Reflections on the Evolving Terrorist Threat to Luxury Hotels: A Case Study on Marriott International

By
David A. Wernick
Mary Ann Von Glinow

The advent of global terrorist networks represents a challenge to international business (IB) theory. Traditionally conceptualized as a type of political risk experienced by multinational enterprises (MNEs) operating in conflictive areas, terrorism has evolved in recent years. The global terrorist networks that dominate the international scene today have different motivations, strategies, tactics, and organizational structures than their secular and ethnic-separatist predecessors and these differences matter for IB theory and practice. Moreover, these groups have shown themselves adaptive, resilient, and capable of striking targets of strategic and symbolic importance in global business and financial centers. This paper examines the changing nature of the terrorist threat to MNEs and the implications for a sector that has been a target of recent attacks: the luxury hotel industry. Structured as a case study of Marriott International, a leading global hospitality provider, the paper analyzes ways the firm is adapting to the evolving threat and the measures it has introduced to safeguard guests, staff, property, and brand. Implications for IB theory and practice are drawn. © 2012 Wiley Periodicals, Inc.
Adapting to this dynamic threat environment will require new strategies and approaches on the part of MNEs, and IB scholars and practitioners can learn much from companies like Marriott International that are on the frontlines of the battle, and at the forefront of innovation.

IB and Management Approaches to Terrorism: A Review and Synthesis

Prior to the attacks of 9/11, terrorism, broadly defined as the threat or use of violence to attain a political goal through intimidation, fear, or coercion (Alexander, Valton, & Wilkinson, 1984), 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 (Kovsky, 1990; Snitch, 1982), attacks were typically small in scale and had limited repercussions beyond the specific subsidiaries or projects targeted. The conventional wisdom among multinational managers was that scarce resources were better spent on revenue-generating activities than on defending personnel and facilities against attacks that were unlikely to occur (Harvey, 1985, 1993). This view was shared by the insurance industry, which until 9/11 treated terrorist attacks as an unnamed...
peril and included coverage against them under standard “all-risk” commercial policies (Michel-Kerjan, 2008).

Although IB and management scholars 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 the topic of terrorism 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 these (Harvey, 1993) treats the topic in a substantive way. This is in sharp contrast to the large body of academic literature published in political science and international relations journals on terrorism, conflict, security, and political risk in the pre- and post-9/11 periods (Henisz, Mansfield, & Von Glinow, 2010).

Not surprisingly, interest in terrorism and its impact on global business has risen sharply among IB and management scholars in the decade following 9/11. In addition to the numerous sessions at the Academy of International Business and Academy of Management 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, cyber-security, and homeland defense, including special issues of the *Journal of International Management* (2005) and the *Journal of International Business Studies* (2010). One such article identified terrorism as a “critical frontier issue” in international management (Ricart, Enright, Ghemawat, Hart, & Khanna, 2004); another labeled it an issue of growing significance to IB scholars, policymakers, and practitioners (Czinkota & Ronkainen, 2009). A series of edited books on terrorism and its business impact have also appeared in print (Burke & Cooper, 2008; Richard- son, Gordon, & Moore, 2009; Suder, 2004, 2006, 2008).

This growing body of literature offers valuable insights into the evolving nature of the terrorist threat and its significance for firms of various sizes, sectors, and for the IB environment in general. For instance, scholars have called attention to the fact that terrorist incidents have both direct and indirect effects on firms, and that the former, while immediate and compelling, are usually of far less import than the latter (Czinkota, Knight, Liesch, & Steen, 2010; Spich & Grosse, 2005). After all, very few firms experience terrorism-related casualties and property destruction, whereas a multitude may experience the indirect effects of terrorist incidents, which run the gamut from sudden declines in buyer demand (Czinkota et al., 2010) to governmental mandates that hinder the movement of people, goods, and money across borders (Bakshi & Gans, 2010; Chambers, Wernick, Zdanowicz, & Von Glinow, 2010; Jain & Grosse, 2009).

The 9/11 attacks are a case in point. While the attacks themselves dealt a devastating blow to the tenants of the World Trade Center and other businesses domiciled in lower Manhattan, generating about $40 billion in direct insurance losses (Kunreuther & Pauly, 2005), the number of firms that suffered casualties and property damage was tiny in comparison to those in the United States and abroad whose operations were disrupted by communications outages, the grounding of transatlantic air traffic, and the border closures that followed the terrorist assault (Sheffi, 2005). As such, firms need to be attuned to the ways in which their relationships with foreign suppliers, customers, and service providers expose them to terrorism-induced vulnerability or “interdependence risk” (Shrader & McConnell, 2002; Starr, Newfrock, & Delurey, 2003) and take steps to bolster flexibility and organizational resilience (McIntyre & Travis, 2006; Sullivan-Taylor & Wilson, 2009).

Other researchers have sought to identify whether certain types of firms and industries are more vulnerable to large-scale terrorist attacks than others. Enderwick (2001), for instance, used concentric bands to conceptualize differing levels of exposure to terrorist incidents involving the use of commercial jets against civilian targets. Likewise, Tan and Enderwick (2006) used a similar concentric band model to map the business implications of the SARS virus—an exogenous shock bearing striking similarities to terrorism in its randomness, adaptability, and the speed with which its effects spread across the globe in early 2003.

Yet other researchers have sought to identify the attributes that make certain firms more resilient following a terrorist incident than others—an important avenue of inquiry given that 40% of businesses that have been affected by a terrorist attack never reopen, and of those that do, 30% close within the following 24 months (Hardy & Roberts, 2003). For example, while all of the major U.S. airlines experienced financial difficulties in the immediate aftermath of 9/11, some rebounded quicker than others. Indeed, four years after the attacks, Southwest Airlines’ stock price had recouped over 90% of its pre-9/11 value, whereas that of United Airlines and US Airways had regained a meager 12 and 23%, respectively (Gittell, Cameron, Lim, & Rivas, 2008). What accounts for this divergence in performance? Gittell and colleagues attribute it to the airline’s no layoff policy,
which has engendered high levels of trust and loyalty amongst workers and strong employee-management ties, its sound financial management, and an appropriate business model. Some of these same elements (i.e., job security) help explain why the Australia-based international travel agency Flight Center quickly regained its market footing in the aftermath of the 9/11-induced global travel slowdown (Dunford & Palmer, 2002).

Other studies have explored the decision-making process that managers go through when considering whether to internationalize under conditions of terrorism-induced uncertainty and risk (Liesch, Steen, Knight, & Czinkota, 2006) and the impact of terrorism on various functional areas within organizations. One important finding is that human resource management (HRM) can play a strategic role in helping firms prepare for and respond to a terrorist attack (Liou & Lin, 2008; Perry & Mankin, 2005).

While all of these studies advance the frontier of knowledge about terrorism and its implications for MNE operations, strategy, and the IB environment, 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 terrorist organizations with broader economic, social, and technological transformations, including the growing complexity and interconnectedness of economic life (Urry, 2003); the increasing power, sophistication, and portability of modern weaponry (Homer-Dixon, 2002); and the clustering of wealth, human capital, and hazardous materials in urban areas (Perrow, 2007). Together, these trends have produced a new and more lethal type of “complex terrorism” (Homer-Dixon, 2002) capable of causing cascading failures throughout markets and societies (Smith & Fisbacher, 2009).

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). 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 by a host of natural and man-made calamities—from Hurricane Katrina in 2005 to the Deepwater Horizon oil spill of 2010.

The conclusion of at least one writer in these fields is that the crisis management theories of the past several decades, premised on linear models and tailored for compartmentalized emergencies, provide little guidance for corporate decision-makers faced with a “new cosmology or risks” (Lagadec, 2009) which are much broader in scale and scope than those of the past. As such, there is an urgent need for 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 world, firms must “prepare to be surprised” and respond with agility (LaPorte, 2007).

