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

Abstract

The advent of global terrorist networks represents a challenge to international business (IB) theory. Traditionally conceptualized as a type of political risk experienced by MNEs with operations 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. This paper examines the changing nature of the terrorist threat and the implications for a sector that has been a target of recent attacks: the international 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, and property. Implications for IB theory and practice are drawn.

INTRODUCTION

The advent of global terrorist networks represents a challenge to international business (IB) theory. To the extent that IB scholars have examined the phenomena of terrorism at all, most have viewed it through the prism of political risk (Simon, 1984), treating it as a micro-level threat primarily afflicting multinational enterprises (MNEs) operating in politically conflictive areas and engaged in natural resource extraction (Alon, Mitchell, & Steen, 2006; Phatak, Bhagat, & Kashlak, 2004). And while this conceptualization may have been appropriate for the parochial terrorist groups of the 1970s and 1980s, which targeted oil pipelines and infrastructure as part of their campaigns against Western imperialism, it is now anachronistic. The terrorist groups that dominate the international scene today differ from their predecessors in motivations, strategy, tactics, and form. Moreover, as this case study demonstrates, these dark networks (Milward & Raab, 2009) are increasingly broadening their targets to include places where international business executives, tourists, and regular citizens convene, such as luxury hotels. 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.

The Mumbai Attacks:

Transnational terrorism struck the international hotel industry with a vengeance in 2008. On Thanksgiving day, a team of ten highly trained assassins, armed with assault rifles, submachine guns, hand grenades, along with satellite phones, BlackBerries, and other high tech devices, launched a three-day siege in Mumbai, India's financial and entertainment capital, killing 166 and injuring 300. Among their targets were two of the city's landmark five-star properties: the Taj Mahal Palace and Tower and the Oberoi Trident complex. Western tourists and businesspeople appear to have been singled out by the assailants for execution, and the final death toll included 28 foreign nationals, six of which were Americans (Rabasa et al., 2009).[1]

After storming the landmark properties, the Lashkar-e-Taiba (LeT) gunmen fired on guests and staff, hurled grenades down staircases, set off improvised explosive devices (IEDs), took hostages as human shields, set fires, and engaged the Indian security forces in firefights. Throughout the siege the assailants received tactical guidance via mobile phone from their controllers in Pakistan, enabling them to navigate the properties with deadly precision. The net result was devastating: three dozen killed at the Taj, scores more wounded, and untold millions of dollars in damage to the colonial-era property. 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, head of the Singapore-based International Centre for Political Violence and Terrorism Research (ICPVTR), has noted (2009), 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,[2] 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).[3]

Nor was the targeting of luxury hotels unusual. According to Stratfor, an Austin, Texas-based security consultancy, the number of major terrorist attacks[4] against hotels around the world has more than doubled in the eight years since 9/11, from 30 to 62, while the number of different countries affected has jumped to 20 from 15 (Stratfor, 2009). Meanwhile, the toll of persons killed and injured in such attacks has increased roughly six-fold during this period. Among the favored targets of the Islamist militants responsible for the lion's share of incidents have been Western-branded luxury hotels such as the Marriott and Sheraton, which together have been attacked 10 times since 9/11. Other brands that have been struck include Hilton, Hyatt, Radisson, Ritz Carlton, Four Seasons, and Days Inn. Figure 1 lists international hotels that have been attacked since 9/11.

****

Figure 1 goes about here

****

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 pre-attack 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 5-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 from enemy governments, they do tend to cause both great harm to a country's collective psyche and economic disruption, and thereby support al Qaeda's strategic aim of bankrupting the U.S. and its allies (Hoffman & Weimann, 2009).

A fourth reason for the upsurge in hotel attacks has to do with the changing organizational composition of the terrorist groups themselves. Following the U.S.-led coalition intervention in Afghanistan after 9/11, al Qaeda evolved from a highly centralized organization to a much flatter entity.[5] Today, the global jihadist movement founded by Osama bin Laden comprises the remnants of the Saudi exile's al Qaeda organization ensconced along Pakistan's rugged northwest frontier, loosely affiliated regional franchises such as LeT in Pakistan, Jemaah Islamiyah (JI) in Indonesia, and the Abu Sayaaf 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

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 U.K. government (Jackson et al., 2007).[6] 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.

