Terrorism and IB: New Directions for Theory and Practice

Abstract

Research on terrorism's impact on management and international business has increased substantially since 9/11. Yet theoretical and conceptual thinking about the nature of the terrorist threat and its implications for MNEs, their stakeholders, and the international business environment remains underdeveloped. We offer a new conceptualization of the terrorist threat that takes into account its enduring features as well as its new dimensions and detail the implications for MNE strategy. Rather than constituting a micro-level political risk, the threat posed by global terrorist networks, we contend, is best understood as a type of macro-level uncertainty. A series of propositions informed by theories of environmental uncertainty and complexity are put forth and the paper concludes with implications and directions for future research.

INTRODUCTION

Scholars, policymakers, and practitioners concur that terrorism is an issue of growing significance to international business (Czinkota & Ronkainen, 2009), and a particular concern to firms with complex, global supply chains (McIntyre & Travis, 2006; Sheffi, 2005). Nonetheless, theoretical and conceptual thinking about the nature of the threat and its implications for multinational enterprises (MNEs) remains underdeveloped. Indeed, many writers continue to conceive of terrorism as a micro-level political risk primarily experienced by MNEs operating in politically conflictive areas (e.g., Alon, Mitchell, & Steen 2006; Phatak, Bhagat, & Kashlak, 2004), and recommend conventional risk management strategies that emphasize avoidance and control (Alexander, 2009; Howell, 2002).

But just as the global business environment has undergone dramatic change in recent decades, so too has terrorism. While some of the leftist and ethnic-separatist terrorist organizations that dominated the international scene in the 1970s and 1980s remain active and others have emerged,[1] these conventional, single-country-focused groups have been eclipsed by global terrorist networks that meld religious fundamentalism with a virulently anti-Western political ideology and exploit the power of modern information technology to plan and execute attacks worldwide (Hoffman, 2006; Milward & Raab, 2009). This new brand of global terrorism was recently on display in Mumbai in November 2008, where a group of 10 Pakistani assassins linked to the al Qaeda affiliate Lashkar-e-Taiba (LeT) laid siege to India's financial capital for nearly three days. Armed with assault rifles, submachine guns, hand grenades, along with satellite phones, BlackBerries, and other high tech devices, the operatives slaughtered nearly 170 people, causing $30 to $40 billion in economic damage, and exacerbating tensions between two nuclear-armed neighbors (Gunaratna, 2009). We argue that this new type of terrorism is a departure from recent variants in terms of its motivations, strategy, tactics, targets, and form, and these changes have important implications for IB and management theory and practice.

This paper proceeds as follows: First, we discuss the underlying characteristics of terrorism. Next, we explore what has been identified in the political science literature as the "new terrorism" (Enders & Sandler, 2006; Hoffman, 2006), and distinguish it from the dominant forms of terrorism practiced in earlier eras. We then review and synthesize the pre- and post-9/11 literature on terrorism and business, focusing on works by management and international business scholars. The following section critiques the conventional IB notion of terrorism as a form of micro-level political risk and considers MNE strategy and corporate response through the conceptual lens of Miller's (1992) framework for integrated risk management – a model that has been highly influential in IB studies of MNE response to environmental uncertainty (Chung, Lu, & Beamish, 2008; Luo & Peng, 1999; Shrader, Oviatt, & McDougall, 2000). Building upon this framework we develop a series of propositions on how MNEs will adapt their strategies to deal with the evolving terrorist threat. In short, we expect that certain types of MNEs will increasingly eschew conventional strategies based on avoidance and control in favor of those rooted in cooperation and flexibility. We conclude with implications and directions for further research.

Terrorism: Definition and Key Characteristics

Over the years, scholars and practitioners have tried unsuccessfully to craft a universally acceptable definition of terrorism (Smelser, 2007). Despite fundamental disagreements over its meaning and manifestations, most observers agree on a few basic facts about terrorism: 1) it is a tactic rather than an ideology (no philosophy of terrorism exists); 2) it is employed by individuals and sub-national groups; 3) it involves the premeditated use or threat of violence against civilians or symbolic targets; 4) it attempts to influence an audience beyond the immediate target; and 5) it has a political motive (Enders & Sandler, 2006).

In recent times, terrorism has been practiced by a broad range of actors across the ideological spectrum -- from Maoist revolutionaries in Peru, to members of the rightist Christian Identity movement in the U.S. (Martin, 2006). Terrorism has also been employed by ethnic,

nationalist, separatist, and religious groups bent on redressing real and perceived injustices (Victoroff, 2005). Given this diversity, and the fact that many militant organizations also have political arms that provide social services, run businesses, and participate in the electoral process, some question whether the term "terrorist" to denote a coherent class of actors has validity (e.g., Tilly, 2004). While terrorism may not be the only "arrow in a political group's quiver," most concur that any dissident group relying on terrorist violence as its primary means of political expression may be called a terrorist group (Weinberg, Pedahzur, & Perliger, 2009).

Terrorism Old and New

Political scientists commonly use the terms "old terrorism" and "new terrorism" to distinguish between the leftist and ethnic-separatist terrorist groups that dominated the international scene from the late 1960s to the mid-1980s, and the religiously inspired groups that hold sway today (Martin, 2006).[2] While the old terrorist groups, which included Germany's Red Army Faction, Italy's Red Brigades, Japan's Red Army, the Irish Republican Army (IRA), Spain's Basque Fatherland and Liberty (ETA), and the Palestinian Liberation Organization (PLO), were determined and ruthless, they were pragmatic actors seeking concrete political ends such as territory, political autonomy, or socialist revolution (Lake, 2002). As such, they tended to be discriminating in their choice of targets and restrained in their use of violence. ETA, for example, often phoned pre-attack warnings to local police so that buildings could be evacuated before the bombs went off. So too did the IRA, which was also known to issue apologies to the families of victims when attacks went awry and "innocents" were killed (Hoffman, 2006). After all, excessive brutality could alienate key constituencies and spark a backlash threatening the organization's viability, as the IRA appears to have learned from its short-lived "proxy bomb" campaign in 1990 (Bloom & Horgan, 2008). As Jenkins (1975) put it, the politically-minded terrorists of past generations wanted "a lot of people watching, not a lot of people dead."

The new terrorist organizations do not adhere to the same rules of the game. Foremost amongst these groups is Osama bin Laden's al Qaeda organization, which has been variously described as a "networked transnational constituency" (Hoffman, 2006), a "leaderless network" (Sageman, 2008), a "dark network" (Milward & Raab, 2009), a "brand" (Zelinsky & Shubik, 2007), and a "terrorist organization, a militant network, and a subculture of rebellion all at the same time" (*The Economist*, 2008). Today's global *jihadist* network comprises the remnants of bin Laden's pre-9/11 organization, ensconced along Pakistan's rugged northwest frontier, loosely affiliated regional franchises such as LeT in Pakistan and Jemaah Islamiyah in Indonesia, "homegrown" militants such as those that carried out the July 2005 (7/7) London transportation system bombings, and legions of sympathizers around the globe connected via the Web. According to Wilkinson (2006), bin Laden and his network are "incorrigible" adversaries, bent on inflicting maximum casualties and economic disruption with no apparent interest in negotiations. This can be seen in their choice of targets, weapons, and techniques – particularly the suicide mission.[3] It can also be seen in their penchant for mounting secondary attacks on first responders at attack sites (Wilkinson, 2006).