A growing literature suggests that firms adopting this kind of proactive approach toward security may not only be better positioned to safeguard lives, physical
Refl ections on the Evolving Terrorist Threat to Luxury Hotels: A Case Study on Marriott International

The destruction wrought at the Oberoi was of commensurate magnitude. India’s economy, meanwhile, sustained an estimated $30 to $40 billion in damage as business ground to a halt and foreign visitors cancelled travel plans (Gunaratna, 2009).

But the Mumbai massacre, while audacious and operationally-sophisticated, was neither unique nor unprecedented. As Rohan Gunaratna (2009), head of the Singapore-based International Centre for Political Violence and Terrorism Research (ICPVTR), has noted, it closely resembled, in tactical terms, the 1975 attack on the Savoy Hotel in Tel Aviv by the Palestinian Liberation Organization (PLO). Both incidents involved amphibious landings, hostage takings, and the use of firearms and grenades. The response of Israel’s commandos to the earlier siege, however, was quite different. Whereas the Indian security forces reacted in a slow and disorganized fashion, the Israelis quickly stormed the hotel, rescued 5 of the 13 hostages, and routed the gunmen, sustaining only three fatalities in the process (Gunaratna, 2009).

Nor was the targeting of luxury hotels unusual. According to Stratfor, an Austin, Texas-based security consultancy, the number of major terrorist attacks against hotels around the world more than doubled in the eight years following 9/11, from 30 to 62, while the number of different countries affected jumped to 20 from 15 (Stratfor Global Intelligence, 2009). Meanwhile, the toll of persons killed and injured in such attacks increased roughly sixfold during this period. Table 1 provides a list of selected terrorist attacks on international hotels between 2002 and mid-2009.

### Table 1: Selected Terrorist Attacks on International Hotels Between 2002 and 2009

| Year       | Hotel          | Location           | Tactic                                                                 | Casualties     | Perpetrator                                      |
|------------|----------------|--------------------|------------------------------------------------------------------------|----------------|--------------------------------------------------|
| 2002       |                |                    |                                                                       |                |                                                  |
| March 27   | Park           | Netanya, Israel    | A suicide bomber entered into the hotel’s dining room and detonated an explosive device | 29 killed 140 injured | Al-Qassam martyrs brigade                        |
| May 8      | Sheraton       | Karachi, Pakistan  | A suicide bomber caused an explosion destroying a Pakistan Navy bus outside the hotel | 14 killed 25 injured | Pakistani jihadi organizations associated with Al-Qaeda (suspected) |
| June 14    | Marriott       | Karachi, Pakistan  | Suicide car bomb exploded near the hotel                              | 11 killed 51 injured | Pakistani jihadi organizations associated with Al-Qaeda (suspected) |
| October 12 | Resort Island of Bali | Bali, Indonesia | Backpack-mounted device carried by a suicide bomber and a large car were detonated | 202 killed 209 injured | Jemaah Islamiya pro-Al-Qaeda (suspected)         |
| November 28| Paradise       | Mombasa, Kenya     | Car bomb exploded outside the hotel                                  | 15 killed 40 injured | Al-Qaeda (suspected)                             |
### TABLE 1 Continued…

| Year   | Date       | Location                     | Description                                                                 | Casualties | Suspect            |
|--------|------------|------------------------------|-----------------------------------------------------------------------------|------------|--------------------|
| 2003   | August 5   | JW Marriott Jakarta, Indonesia | A suicide bomber detonated a car bomb outside the lobby                      | 14 killed 150 injured | Jemaah Islamiya    |
| 2004   | May 9      | Four seasons Baghdad, Iraq   | A bomb struck the hotel and tore apart chairs and part of the ceiling of the bar | 0 killed 8 injured | Al-Qaeda in Iraq (suspected) |
|        | July 2     | Sheraton Baghdad, Iraq       | Perpetrators rigged several rocket launchers to fire on a timer from a bus   | 0 killed 0 injured | Al-Qaeda in Iraq (suspected) |
|        | October 7  | Hilton Taba, Egypt           | A suicide bomber drove an explosive laden car into the lobby                 | 33 killed 150 injured | Al-Qaeda (suspected) |
|        | October 28 | Marriott Islamabad, Pakistan | A bomb went off inside the hotel, causing damage to the lobby                 | 0 killed 15 injured | Pro-Al Qaeda Jihadis of Pakistan (suspected) |
| 2005   | February 17 | Marina Sungai Kholok, Thailand | A car bomb was detonated outside the hotel                                 | 7 killed 40 injured | Unknown            |
|        | April 3    | Green World Palace (GW) Songkhla, Thailand | A bomb planted on a motorcycle exploded in front of the hotel | 0 killed 0 injured | Unknown            |
|        | July 23    | Ghazala Gardens Sinai Peninsula, Egypt | A truck bomb was driven into the lobby                                       | 45 killed 100 injured | Abdullah azzam brigades |
|        | July 23    | Movenpick Sinai Peninsula, Egypt | A bomb was hidden in a suitcase and exploded outside the hotel               | 3 killed 25 injured | Abdullah azzam brigades |
|        | October 1  | Resort Island of Bali Ball, Indonesia | Three bomb attacks occurred in two tourist areas                             | 32 killed | Jemaah Islamiyah  |
|        | November 9 | Grand Hyatt, Radisson SAS, and Days Inn Amman, Jordan | Two suicide bombers entered Radisson hotel’s ballroom and detonated. Bomb detonated outside Hyatt’s hotel. At the Days Inn, the bomber entered the restaurant and exploded | 57 killed 115 injured | Al-Qaeda in Iraq |
| 2007   | January 26 | Marriott Islamabad, Pakistan | A suicide bomber blew himself up in the parking lot                          | 1 killed 7 injured | Al Qaeda and Tehrik-i-Taliban Pakistan |
|        | May 15     | Marhaba Peshawar, Pakistan   | A suicide attacker detonated a bomb that ripped through the crowded hotel’s restaurant | 25 killed 32 injured | Unknown            |
|        | May 27     | JB Songkhla, Thailand        | Ione bomb was hurled into the hotel and another one outside the hotel        | 0 killed 7 injured | Unknown            |
|        | May 27     | Lee Garden Songkhla, Thailand | Explosion caused by a bomb                                                   | 0 killed 6 injured | Unknown            |
|        | June 25    | Mansour Baghdad, Iraq        | A man wearing a belt of explosives walked into the lobby and detonated his bomb | 12 killed 18 injured | Al Qaeda in Iraq (suspected) |
|        | December 31 | Riviera Sungai Kholok, Thailand | Two bombs were hidden behind loud-speakers of the hotel’s discotheque, and an explosive laden motorcycle detonated at the parking lot | 0 killed 13 injured | Unknown |
|        | December 31 | Marina Sungai kholok, Thailand | A bomb hidden inside a cigarette packet exploded in the discotheque          | 0 killed 14 injured | Unknown            |
**TABLE 1 Continued…**

| Date       | Location      | Event Description                                                                 | Casualties          |
|------------|---------------|-----------------------------------------------------------------------------------|---------------------|
| 2008       |               |                                                                                  |                     |
| January 1  | Presidential  | Port Harcourt, Nigeria                                                            | 12 killed 0 injured | Unknown            |
| January 14 | Serena        | Kabul, Afghanistan                                                                 | 6 killed 6 injured  | Taliban            |
| March 15   | Peshawar, Pakistan | A car bomb detonated in the luxurious CS hotel parking lot                     | 2 killed 16 injured | Unknown            |
| August 20  | Sophie        | Bouira, Algeria                                                                  | 12 killed 15 injured | Al Qaeda in the Islamic Maghreb (suspected) |
| September 20 | Marriott  | Islamabad, Pakistan                                                             | 60 killed 250 injured | Lashkar-e-Jhangvi pro-Al-Qaeda (suspected) |
| November 26–29 | Taj Mahal, Oberoi Trident Hotel | India Mumbai | Six terrorists carrying hand-held weapons forced their way into the hotels | 71 killed- 36 Taj Mahal, 35 Oberoi 250 injured | Lashkar-e-Taiba of Pakistan |
| 2009       |               |                                                                                  |                     |
| June 9     | Pearl Continental Hotel | Peshawar, Pakistan | Three terrorists forced their way into the parking lot and blew up an explosive-laden truck | 16 killed 60 injured | Tehrik-i-Taliban Pakistan |
| July 17    | Marriott, Ritz Carlton | Jakarta, Indonesia | Two suicide bombers detonated explosives simultaneously in the two hotels | 9 killed 42 injured | Jemaah Islamiyah |

as the Marriott and Sheraton, which together have been attacked 10 times since 9/11. Other brands that have been struck include the Hilton, Hyatt, Radisson, Ritz Carlton, Four Seasons, and Days Inn.