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 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). In the famous words of Rand Corp. terrorism authority 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 Andrews, 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.[7] 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 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).

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 from enemy governments), 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 Taba, 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 et al., 2009).[8]

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" (The Associated Press, 2009). 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 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.[9]

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 U.S. 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, D.C., and other major U.S. 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 U.S. 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 U.S., including stadiums, entertainment complexes, and hotels. The alerts followed the arrest of Afghan-American immigrant Najibullah Zazi, a 24-year-old high veteran of al Qaeda training camps in Pakistan, for planning a series of attacks on a major U.S. city with hydrogen-peroxide bombs, similar to those used in the 7/7 London bombings (Bergen, 2009).[10]

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, employees, and properties, 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 precautions against a terrorist attack. 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 by an act of industrial sabotage more than two decades ago. On New Year's Eve in 1986, three disgruntled employees of the DuPont Plaza Hotel in San Juan, Puerto Rico decided to exact revenge on management for a labor dispute by setting a small fire in a ballroom to frighten guests and drive down occupancy rates. Tragically, the small fire turned into a raging inferno that led to 97 deaths and 150 injuries. The litigation that followed this incident produced nearly $2 billion in claims and remains one of the largest civil cases in history (Willis North America, 2009).

More recently, victims and relatives of those killed in the 2004 suicide attack on the Hilton Taba Hotel and Casino on Egypt's Sinai Peninsula have filed a wrongful death lawsuit in Jerusalem against the Hilton Hotel chain for failing to thwart the suicide bomber who rammed his explosives-filled vehicle into the lobby, killing 33. The plaintiffs, who include over 100 survivors and relatives of victims, sued Hilton in 2006 in the U.S. District Court for the Southern District of New York, claiming that lax hotel security amounted to negligence, but in 2008 a U.S. District Judge ruled that Egypt or Israel would be a better forum for the case because the plaintiffs had no connection to the United States (Friedman, 2009).

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. Brian Jenkins (2009), for example, has observed that fewer than 500 hotel guests worldwide have been killed by terrorists over the past 40 years, out of a total global hotel guest population at any time of nearly 10 million. Meanwhile, the cost of counter-terrorism measures, whether covering windows with shatter-resistant film or deploying EVDs to screen vehicles, can be high.[11] 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.

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 herders, the company, originally called Hot Shoppes, Inc., started out as a nine-stool root beer stand in the Columbia Heights neighborhood of Washington, D.C. (Marriott, 2003). During the 1930s and 1940s, Marriott established his own chain of "Hot Shoppes" cafeteria-style restaurants, serving cold drinks and hot meals. 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 U.S., 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, the company's senior management tapped Orlob to develop a comprehensive crisis management plan, back when few hotels had such programs.

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 expropriations to earthquakes. The team spanned the company's many different divisions and included representatives from human resources, operations, legal, risk management, public relations, and finance. To assist the team, Orlob developed an in-house intelligence capacity led by analysts in Washington, D.C. 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 non-compliance 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, which had been dubbed by Gunaratna 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. Finally, the hotel itself was set back 132 feet from the vehicle inspection point – a distance that exceeded U.S. 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 explosives-laden truck into the hotel lobby, the casualty count may have topped one thousand (Gunaratna, 2008).[12]

Target Hardening

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 non-essential 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.[13] Since terrorists often seek employment at hotels as cover for conducting surveillance, a further way to harden targets is to conduct rigorous background checks of job candidates to weed out those with criminal records questionable past associations, although, as Orlob points out, it is often impossible to determine whether a candidate covertly subscribes to a violent political ideology.[14]

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 counter-terrorism imperative. To assist in this endeavor, Marriott has produced a series of colorful "See Something? Say Something!" security awareness posters that are hung in non-public 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.[15]

Partnerships with Other Stakeholders

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.[16] He also believes that hotel staff and government security forces should conduct periodic “familiarization drills” so they understand the hotel’s layout and in the event of an emergency.

Marriott’s security chief also believes that hotel chains can benefit from establishing closer inter-industry ties and has taken an active role in the U.S. 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. As Orlob (2009) recently 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, 2008). And while few hotels currently call attention to the security features of their hotels let alone market them, this may change in the future – especially if attacks continue to increase in scope and intensity. As Orlob observes, "People visiting (high risk) environments aren't looking for the softest beds now, or the best meeting space; they're looking for the best security. If you invest in security, you'll get the customers (Meyers, 2009)."