But the jihadist groups that dominate the international terrorism scene today are not just different from their secular and ethnic-separatist counterparts in their motivations and bloodlust -- they are also more technologically savvy. The Mumbai case is illustrative. The 10 operatives that carried out the attacks used digital technology to conduct preoperational surveillance of their targets, made their way across the Arabian Sea from Karachi to Mumbai aided by global positioning systems, communicated by satellite phone with their handlers during the journey, and quickly located their targets once on land, having studied satellite images from Google Earth. Once the shooting began, the attackers were in constant communication with their foreign handlers using cell phones linked to a Voice over Internet Protocol (VoIP) account – a system designed to thwart the efforts of Indian security forces to trace and intercept the calls (LaRaia & Walker, 2009). According to Mumbai police, the gunmen made or received some 284 calls over

the course of the siege, running nearly 1,000 minutes (Unnikrishnan et al., 2009). Those calls, routed through a New Jersey-based VoIP provider, enabled the handlers, watching the events unfold live on television, to alert the shooters to the movements of security forces, thereby prolonging the carnage. The handlers also used these conversations to exhort the gunmen to carry out the attacks until the bitter end (Rabasa et al., 2009). Figure 1 captures the salient differences between old and new terrorist groups.

****

Figure 1 goes about here

****

IB and Management Approaches to Terrorism: A Review and Synthesis

Prior to the attacks of 9/11, terrorism was not a central concern to most MNEs, aside from those engaged in natural resource extraction or operating in conflictive areas. Although business executives were frequent targets of terrorism (Snitch, 1982), attacks were typically small in scale, had limited geographical repercussions, and could be mitigated through risk management strategies emphasizing avoidance and hedging (Wells, 1998). The conventional wisdom amongst managers was that scarce resources were better spent on revenue-generating activities than on defending against attacks unlikely to occur (Harvey, 1993). This view was shared by the insurance industry, which until 9/11, continued to treat terrorist attacks as an unnamed peril and include coverage against them under standard "all risk" commercial policies (Michel-Kerjan, 2008).

Thus, terrorism has traditionally attracted little attention from IB and management scholars. Although writers occasionally examined issues such as terrorism preparedness (Barton, 1993; Kuhne & Schmitt, 1979), crisis response strategies (Gladwin & Walter, 1980), and the impact of terrorism perceptions on the movement of managers between headquarters and overseas subsidiaries (Maddox, 1990), most scholars paid it little notice. According to Kotabe (2005), terrorism prior to 9/11 was considered a "random political risk of relatively insignificant

proportions." Indeed, just eight articles in the *Journal of International Business Studies* prior to 9/11 mention terrorism, and only one of which (Harvey, 1993) treats the topic in a substantive way.

Not surprisingly, interest in terrorism and its impact on international firms and the global economy has increased amongst IB and Management scholars in the aftermath of 9/11. In addition to the numerous sessions at the Academy of International Business annual meetings devoted to terrorism and its impact on firms and organizations, a spate of scholarly articles have appeared in IB and management journals examining the topics of international terrorism, corporate security, and homeland defense, including special issues of the *Journal of International Management* (2005) and the *Journal of International Business Studies* (in press). The topic of terrorism and its impact on global business has also been explored by scholars from a range of social science disciplines in a series of edited books (Burke & Cooper 2008; Richardson, Gordon, & Moore, 2009; Suder, 2004, 2006, 2008).

Recent cross-disciplinary scholarship on the economic and business aspects of terrorism may be segmented into two camps: empirical and conceptual studies. The former, written primarily by economists and political scientists, tend to investigate both the macro-level effects of terrorism (i.e., its impact on countries and the global economic environment) and the micro level effects (i.e., its impact on industries and value chains). They tend to be analytical rather than prescriptive. The latter, written primarily by management, marketing, and strategy scholars, tend to focus on the effects of terrorism at three different levels of analysis: the macro, micro, and the primary (i.e., its influence on individuals and firms). They tend to be both analytical and prescriptive. Since the empirical literature has recently been reviewed elsewhere (Bird, Bloomberg, & Hess, 2008; Frey, Luechinger, & Stutzer, 2007; Keefer & Loayza, 2008), we will focus on the conceptual studies.

Published in the weeks after 9/11, Enderwick (2001) offered an early attempt to gauge the immediate and longer term consequences of the terrorist attacks on New York and

Washington for the IB environment. Using concentric bands, the author identified four separate categories of possible impacts. Located within the first, innermost band (i.e., primary impacts) are the global tourism and airline sectors, which could be expected to experience the most immediate and severe consequences from the catastrophe given the use of commercial jets as terrorist weapons. The second band (i.e., secondary impacts) contains the insurance, investment, transportation, security, and intelligence sectors, which could be expected to experience both negative effects (e.g., high payouts to policy holders) and positive consequences (e.g., greater demand for security-related products and services). The third and fourth bands, respectively titled "response-generated impacts" and "long term issues," deal with policy-related issues and concerns associated with terrorism and its prevention rather than industry-specific impacts.

Czinkota, Knight, Liesch, & Steen (2005) also examine the myriad ways in which terrorism affects firms, industries, and public sector entities. Using contingency theory as a framework, they demonstrate how terrorism produces both direct impacts, including physical damage to facilities and personnel, and indirect impacts, including sudden and sharp declines in buyer demand (affecting firms through reduced revenues), unpredictable shifts or interruptions in value and supply chains (affecting buyers), and pressures for new policies at the state, national and supranational levels to curb terrorism (affecting public entities). While an MNE's chances of being directly harmed by a terrorist attack are "statistically insignificant," the odds of being indirectly affected are considerable and growing – especially for firms with complex global supply chains. As such, managers aim to reduce their firms' vulnerabilities and maximize flexibility through measures such as contingency planning, inventory management, and supply chain adjustments. Other authors including Sheffi (2005) and McIntyre & Travis (2006) offer broadly similar recommendations.

Two additional studies that draw upon IB theories and frameworks to explain terrorism's effects on MNEs and the global business environment are Li, Tallman, and Ferreira (2005), and Suder and Czinkota (2005). The former expands Dunning's "static" eclectic paradigm (1988) into

a "dynamic" model of global strategic management that can aid in understanding how "exogenous shocks" like 9/11 affect MNE decision-making and performance. It does so by integrating strategic management concepts (i.e., resources, strategy, structure, and adaptation) into its framework. The latter study incorporates terrorism into the eclectic paradigm as a key dimension that could alter international production strategies and undermine competitiveness by raising transaction costs and discouraging interfirm transfers of personnel and technology. Like Czinkota et al. (2005), Suder and Czinkota identify MNE vulnerabilities to terrorism and suggest concrete steps firms may take to mitigate risks, most of which focus on supply chain management. Unlike Czinkota et al., (2005), however, the authors' principal focus is on MNE value chains – not firms, buyers, and public entities.

The impact of terrorism on international competitiveness is further explored by Spich and Grosse (2005). Grounded in systems theory, this study conceptualizes the U.S. government-business nexus as a hierarchy of interdependent nested systems that are vulnerable in different ways to a "shock event" like 9/11. Focusing primarily on the national level, where homeland security policies are devised, the authors catalogue the terrorism-related costs and risks that U.S. firms conducting international business may experience, and trace their international competitiveness implications.