**Why Hotels?**

Why are luxury hotels—particularly Western branded properties—suddenly in the terrorists’ crosshairs? The reasons are myriad: First, hotels are symbolic targets of Western affluence and influence that attract precisely the kind of people the militants seek to eliminate—foreign diplomats, businesspeople, tourists, and local elites. Second, luxury hotels, like restaurants, night clubs, shopping malls, and public transportation systems, are “soft targets,” presenting few obstacles to determined terrorists. Indeed, hotels are open environments with multiple points of entrance and egress and a constant flow of traffic, including hotel guests and visitors, staff, merchants, and delivery people. Hotels also lend themselves to preattack reconnaissance, with floor plans, photos, and panoramic video clips of public areas often available over the Internet. Government and military facilities, by contrast, are much more heavily guarded. Even commercial aircraft, the preferred soft target of the 1970s and 1980s, are much better protected since 9/11—though not inviolable, as the Christmas day 2009 attempt against a Detroit-bound Northwest Airlines passenger jet demonstrates.

Third, the terrorists have discovered that a successful attack on a five-star property 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 recruitment. And while these types of “spectaculars” have rarely succeeded in winning the terrorists concessions, they do tend to cause both great harm to a country’s collective psyche and economic disruption, and thereby support the terrorists’ strategic aim of bankrupting the United States and its allies.⁶

A fourth reason for the upsurge in hotel attacks has to do with the changing organizational composition of the terrorist groups themselves. Following the US-led coalition intervention in Afghanistan after 9/11, al Qaeda evolved from a highly centralized organization to a much flatter entity.⁷ Today, the global jihadist movement founded by Osama bin Laden comprises the remnants of the Saudi exile’s al Qaeda organization enconced along Pakistan’s rugged northwest frontier; loosely affiliated regional franchises such as LeT in Pakistan, Jemaah Islamiyah (JI) in Indonesia, and the Abu Sayaaф Group in the Philippines; “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 or in spirit. These affiliated groups typically lack the resources and training to mount a successful attack on a Western embassy or airline, and so have turned their attention to easier targets—hotels (Gunaratna, 2009).

**The Hotel Threat: Déjà vu All Over Again?**

The targeting of hotels by terrorist organizations is not a new phenomenon. Among the earliest such attacks was the 1946 bombing of the King David Hotel in Jerusalem by the Zionist paramilitary organization the Irgun. The blast, aimed at British government and military offices located on the premises rather than hotel guests or staff, killed 91 and injured 46 (Hoffman, 2006). The PLO, as previously mentioned, attacked the Savoy in Tel Aviv in 1975, although the group had a decided preference for hijacking passenger aircraft (Ensalaco, 2008). The Irish Republican Army (IRA) regularly targeted hotels and other commercial enterprises during its campaign of violence against the UK government (Jackson, Dixon, & Greenfield, 2007). And attacks on Spanish hotels and resorts have been a staple of Euskadi Ta Askatasuna’s (ETA) repertoire during its 50-year struggle for an independent Basque homeland (Lutz & Lutz, 2006). But the new wave of post-9/11 attacks on hotels is different in important respects from those of the past. As Yogi Berra might have put it, this is not a case of “déjà vu all over again.”

The leftist and ethnic-separatist terrorist groups that dominated the international scene in the 1970s and 1980s, while determined and ruthless, typically sought to minimize civilian casualties. ETA, for example, often phoned preattack 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). In the famous words of Rand Corporation terrorism expert Brian Jenkins (1975), the politically minded terrorists of past generations wanted “a lot of people watching, not a lot of people dead.”

Al Qaeda and its affiliates do not adhere to the same rules of the game. According to Paul Wilkinson, Chairman of the Advisory Board of the Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St Andrew’s, bin Laden’s 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. It can also be seen in their penchant for mounting secondary attacks on first responders at attack sites and avid interest in unconventional weapons (Wilkinson, 2006).

**Technological Savvy**

But the Islamist 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 terrorists used digital technology to conduct preoperational surveillance of the properties, 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, Ahmed Ali, & Kartikeya, 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).

**Tactical Innovation**

Just as the 9/11 hijackers rewrote the terrorist playbook by flying passenger jets into iconic buildings (rather than
attempting to win concessions such as ransoms or the release of imprisoned comrades), their Islamist disciples have continued to adapt their methods and techniques. Between 9/11 and 2005 the preferred mode of attack was the vehicle-borne improvised explosive device (VBIED) driven by a suicide bomber. This was the modus operandi for the 2002 bombings of the Sheraton and Marriott hotels in Karachi, the 2003 attack on the JW Marriott in Jakarta, and the 2004 assault on the Hilton Hotel and Casino in Tabia, Egypt.

As hotels began to harden their perimeter defenses with check points manned by armed guards, blast walls, barricades, hydraulic barriers, and the like, terrorists have sought out new and innovative modes of attack. The 2008 Mumbai attacks were an obvious attempt to thwart such defenses. So, too, were the July 2009 twin suicide attacks on the JW Marriott and Ritz Carlton in Jakarta, carried out by a pair of JI operatives, one of which had checked into the former property as a guest days prior to the attack (Deutsch, 2009). On the morning of the attacks, the 18-year-old JW Marriott bomber made his way to a lounge in the hotel’s lobby, approached a group of businessmen attending a breakfast meeting, and detonated his backpack IED, killing himself and five others. Moments later, the second bomber detonated his explosive device in a restaurant in the adjacent Ritz-Carlton hotel, killing himself and two others. All told, nine were killed and 42 injured. An unexploded bomb found in the room of the Marriott attacker suggests that an additional blast had been planned (Jerard, Astuti, & Feisal, 2009).

Weighing the New Threat

It has been said in the past that international hotels have been willing to roll out the red carpet to nearly anyone with a decent outfit and money for a cup of coffee. That has begun to change in the aftermath of the recent attacks. Hotel managers and corporate security directors have introduced a wide array of new measures to safeguard their high threat properties—from walk-through metal detectors to bomb-sniffing dogs. The Grand Hyatt Hotel in Jakarta, for example, has security guards inspect all vehicles for explosives before permitting them to approach the entrance, guest baggage is checked for weapons, and everyone—guests, staff, and delivery people—must pass through metal detectors before entering buildings. Other hotels in Jakarta, such as the Hilton and JW Marriott, have gone even further, limiting lobby access only to registered guests (Brady, 2009), while Marriott has outfitted many of its properties in Southeast Asia and the Middle East with shatter-resistant window film, bollards, barriers, explosive vapor detectors (EVDs), and X-ray machines, metal detectors, and bomb-sniffing dogs.

But it is not only business class hotels in politically volatile locations that are taking the terrorist threat more seriously these days. Five-star properties in major US cities have raised their security awareness since Mumbai, with many increasing lobby security and some developing “active shooter” programs to deal with snipers and teams of assassins. Meanwhile, local police in New York, Washington, DC, and other major US cities have begun sharing intelligence with security directors at hotels and providing suggestions on everything from access control to closed circuit television monitoring (Norton, 2009). The threat to US hotels was underscored by the September 2009 FBI and Department of Homeland Security bulletins warning of possible terrorist plots against civilian “soft targets” in the United States, including stadiums, entertainment complexes, and hotels. The alerts followed the arrest of Afghan-American immigrant Najibullah Zazi, a 24-year-old veteran of al Qaeda training camps in Pakistan, for planning a “Mumbai-on-the-Hudson” style attack with hydrogen-peroxide bombs, similar to those used in the 7/7 London bombings (Hoffman, 2010).

