: frequency, and measurability.

**Table 3 – Classifying Terrorist Acts in Banking**

|  |  |  |  |
| --- | --- | --- | --- |
| **Key dimensions \ Terrorist activity** | **Frequency of occurrence** | **Cost, Revenue and Risk Impacts, CRR** | **Measurability** |
| **9/11 attacks in USA** | Infrequent | Low direct cost; high lost-business cost | Fractile; unknown distr. |
| **ATM bombings in South Africa** | 600 per year in mid-2000s | Regular cost & risk | Yes, regular |
| **Kidnappings in Colombia** | 1000 per year in 2000s | Regular cost & risk | Yes, regular |
| **Money laundering in USA** | continuous | Regular compliance costs | Yes, understandable |

The **frequencies** of these categories of terrorist event show that most of them happen relatively often, though typically they have a limited impact on the banks. At least in the countries where these activities have been examined, the events have occurred many times per year. This is not to say that the events are predictable, but that the approximately number of occurrences can be estimated and in principle planned for. The 9/11 event was different, and thus must be viewed in a separate category of frequency and probability.

The **measurability** of the terrorist activities’ impacts on banks is reasonably manageable in three of the four events covered. The cost of replacing automatic teller machines, the cost of freeing a kidnapped employee, and the cost of complying with anti-money laundering rules are all known from past experience and can be reasonably estimated for future occurrences. The 9/11 event on the other hand is a ‘fractile’[[20]](#endnote-20) event, without a predictable distribution of occurrence or of expected impact. As with the events like the current sub-prime mortgage crisis and the frauds perpetrated by Nick Leeson on Barings Bank (1995) and Jerome Kerviel on Société Générale (2008), the 9/11 terrorist attack happened unpredictably and infrequently, and it could have had a devastating effect on any particular bank or on banks more generally.

The dimensions of terrorist activities as related to banks and banking show that most of them fit a traditional financial structure, with measurable impacts, frequency distributions that can be established, and generally a relatively low impact on the financial service provider. Fractile events such as 9/11 could have a much greater impact, and their likelihood of occurrence is essentially unknown – so they are categorically different from the other events.

**Different Situations for Different Banks**

At this juncture, it is important to make that point that banks are not a homogenous industry grouping. Major differences exist for various types of banks when it comes to terrorist attacks or events. For example, investment banks are almost completely exempt from attacks on ATMs, because they do not offer deposit accounts that people would access for cash withdrawals at ATMs. It is possible for an investment bank, through its cash management account or financial management account (CMA or FMA) to give clients access to deposit-type facilities, but these facilities are operated through a commercial bank’s ATM network. In sum, investment banks face a somewhat different scope of terrorist risks as compared with commercial banks – though the differences are not complete. Both types of banks face the problem of money laundering, of kidnapping, and of 9/11-type attacks. Table 4 shows some key categories of banks for which terrorism impacts may differ.

**Table 4**

**Impacts of Terrorist Events on Different Types of Banks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Terrorist activity / bank categories** | **9/11 attacks in USA** | **ATM bombings in South Africa** | **Kidnappings in Colombia** | **Money laun-dering in USA** |
| **Investment vs commercial banks** | same | No or low risk for investment banks | same | Lower risk for invest banks |
| **Single-location vs multiple location banks** | Much greater risk | Single-location banks may be more defensible | Single-location banks may be more defensible | same |
| **Domestic vs multinational banks** | Lower risk for multinational banks | Lower relative risk for banks with ops in other countries | Diversification benefits for MNBs | Possibly larger risk for MNBs |
| **Banks in different countries** | Very different risks | Very different risks | Very different risks | Somewhat different risks |

Single-location banks face different terrorist risk profiles than geographically-diversified banks. The single location puts a bank at much greater risk from a 9/11-type terrorist event, and probably of a kidnapping event, since all activities are centralized in that location. This physical structure does not, on the other hand, affect the bank’s use of ATM networks, or of dealing with the problem of terrorist funds that might be laundered through the bank.