While all of these studies advance the frontier of knowledge about terrorism and its implications for the global economy, countries, industries, and MNEs and their managers, as a collection they fail to capture what is truly novel about the present wave of terrorism – its form, motive, and scale -- and how these changes make it a much more serious threat than that posed by the terrorist groups of the recent past. Moreover, they fail to link these changes in the nature of terrorism with changes that have occurred in the modern industrial societies in recent years, including the growing complexity and interconnectedness of economic and technological systems (Urry, 2002), and the increasing clustering of wealth, human capital, and hazardous materials

(Perrow, 2007), and explain how the confluence of these changes has produced a new and more lethal type of "complex terrorism" (Homer-Dixon, 2002).

If IB and management scholars have been generally slow to grasp these changes and their implications for MNEs and other organizations, the same cannot be said of scholars in the fields of risk studies (Kunreuther, 2002; Slovic, 2002), and catastrophe and disaster research (Clarke, 2008; LaPorte, 2007; Perrow, 2007; Weick & Sutcliffe, 2007). Indeed, there has been a surge of writings in these domains on terrorism and other low probability, high consequence (i.e., extreme) events since 9/11, spurred not only by the terrorist attacks on New York and Washington, but by the series of other large scale catastrophes that have followed since, including the 2003 U.S.-Canada blackout and Hurricane Katrina in 2005.

The conclusion of at least one prominent writer in these fields is that the crisis management theories of the past several decades, anchored in Cartesian philosophy, linear models, and tailored for compartmentalized emergencies, provide little guidance for decision-makers faced with a "new cosmology or risks" (Lagadec, 2008), much broader in scale and scope than those of the past. As such, there is an urgent need for "new thinking" (Mitroff, 2004), "new conceptual tools" (Clarke, 2008), and indeed a "radical shift in paradigm and practice" (Michel-Kerjan, 2008). Such a shift involves moving away from an orientation of seeking to avoid unplanned contingencies (i.e., surprises) through the deployment of standardized plans and tools to one that acknowledges that in an increasingly complex and chaotic world, firms must "prepare to be surprised," and respond with speed and agility (LaPorte, 2007).

Political Risk, Terrorism & Risk Management

IB scholars have had a longstanding interest in the influence of non-business factors including strikes, riots, rebellions, terrorism, and other forms of socio-political violence on MNE behavior and the dynamics of the MNE-government relations (Aharoni, 1966; Robock, 1971). Traditionally, such phenomena have been subsumed under the conceptual rubric of "political

risk," broadly defined as discontinuities in the political environment that are difficult to anticipate and threaten firm profitability, performance, operations, and/or strategy (Robock, 1971; Kobrin, 1979). These discontinuities have been typically associated with firms employing the FDI mode of entry (Oetzel, Getz, & Ladek 2007). Depending on the number and range of firms affected by the phenomena, these risks have been classified as either "micro" (i.e., affecting select projects, firms or industries) or "macro" (i.e., affecting many or all firms), but in either case, the risks have typically been viewed as a country-specific phenomena (Robock, 1971).

Simon (1984) offered an early and influential framework for conceptualizing political risk. Terrorist attacks, according his framework, represented a direct-internal risk that emanated from the *host society* – in the same league as protests, strikes, riots, and demonstrations. By contrast, expropriations, restrictions on remittances, wage and price controls, and the like, represented direct-internal political risks, which originated in the *host government*. While Simon did not analyze corporate response to political risk in great detail, the implications of his model for MNEs seeking to minimize their exposure to terrorism and other forms of socio-political violence were fairly straightforward: carefully scan the environment for signs of strife and avoid countries prone to instability and unrest. MNEs seeking to avoid trouble might also delay investments to the extent possible (Rivoli & Salorio, 1996), limit their size and scope (Delios & Henisz, 2000), and obtain political risk insurance and multilateral guarantees (Wells, 1998).

Integrated Risk Management & Terrorism

Miller (1992) took up the issue of how to conceptualize corporate response to the types of political risks catalogued by Simon (along with other risks of a non-political nature). His framework for integrated risk management identified five generic strategies that MNEs can employ to manage "strategic uncertainties" in the international environments in which they operate: avoidance, control, cooperation, imitation, and flexibility. Avoidance might involve divestiture for firms with existing investments, or postponement for firms in the pre-investment stage, whereas control might entail engaging in political activities (e.g., lobbying), gaining market

power to influence the behavior of competitors, and undertaking vertical integration to control input or demand uncertainties. Cooperation would typically involve forming long-term contractual agreements with suppliers and buyers, alliances or joint ventures, and participation in various consortia, whereas imitation might entail mimicking the behavior of rivals to prevent them from achieving a competitive advantage. Finally, flexibility might involve diversification of products, suppliers, or geographic markets to enhance internal responsiveness (Miller, 1992).

Although not formulated with the specific threat of terrorism in mind, two of the model's five strategies broadly describe the ways MNEs have traditionally dealt with the terrorist menace: avoidance and control. The case of Argentina in the early 1970s is illustrative. When the political climate deteriorated, MNEs with longstanding operations in the country, including General Motors, Fiat, Coca-Cola, Kodak, and IBM suddenly became targets for assassinations, kidnappings, and extortion demands by the Montoneros, a Marxist urban guerrilla movement, and other leftist terrorist groups. The Ford Motor Company, which employed 8,500 workers and produced nearly 50,000 vehicles a year in the country, initially responded to the extortion demands that followed the assassination of one of its local managers in 1973 by attempting to control the situation – they "donated" over $1 million in medicines and ambulances to local hospitals and food and school supplies to the poor (Gladwin & Walter, 1980). When fresh attacks on managers and facilities followed the payments, however, Ford opted for avoidance – it transferred foreign executives and their families out of the country.

Ford was not alone in choosing avoidance. Many other MNEs moved expatriate staff and their families out of the country or closed down operations entirely, whereas others contemplating investments, including Exxon and Dow Chemical, put their plans on hold (Gladwin & Walter, 1980). Indeed, the U.S. State Department estimates that the number of American businessmen in Argentina fell from over 1,200 in 1972 to 100 in 1975, and few personnel returned prior to 1978 (Purnell & Wainstein, 1981). Those MNEs that opted to remain in country attempted to control

their environment by increasing security at facilities, outfitting executives with bodyguards and armored cars, and providing security training for executives (Gladwin & Walter, 1980).

These core strategies of avoidance and control made sense as a means of dealing with the threat posed by conventional, politically-minded terrorist groups such as the Montoneros – and still do to some extent. For example, Chevron and other oil MNEs operating in the Niger Delta have responded to threats and attacks by militants on personnel and pipelines in recent years by periodically suspending operations (i.e., avoidance) (Oetzel et al., 2007). Likewise, multinational transportation companies such as A.P. Moller-Maersk have responded to the upsurge in pirate attacks off of the coast of Somalia by rerouting some of its ships away from the Gulf of Aden and around the Cape of Good Hope at the Southern tip of Africa, adding significant costs and travel time to the typical journey (Alexander & Richardson, 2009).[4]

MNEs have also attempted to control the terrorist threat by enlisting the support of local governments, militaries, and on occasion, paramilitary organizations. Chiquita Brands International, for example, made some $1.7 million in illicit payments to members of the rightist United Self-Defense Forces of Colombia between 2001 and 2004 to protect it from leftist guerrillas -- a move that led to criminal lawsuits against the company and ultimately the payment of a $25 million fine (Alexander, 2009).

