Aligning strategy to threat: a baseline anti-terrorism strategy for hotels

Aligning Strategy to Threat:
A Baseline Anti-Terrorism Strategy for Hotels

Dr Alexandros Paraskevas
Senior Lecturer in Strategic Risk Management

Oxford Brookes University
Oxford School of Hospitality Management

PLEASE CITE AS:

Paraskevas, A. (2013). Aligning Strategy to Threat: A Baseline Anti-terrorism Strategy for Hotels, *International Journal of Contemporary Hospitality Management*. 25(1), pp. 140-162.

Abstract

Purpose: Although the threat of terrorist attacks is not a new phenomenon for hotels, limited literature exists on measures that hotels can take to prevent them or limit their damage. The purpose of this paper is to propose a baseline strategy to address this threat.

Design/methodology/approach: Using the terrorist attack cycle and the security function models introduced in this paper, nineteen hotel security experts, members of an international working group on terrorism, were tasked to reach consensus on a baseline anti-terrorist strategy for a hotel. To reach this consensus, the study employed the Nominal Group Technique.

Findings: The study presents a six-step baseline anti-terrorism strategy and a series of measures and actions under each step. In the centre of this strategy lies the disruption of the terrorist attack cycle.

Research limitations/implications: There are limitations inherent to the Nominal Group Technique which may not allow the generalisability of the findings. However, every effort was made to ensure the reliability and validity of the study.

Practical implications: The study suggests a shift from physical protection alone to a more intelligence-led approach. Counter-surveillance, terrorist behavioral analysis, higher visibility of security measures, stronger relationships with local community leaders, collaborative relationships with emergency response agencies and strategic use of risk intelligence providers will have to take a higher place in the agendas of hotel security departments.

Originality/value: The paper presents for the first time two models that industry practitioners will find useful when designing security policies: the terrorist attack cycle and the security function model. Each component of the proposed strategy provides a

starting point for the design of security strategies tailored on the security needs and budget of any hotel property.

Key words: Terrorism; Terrorist Attack Cycle; Hotel Security Function; Physical Protection; Counter-surveillance; Intelligence-led Security.

Aligning Strategy to Threat:
A Baseline Anti-Terrorism Strategy for Hotels

1. Introduction

In the last decade the hotel industry has witnessed a series of terrorist attacks with vehicle-borne improvised explosive devices (VBIEDs – car bombs, such as in the 2003 JW Marriott bombing in Jakarta, Indonesia or the 2004 attack in Taba Hilton, Sinai peninsula), suicide bombers (e.g., the 2005 triple bombing of the Grand Hyatt, the Radisson SAS and the Days Inn in Amman, Jordan and the double bombing of the JW Marriott and the Ritz Carlton in Jakarta, Indonesia in 2009) and storming assaults (the 2008 Taj and Oberoi hotel attacks in Mumbai, India, the 2011 Intercontinental attack in Kabul, Afghanistan).

In response to such attacks, many hotels introduced both physical and technical measures that control the free flow of people and vehicles to hotel areas (stand-off zones, drop-arm barriers and bollards, metal and explosive vapor detectors, etc). In many cases however (e.g., the 2008 Islamabad Marriott attack in Pakistan and the 2009 double Jakarta bombings) these measures did not manage to provide a high level of protection to hotels. Further 'hardening' of hotels with armed security personnel has not been a deterrent for terrorists as evidenced in attacks such as those on the Serena Hotel in Kabul, Afghanistan (in 2007, 2008 and 2010) or on the Pearl Continental in Peshawar, Pakistan in 2009.

Looking back in history, physical protection measures alone were never able to avert a terrorist attack to a hotel. The very first hotel bombing in history was carried out in 22 July 1946 on the King David Hotel in Jerusalem by the Irgun, a militant Jewish underground organization of the time (Martin, 2009). The hotel was hosting the Headquarters of the British Mandatory authorities of Palestine, the Secretariat of the Government of Palestine and the Headquarters of the British Forces in Palestine and Transjordan and although there are no formal records about the security in place at the time, there is no doubt that such a location would be well protected. The Irgun bomb attack caused the collapse of the hotel's southern wing which housed the Mandate's intelligence records about Irgun, the Hagana, Lehi, and other Jewish paramilitary groups. With a death toll of 91, this hotel attack is considered one of the bloodiest but also most successful (in terms of outcomes for the terrorists) attacks in the history and provided a model for further attacks towards the end of the 20th century (Enders and Sandler, 2006; Martin, 2009). Another example of a hotel targeted in spite of its physical protection measures is the Hotel Europa in Belfast which is characterized as the "world's most bombed hotel" with 33 bombings by the Provisional IRA in the period between 1972 and 1994 (Wylie, 2001). It appears therefore that, regardless of whether they are 'soft' or 'hardened' targets, hotels need to go beyond current practices and take a more strategic approach in their security planning in order to respond more effectively to the threat of terrorism.