The Impetus for Enhanced Security Measures

While the primary impetus for the adoption of enhanced security measures by hotel operators is concern for the safety of their customers and employees, they have also been moved to action by concerns over “reputational risk”—damage to a company’s brand by management’s failure to take reasonable security precautions. Possible litigation brought by families of victims in the aftermath of a terrorist event that could have been foreseen or managed in a more effective manner has also forced hotel executives to concentrate on security (Dubuc, 2009).

The vulnerability of hotels to such litigation was aptly demonstrated when victims and relatives of those killed in the 2004 suicide attack on the Hilton Taba Hotel and Casino on Egypt’s Sinai Peninsula filed a wrongful death lawsuit against the hotel chain. The lawsuit sought damages from Hilton for failing to thwart the suicide bomber who rammed his explosives-filled vehicle into the lobby, killing 33. The plaintiffs, who included over 100 survivors and relatives of victims, sued Hilton in 2006 in the US District Court for the Southern District of New York, claiming that lax hotel security amounted to negligence. A US District Judge later dismissed the case, ruling that Egypt or Israel would be a better forum for the case because the plaintiffs had no connection to the United States (Friedman, 2009).
Finding the right balance between openness and convenience on the one hand, and guest safety and security on the other, is a challenge, says Marriott vice president for global safety and security Alan Orlob, but it is not impossible. And a growing number of hoteliers, large and small, domestic and foreign, are looking to Marriott, the Bethesda, Maryland—based company, for guidance on how to prepare for and manage the evolving terrorism threat. After all, their properties have been struck six times since 9/11.

Marriott International: From Root Beer Stand to Hotel Giant

With over 3,200 hotels in 67 countries and territories and annual sales of more than $13 billion, Marriott International is a giant in the world of hospitality. Founded in 1927 by J. Willard Marriott, the son of Utah sheep herd- ers, the company, originally called Hot Shoppes, Inc., started out as a nine-stool root beer stand in Washington, DC’s Columbia Heights neighborhood. During the 1930s and 1940s, Marriott established his own chain of “Hot Shoppes” cafeteria-style restaurants. Willard’s son, J.W. (Bill) Marriott, Jr., took over the corporate reins in the 1950s and refocused the business on lodging. Under his leadership, Marriott blossomed into a hotel juggernaut, as the post-WWII economic boom sparked a growing demand for affordable lodging, particularly along well-traveled U.S. interstate highways. Nowadays most of the company’s hotels, which include JW Marriott, Ritz Carlton, Residence Inn, Renaissance, and Courtyard, are owned and operated by others through franchise agreements (Rosenwald, 2007).

Overseas Expansion

Marriott’s overseas expansion began in 1993. At the time, it had only a handful of properties outside the United States, but company executives anticipated strong future growth fueled by the spread of free trade and market-oriented reforms throughout the developing world. Believing that safety and security would be key issues for Marriott’s customers as it grew its international footprint—particularly in areas with high crime rates and a recent history of political turmoil—the company’s senior management tapped Orlob to develop a comprehensive crisis management plan, back when few hotels had such programs.14

A former Green Beret with the U.S. Army Special Forces, Orlob embraced the task with gusto. He began by forming a crisis management team capable of dealing with a wide array of contingencies—from government

Security: How Much and What Kind?

While few in the hospitality industry would dispute the need for more robust security at hotels in conflict zones, there is little consensus about what should be done to protect properties in less dangerous environs. Should hotels far removed from the front lines of the War on Terror—say in Seattle or Stockholm—require the same heightened level of security as those in Kabul or Karachi? After all, terrorist attacks on hotels, while on the rise, remain a low risk threat, and guests are far less likely to fall prey to terrorism than to be robbed, assaulted, or injured in a fire (Jenkins, 2009). Meanwhile, the cost of counter-terrorism measures, whether covering windows with shatter-resistant film or deploying EVDs to screen vehicles, can be high. Beyond costs, some executives worry that the presence of visible security measures—be they metal detectors, bomb-sniffing dogs, or gun-toting security guards—may undermine the welcoming ambiance that luxury hotels work hard to cultivate and drive away guests.

While the primary impetus for the adoption of enhanced security measures by hotel operators is concern for the safety of their customers and employees, they have also been moved to action by concerns over “reputational risk”—damage to a company’s brand by management’s failure to take reasonable security precautions.
expropriations to earthquakes. The team spanned the company’s many different divisions and included representatives from human resources, operations, legal affairs, risk management, public relations, and finance. To assist the team, Orlob developed an in-house intelligence capacity led by analysts in Washington, DC, and Hong Kong. These analysts would monitor global developments on a 24/7 basis and provide timely risk assessments. But perhaps most importantly, Orlob devised a three-tiered, color-coded system to alert hotel managers in the Marriott chain of the varying threat levels at specific locations around the world and provide security-related procedures to follow (Orlob, 2004).

Under Marriott’s threat warning system, hotels can be assigned to one of three threat conditions: blue, yellow, or red. Under Threat Condition Blue, hotel managers must verify guests’ identities upon check-in with a photo ID, increase security patrols around properties, and review bomb threat evacuation plans with staff, among other things. Threat Condition Yellow, which could be triggered by a rise in terrorism or political upheaval in the area, requires hotels to check guests entering properties, restrict parking within close proximity to buildings, and halt luggage storage. Finally, under Threat Condition Red, which could result from intelligence indicating a specific threat against a property, hotels must inspect vehicles for explosives at checkpoints, examine luggage, and direct visitors through metal detectors at limited entry points. Adherence to these procedures is ensured by twice-yearly unscheduled visits from third-party auditors, and general managers found to be in noncompliance are subject to harsh disciplinary action.

**Meeting the Evolving Terrorist Threat: What Is to Be Done?**

The first step in meeting the evolving terrorist threat, says Orlob, is acknowledging that even the most robust countermeasures may not defeat an attack. This point was made abundantly clear by the September 2008 suicide truck bombing of the Marriott Hotel in Islamabad. The hotel had formidable antiterrorism 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. Finally, the hotel itself was set back 132 feet from the vehicle inspection point—a distance that exceeded US government standards—to help shield guests and property from a possible blast (Gunaratna, 2008).

Notwithstanding these measures, 56 people died and 270 were injured when a suicide bomber from the al Qaeda affiliate Lashkar-e-Jhangvi detonated his charge after his vehicle slammed into the Delta Barrier. The blast from the powerful 1,320-pound bomb ripped a 25-foot-deep by 60-foot-wide crater in front of the hotel, destroyed most of the upper floor rooms of the property, and ignited a blaze that burned for two days. Had the bomber achieved his goal of ramming the explosive-laden truck into the hotel lobby, the casualty count may have topped one thousand (Gunaratna, 2008).15

**Target Hardening**

Since preventing attacks like those carried out against Marriott in Islamabad and Jakarta is largely impossible once they have reached their operational stage; Orlob believes that hotels need to focus attention on measures that discourage such attacks in the first place, and involve “target hardening.” Although typically associated with visible security measures such as barricades and blast walls, target hardening also entails more subtle methods that often go undetected. For instance, one of the best ways to harden a target, says Orlob, is to limit public disclosure of nonessential information about a property such as building diagrams. Dispatching both plainclothes security officers and uniformed “greeters” to lobby areas to discreetly look for individuals casing buildings or taking suspicious photographs of entrances or security cameras is another.16 Since terrorists often seek employment at hotels as cover for conducting surveillance, a further way to harden targets is to conduct rigorous background

---

**Preventing attacks like those carried out against Marriott in Islamabad and Jakarta is largely impossible once they have reached their operational stage.**

DOI: 10.1002/tie
checks of job candidates to weed out those with criminal records and questionable past associations, although, as Orlob points out, it is often impossible to determine whether a candidate covertly subscribes to a violent political ideology.17

Awareness Training

Training employees to develop a heightened sense of awareness of the types of circumstances that could represent a threat to hotel guests and property—and immediately report them to security personnel—is another counterterrorism imperative. To assist in this endeavor, Marriott has produced a series of colorful “See Something? Say Something!” security awareness posters that are hung in nonpublic areas of its hotels. A poster titled “Back of the House,” for example, encourages food service and maintenance crews to be watchful for individuals photographing the property’s service entrances, as well as for tampered locks and unattended packages; another titled “Guest Room and Guest Floor” instructs housekeeping staff to report the presence of weapons, hotel diagrams, and other suspicious items found in guest rooms.