Whether avoidance and control remain the best strategies for dealing with the emerging threat posed by global terrorist networks is doubtful. After all, opting for avoidance may involve ceding promising opportunities in growing markets to competitors. Control, meanwhile, is exceedingly difficult to achieve against terrorist networks that are resourceful, adaptive, resilient, and comprised of operatives willing to kill themselves in the process of carrying out their deeds. This point was made abundantly clear by the September 2008 suicide truck bombing of the Marriott Hotel in Islamabad. The hotel, which had been dubbed by terrorism expert Rohan Gunaratna (2008) as "the world's most protected hotel," had formidable anti-terrorism systems in place at the time of the attack, including 60 security officers on duty, four bomb sniffing dogs, 62

security cameras monitored by three security officers, under-vehicle cameras, and walk-through metal detectors to screen everyone entering the building. In addition, the hotel's approach was protected by a Delta Barrier -- a combination drop-down and hydraulic barrier – manned by shotgun-armed security officers (Orlob, 2009). Notwithstanding these measures, 56 people died and 270 were injured when a suicide bomber from an al Qaeda affiliated group detonated his charge after his vehicle slammed into the Delta Barrier (Gunaratna, 2009).

Less than a year later a suicide bomber again struck a heavily fortified Marriott property – this time in Jakarta. Rather than attempting to force his way past heightened security, the bomber simply disguised himself as a guest and checked into the hotel. Two days later he approached a group of local and foreign businessmen attending a breakfast meeting in the hotel's lobby and detonated the improvised explosive device hidden in his backpack, killing himself and five others (Jerard et al., 2009).

The New Terrorism: Risk or Uncertainty?

There is a vast literature in the social sciences on the nature of risk and uncertainty that can largely be traced back to Knight (1921). Risk has been used to describe situations in which probability distributions are knowable and can be assigned specifiable outcomes. Thus, outcomes can be completely contracted on in the market (e.g., insurance). Likewise, the decision-maker could forego prospects of a negative outcome by foregoing the risky event following a rational evaluation of predicted payoffs (Aharoni, 1966). Uncertainty, by contrast, describes situations where both the probabilities and outcomes are unknowable. Compared to risk, uncertainty involves situations of far greater novelty or ambiguity and which defy statistical modeling (March & Simon 1958). For Knight and his direct scholarly descendants, the concept of uncertainty

provided the justification for the entrepreneur and explained how firms could achieve positive economic rents regardless of industry structure.

The notion that terrorism and other extreme events are "uncertainties" rather than "risks" has spawned recent attempts to explain and categorize these incidents. Meyer's (1982) concept of environmental jolts, which he described as "transient perturbations whose occurrences are difficult to foresee and whose impact on organizations are disruptive and often inimical," has been employed by Katz and Shepherd (2004), Tan and Enderwick (2006), and Sullivan-Taylor and Wilson (2009) in reference to terrorist incidents. Related concepts include "rude surprises" (LaPorte, 2007), "black swans" (Taleb, 2007), and "wicked incidents" (Camillus, 2008). Regardless of label, there is growing agreement that the large-scale terrorist attacks favored by the al Qaeda network constitute extreme events that emerge suddenly, spread rapidly across economies and national frontiers, defy prediction, and have unintended consequences (Pina e Cunha, Clegg, & Kamoche, 2006).

A complimentary research stream for understanding and dealing with uncertainty builds upon causal textures theory proposed by Emery and Trist in their seminal 1965 paper. Indeed, scholars such as Selsky and McCann (2008) have argued that the growing threat to organizations and society from global terrorism and other extreme events, both natural and manmade, stem primarily from environmental changes that have given rise to unprecedented complexity and dynamism (i.e., turbulent causal textures). Characteristics of this environment include rapid technological change, interconnections between systems, and frequent shocks which are difficult, if not impossible, to anticipate. The result is a continuous sequence of unforeseen events that have the tendency to cascade from one system to another, causing severe disruptions that tax the ability of organizations to respond. Traditional strategic planning approaches built around deterministic thinking and execution, they argue, are of limited utility in dealing with such environments and what is needed are new ways of thinking and responding, centered on imagination and holistic thinking.

We argue that this conceptualization of the new terrorism as a form of extreme uncertainty emanating from dark networks of religiously inspired militants embedded in a complex, interdependent global system, is a more fruitful way of thinking about the phenomena than is the conventional IB approach of viewing it as a type of micro-level political risk. We next offer a series of propositions based on this premise.

Propositions

Organizational Size. In recent years there has been a noteworthy shift in terrorist targeting. While the al Qaeda network continues to plan and execute attacks on military installations and government buildings, primarily throughout the Middle East and Southeast Asia, it has been increasing its attacks on business facilities, public transportation systems, and other "soft targets." Indeed, the principal targets of the November 2008 assault on Mumbai included five different types of soft targets: tourist hotels, a train station, a restaurant, a hospital, and a residential complex (Rabasa et al., 2009). There are numerous reasons for the shift. First, soft targets by definition are more accessible than traditional hard targets such as Western embassies and airlines, which in most cases have experienced security upgrades since 9/11. Second, members of the al Qaeda network typically lack the resources and training to mount successful attacks on hard targets. And third, certain types of soft targets, like Western branded luxury hotels, can yield rewards equivalent to an attack on an embassy, including scores of casualties, widespread panic, and extensive media attention – all of which are a boon to terrorist recruitment (Gunaratna, 2009).

While in theory, businesses of all sizes are equally vulnerable to terrorism, in practice, large MNEs bear exponentially greater risks. After all, they represent much more inviting targets to terrorists seeking destruction and publicity. Large MNEs are also more likely than smaller firms to suffer the indirect consequences of attacks, which range from sudden macroeconomic shifts to the closure of airports and seaports (Czinkota et al., 2005). Large MNEs are also more likely than small firms to be sued for failing to prepare for or prevent terrorist incidents

(Cameron, 2007). While large MNEs may be more vulnerable to the direct and indirect effects of terrorism as well as litigation, they also typically have access to greater financial resources and thus may be in a better position to adopt new and innovative technologies, practices, and strategies to mitigate terrorism risk. As such, we expect the following:

Proposition 1 - Large MNEs will be more likely to become leaders and innovators in developing new strategies for managing terrorism risks.

Country of Origin. Coupled with the shift toward attacks against soft targets in recent years has been an increase in al Qaeda rhetoric exhorting followers to strike against symbols of Western capitalism (Riedel, 2007). Indeed, on several occasions bin Laden and his second-in-command Ayman al Zawahiri have called for strikes against economic infrastructure with the aim of "bankrupting" the U.S. and its allies (Hoffman & Weimann, 2009). It hasn't been empty rhetoric; there has been a notable increase in attacks against Western economic targets since 9/11 (Bergen, 2008). Among the network's favored targets have been Western branded luxury hotels such as the Marriott and Sheraton, which together have been attacked 10 times since 9/11. Other Western chains that have been struck include Hilton, Hyatt, Radisson, Ritz Carlton, Four Seasons, and Days Inn (Stratfor Global Intelligence, 2009). The decision by al Qaeda's leadership to target the West's "economic lifelines" is very much in keeping with the "clash of civilizations" thesis put forth by Samuel Huntington (1996). Given their comparatively greater vulnerability to terrorism, we expect Western MNEs to spearhead new approaches to mitigating the threat. As such, we propose:

Proposition 2 - Companies associated with Western civilization countries, particularly the U.S., will be more likely to become leaders and innovators in developing new strategies for managing the risk of terrorism.