The importance of terrorism in hospitality and tourism is reflected in a significant body of literature dedicated to the study of this phenomenon. However, the largest part of this literature either takes a case study approach and analyses the attacks and their impacts (e.g., Araña and León 2008; Drakos and Kutan, 2003; Henderson, 2003; O'Connor *et al.*, 2008; Pizam and Smith, 2000; Sönmez *et al*., 1999; Yechiam *et al*., 2005) or looks at marketing recovery efforts of destinations attacked by terrorists (Beirman, 2002; Blake and Sinclair, 2003; Gurtner, 2007; Israeli and Reichel, 2003; Pratt, 2002; Rittichainuwat and Chakraborty, 2009; Stafford *et al*., 2002).

The research on a strategic approach to address the terrorism threat, however, is quite limited (Paraskevas, 2008; Paraskevas and Arendell, 2007) and this paper aims at narrowing this gap first by drawing from the terrorism literature a model for the 'terrorist attack cycle' (TAC) and from the extant crisis management and generic security literature a model for the security function per se. Then, it uses these models with a group of nineteen hotel security experts and the nominal group technique (NGT) to develop and propose a baseline anti-terrorism strategy for hotels.

2. Literature review

2.1. Terrorism and Terrorist Motivations

There are so many competing (though sometimes partially overlapping) definitions for terrorism (Schmid and Jongman, 1988) that Gearty (1996, p. xi) argued that the phenomenon is "shrouded by terminological confusion". Several scholars have attempted to identify the defining criteria for terrorism (e.g., Gupta, Horgan and Schmid, 2009; Martin, 2009; Ruby 2002) which are broadly agreed to be: premeditated use of illegal and often extraordinary and unconventional force; action triggered by political or other ideological motives; attacks directed towards non-combatants (soft civilian and passive military targets); actors are sub-national groups or clandestine agents; acts aimed at purposefully affecting (creating of a fearful state of mind) an intended audience (much wider than the immediate victims). English (2009, p. 24) offers a comprehensive definition of the term:

> Terrorism involves heterogeneous violence used or threatened with a political aim; it can involve a variety of acts, of targets, and of actors; it possesses an important psychological dimension, producing terror or fear among a directly threatened group and also a wider implied audience in the hope of maximizing political communication and achievement; it embodies the exerting and implementing of power, and the attempted redressing of power relations; it represents a subspecies of warfare, and as such it can form part of a wider campaign of violent and non-violent attempts at political leverage.

Hotels are broadly considered as 'soft' targets, i.e., targets that are difficult to protect and easy to penetrate and, by their business, social and symbolic nature, lend themselves as primary means to achieve the terrorists' objectives listed in the definition above. Hennelly (2008) notes that the continuous flow of people in and out of a hotel poses a challenge for its protection from a terrorist attack. Carlisle (2007) comments on how Dihren Barot was not challenged at all in carrying out surveillance and reconnaissance in top London hotels such as the Berkeley, the Savoy, the Hyatt Carlton Tower, the Marble

Arch Marriott and the Park Lane Intercontinental. Pizam (2010, p. 1) on the other hand, argues that hotels provide the terrorists with an "exceptional opportunity to carry out their heinous acts". He states three main reasons: they are not properly guarded for the fear of alienating the guests; the media will disseminate the terrorists' message worldwide, "loud, clear and fast"; and due to their nature of hosting "foreign devils", they offer a ''legitimate'' justification for the attack. Richter and Waugh (1986) emphasize that the symbolic values of wealth, freedom of choice, independence and everything that is associated with Western consumption and corruption make hotels primary targets for a terrorist group.