Multinational banks presumably have a smaller failure or catastrophe risk than single-country banks, because any systemic problem in one country can, in principle, be mitigated with activities in other countries. A bank such as Bank of America, large but with almost all of its activities in the US domestic market, should be much more at risk in a terrorist attack within the US than Citibank, with its branches and other facilities and activities spread over more than 100 countries. Similarly, Lloyds TSB, with its largely UK-based facilities and activities, should be much more subject to the negative impacts of a terrorist attack in the UK than HSBC, with operations around the world, extensively in emerging markets as well as in Triad countries.

And finally, terrorist risks are quite different across countries. So, a bank operating in Colombia or in South Africa would have a much greater terrorist risk than a bank operating in Luxembourg or Costa Rica.

One can conclude here that because banks are different in type of services, location in market segments, country market locations and size/number of separate operations, there is no “one security policy fits all banks” strategy. Different contexts suggest a contingency approach that takes differences into consideration. This will allow standardization of approach where there are commonalities (eg. ATM practices are the same in most countries) and a customization approach where unique sets of conditions warrant specializations of policy and practice.

**Conclusions**

The plan for this paper is to make some important contributions to the analytic practices of businesses that need to develop strategies, policies and practices to manage the strategic security issue for business. We therefore conclude with a review of some of those contributions

First, the analysis in this paper raises security issues to a strategic, rather than an operational level. Banks need to deal with the issue of terrorist risk as a strategic concern, rather than as a simple cost in an operational context. With globalization as a driving market phenomenon, firms will continue to expand their operations into increasingly complex business environments. Besides the standard strategic analyses of competition, markets, technology and the like, security must now be consider an equal strategic issue that enters into the strategic calculus of the company.

Second, by looking at the security exposure issue as a gaming phenomenon, game theory applications can make important contributions to scoping out strategic options and choices. The terrorist/target relationship has a clear gaming logic for both the target (banks) and the terrorists. We show that both are involved in a game of cost imposition and reduction of gains (ROI) game that essentially has no end date. This means that security exposure is a constant strategic situation and organizational challenge that must be managed on a continuing basis. It is not a one-time problem that can be ‘solved’.

Third, we have identified and examined four general (universal) security risks facing banks, and presented empirical evidence from several countries to show the dimensions of the risks and a structured method for exploring and dealing with these risks.

Lastly, we offer a security exposure classification system, to assist the strategic decision makers to make better sense of the security challenge they are facing. We offer an analytic model, the CRR model, to assess and compare relative terrorist events outcomes in banking. It gives a security exposure profile for existing activities, and for planning future activities. We suggest that this model, while most germaine to banking interests, has possible applications to other businesses with modifications of the variables in the security exposure analysis.

In closing, we offer the opinion that banks have a unique, non-substitutable role in all political economies which makes them potentially less serious targets for terrorism than has been originally supposed after the 9/11 event. Because of the services they offer to all economic agents, it is in the interest of these agents to keep the banking system working relatively effectively, because the success of their own operations, business or terrorist, is dependent on the services that banks offer. Again the financial crisis of 2008 demonstrates this clearly. Thus we are not convinced that the risks of any of these terrorist activities present the kind of cataclysmic (fractile) failure risk of other internal activities such as bank fraud and external activities such as the subprime mortgage crisis.

**References**

Alexander, Dean C., *Business Confronts Terrorism: Risks and Responses*. Madison, Wisconsin. The University of Wisconsin Press, 2004.

Banks, William C., Renée de Nevers, and Mitchel B. Wallerstein. *Combating Terrorism: Strategies and Approaches*. Syracuse, New York: Syracuse University Press, 2007.

Biersteker, Thomas J, and Sue E. Eckert (eds.) *Countering the financing of terrorism*. New York: Routledge, 2007.

Chen, Andrew and Thomas F. Siems, “The effects of terrorism on global capital markets”, *European Journal of Political Economy*, vol.20, Issue 2, June 2004. pp. 349-366.

Grosse, Robert, *Drugs and Money: Laundering Latin America’s Cocaine Dollars*. New York: Praeger, 2001.

Katona, Peter, Michael D. Intiligator and John P. Sullivan (eds.), *Countering Terrorism and WMD: Creating a global counter-terrorism network*. New York. Routledge, 2006.