Status. It is unlikely that MNEs will uniformly perceive themselves to be equally vulnerable and take steps to mitigate their exposure. Some will continue to view terrorism as a low probability event, and devote few resources to managing this threat, while others will take a much more proactive stance, seeking out innovative and collaborative solutions. MNE managers will assess their exposure to global terrorism based on the status and reputation of their organization and brand names. By virtue of their prominence, high status organizations will perceive a greater threat of a direct attack (Podolny, 1993). Moreover, high status MNEs may perceive that they have more to lose by failing to plan and respond appropriately. Strategic management research suggests that firms will look towards their unique resource endowments to formulate the most effective response to environmental challenges (Barney, 1991). Prior research on organizational status suggests that high status firms enjoy superior cooperative ties with regulators, customers, suppliers, and industry counterparts (Podolny & Phillips, 1996, Podolny, 2001). For this reason we propose that they will emphasize cooperative solutions over alternative approaches.

Proposition 3 – MNEs with a high degree of organizational status will be more likely to emphasize cooperative strategies for managing the risk of terrorism.

Internationalization. During the 1980s and 1990s, many MNEs with overseas manufacturing operations adopted just-in-time (JIT) management practices. The result was dramatic gains in productivity, customer service, and product quality, as well as drastically reduced inventory costs (Sheffi, 2005). Yet as companies have trimmed the waste and integrated distant suppliers into their global production networks, they have also increased their exposure to supply disruptions – a lesson brought home by 9/11. Indeed, in the days following 9/11, Toyota came within 15 hours of having to halt production of its Sequoia SUV plant in Princeton, Indiana because one of its

suppliers did not have enough steering sensors on hand and could not airlift in additional inventory from its supplier in Germany. The Ford Motor Company, meanwhile, was forced to idle five of its U.S. plants because trucks filled with engines, drive trains and other critical components were snarled in traffic at the Canadian border. The result was 12,000 units of lost production and financial losses on the order of $30 million (Sheffi, 2005).

Given the vulnerabilities that MNEs with global operations have to these types of disruptions, it is logical that some will choose to adapt their strategies to emphasize flexibility and resilience. Among the various flexibility-enhancing moves they may take include establishing dual procurement systems, whereby the majority of inputs or final products are purchased from inexpensive offshore suppliers, while a portion of the components are sourced from local suppliers. They may also engage in "near shoring," develop contingency transportation modes, and modify lean inventory management systems to permit greater slack (Sheffi, 2005). As such, we propose the following:

Proposition 4 - Firms with a high degree of internationalization will be more likely to emphasize flexibility strategies for managing the risk of terrorism.

Contribution to the Literature

This paper has sought to advance the intellectual discussion within the IB and management disciplines of what terrorism is, who practices it, and the variety of ways in which it impacts MNEs and the IB environment. By drawing on a rich and varied inter-disciplinary set of research it has shown that terrorism is a complex and multidimensional phenomena that has evolved markedly over time. Notwithstanding this complexity and dynamism, we have identified two basic types of terrorism that exist on the world scene today -- old terrorism and new terrorism -- and argued that it is a serious mistake to conflate the two. The former is comprised of secular and ethnic-separatist organizations with concrete and limited political agendas. These groups are

typically discriminating in their choice of targets and restrained in their use of violence. They seek to influence an audience rather than cause wanton destruction and are open to bargaining.

The latter is carried out by dark networks of religiously motivated militants with opaque and often supranational political agendas. These groups are bent on punishing their enemies through large scale attacks that cause panic, destruction, and mass casualties and their demands appear to be non-negotiable. Whereas the activities of the old terrorists are somewhat predictable (even if the exact targets are not known in advance) and their effects are typically localized, those of the new terrorists are hard (if not impossible) to forecast and their effects have a tendency to spread across national frontiers, with potentially catastrophic consequences for MNEs and other organizational actors far beyond the target nation. As such, we have argued that the new terrorism of al Qaeda and its global network of affiliates and sympathizers fits uncomfortably with traditional conceptions of political risk and have offered a new framework for understanding how these events affect MNEs. We have also analyzed the range of strategic moves MNEs may take to mitigate these risks.

Implications for Practice

This research has important implications for corporate planners and risk managers. First it suggests that global terrorist networks are a growing and dynamic threat that commands attention and resources. It also requires new strategic responses since the conventional tool kit biased toward avoidance and defensive strategies is of limited utility. We have argued that the most promising risk management strategies involve enhancing cooperation, flexibility, and resilience. We next examine three broad techniques that may help MNEs manage this evolving threat: 1) environmental scanning and vulnerability assessments; 2) scenario planning and simulations; and 3) business continuity planning. While none of these techniques is new, their implementation requires novel adaptations.

Environmental Scanning & Vulnerability Assessments

In the aftermath of 9/11, a number of authors have suggested that MNEs should more carefully scan the environment for potential trouble spots (Bremmer & Keat, 2009; Kurtzman &Yago, 2007) and keep a safe distance from countries experiencing terrorism or political strife (Suder, 2004). While we endorse the idea that MNEs should be attuned to elements in their external environments that could portend trouble (e.g., growing anti-Western sentiment, violent attacks on MNE personnel, etc.), such advice ignores the fact that terrorism is now a global problem endemic to all major global business markets, with systemic effects that cannot easily be avoided.

A more useful approach to environmental scanning, we contend, involves combining external assessments with internal analysis. Such analysis might involve conducting "stress tests" to identify vulnerabilities across the firm's internal value chain that could be the source of disruption (Chopra & Sodhi, 2004). A typical stress test might involve a manufacturer identifying key suppliers, customers, plant capacity, distribution centers and shipping lanes, and then surveying locations and amounts of inventory represented by components, work-in-progress and finished goods. After completing such an assessment, managers might then attempt to determine how to respond to a terrorist incident or other disruption which affected either the supply of critical components or demand for finished goods.

Scenario Planning & Simulations

Scenario planning has enjoyed growing popularity in recent years. The technique typically involves assembling a diverse group of people from inside and outside the organization to review company strategies, analyze information on external trends, and identify key business drivers and potential sources of disruption and then construct hypothetical scenarios. And while conventional forms of scenario planning remain useful, we believe the technique should be

broadened in scope to involve many different departments within a company, and indeed, the entire organizational field (e.g., suppliers, trading partners, consulting groups, governments). Moreover, scenarios should not be viewed narrowly as a way to avoid terrorism, but as a learning tool to help managers understand other potential global risks and hazards (i.e., natural disasters, financial crises) that could affect operations. Other tools and strategies that managers can use to deal with uncertain environments, include simulations, role playing exercises such as "internal assassins" and "wheel of crisis" (Mitroff, 2004), and worst-case thinking (Clarke, 2008).

Business Continuity Planning

For most MNEs, the probability of being directly victimized by transnational terrorism remains low. Yet the consequences of an attack on the firm or a critical value chain partner that disrupts production, threatens the supply of key inputs, or puts a key customer out of business are exceedingly high. Indeed, research shows that 40 percent of businesses that have been affected by a terrorist attack never reopen, and of those that do, 30 percent close within the following 24 months (Hardy & Roberts, 2003). As such, business continuity planning (BCP), broadly defined as strategies and processes that enable firms to prevent, manage, and recover from disasters, has become an imperative for most MNEs. Elements of BCP strategies typically include data mirroring, establishing a command and control center for decision-making and communications (i.e., disaster committee), and drafting a BCP plan that regularly audited, tested, and refined (Then & Loosemoore, 2006). Given the fact that managers are increasingly being held accountable by government authorities for the safety of their employees, with harsh penalties for non-compliance in many countries, business continuity planning should play an increasingly central role in the strategies of MNEs in the coming years.