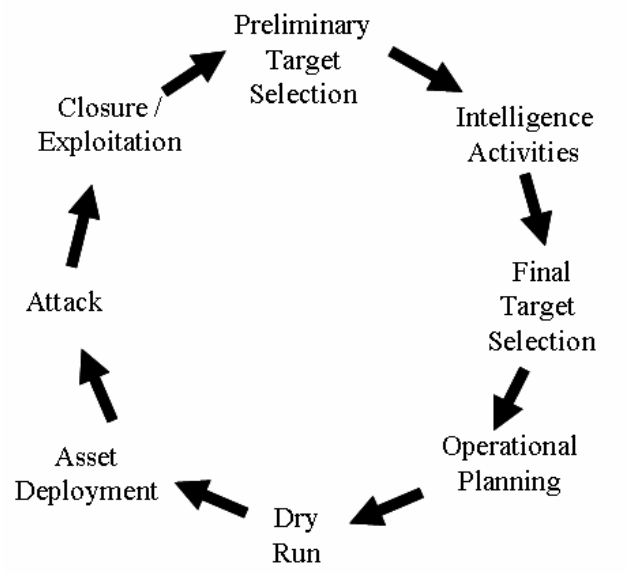
Even when attacks seem irrational to the wider public, one needs to remember that terrorists always act as 'rational actors' and political utility maxi misers constantly weighing cost and benefits for each attack (Fussey 2011; McCormick, 2003). Although every terrorist attack has a specific political aim and carries a message, the terrorists carrying the attack may be motivated by their own personal agendas. These may stem from completely different political, religious and psychosocial experiences such as strongly perceived oppression, humiliation or persecution, an extraordinary need for collective vengeance or a drive for expression of intrinsic aggressiveness (Victoroff, 2005). Goertzel (2002) argues that terrorists often rationalize their atrocities on moral ground as they believe that their actions are defensive; they are saving themselves from the great evil and they are compelled to commit their violence. In the 2005 triple hotel bombing in Amman resulting in the death of 57 Muslims, for example, Al Qaeda justified the attack by stating that they had "struck only after becoming confident that these hotels are centers for launching war on Islam and supporting the Crusaders' presence in Iraq and the Arab peninsula and the presence of the Jews on the land of Palestine" (Fox News, 2005).

2.2. The Terrorist Attack Cycle

In accordance with the concepts of 'rational action' (Fussey, 2011; McCormick, 2003) and 'warfare' (English, 2009), all terrorist attacks follow to some extent the same pattern of activities, known as the "terrorist attack cycle". STRATFOR (2005) suggests six distinct stages: target selection, planning, deployment, attack, escape and media exploitation, whereas the U.S. Department of Homeland Security (U.S. DHS, 2009) proposes a similar cycle with seven stages. For the purposes of this study, these cycles were adapted to the one presented in Fig. 1, which consists of eight different stages. It was felt that the proposed distinction of the various stages would further facilitate the identification of terrorists' vulnerabilities in the attack cycle and the development of appropriate interventions in the security function.

Preliminary selection of alternative targets. This is the first stage of the attack cycle and normally depends on the terrorist group's objectives (target's symbolic value, target that will create greater media attention or on which the attack will cause the maximum possible damage, etc.) and its operational capabilities.

Fig. 1 - The Terrorist Attack Cycle



Intelligence activities. The terrorists undertake a set of activities aiming at the evaluation of the selected targets by collecting information through basic research, surveillance and reconnaissance.

Final target selection. The intelligence generated in the previous stage is used to evaluate the various targets against criteria such as: resources and capabilities necessary to carry out the attack on a particular target; expected attack impact; target symbolism; and, finally, the number and demographics of targeted population (Weaver *et al*., 2001).

Operational planning. Once the decision on the target is made, the method and timing of attack, the equipment, the personnel and the training required to carry it out are decided upon. This stage also includes the funding, the management of supply chain and the logistics of the operation

Dry-runs. Before the execution of the final operation, plans may be 'rehearsed' in simulated conditions by the operatives in order to identify potential planning flaws and unanticipated problems and verify that the assumptions made during the operational planning have not changed (Fussey, 2011).

Asset deployment. In this stage the group's logistics unit will prepare and place all required supplies at or near the target, the operatives will leave their safe houses, assemble teams and weapons and prepare the attack.

Attack. This is when the operational plan is carried out. Once it is set in motion, it is difficult to be averted, since the attackers have the advantage of surprise and with the intelligence available will have planned for and neutralized any measures.