KPMG, *Global Anti-Money Laundering Survey 2007*. <http://www.kpmg.com/SiteCollectionDocuments/Global%20Anti-money%20laundering%20survey%202007.pdf>

Mandelbrot, Benoît, and Richard L. Hudson, *The (Mis)Behavior of Markets: A Fractal View of Risk, Ruin, and Reward*. New York: Basic Books, 2004.

Post, Jerold M., *The Mind of the Terrorist: The Psychology of Terrorism from IRA to Al Queda*; New York. Palgrave/MacMillan, 2007.

Sheffi, Yossi, The Resilient Enterprise:Overcoming Vulnerability for Competitive Advantage; The MIT Press, Cambridge, Massachusetts, 2007.

Skorodumov, Boris I, “Protecting Bank Networks from Acts of Computer Terrorism”, in [*Terrorism: Reducing Vulnerabilities and Improving Responses: U.S - Russian Workshop Proceedings*](http://www.nap.edu/catalog.php?record_id=10968) (2004).

U.S. Congress, House, Committee on Financial Services, Subcommittee on Oversight and Investigations; “The terror finance tracking program: Hearing on July 11, 2006. <http://purl.access.gpo.gov/GPO/LPS79130>

US Department of State, *Country Reports on Terrorism 2007*. Washington, D.C. US Government, 2008. <http://www.state.gov/documents/organization/105904.pdf>

N**otes**

1. Although individual leaders can be targets of assassination or kidnapping. But there loss is often less disrupting because of built in systems of organizational memory and momentum. [↑](#endnote-ref-1)
2. Business continuity is a related strategic issue that concerns itself with organization preparation and ability to continue operation in the face of sudden, large scale massive disruptions which result from either natural (e.g. earthquakes) or human (war, depressions) events. Terrorism can but does not necessarily involve actions of mass destruction (AMD). [↑](#endnote-ref-2)
3. Of course as barriers to entry increase, there are costs to the organization in terms of loss of the organization’s system openness and increased costs of defense. This requires management to therefore engage in a cost benefit calculation, like the CRR, to optimize the balance between security and openness. [↑](#endnote-ref-3)
4. One result of this is that the marginal utility of defense against terrorism has a high natural ROR because, after the first event, which is usually the most destructive, the next level of potential destruction can only be less because the worst case, a defenseless attack, has already passed and is not likely to be repeated. [↑](#endnote-ref-4)
5. (Martin Wolf “Congress decides it is worth risking another depression”. Editorial, *Financial Times* October 1, 2008 p 13.) . [↑](#endnote-ref-5)
6. Self inflicted injury that leads to a near collapse of global banking could only be a fantasy dream of terrorists. This raises the question of whether internally driven causes of collapse are actually more effective in bringing terrorist results without the terror. Are bankers their own terrorists? It can be argued that perhaps a misplaced focus of control on potential external agents totally overlooked the possibility of “accidental” internal agents bringing about terror-like outcomes of panic and irrational responses. [↑](#endnote-ref-6)
7. “Terrorists, terrorist-front companies, and individuals contributing to terrorist groups have at their disposal the vast, multinational banking system. Bankers and law enforcement officials have difficulties distinguishing account holders with benign intentions from monies earmarked for terrorist goals. Should persons with malevolent intent place their funds at offshore banks with strict secrecy rules then the challenge to uncover terrorist financing is that much more difficult. Terror groups also use shell companies further complicates undermining terror financing” Alexander, 2004 pg 68… [↑](#endnote-ref-7)
8. We note that there is not necessarily a unity in terrorist agendas. Terrorists may have mixed agendas and may actually work against each other. They may have an agreement on ends but not on means. Thus one group’s goal of destroying banks does not fit the agenda of groups that use them as agents of business. [↑](#endnote-ref-8)
9. Natural events are not terrorist events. We know that natural events, either weather induced or earth induced (earthquakes, hurricanes, tsunamis, wild fires, floods, blizzards) can produce disruptive and destructive effects to people and organizations. Though the outcome may be what any terrorist might dream of achieving, such events are still considered “acts of God” and not purposeful events by most people. However, they are still business security/continuity events and must be planned for. In this paper we are concerned only with purposeful human intentions and actions to proactively use terror as a strategy to achieve goals. [↑](#endnote-ref-9)
10. These are total costs from the attacks, not limited to the costs incurred specifically by banks. In fact, the costs incurred by banks were fairly low, except for the loss of employees’ lives. [↑](#endnote-ref-10)
11. # The destruction of physical assets was estimated in the national accounts to amount to $14 billion for private businesses, $1.5 billion for state and local government enterprises and $0.7 billion for federal enterprises. Rescue, cleanup and related costs have been estimated to amount to at least $11 billion for a total direct cost of $27.2 billion. Source: <http://www.ccc.nps.navy.mil/si/aug02/homeland.asp>