Designing with Security in Mind

One of the biggest challenges hotel operators face in shielding their guests from possible terrorist attacks is that many existing properties were built with aesthetics, convenience, and cost uppermost in mind—not safety from suicide bombers and urban guerrillas. As such they often have built-in features that make them vulnerable to Mumbai-style assaults including long hallways, spiral staircases, and towering atriums (Bradsher, 2008). They may also be situated close to busy streets, giving terrorists easy access, or within close proximity to embassies or government buildings, leaving them vulnerable to collateral damage from attacks directed elsewhere.

Since retrofitting older buildings for enhanced security is both difficult and expensive, Marriott works with designers and architects at the inception of new projects to ensure that security is given prominence. Requirements for hotels to be built in high threat locations include shatter-resistant window film, walk-through metal detectors, exterior security cameras, bomb-sniffing dogs (where culturally permissible), and hydraulic barriers like those that stopped the al Qaeda truck bomber from leveling the Marriott in Islamabad in 2008. Security features for properties slated for lower risk locations are determined on a case-by-case basis following comprehensive risk assessments.18

Stakeholder Partnerships

Perhaps the most important step in countering the terrorist threat, says Orlob, involves forging closer ties with stakeholders in both government and the private sector. Key partnerships for Marriott include those with local police and first responders. The importance of these relationships was underscored by the Mumbai siege, which was all the more deadly because the Indian National Security Guard commandos that were called in to evacuate the Taj Mahal Palace and Trident Oberoi appeared to be less familiar with the building layouts of these hotels than the terrorists (Rabasa et al., 2009). To prevent this type of catastrophe from occurring at one of its hotels, Marriott requires general managers to provide authorities with detailed photos and floor plans along with contact information for key executives.19 He also believes that hotel staff and government security forces should conduct periodic “familiarization drills” so they understand the hotel’s layout in the event of an emergency.

Marriott’s security chief also believes that hotel chains can benefit from establishing closer interindustry ties and has taken an active role in the US State Department’s Overseas Security Advisory Council’s (OSAC) hotel sector working group. Established in July 2008, the working group, which includes the security directors of at least eight major hotel companies, provides a forum for exchanging information, sharing best practices, and discussing how new technologies can be used to better protect guests and facilities. Already, the partnership has generated positive results; a surveillance detection program in place at the JW Marriott Hotel in Jakarta, Indonesia, was recently successful in interdicting a terrorist organization that was planning attacks on government and private targets.20 As Orlob (2009) told Congress, “We understand that an attack against any hotel in a major city will have a deleterious effect on the city, as well as a wider effect on the entire hotel industry.”

Return on Security Investment?

It is no secret that hospitality industry executives, like those in other sectors, have traditionally viewed security investments as sunk costs that detract from the bottom line, while adding little or nothing to the top (Enz, 2009). Nonetheless, there appears to be growing recognition amongst hospitality executives that securing hotels against terrorism can also bring financial benefits. After all, surveys indicate that guests rank security at the top of their list of priorities when choosing destinations, and are willing to pay a premium for it (Slevitch & Amit,
Reflections on the Evolving Terrorist Threat to Luxury Hotels: A Case Study on Marriott International

and now calls on managers to inquire about a host of terrorism-related issues before recommending specific properties, such as: whether blueprints have been provided to security officials; whether secondary communication systems exist for guests trapped inside rooms in the event of an attack; whether hotel staff have been trained in evacuation techniques; and what surveillance systems are in place to assist authorities in the event of an incident.

The Way Forward: Paradigm Shift?

In the past, hotels and other soft targets have tended to adopt a “bunker mentality” when faced with a rising terrorist threat. While protecting the perimeter continues to be a key imperative, the latest round of suicide and guerrilla-style attacks throughout the Middle East and Asia suggest that it is no longer sufficient, as resourceful terrorists will often find ways to penetrate even the most robust defenses. As such, some observers believe that luxury hotels—particularly those located in high threat locations—need to adopt a new mindset. Gunaratna, for example, believes that international hotels need to begin operating on the principle that terrorist attacks against their facilities are “inevitable” and take action to build resiliency. This involves embedding security into everything from architectural designs to hiring practices, while developing intelligent systems to thwart hostile surveillance, and crafting more effective emergency response plans that involve close collaboration between the government and private sector. Adopting such an approach, however, he cautions, will be neither easy nor cheap and is likely to be resisted by general managers who believe that luxury properties should focus exclusively on terrorism-related issues before recommending specific properties, such as: whether blueprints have been provided to security officials; whether secondary communication systems exist for guests trapped inside rooms in the event of an attack; whether hotel staff have been trained in evacuation techniques; and what surveillance systems are in place to assist authorities in the event of an incident.

Implications for Business Travelers

In view of the rising Islamist threat to international hotels, some private security consultants have begun advising their clients traveling to the Middle East and Southeast Asia to avoid Western five-star brands in favor of smaller, locally owned properties. Stratfor, for example, has advised travelers to “avoid large chain hotels dominated by Western clientele” and instead choose smaller boutique hotels where they will be less conspicuous (Stratfor Global Intelligence, 2009). Some multinational enterprises appear to be heeding this advice. For example, it was reported that ConocoPhilips removed Marriott’s two Jakarta properties from their company’s preferred hotel list following the 2009 suicide attacks in that city (Darson, 2009). However, the notion that Western brands should be avoided is not universally endorsed. Bruce McIndoe, president of Annapolis, Maryland–based iJET Intelligent Systems, emphasizes that terrorism remains a low probability threat to international business travelers—far lower than that of crime or fire—and that international chains typically have higher standards for general safety and security for guests. Moreover, as Orlob (2009) points out, the presence of restaurants, night clubs, fitness centers, and business centers on site at Western branded luxury hotels means that international business travelers seeking these amenities are not forced to venture off the premises, thereby inviting other security risks.

Regardless of where they stay, there is growing consensus that Western travelers visiting high-threat locations should take specific steps to reduce their risk of falling victim to terrorism. These steps, according to Mike Ackerman of the Miami-based Ackerman Group LLC, include choosing hotels situated in walled compounds with robust perimeter security and at a considerable distance from public streets. In addition, he counsels clients to request rooms located away from lobby areas, parking lots, and public-access roads, preferably between the second and sixth floors (to permit firefighter access), and to limit time spent in public areas. The Association of Corporate Travel Executives (2008), meanwhile, updated its advice to business travel managers following the Mumbai attacks and now calls on managers to inquire about a host of terrorism-related issues before recommending specific properties, such as: whether blueprints have been provided to security officials; whether secondary communication systems exist for guests trapped inside rooms in the event of an attack; whether hotel staff have been trained in evacuation techniques; and what surveillance systems are in place to assist authorities in the event of an incident.

Regardless of where they stay, there is growing consensus that Western travelers visiting high-threat locations should take specific steps to reduce their risk of falling victim to terrorism.
maximizing guest comfort and convenience and pursuing profits. Nevertheless, as Gunaratna points out, unless there is a “paradigm shift” in the way hotels around the world conceive of and manage this new and rapidly evolving threat, the lives of their guests and employees, their reputations, and indeed their long-term economic viability will be at risk.