Directions for Future Research

Extreme events, of which global terrorism is but one category, are occurring with increasing frequency. According to one study, ten of the world's twenty most costly insured catastrophes since 1970 have taken place since 2001 (Kunreuther & Michel-Kerjan, 2007). There is an urgent need for IB and management scholars to probe the nature of these events, the risks they pose to MNEs of different sizes, nationalities, and industries, and how the continuing process of globalization is increasing their frequency and severity. A better understanding of the specific strategies that can be taken to prepare for the occurrence of these events and mitigate their consequences is also needed.

One promising avenue of inquiry involves the study of interdependent security risks. These are the relatively novel risks caused by complex, integrated technical and financial systems wherein failures of a weak link can cascade throughout the system causing severe disruption (Heal, Kearns, Kleidorfer, & Kunreuther, 2006). The Northeast blackout of August 2003 is a prime example of such a risk. The event, which affected 50 million people in Canada and eight U.S. states, had a seemingly benign cause: the failure of a power company in Ohio to trim trees in part of its rural service area. When the overgrown trees came in contact with high-voltage power lines, they triggered an outage, which cascaded throughout the system, leading to the shutdown of over 100 power plants and costing $6 billion. While preventing such events is not possible, organizations can manage their impact by forging partnerships within and across industries and with public sector entities (Kunreuther & Michel-Kerjan, 2007).

Management and IB scholars might also seek to identify the attributes that make some firms more resilient to terrorism and other extreme events than others. For example, while all of the major U.S. airlines experienced difficulties in the immediate aftermath of 9/11, some bounced back much faster than others. Indeed, four years after the attacks, Southwest Airlines' stock price had recouped over 90 percent of its pre-9/11 value, whereas that of United Airlines and US Airways had regained a meager 12 and 23 percent, respectively (Gittell, Cameron, Lim, & Rivas, 2008). What accounts for this divergence in performance? Gittell and colleagues attribute it to

Southwest's comparatively strong employee relationships (relational reserves), high cash flow and low debt levels (financial reserves), and having a viable business model based on low unit costs. The research on high reliability organizations (e.g., La Porte, 2006; Weick & Sutcliffe, 2007) provides a solid theoretical foundation for work in this area.

Conclusion

Terrorism is an increasingly serious threat to MNEs that merits additional attention from both IB scholars and practitioners. In addition to traditional leftist and ethnic-separatist groups, MNEs must contend with a new and more lethal variant represented by al-Qaeda, its affiliates, and its legions of sympathizers across the globe. Dealing effectively with this "new species of trouble" (Slovic, 2002) will require new thinking and different strategies than those used to manage political risks emanating from sovereign governments and host society political actors with limited aims and agendas. MNE strategies aimed at cooperation and bolstering flexibility and resilience, both within the firm itself and across the extended enterprise, offer the best line of defense for dealing with this evolving global threat.

Figure 1 - Features Distinguishing Old and New Terrorism

Old Terrorists	New Terrorists
• Secular; this worldly • Centralized and hierarchical • Instrumental violence • Bounded constituency • Limited collateral damage • Hard targets • Willing to negotiate or compromise • Claim responsibility • Nonsuicide missions • Conventional weapons • Professional cadres • State sponsorship and control	• Religious; otherworldly • Decentralized and autonomous • Expressive violence • Unbounded constituency • Maximal collateral damage • Hard and soft targets • Reluctant to negotiate or compromise • Often do not claim responsibility • Suicide missions • Interest in WMD • Professional cadres and amateurs • Independent of state sponsorship/control

Adapted from Enders & Sandler (2006)

REFERENCES

Aharoni, Y. 1966. *The foreign investment decision process*. Cambridge: Harvard University Press.

Alexander, D. C. 2009. Dancing with wolves: avoiding transnational corporation interactions with terrorist groups. In H. W. Richardson, P. Gordon, & J. E. Moore II (Eds.). 2009. *Global business and the terrorist threat*. Cheltenham, UK: Edward Elgar.

Alexander, Y. & Richardson, T. B. 2009. *Terror on the high seas: From piracy to strategic challenge*. Westport, CT: Praeger Security International.

Alon, I., Gurumoorthy, R., Mitchell, M. C., & Steen, T. 2006. Managing micro political risk: A cross-sector examination. *Thunderbird International Business Review*, 48(5): 623-642.

Barnett, A., Abraham, M. & Schimmel, V. 1979. Airline safety: Some empirical findings. *Management Science*, 25(11): 1045-1056.

Barney, J. 1991. Firm resources and sustainable competitive advantage. *Journal of Management*, 17: 99-120.

Barton, L. 1993. Terrorism as an international business crisis. *Management Decision*, 31(1): 22-26.

Benjamin, B.A., & Podolny, J.M. 1999. Status, quality, and social order in the California wine industry. *Administrative Science Quarterly*, 44: 563-590.

Bergen, P. 2008. Al Qaeda, the organization: a five-year forecast. *The ANNALS of the American Academy of Political and Social Science*, 618 (1): 14-30.

Bird, G., Blomberg, S. B. & Hess, G. D. 2008. International terrorism: Causes, consequences and cures. *The World Economy*, 31(2): 255-274.

Blomberg, S. B. & Hess, G. D. 2006. How much does violence tax trade? *Review of Economics and Statistics*, 88: 599–612.

Bloom, M. & Horgan, J. 2008. Missing their mark: The IRA's proxy bomb campaign. *Social Research*, 75(2): 579-614.

Bremmer, I. & Keat, P. 2009. *The fat tail: The power of political knowledge for strategic investing*. New York: Oxford University Press.

Burke, R. J. & Cooper, C. L. (eds.). 2008. *International terrorism and threats to security: Managerial and organizational challenges***.** Cheltenham, PA: Edward Elgar.

Cameron, D. 2007. Managing travel risk: a duty care toolkit. *Journal of Business Contingency and Emergency Planning*, 1(2): 158-166.

Camillus, J.C. 2008. Strategy as a wicked problem. *Harvard Business Review*, 86(5): 98-101.

Chen, A. H. & Siems, T. F. 2004. The effects of terrorism on global capital markets. *European Journal of Political Economy,* 20(2): 249-266.

Chopra, S. & Sodhi, M. 2004. Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review***,** 46(1): 53-61.

Chung, C., Lu, J., & Beamish, P. 2008. Multinational networks during times of economic crisis versus stability. *Management International Review*, 48(3): 279-295.

Clarke, L. 2008. Possibilistic thinking: A new conceptual tool for thinking about extreme events. *Journal of Social Research*, 75(3): 669-690.

Czinkota, M. R., Knight, G. A., Liesch, P. W., & Steen, J. 2005. Positioning terrorism in management and marketing: Research propositions. *Journal of International Management*, 11(4): 581-604.

Czinkota, M. R. & Ronkainen, I.A. 2009. Trends and indications in international business: Topics for future research. *Management International Review*, 49: 249-266.

Delios, A. & Henisz, W. J. 2000. Japanese firms' investment strategies in emerging economies. *Academy of Management Journal,* 43: 305-323.

Dunning, J. H. 1988. The eclectic paradigm of international production: A restatement and some possible extensions. *Journal of International Business Studies*, 19: 1-32.