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, 2009). Likewise, Jack Cloonan, a special agent for the FBI's Osama bin Laden unit from 1996 to 2002, believes that Westerners traveling to places like Indonesia and Pakistan should avoid "marquee names" (Goldman, 2009). Some multinational enterprises appear to be heeding their advice.[17]

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 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 (Orlob, 2009). "Overall, it's best to stay in four or five star hotels, which cater to VIPs that demand higher security precautions," says McIndoe.

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 travelers 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.[18] The Association of Corporate Travel Executives, 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 (ACTE, 2008).

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 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 scarcely evolved over the past 25 years. Writing in the Journal of International Business Studies in 1984, Jeffrey D. Simon offered a framework for conceptualizing political risk that remains influential. According his framework, 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, 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 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 investment insurance, multilateral guarantees, and political risk insurance (Wells 1998).

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. 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 latter often accomplished through heavy investments in perimeter security.

The Marriott case suggests that for MNEs – especially those involved in the international hotel sector -- it may be time for a re-think. 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. To succeed in this new environment, it is becoming abundantly clear that MNEs need to reach out to governments, other stakeholders and even competitors to form partnerships and alliances that may help them understand the nature of the threat, analyze their specific vulnerabilities, and take action to thwart potential attacks. MNEs must also build flexibility and resilience into their operations, so that if and when an attack does occur, systems are in place to manage the crisis, mitigate loss of life, and assist with the recovery process.

Figure 1 – Selected Terrorist Attacks on International Hotels Since 9/11

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	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)
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	Bali, 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 loudspeakers of the hotel's discotheque, and a 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
2008					
January 1	Presidential	Port Harcourt, Nigeria	A gunmen killed civilians that were returning from mass to the hotel	12 killed 0 injured	Unknown
January 14	Serena	Kabul, Afghanistan	Three militants opened fire on security guards with guns and hand grenades on the perimeter of the hotel	6 killed 6 injured	Taliban
March 15	Cs Pattani	Pattani Province, Thailand	A car bomb detonated in the luxurious CS hotel parking lot	2 killed 16 injured	Unknown
August 20	Sophie	Bouira, Algeria	A bomb was detonated near the hotel as a passenger bus drove by	12 killed 15 injured	Al Qaeda in the Islamic Maghreb (suspected)
September 20	Marriott	Islamabad, Pakistan	A truck bomber carrying about one ton of explosives blew the truck up at the gate	60 killed 250 injured	Lashkar-e-Jhangvi pro-Al-Qaeda (suspected)
November 26-29	Taj Mahal, Oberoi Tridient	India Mumbai	Six terrorists carrying hand-held weapons forced	71 killed- 36 Taj Mahal, 35 Oberoi	Lashkar-e-Taiba of Pakistan

	Hotel		their way into the hotels	250 injured	
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

References

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.

Bergen, P. 2009. *Reassessing the evolving al Qaeda threat to the homeland*. Statement before the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, United States House of Representatives.

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

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

Brady, S. 2009. Wake-up call: lessons learned from Mumbai. *Condé Nast Traveler*, February. http://www.concierge.com/cntraveler/articles/500281. Accessed 30 November 2009.

Brenner, M. 2009. Anatomy of a siege. *Vanity Fair*, November. http://www.vanityfair.com/politics/features/2009/11/taj-hotel-siege-200911. Accessed 30 December 2009.

Darson, L. 2009. Travel managers fret over security. *The Transnational: A Multinational Travel Newsletter*, 2 September. http://www.thetransnational.travel/news.php?cid=Marriott-hotel-risk-security.Sep-09.02. Accessed 7 December 2009.

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. http://abcnews.go.com/International/wireStory?id=8307976. Accessed 7 December 2009.

Dey, J. 2009. 36,000 bullets to kill 9 terrorists. *Mid-Day*, 27 November. http://www.mid-day.com/news/2009/nov/271109-26-11-Lashkar-e-Taiba-men-mumbai-terror-attack-Ajmal-Qasab.htm. Accessed 9 December 2009.

Dubuc, C. 2009. A wake up call, the shadow of 9/11: terrorism and premises liability for hotels. *Hospitality.net*, 3 October. http://www.hospitalitynet.org/news/154000320/4043562.search?query=shadow+of+9%2f11%3a+terrorism+and+premises+liability+. Accessed 9 December 2009.