**Implications for IB Theory**

Unlike terrorist organizations themselves, IB thinking on terrorism has evolved very slowly over the past three decades. Writing in the *Journal of International Business Studies* in 1984, Jeffrey D. Simon offered a framework for conceptualizing political risk that remains influential (e.g., Alon et al., 2006; Czinkota et al., 2010). He argued that terrorist attacks 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, stemming from the *host government*. While Simon did not analyze corporate response to political risk in great detail, the implications for MNEs seeking to minimize their exposure to terrorism and sociopolitical violence were fairly straightforward: carefully scan the environment for signs of strife and avoid countries prone to instability and unrest (Kobrin, 1982), delay investments to the extent possible (Rivoli & Salorio 1996), limit their size and scope (Delios & Henisz, 2000), and purchase political risk insurance (Wells, 1998).

Miller (1992) took up the issue of how to conceptualize corporate response to both the types of political risks catalogued by Simon and those of a nonpolitical nature. His framework for integrated risk management identified both financial and strategic approaches for managing environmental uncertainty. The former included activities that could be pursued without altering corporate strategy, such as purchasing insurance and futures contracts, whereas the latter comprised five strategies: avoidance, control, cooperation, imitation, and flexibility. MNEs have traditionally dealt with the terrorist menace by employing the first two of Miller’s five strategies: avoidance and control. Avoidance has typically been achieved by forgoing business opportunities in countries prone to terrorism or locating operations in remote areas of the country, whereas control has been accomplished through investments in security training for executives and perimeter fortifications for facilities (Ackerman, 2008). Taken together, these moves represent what Kapstein (2006) has described as an “enclave strategy.”

The Marriott case suggests that for MNEs involved in the international hotel sector it may be time for a rethink. After all, opting for avoidance may involve ceding promising opportunities in growing markets to competitors, while control 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.

To succeed in this new environment, it is becoming abundantly clear that MNEs need to make Miller’s third strategy (i.e., “cooperation”) a priority. This involves forging ties with a wide range of stakeholders including governmental authorities at various levels, police forces, and even industry competitors through business associations and informal networks to share information on emerging threats and develop security-related best practices. Some of these alliances may be ad hoc and short-lived, whereas others may be more enduring. An example of the latter is the Customs-Trade Partnership Against Terrorism (C-TPAT), a voluntary public–private partnership initiative launched by US Customs and Border Protection in November 2001, that offers the promise of expedited customs clearance and fewer inspections to importers that conduct security audits of their supply chains and correct vulnerabilities that could be exploited by terrorists. The program, which had swollen to over 8,000 members by 2010, has already led to an improvement in global trade security and is delivering tangible financial benefits for its member companies (US Customs and Border Protection, 2011).

But strategic cooperation may also involve other forms of collaboration such as inviting outsiders such as the media to participate in scenario planning sessions, war-game simulations, and other strategic forecasting exercises to help firms identify specific vulnerabilities and think creatively about possible solutions (Pollard & Hotho, 2006). As research on multistakeholder partnerships between MNEs and non-governmental organizations suggests, these alliances can help enhance firm legitimacy and reduce risks while serving as a source of creativity and innovation that lead to new business opportunities (Hart & Sharma, 2004).

MNEs also need to make Miller’s fifth strategy (i.e., “flexibility”) a strategic priority. What this means will vary from industry to industry. For global manufacturers it may involve diversification of suppliers, inventory management, and contingency transportation planning (Sheffi, 2005). For hotel chains like Marriott, flexibility involves attention to business continuity planning (BCP), namely, devising specific guidelines for managing a crisis. BCP may involve everything from mirroring data to...
establishing emergency building evacuation procedures. Such plans must be regularly audited, tested, and refined, so that they can be executed with precision when needed. The critical importance of the BCP process was laid bare on 9/11 in the contrasting fortunes of two financial services companies headquartered in the World Trade Center (WTC): Morgan Stanley and Cantor Fitzgerald. The former escaped the tragedy relatively unscathed, with all but 13 of its 2,700 employees surviving the attacks (Ripley, 2008), whereas the latter lost more than two thirds of its 960 employees, including its entire board of directors, president, vice chairman, chief operating officer, and chief financial officer (Parrett, 2007). A key difference: Morgan Stanley had implemented a state-of-the-art disaster contingency plan after the first attempt on the WTC in 1993 and was prepared for the possibility of a future attack.

Terrorist attacks on corporations are likely to be a permanent feature of the international business landscape, and the hospitality industry is clearly at risk. But the outlook is not necessarily bleak. By taking a proactive approach to security and making cooperation and flexibility centerpieces of corporate strategy, MNEs have much to gain. They can reduce their exposure to attack, protect lives and assets, enhance enterprise resilience, and satisfy shareholder and stakeholder demands for greater care and due diligence. And to the extent that customers begin to place more value on safety in the face of heightened risks and uncertainties, companies regarded as security leaders stand to reap significant financial benefits.

Notes
1. A 2007 survey of 154 board-level executives of MNEs conducted by Lloyd's and the Economist Intelligence Unit (EIU) found that 43 percent of the respondents identified violent groups with religious motivations as likely to pose the greatest threat to their business over the next five years.

2. Although Westerners were specifically targeted—including Jews and American and British passport holders—local elites were not spared; the general manager of the Taj Mahal Palace and Tower’s pregnant wife and two young children were among those killed when gunmen stormed the building (Brenner, 2009).

3. According to an Indian government report, the Mumbai police and the National Security Guard required 36,000 bullets to subdue the 10 Lashkar-e-Taiba gunmen, whereas the terrorists killed 166 and injured 300 with just 10,500 rounds of ammunition (Dey, 2009).

4. There were also similarities between the Mumbai assault and the 1972 Lod airport attack by members of the Japanese Red Army, which involved an armed assault on a public space using firearms and grenades (Rabasa et al., 2009), and the 1993 New York landmarks plot, which called for raids by teams of heavily armed assassins on the Waldorf Astoria, St. Regis, and United Nations Plaza hotels, along with bombings of the Lincoln and Holland tunnels (Stratfor Global Intelligence, 2009).

5. Stratfor defines a major attack as one in which one or more IEDs were detonated or a hotel received rocket or mortar fire; an armed assault (like Mumbai); or a non-IED rocket attack that resulted in casualties.

6. Former al Qaeda leader Osama bin Laden was very explicit about his strategic aim of defeating the West by crippling its economy: “We were patient fighting the Soviet Union with small humble arms for ten years, we depleted their economy till they vanished, all grace be to Allah. You should take a lesson from that, we will be patient fighting you, Allah’s willing, till either one of us dies” (Weimann, 2009).

7. Some contend that al Qaeda today is not an organization in the formal sense, but a “networked transnational constituency” (Hoffman, 2006), a “leaderless network” (Sageman, 2008), a “missionary enterprise” (Jenkins, 2007), 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).

8. Among the IRA’s favorite targets was the Hotel Europa in Belfast, which it bombed more than 30 times during its heyday (Wylie, 2001).

9. Suicide missions are typically more accurate and lethal than conventional attacks because the attackers make last minute adjustments and penetrate deeper into target zones. The result is that suicide attacks cause an average of 12 fatalities per incident, whereas non-suicidal attacks kill less than one person per incident on average (Pape, 2006). And while it is true, as Pape (2006) points out, that many suicide bombers are secular nationalists rather than religious extremists, it also appears to be the case that al Qaeda and its Islamist ideology are responsible for the growing popularity of the suicide missions, the rise in the number of organizations embracing the tactic, and the sharp increase in attacks on civilians (Mohaghad, 2008).

10. Authorities believe the JW Marriott bomber assembled his IED in his guest room with material smuggled into the hotel by a confederate who worked on the premises as a florist. The Ritz Carlton bomber, meanwhile, is thought to have gained access to the hotel complex by posing as an assistant to the very same florist, who was reportedly killed in a raid by police a month after the attacks (Jerard et al., 2009).

11. Interview, Alan Orlob, Marriott International Vice President Corporate Security, December 24, 2009.

12. Indeed, the cost of a single EVD unit is roughly $25,000, and large hotels with multiple entrances typically require several units (Jerard et al., 2009).