Closure / Media Exploitation. The closure of the operation will depend on whether an escape is planned at tactical level for the operatives or if the mission is a suicide attack. Since media exploitation and ideological statements are primary objectives in any operation, the group will have a plan to communicate its messages to the intended publics (adversaries and supporters).

Given this cycle, national counter-terrorism forces, intelligence and security services are looking for gaps and vulnerabilities in it and aim to disrupt it, interdict the attack and eventually apprehend the terrorists. The target's security function plays an important role here, since it is exposed to the terrorists' activities from the beginning of the attack cycle and may have many opportunities to detect their intentions and disrupt these activities from an early stage.

2.3. Terrorism, Crisis Management and the Security Function

In the crisis management literature, terrorism has been classified as a type of 'man-made crisis' (Mitroff, 2005). A terrorist attack can be considered as a crisis, i.e., a "low-probability, high-impact event that threatens the viability of the organization and is characterized by ambiguity of cause, effect, and means of resolution, as well as by a belief that decisions must be made swiftly" (Pearson and Clair, 1998, p. 60). Crisis management thinking can therefore be a useful conceptual framework in dealing with the terrorist threat.

One model of crisis management which is perhaps the most cited in the literature is the 'PPRR model'. This model has its origins in the disaster management field and consists of four phases: Prevention; Preparedness; Response; and Recovery also known as "Comprehensive Emergency Management" model (Drabek, 1985; Perry, 1985). In some versions of the model (e.g., McLoughlin, 1985; Tierney, 1989; Coppola, 2006), the Prevention phase is replaced with Mitigation (MPRR), although without a significant change in meaning. This model has its roots in the field of preventive psychiatry, namely the work of Caplan, who described three levels of "crisis intervention" (Caplan, 1964, pp. 16-17):

1. *Primary Intervention*, which consists of activities that are directed at 'reducing incidence', i.e., aim at preventing a crisis from occurring (and would correspond to 'prevention' in the PPRR model);

2. *Secondary Intervention* aims at 'reducing prevalence by shortening the duration of the crisis', i.e., consists of the actions taken once the crisis manifests itself in order to minimize its adverse impact and contain it as much as possible at a manageable level (this would correspond to the 'response' element in PPRR); and,

3. *Tertiary Intervention*, which involves actions 'reducing severity and disability', i.e., activities providing long-term follow-up help to those affected by the crisis (this would correspond to 'recovery' in PPRR).

An improved version of the PPRR is also recommended by Mitroff in several of his studies over time (e.g., Shrivastava and Mitroff, 1987; Pearson and Mitroff, 1993, Mitroff, 2004). More specifically, building on earlier work (Mitroff, 1988), he suggested a model in which he distinguished six phases in crisis management: signal detection; preparation/prevention; containment (damage limitation); business recovery; no-fault learning and redesign (Mitroff, 2005:210).

These crisis management models have set a foundation for the development of the security function as the organization's principal line of protection and assurance against internal and external threats (Schweitzer, 1987). These threats may range from fraud, theft and malfeasance to money laundering, employee conduct, and response to major events including natural and man-made disasters (Broder, 2006). Regardless of the threats that the security function is protecting an organization from, the approach to protection largely follows the same system design, known also as the 'Sandia Methodology' (Danneels, 2000). This methodology was originally developed by Sandia National Laboratories in order to design a physical protection system for nuclear power plants. The Sandia Methodology emphasizes three security function components: 'detect', 'delay' and 'respond' which have clear links with the PPRR and Mitroff's (2005) model of crisis management.

The phases labeled 'Signal Detection' and 'Preparation/Prevention' in Mitroff's model constitute the proactive approach to crisis management and determine the readiness of the organization to deal with a crisis. Shaeffer and Mano-Negrin (2003) argue that these phases enable the organization "to foresee and effectively address internal or exogenous adversary circumstances with the potential to inflict a multidimensional crisis, by consciously recognizing and proactively preparing for its inevitable occurrence" (p. 575). In the signal detection phase, crisis management activities focus on seeking signals that might warn of a crisis, and isolate these from other more normal signals that occur in the daily operations of organizations. With appropriate signal detection mechanisms in place, crisis signals can be picked up in time and then, some -if not all- crises can be averted before they happen. The *detect* component of Sandia's security model refers to the discovery of an adversary's overt or covert action. It involves a sensing mechanism which reacts to a stimulus and initiates an alarm. The information from the sensor is evaluated by a security person and the alarm is judged as valid or invalid.