    [↑](#endnote-ref-11)
12. The process of cleaning up and rebuilding has certainly taken much longer than one year. The construction of a monument to memorialize the terrorist attack was not completed by 2008, and other building in the area affected by the destruction had not been fully completed by that time, seven years later. Still, the main clean-up was accomplished fairly rapidly, as was the rebuilding of the area in lower Manhattan. And security has been increased dramatically in the Wall Street area. [↑](#endnote-ref-12)
13. The losses from the terrorist attacks for the insurance industry (including reinsurance) are estimated at between $30 and $58 billion with the main uncertainty concerning liability insurance. By comparison the losses associated with Hurricane Andrew's 1992 damage in Florida came to around $21 billion. Even if the final cost is close to the lower estimate, insured losses in 2001 are likely to have been the highest ever. Source: <http://www.ccc.nps.navy.mil/si/aug02/homeland.asp> [↑](#endnote-ref-13)
14. Data from US Bureau of Economic Analysis webpage, <http://www.bea.gov/national/nipaweb/TableView.asp?SelectedTable=1&FirstYear=2007&LastYear=2008&Freq=Qtr> [↑](#endnote-ref-14)
15. Departamento Nacional de Planeacion, 2004 study on Kidnappings in Colombia. <http://www.dnp.gov.co/archivos/documentos/DJS_Documentos_Publicaciones/Boletin_Secuestro.pdf> [↑](#endnote-ref-15)
16. See Grosse (2001) Chapter 5. [↑](#endnote-ref-16)
17. The US Treasury Department established the Financial Crimes Enforcement Network, FINCEN, in 1990, to keep the records of these potential money laundering transactions, and later of the Suspicious Activity Reports, SARs. In 2005, more than 12 million Cash Transaction Reports (CTRs) alone were filed, obviously creating a major challenge of information overload to the authorities who would like to use the information for law enforcement. [↑](#endnote-ref-17)
18. Risk avoidance in this manner is conceptually possible, but due to unforeseen events and actions, it may not be possible to really eliminate the risk through this strategy. It is like avoiding exchange risk by working in your domestic currency alone – when your key competitors produce their products in a foreign lower-cost location. [↑](#endnote-ref-18)
19. The Bank of Credit and Commerce International, BCCI (affectionately known as the Bank of Crooks & Criminals, Incorporated), is probably the best-known example of a bank that actively pursued money laundering business, during the 1980s. When the bank was found guilty of criminal money laundering in 1990, its charter was revoked and penalties were imposed, to the point that the bank failed and ceased to exist. [↑](#endnote-ref-19)
20. The term “fractile” was popularized in discussions of financial crises that occur very infrequently, very unpredictably, and with immense consequences. Benoit Mandelbrot invented the idea of fractal distributions (and fractiles) in 1975, to describe geometric distributions that are completely irregular (and thus unpredictable). For example, the failure of the hedge fund Long-Term Capital Management in 1998 was due to a fractile event in the financial markets when emerging market crises in Asia and Russia led to a flight to high-quality bonds, and LTCM’s speculative positions on a range of bonds turned into losses, and ultimately a run on the company’s stock that produced a bankruptcy. The probability of the fractile event, using previous bond market history, was almost infinitely small – but it happened, and brought down the institution as a result. Fractile refers to the idea of measuring probabilities with quantiles of a distribution, and the fracturing of the distribution from an unmeasured, unexpected source. This fracture takes the risk of an event out of the expected distribution, and can lead to very different outcomes such as the financial catastrophes discussed here. [↑](#endnote-ref-20)