The Economist. 2008. Winning or losing? *A special report on al-Qaeda*, 17 July. http://www.economist.com/Specialreports/specialreportslist.cfm?category=455025

Emery, F. & Trist, E. 1965. The casual texture of organizational environment. *Human Relations,* 18: 21-32.

Enders, W. & Sandler, T. 2006. *The political economy of terrorism*. Cambridge: Cambridge University Press.

Enderwick, P. 2001. Terrorism and the international business environment. *AIB Insights*. Special Electronic Issue: 1-5.

Frey, S. B., Luechinger, S. & Stutzer, A. 2007. Calculating tragedy: Assessing the costs of terrorism. *Journal of Economic Surveys*, 21(1): 1-24.

Gladwin, T. N. & Walter, I. 1980. *Multinationals under fire: Lessons in the management of conflict*. New York: Wiley.

Gittel, J. H., Cameron., K., Lim, S., & Rivas, V. 2008. Airline industry responses to September 11th. In Burke, R. J. and Cooper, C. L. (eds.), *International terrorism and threats to security: Managerial and organizational challenges: 267-290.* Cheltenham, UK: Edward Elgar.

Gunaratna, R. 2008. Marriott in flames: the attack on the world's 'most protected' hotel. *Insite*, 1(7): 9-15.

Gunaratna, R. 2009. Mumbai investigation: the operatives, masterminds and enduring threat. *Peace and Security Review*, 2(1): 1-16.

Hardy, V. & Roberts, P. 2003. International emergency planning for facilities management. *Journal of Facilities Management,* 2(1): 7-25.

Harvey, M. G. 1993. A survey of corporate programs for managing terrorist threats. *Journal of International Business Studies*, 24(3): 465-477.

Heal, G., Kearns, M., Kleidorfer, P., & Kunreuther, H. 2006. Interdependent security in interconnected networks. In Auerswald, P., Branscomb, L. M., La Porte, T. M., & E.O. Michel-Kerjan (Eds.), *Seeds of disaster, roots of response: How private action can reduce public vulnerability*. New York: Cambridge University Press.

Homer-Dixon, T. 2002. The rise of complex terrorism. *Foreign Policy*, 128: 52-62.

Hoffman, B. 2006. *Inside terrorism (Second Edition*). New York: Columbia University Press.

Howell, L. D. 2002. Managing political risk in the age of terrorism. In Choi, J. & Powers, M. (eds.), *International finance review volume 3. Global risk management: Financial, operational, and insurance strategies.* Elsevier Science.

Huntington, S. 1996. *The Clash of Civilizations and the Remaking of World Order***.** New York: Simon & Schuster.

Jerard, J., Astuti, F., Feisal, M. 2009. *Bombing of JW Marriot and Ritz Carlton, Jakarta*. Nanyang Technological University, Singapore: International Centre for Political Violence and Terrorism Research.

Keefer. P. & Loayza, N. 2008. Overview: Terrorism, economic development, and political openness. In Keefer, P. & N. Loayza (Eds.), *Terrorism, economic development, and political openness.* Cambridge: Cambridge University Press.

Knight, F. H. 1964. *Risk, uncertainty, and profit***.** New York: Sentry Press.

Kobrin, S. J. 1979. Political risk: A review and reconsideration**.** *Journal of International Business Studies*, 10: 67-80.

Kogut, B & Kulatilaka, N. 1994. Operating flexibility, global manufacturing, and the option value of a multinational network. *Management Science***,** 40(1):123-139.

Kotabe, M. 2005. Global security risks and international competitiveness. *Journal of International Management,* 11(4): 453-455.

Kuhne, R. J. & Schmitt, R. F. 1979. The terrorist threat to corporate executives. *Business Horizons*, 22(6): 77-82.

Kunreuther, H. 2002. Risk analysis and risk management in an uncertain world. *Risk Analysis*, 22(4): 655-664.

Kunreuther, H. C. & Michel-Kerjan, E. O. 2007. *Assessing, managing and benefiting from global interdependent risks: the case of terrorism and natural disasters*. Proceedings of CREATE Symposium, 17-18 August 2007, Los Angeles, USA.

Kurtzman, J. & Yago, G. 2007. *Global edge*. Boston: Harvard Business School Press.

Lagadec, P. 2008**.** *A new cosmology of risks and crisis time for a radical shift in paradigm and practice***.** Ecole Polytechnique Centre National de la Recherche Scientifique. Working Paper. August. http://hal.archives-ouvertes.fr/docs/00/33/83/86/PDF/PL_2008-08.pdf.

Lake, D. 2002. Rational extremism: understanding terrorism in the twenty-first century. *International Organization*. Spring: 15-29.

LaPorte, T. R. 2007. Anticipating rude surprises – Reflections on crisis management without end. In D. E. Gibbons (Ed.), *Communicable crises: Prevention, response, and recovery in the global arena:* 27-44. Charlotte, NC: IAP Publishing.

LaRaia W., & Walker, M. 2009. The siege in Mumbai: A conventional terrorist attack aided by modern technology. In M.R. Haberfeld & A. von Hassell (Eds.), *Understanding of Terrorism*. New York: Springer.

Li, S., Tallman, S. B. & Ferreira, M. P. 2005. Developing the eclectic paradigm as a model of global strategy: An application to the impact of the Sep. 11 terrorist attacks on MNE performance levels. *Journal of International Management,* 11(4) : 479-496.

Luo, Y. & Peng, M.W. 1999. Learning to compete in a transition economy: Experience, environment, and performance. *Journal of International Business Studies*, 30(2): 269-296.

Maddox, R. 1990. Terrorism's hidden threat and the promise for multinationals. *Business Horizons*, 33(6): 48-52.

March, C. & Simon, H. 1958. *Organizations*. New York: John Wiley & Sons.

Martin, G. 2006. *Understanding terrorism: challenges, perspectives, and issues*. Thousand Oaks, CA: Sage.

McIntyre, J. R. & Travis, E. F. 2006. Global supply chain under conditions of uncertainty: Economic impacts, corporate responses, strategic lessons. In G. S. Suder (Ed.), *Corporate strategies under international terrorism and adversity*. Cheltenham, UK: Edward Elgar.

Meyer, A.D. 1982. Adapting to environmental jolts. *Administrative Science Quarterly*, 27(4): 515-537.

Michel-Kerjan, E. O. 2008. Toward a new risk architecture: The question of catastrophe risk calculus. *Social Research*, 75(3): 819-854.

Miller, K. D. 1992. A framework for integrated risk management in international business. *Journal of International Business Studies,* 23: 311-331.

Milward, H. B. & Raab, J. 2009. Dark networks and the problem of Islamic Jihadist terrorism. In S. Goldsmith & D. F. Kettl (Eds.), *Unlocking the power of networks: keys to high-performance government*: 168-189. Washington, D.C.: Brookings Institution Press.

Mitroff, I. 2004. Think like a sociopath, act like a saint. *Journal of Business Strategy,* 25(12): 42-53.

Moghadam, A. 2008. *The globalization of martyrdom*. Baltimore: Johns Hopkins University Press.

Oetzel, J., Getz, K., & Ladek, S. 2007. The role of multinational enterprises in responding to violent conflict: A conceptual model and framework for research. *American Business Law Journal*, 44(2): 331-358.

Orlob, A. 2009. Statement before the Committee on Homeland Security and Governmental Affairs, U.S. Senate. Hearing on lessons from the Mumbai terrorist attacks.

Pape, R. A. 2006. *Dying to win: the strategic logic of suicide terrorism*, Random House, New York.