Early detection of warning signals will help the organization take the appropriate measures in the prevention/preparation phase. In this second stage, Mitroff considered preparation and prevention as one set of activities rather than two separate as advocated by the PPRR model. In his view, organizations can be either "crisis prone" or "crisis prepared" (Mitroff, 2005). However, Sandia's model does not adequately address this aspect.

During Mitroff's "containment/damage limitation" phase, crisis management aims at prevent further escalation of the crisis and controlling the damage resulting from it. Since organizations usually have limited time to make an intensive crisis management plan for

damage control while the crisis is unfolding, having in advance well-prepared plans is crucial. The *delay* component of Sandia is the slowing down of adversary progress and can be accomplished by people, barriers, locks, and activated delay mechanisms. There are clear links between this component of the security function, Mitroff's "containment/damage limitation" phase and Caplan's secondary intervention in the PPRR model.

Finally, the *respond* component consists of actions taken by the security personnel to interrupt adversary progress and prevent adversary success (Garcia, 2001; 2006). This component is again more clearly linked with the secondary intervention (response in the PPRR model) although one could also detect links with the tertiary intervention as well as with some elements of Mitroff's "recovery" phase in terms, perhaps, of business continuity.

Although the Sandia Methodology has set a good foundation for security systems design, it is evident that it does not address several aspects of crisis management as it should. Among the criticisms that it received, one is that it is rather reactive and passive. As discussed earlier, the terrorists are rational actors who weigh the costs and risks involved in attacking a particular target against the group's objectives and potential benefits of this attack. The security function should, therefore, aim also at measures that *deter* the attack by creating a perception of unacceptable risk to those planning an attack. Deterrence can be achieved by providing a highly visible security, by increasing security levels in response to threats and by making frequent, unpredictable changes in security procedures (Morral and Jackson, 2009). Azahari Husin, Jemaah Islamiyah's alleged mastermind of both Bali bombings, noted in a 34-page document retrieved from his computer that the operational plan for the second bombing had to be altered because "security was tighter". Indeed, the police in Bali had increased the number of intelligence officers from 70 to 256, making it too risky for the terrorists to bring in a large amount of explosives and more difficult to rent undetected a house with a garage to assemble the bomb (La Guardia, 2006). Radlauer (2006, p. 609) maintains that deterrence is the 'holy grail' of counter-terrorism, arguing that if enough potential terrorists can be convinced that carrying out attacks is a bad idea, all the investment in target-hardening, security checks, and other means of countering the terrorism treat will no longer be necessary.

Grosskopf (2004, 2006) presents a slightly different antiterrorism-specific (as opposed to a generic security function) model in which he includes all those physical, technological and operational measures intended to 'devalue', 'deter', 'deny' and 'defend' a potential target against acts of terrorism. Considering that the 'defend' component corresponds to Sandia's 'respond', Grosskopf's model introduces two new components: devalue and deny. He explains that to *devalue* a potential target is to lessen its significance for terrorists. The focus here is not to improve security but to modify the potential target in such a way that would result in less gain to the terrorists in the event of an attack. For example, by using CPTED (Crime Prevention Though Environmental Design) techniques (Cozens, Saville and Hillier, 2005) to minimize large assemblies of people in certain parts of the hotel such as gardens, meeting rooms or lobbies, the attractiveness of these areas to a terrorist will be reduced. The *deny* component refers to the protection of the

target by preventing the access of both adversaries and their resources to it. The removal or reinforcement of areas where explosive devices could be stored (e.g., garbage bins), a 'stand-off' distance of more than 100 feet, physical barriers, control points, screening policies and layered access to areas may be some of the denial measures that can be employed (Coaffee and Bosher, 2008).

Finally, Paraskevas and Arendell (2007) propose a comprehensive anti-terrorism strategy framework which includes all the above components but also introduces two additional ones: communication and continuity. Their study suggests that the *communicate* component of the strategy should not be confined to marketing and recovery activities but include specific notification and awareness practices both internally (among the organization's stakeholders) and externally (media and various target markets). The *continue* component refers to the ability of the organization to protect critical business processes and resources in the case of a terrorist attack. The speedy resumption of these processes and the safety of staff and customers are central to the security function. With these two extra components the security function becomes more compatible with the PPRR and Mitroff's model by incorporating a significant part of the "recovery" phase. Title IX of the 9/11 Commission Act, which came later that year, confirmed the Paraskevas and Arendell (2007) framework by requiring preparedness in both communications and continuity of operations (NCTC, 2007).