The Economist. 2008. Winning or losing? A special report on al-Qaeda. 19 July, 3-12.

Ensalaco, M. 2008. *Middle Eastern terrorism*. Philadelphia: 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. Taba attacks survivors sue Hilton Hotels. *Jerusalem Post*. http://www.jpost.com/servlet/Satellite?cid=1259243055914&pagename=JPArticle%2FShowFull. Accessed 10 December 2009.

Goldman, R. 2009. Are U.S. owned hotels terror targets? *ABC News*, 17 July. http://abcnews.go.com/print?id=8112518. Accessed 30 November 2009.

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. http://www.pvtr.org/pdf/GlobalAnalysis/MumbaiAttacks.pdf. Accessed 30 November 2009.

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

Hoffman, B. & Weimann, G. 2009. Econo-jihad. *National Interest Online*, 13 May. http://www.nationalinterest.org/Article.aspx?id=21464. Accessed 30 November 2009.

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

Jenkins, B. 1975. International terrorism: a new mode of conflict. In D. Carlton and C. Schaerf (Ed), *International terrorism and world security:* 13-49. London: 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 Marriot and Ritz Carlton, Jakarta*. Nanyang Technological University, Singapore: International Centre for Political Violence and Terrorism Research.

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:* 309. NY: Springer New York.

Lutz, J. M. & Lutz, B. J. 2005. Terrorism as economic warfare. *Global Economy Journal.* 6(2): 1-20.

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.

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

Myers, P. 2009. News flash: In-Security. *Connect: The Business Traveler Magazine of Carlson Wagonlit Travel*. http://connectcwt.com/2009/10/01/news-flash-6/. Accessed 30 November 2009.

Neild, B. 2009. Why hotels are tempting targets for terrorists. *CNN.com*, 17 July. http://edition.cnn.com/2009/WORLD/asiapcf/07/17/hotel.attacks/index.html. Accessed 30 November 2009.

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), no. 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. *Dying to win: the strategic logic of suicide terrorism*. New York: Random House.

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

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

Rassler, D. 2009. Al-Qaida's Pakistan strategy. *CTC Sentinel*, 2(6), 1-3.

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

Rosenwald, M. 2007. Root Beer Roots. http://www.washingtonpost.com/wpdyn/content/article/2007/06/26/AR2007062601413.html. Accessed 9 December 2009.

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

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.

Spadanuta, L. 2009. Ensuring an uneventful stay. *Security Management*. http://www.securitymanagement.com/print/5415. Accessed 30 November 2009.

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

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

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.

Willis North America. 2009. Hotel security in an insecure world. *Willis Views*, November. http://www.willis.com/Documents/Publications/Industries/Real_Estate/Views_Nov_09_Real_Estate_Newsletter.pdf. Accessed 30 November 2009.

Wylie, I. 2001. He's Belfast's security blanket. *Fastcompany.com*. http:www.fastcompany.com/magazine/53/europa.html. Accessed 30 November 2009.

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 2008.

NOTES

[1] 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).

[2] 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).

[3] 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, 2009).

[4] 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.

[5] 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 and Shubik, 2007), and a "terrorist organization, a militant network, and a subculture of rebellion all at the same time" (The Economist, 2008).

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

[7] 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 (Moghadam, 2008).

[8] Authorities believe the JW Marriott bomber assembled his IED in his guest room with materiel 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).

[9] Interview, Alan Orlob, Marriott International Vice President Corporate Security, December 24, 2009

[10] Terrorism scholar Bruce Hoffman described Zazi's plot, which is believed to have been planned for the eight-year anniversary of 9/11 and targeted locations around Manhattan, as "Mumbai-on-the-Hudson" (Bergen, 2009).

[11] 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).

[12] 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).

[13] 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).

[14] Interview, Alan Orlob, Marriott International Vice President Corporate Security, December 24, 2009

[15] Interview, Alan Orlob, Marriott International Vice President Corporate Security, December 24, 2009

[16] 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

[17] Following the 2009 Jakarta bombings it was reported that ConocoPhilips removed Marriott's two Jakarta properties from their company's preferred hotel list (Darson, 2009).

[18] Interview, Mike Ackerman, the Ackerman Group LLC, December 24, 2009