Perrow, C. 2007. *The next catastrophe: Reducing our vulnerabilities to natural, industrial, and terrorist disasters*. Princeton: Princeton University Press.

Pina e Cunha, M., Clegg, S. R. & Kamoche, K. 2006. Surprises in management and organization: Concept, sources and a typology**.** *British Journal of Management*, 17: 317–329.

Pham, J. P. 2009. The pirate economy. *Foreign Policy*, 14 April. http://www.foreignploicy.com?story/cms.php?story_id=4817&print=1

Phatak, A. V., Bhagat, R. S., & Kashlak, R. J. 2004. *International management: Managing in a diverse and dynamic global environment*. Boston: McGraw-Hill Irwin.

Podolny, J. M. 1993. A status-based model of market competition. *American Journal of Sociology*, 98: 829-872.

Podolny, J. & Phillips D. 1996. The dynamics of organization status. *Industrial and Corporate Change*, 5: 453-371.

Podolny, J.M. 2001. Networks as pipes and prisms of the market. *American Journal of Sociology*, 107: 33-60.

Purnell, W. & Wainstein, E. S. 1981. *Problems of U.S. businesses operating abroad in terrorist environments***.** Santa Monica: Rand Corporation.

Rabasa, A., Blackwill, D. R., Chalk, P., Cragin, K., Fair, C. C., Jackson, B. A., Jenkins, B. M., Jones, S. G., Shestak, N. and Tellis, A. J. 2009. *The Lessons of Mumbai*, Santa Monica, CA: Rand Corporation.

Richardson, H. W., Gordon, P., Moore, J. E. II. 2009. *Global business and the terrorist threat*. Cheltenham, UK: Edward Elgar.

Riedel, B. 2007. Al Qaeda Strikes Back**.** *Foreign Affairs*. 86(3): 24-40.

Rivoli, P. & Salorio, E. 1996. Foreign direct investment and investment under uncertainty. *Journal of International Business Studies,* 27(2): 335-357.

Robock, S. H. 1971. Political risk identification and assessment. *Journal of World Business*, 6(4): 6-20.

Sageman, M. 2008. *Leaderless Jihad*. Philadelphia: University of Pennsylvania Press.

Selsky, J.W. & McCann, J.E. 2008. Managing disruptive change and turbulence through continuous change thinking and scenarios. In Ramirez, R.,Van der Heijden, K. & J. W. Selsky

(Eds.), *Business planning for turbulent times: New methods for applying scenarios.* London: Earthscan Publishing.

Sheffi, Y. 2005. *The resilient enterprise*. Cambridge: MIT Press.

Shrader, R. C., Oviatt, B. M. & McDougall, P. P. 2000. How new ventures exploit tradeoffs among international risk factors: Lessons for the accelerated internationalization of the 21st century. *Academy of Management Journal,* 43: 1227-1247.

Simon, J. D. 1984. Political risk assessment: Past trends and future prospects. *Journal of International Business Studies,* 15(3): 123-143.

Slovic, P. 2002. Terrorism as hazard: A new species of trouble. *Risk Analysis,* 22(3): 425-26.

Smelser, N. J. 2007. *The faces of terrorism: social and psychological dimensions*. Princeton: Princeton University Press

Snitch, T. H. 1982. Terrorism and political assassinations: A transnational assessment 1968-80. *The ANNALS of the American Academy of Political and Social Science,* 463(1): 54-68.

Spich, R & Grosse R. 2005. How does homeland security affect U.S. firms' international competitiveness? *Journal of International Management,* 11(4): 457-478.

Stratfor Global Intelligence. 2009. Special security report: The militant threat to hotels. http://www.stratfor.com/needtoknow/STRATFORMiltantHotels.pdf

Suder, G. S. (ed.) 2004. *Terrorism and the international business environment: the security-business nexus*. Cheltenham, PA: Edward Elgar.

Suder, G. S. & Czinkota, M. R. 2005. Towards an understanding of terrorism risk in the MNE. *Multinational Business Review,* 13(3): 3-23.

Suder, G. S. (Ed.). 2006. *Corporate strategies under international terrorism and adversity*. Cheltenham, PA: Edward Elgar.

Suder, G. S. (Ed.). 2008. *International business under adversity, a role in corporate responsibility, conflict prevention and peace*. Cheltenham, PA: Edward Elgar.

Sullivan-Taylor, B., Wilson, D. C. 2009. Managing the Threat of Terrorism in British Travel and Leisure Organizations. *Organization Studies*, 30(2): 251-276.

Taleb, N. N. 2007. *The black swan: the impact of the highly improbable*. New York: Random House.

Tan, W. J., Enderwick, P. 2006. Managing threats in the global era: the impact and response to SARS. *Thunderbird International Business Review*, 48(4): 515-537.

Then, S. K. & Loosemore, M. 2006. Terrorism prevention, preparedness, and response in built facilities, *Facilities,* 24(5-6): 157-176.

Tilly, C. 2004. Terror, terrorism, terrorists. *Sociological Theory*, 22(1): 6-13.

Unnikrishnan, C., Ahmed Ali, S. & Kartikeya. 2009. 26/11 calls traced to pak serving colonel. *Times of India*, 22 February.

Urry, J. 2002. The global complexities of September 11th. *Theory Culture and Society*, 19(4): 57-69.

Victoroff, J. 2005. The mind of a terrorist: a review and critique of psychological approaches. *Journal of Conflict Resolution*. 49(1): 3-42.

Weick, K. E. & Sutcliffe, K.M. 2007. *Managing the unexpected: Resilient performance in an age of uncertainty (Second Edition)*. San Francisco: Jossey-Bass.

Weinberg, L., Pedahzur, A. & Periliger, A. 2009. *Political parties and terrorist groups*. London: Routledge Taylor and Francis Group.

Wells, L.T. Jr. 1998. God and fair competition. In T. Moran (Ed.), Managing international political risk. Malden: Blackwell Publishers.

Wilkinson, P. 2006. *Terrorism versus democracy: the liberal state response. Second edition.* London: Frank Cass.

Zelinsky, A., & Shubik, M. 2007. Terrorist groups as business firms: A new typological framework. *Social Science Research Network*. http://ssrn.com/abstract=959258. Accessed 1 September 2009.

NOTES

[1] Examples of the former include Colombia's Revolutionary Armed Forces (FARC) and Spain's Basque Fatherland and Liberty (ETA); an example of the latter is Nigeria's Movement for the Emancipation of the Niger Delta (MEND).

[2] In the late 1970s, all active international terrorist groups had secular goals and beliefs, a majority professing some type of Marxism; by the end of the 1990s, roughly one-third of all active international terrorist groups could be classified as "religiously motivated," the majority espousing an extremist interpretation of Islam (Wilkinson, 2006).

[3] While it is true that many suicide bombers are secular nationalists rather than religious extremists (Pape, 2006), al Qaeda and its jihadist ideology appear to be responsible for the growing popularity of suicide missions, the rise in the number of organizations embracing the tactic, and the sharp increase in attacks on civilians (Moghadam, 2008).

[4] Whether these pirates are terrorists or criminals is debatable. Their motivations appear to be economic rather than political in nature, yet some believe a tactical nexus may be developing between pirates and Islamist militants. Indeed, the al Qaeda-linked Somali terrorist group al-Shabab, which has been designated a foreign terrorist organization by the U.S. government, is thought to receive a cut of the profits from maritime attacks that originate on soil under its control in southern Somalia (Pham, 2009).