13. Marriott has been approached by numerous hotel chains for security-related advice and suggestions and it has shared information and best practices so that others can benchmark against their own programs.

14. Interview, Alan Orlob, Marriott International Vice President Corporate Security, July 25, 2010.

15. Some 1,500 people were inside the hotel at the time of the bombing, many of them non-registered guests packed into the property’s restaurants and ballroom to celebrate Iftar, the breaking of the Ramadan fast (Gunaratna, 2008).

16. In addition to enhancing security, the deployment of greeters may have customer service benefits, as guests may interpret the attentiveness of hotel staff as an attempt to “go the extra mile” (Spadanuta, 2009).

17. Interview, Alan Orlob, Marriott International Vice President Corporate Security, December 24, 2009.

18. Interview, Alan Orlob, Marriott International Vice President Corporate Security, December 24, 2009.

19. This information is typically stored on a secure server and supplied to authorities following an attack. Interview, Alan Orlob, Marriott International Vice President Corporate Security, December 24, 2009.

20. Interview, Alan Orlob, Marriott International Vice President Corporate Security, July 25, 2010.

21. Interview, Mike Ackerman, the Ackerman Group LLC, December 24, 2009.

References

Ackerman, M. (2008). Counterterrorism strategies for corporations. Amherst, NY: Prometheus Books.

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

Alexander, Y., Valton, D., & Wilkinson, P. (1979). Terrorism: Theory and practice. Boulder, CO: Westview Press.

Alon, I, Gurumoorthy, R., Mitchell, M. C., & Steen, T. (2006). Managing micropolitical risk: A cross-sector examination. Thunderbird International Business Review, 48(5), 625-642.

Association of Corporate Travel Executives. 2008. Mumbai Attacks Encourage Risk Management by Business Travel Managers. Retrieved December 9, 2009, from www.acte.org/docs/ACTE_Traveler_Safety_Recommendations_Dec_2008.pdf

Bakshi, N., & Gans, N. (2010). Securing the containerized supply chain: Analysis of government incentives for private investment. Management Science, 56(2), 219–233.

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

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

Bradsher, K. (2008, December 1). Analysts say it will be difficult to shield luxury hotels from terrorist attacks. New York Times. Retrieved November 30, 2009, from www.nytimes.com/2008/12/01/world/asia/01hotel.html

Brady, S. (2009, February). Wake-up call: Lessons learned from Mumbai. Condé Nast Traveler. Retrieved November 30, 2009, from www.concierge.com/cntraveler/articles/500281

Bremer, M. (2009, November). Anatomy of a siege. Vanity Fair. Retrieved November 30, 2009, from www.vanityfair.com/politics/features/2009/11/taj-hotel-siege-200911

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

Chambers, D., Wernick, D., Zdanowicz, J., & Von Glinow, M. (2010). How dangerous are measurement errors to homeland security? Thunderbird International Business Review, 52(6), 553–569.

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., Liesch, P. W., & Steen, J. (2010). Terrorism and international business: A research agenda. Journal of International Business Studies, 41, 826–843.

Czinkota, M. R., & Ronkainen, I. A. (2009). Trends and indications in international business: Topics for future research. Management International Review, 49(2), 249–265.

Darson, L. (2009, September 2). Travel managers fret over security. The Transnational: A Multinational Travel Newsletter. Retrieved December 7, 2009, from www.thetransnational.travel/news.php?cid=Marrriott-hotel-risk-security.Sep-09.02

Delios, A., & Henisz, W. J. (2000). Japanese firms’ investment strategies in emerging economies. Academy of Management Journal, 43, 305–323.

Deutsch, A. (2009). Jakarta hotel florist plotted deadly bombings. Retrieved December 7, 2009, from http://abcnews.go.com/International/wireStory?id=8307976

Dey, J. (2009, November 27). 36,000 bullets to kill 9 terrorists. Mid-Day. Retrieved December 9, 2009, from www.mid-day.com/news/2009/nov/27/1109-26-11-Lashkar-e-Taiba-men-mumbai-terror-attack-Ajm
al-Qasab.htm

Dubuc, C. (2009, October 3). A wake up call, the shadow of 9/11: Terrorism and premises liability for hotels. Hospitality.net, Retrieved December 9, 2009, from www.hospitalitynet.org/news/15/4003020/403562 .search?query=shadow+of+9%2F11%3a+terrorism+and+premises+liabiliy+

Dunford, R., & Palmer, I. (2002). Managing for high performance? People management practices in flight centre. Journal of Industrial Relations, 44(3), 376–396.

The Economist. (2008, July 19). Winning or losing? A special report on al-Qaeda. Retrieved December 9, 2009, from www.nytimes.com/2008/12/01/world/asia/01hotel.html

Enderwick, P. (2001). Terrorism and the international business environment. AIB Insights, Special Electronics Issue, pp. 1–5.

Ensallaco, M. (2008). Middle Eastern terrorism. Philadelphia, PA: University of Pennsylvania Press.

Enz, C. A. (2009). The physical safety and security features of U.S. hotels. Cornell Hospitality Quarterly, 50(4), 553–560.

Friedman, R. (2009). Tabo attacks survivors sue Hilton Hotels. Jerusalem Post. Retrieved December 10, 2009, from www.jpost.com/servlet/Satellite?cid=1259243053914&pagename=JPArticle%2FShowFull...
Gittel, J. H., Cameron, K., Lim, S., & Rivas, V. (2008). Airline industry responses to September 11th. In R. J. Burke & C. L. Cooper (Eds.), International terrorism and threats to security: Managerial and organizational challenges. Cheltenham, England: Edward Elgar.

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

Goldberg, J. E. (1990). The terrorist threat to corporations. In G. S. Roukis, H. Conway, & B. H. Charnov (Eds.), Global corporate intelligence: Opportunities, technologies, and threats in the 1990s (pp. 179–193). Westport, CT: Quorum Books.

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. Retrieved November 30, 2009, from www.psvr.org/pdf/GlobalAnalysis/MumbaiAttacks.pdf

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

Hart, S. L., & Sharma, S. (2004). Engaging fringe stakeholders for competitive imagination. Academy of Management Executive, 18(1), 7–18.

Harvey, M. G. (1985, January–February). A new corporate weapon against terrorism. Business Horizons.

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

Henisz, W. J., Mansfield, E. D., & Von Glinow, M. (2010). Conflict, security, and political risk: International Business in challenging times. Journal of International Business Studies, 41, 759–764.

Herbner, B., Elliot, D., & Schwartz, E. M. (2004). Business continuity management: Time for a strategic role? Long Range Planning, 37, 435–457.

Hoffman, B. (2006). Inside terrorism (2nd ed.). New York, NY: Columbia University Press.

Hoffman, B. (2010, April 20). American jihad. National Interest Online. Retrieved July 31, 2010, from www.nationalinterest.org/Article.aspx?id=23200

Homer-Dixon, T. (2002, January–February). The rise of complex terrorism. Foreign Policy, pp. 52–62.

Howell, L. D. (2001). Dealing with Political Risk: A Manager’s Toolkit. In L. D. Howell (Ed.), Political Risk Assessment: Concept, Method, and Management. East Syracuse, NY: The PRS Group, Inc., 167–188.

Jackson, B. A., Dixon, L., & Greenfield, V. A. (2007). Economically targeted terrorism: A review of the literature and a framework for considering defensive approaches. Santa Monica, CA: RAND Center for Terrorism Risk Management Policy.

Jain, S., & Grose, R. (2009). Impact of terrorism and security measures on global business transactions: Some international business guidelines. Journal of Transnational Management, 14(1), 42–73.

Jenkins, B. (1975). International terrorism: A new mode of conflict. In D. Carlton & C. Schaefer (Eds.), International terrorism and world security (pp. 13–49). London, England: Croom Helm.

Jenkins, B. (2007). Introduction. In J. O. Ellis (Ed.), Terrorism: What’s coming, the mutating threat. Oklahoma City, OK: Memorial Institute for the Prevention of Terrorism.

Jenkins, B. (2009). Terrorists can think strategically: Lessons learned from the Mumbai attacks. Statement Before the Committee on Homeland Security and Governmental Affairs, United States Senate, Hearing on Lessons from the Mumbai Terrorist Attacks.

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

Kapstein, E. (2006, March 17). Avoiding unrest in a volatile environment, in Mastering Uncertainty, a four-part weekly supplement to The Financial Times, Part 1: “Seeking Shelter from the Storm.”

Kobrin, S. J. (1982). Managing political risk assessment: Strategic response to environmental change. Berkeley, CA: University of California Press.

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

Kovský, S. (1990). Corporate terrorism: A new global threat. Management Review, 79(10), 39–42.

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

Kunreuther, H., & Pauly, M. (2005). Terrorism loses and all perils insurance. Journal of Insurance Regulation, 23(4), 3–19.

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

Lagadec, P. (2008). A new cosmology of risks and crises: Time for a radical shift in paradigm and practice. Review of Policy Research, 25(4), 473–486.

LaPorte, T. F. (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. Charlotte, NC: Information Age.

LaRaia, W., & Walker, M. (2009). The siege in Mumbai: A conventional terrorist attack aided by modern technology. In M. R. Haberfeld & A. Hassell (Eds.), A new understanding of terrorism: Case studies, trajectories and lessons learned. New York, NY: Springer.

Liesch, P., Steen, J., Knight, G., & Czinkota, M. R. (2006). Problematizing the internationalization decision: Terrorism-induced risk. Management Decision, 44(6), 809–823.

Liu, D., & Lin, C. (2008). Human resources planning on terrorism and crises in the Asia Pacific region: Cross-national challenges, reconsideration, and proposition from Western experiences. Human Resource Management, 47(1), 49–72.

Lloyd’s and The Economist Intelligence Unit. (2007). Under attack: Global business and the threat of political violence. www.lloyds.com/\NR/rdonylrees/0926E705-A16C-4432-B067-A9925A9EFEAB/0/360terrorismreport.pdf

Lutz, J. M., & Lutz, B. J. (2006). Terrorism as economic warfare. Global Economy Journal, 0(2), 1–20.

Maddox, R. C. (1990). Terrorism’s hidden threat and the promise for multinational corporations. Business Horizons, 33(6), 48–52.

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

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, B., & Raab, J. (2009). Dark networks and the problem of Islamic jihadist terrorism. In D. F. Kettl & S. Goldsmith (Eds.), Unlocking the power of networks: Keys to high-performance government. Washington, DC: Brookings Institution Press.

Mitroff, I. I., & Alpaslan, M. C. (2003). Preparing for evil. Harvard Business Review, 81(4), 109–115.

Moghaddam, A. (2008). The globalization of martyrdom. Baltimore, MD: Johns Hopkins University Press.

Myers, P. (2009). News flash: In-security. Connect: The Business Traveler Magazine of Carlson Wagonlit Travel. Retrieved November 30, 2009, from http://connectctw.com/2009/10/01/news-flash-6/

Norton, M. L. (2009). Statement before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, Hearing on lessons from the Mumbai terrorist attacks.

Orlob, A. (2004). Protecting soft targets—the JW Marriott Jakarta case study. Journal of Homeland Security and Emergency Management, 1(3), 304.

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). Inside terrorism (2nd ed.). New York, NY: Random House.

Pape, R. A. (2006). Dying to win: the strategic logic of suicide terrorism. New York, NY: Random House.
additional assessment 1968–80. The ANNALS of the American Academy of
Public Personnel Management, 34(2), 175–192.

Pollard, D., & Hotho, S. (2006). Risks, scenarios, and the strategic management process. Decision Management, 44(6), 721–736.

Rabasa, A., Blackwill, D. R., Chalk, P., Cragin, K., Fair, C. C., Jackson, B. A., ... Tellis, A. J. (2009). The lessons of Mumbai. Santa Monica, CA: Rand Corporation.

Ricart, J., Enright, M., Ghemawat, P., Hart, S., & Khanna, T. (2004). New frontiers in international strategy. Journal of International Business Studies, 35(3), 175–183.

Richardson, H. W., Gordon, P., & Moore, J. E. II. (2009). Global business and the terrorist threat. Cheltenham, England: Edward Elgar.

Ripley, A. (2008). The unthinkable: Who survives when disaster strikes and why. New York, NY: Crown.

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

Rollins, J., & Wyler, L. S. (2010). International terrorism and transnational crime: Security threats, U.S. policy, and considerations for Congress. Congressional Research Service. Retrieved August 1, 2010, from http://fas.org/sgp/crs/terror/R41004.pdf

Rosenwald, M. (2007, July 1). Root beer roots. Retrieved December 9, 2009, from www.washingtonpost.com/wp-dyn/content/article/2007/06/26/AR2007062601413.html

Sageman, M. (2008). Leaderless jihad. Philadelphia, PA: University of Pennsylvania Press.

Sheffi, Y. (2005). The resilient enterprise. Cambridge, MA: MIT Press.

Shrader, R., & McConnell, M. (2002). Security and strategy in the age of discontinuity: A management framework for the post-9/11 world. Strategy + Business, 26, 1–12.

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

Slevitch, L., & Amit, S. (2008). Management of perceived risk in the context of destination choice. International Journal of Hospitality and Tourism Administration, 9(1), 85–102.

Slovic, P. (2002). Terrorism as hazard: A new species of trouble. Risk Analysis, 22(3), 425–426.

Smith, D., & Fishbacher, M. (2009). The changing nature of risk and risk management: The challenges of borders, uncertainty and resilience. Risk Management, 11(1), 1–12.

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.

Sarr, R., Newfrock, J., & Delurey, M. (2003). Enterprise resilience: Managing risk in the networked economy. Strategy + Business, 50, 1–10.

Stratfor Global Intelligence. 2009. Special security report: The militant threat to hotels. Austin, TX. Retrieved November 30, 2009, from www.stratfor.com/needtoknow/STRATFORMilanHotels.pdf

Suder, G. S. (Ed.). (2004). Terrorism and the international business environment: The security-business nexus. Cheltenham, England: Edward Elgar.

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

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

Sullivan-Taylor, B., & Wilson, D. (2009). Managing the threat of terrorism in British travel and leisure organizations. Organization Studies, 30(2/3), 251–262.

Tan, W., & Enderwick, P. (2006). Managing threats in the global era: The impact and response to SARS. Thunderbird International Business Review, 48(4), 515–536.

Unnikrishnan, C., Ahmed Ali, S., & Karikkeya. (2009, February 22). 26/11 calls traced to pak serving colonel. Times of India. Retrieved November 30, 2009, from http://timesofindia.indiatimes.com/india/26/11-calls-traced-to-Pak-serving-colonel/articleshow/4190923.cms

Urry, J. (2005). Global complexity. Cambridge, England: Polity Press.

US Customs and Border Protection. (2010). Customs-Trade Partnership Against Terrorism: 2011 Costs & Savings Survey. Retrieved May 25, 2012, from www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_news_reports/2011_cost_savings.ctt/2011_cost_savings.pdf

Weimann, G. (2009, June 4). War by other means: Econo-Jihad. YaleGlobal. Retrieved July 1, 2010, from http://yaleglobal.yale.edu/content/econo-jihad. Accessed 1 July 2010.

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

Wernick, D. (2006). Terror incognito: International business in an era of heightened geopolitical risk. In G. Suder (Ed.), Corporate strategies under international terrorism and adversity (pp. 59–82). Cheltenham, England: Edward Elgar.

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

Wylie, I. (2001). He’s Belfast’s security blanket. Fastcompany.com. Retrieved November 30, 2009, from www.fastcompany.com/print/5415

Zelinsky, A., & Shubik, M. (2007). Terrorist groups as business firms: A new typological framework. Social Science Research Network. Retrieved September 1, 2008, from http://ssrn.com/abstract=959258