The review of this literature, allows a further alignment of the security function with the dominant crisis management models as presented in Table 1. The detection of adversary activity is in line with Mitroff's signal detection whereas deterrence is clearly a proactive and preventive function ("detect" and "deject" in the refined security function model). The *delay*, *devalue* and *deny* components are proactive and aim at the protection of the organization and its preparedness for an adversary's actions ("protect"). The *defend* component is deployed in response to adversary action and aim at its containment and the limitation of its impact ("deflect"). The immediate resumption and *continuity* of mission-critical business activities as well as the full restoration and recovery of the business, requires clear *communication* processes and full *connectivity* with all the organization's stakeholders ("connect"). Finally, activities in line with Mitroff's learning and redesign mechanisms (such as ongoing threat/vulnerability analysis, organizational learning from adversary activities, security process testing, maintenance and redesign) require a culture of continuous reflection and of process review and improvement ("reflect").

Although the hotel industry is using many, if not all, of the above components of the security function to respond to the threat of terrorism, most efforts appear to focus on measures that address only specific hotel vulnerabilities. There have been some attempts for the development of industry security standards either in the form of national regulation, such as the SS545:2009 Singapore Standard for Hotel Security (SPRING Singapore, 2009), or from private sector initiatives (Stelter, 2009). However, there does not seem to be a universally accepted 'baseline anti-terrorism hotel strategy' that uses these security function components to reduce the likelihood of a terrorist attack.

Table 1 – The Security Function Model

PPRR Model *(Coppola, 2006; Drabek, 1985; Tierney, 1989)*	**Crisis Management Mechanisms** *(Mitroff, 2005)*	**Security Function** *(Danneels, 2000; Grosskopff, 2006; Morral & Jackson, 2009; Paraskevas & Arendell, 2007)*	**Refined Security Function**
	Signal Detection	Detect	Detect
Prevention	Prevention/ Preparedness	Deter	Deject
Preparation		Devalue Delay Deny	Protect
Response	Containment/ Damage Limitation	Defend	Deflect
Recovery	Recovery	Continue Communicate	Connect
	No-Fault Learning		Reflect
	Redesign		

3. Research Design

The study was conducted using the Nominal Group Technique (NGT), a technique that helps groups generate ideas and reach consensus through a four-stage structured process: problem introduction; individual (silent) idea generation; sharing of ideas in a 'round-robin' fashion; group discussion; voting and ranking (Delbecq, Van de Ven and Gustafson, 1986). It is a technique that enables researchers gather information from relevant experts and facilitates creative problem solving by means of judgmental decision making in situations where there are no guiding examples of research in the literature. For the purposes of this study, the judgments of experts were integrated to establish a baseline anti-terrorism strategy.

Consensus building techniques are often used by hospitality and tourism researchers (Paraskevas and Saunders, 2012) and NGT, in particular, has been employed to explore a number of issues in the sector. Brown and Giles (1994), for example, used NGT in their study of Byron Bay, New South Wales, to assess the residents' behavioral adaptations to periods of peak tourism demand. Olsen (1995) used nominal group sessions with senior level hospitality executives focusing on the business environment of the multinational hotel industry and the forces driving change in it. Lockyer (2005) applied the technique to investigate the factors that influence the selection of hotel accommodation by guests whereas, more recently, Clark (2008) used it to formulate marketing strategies for a convention centre and Formica and Kothari (2008) to determine the forces that are likely to affect the future of tourism in the area of Pennsylvania, New Jersey, and Delaware from 2006 to 2010. Carlsen and Liburd (2008) suggested that one of the research techniques to be used in their work aiming to develop a comprehensive research agenda for crisis management and market recovery in tourism should be the NGT.

The research sample was purposively selected among thirty-four hotel security professionals based in United Kingdom, France, Belgium, Italy, Spain and the Netherlands. Although they are all based in Europe, the scope of their companies' business activities is global and include areas with high terrorism threat. They were approached by e-mail and phone and nineteen of them agreed to participate and received written information about the aim of the study and the procedure to be followed. Of the nineteen participants, thirteen represented nine international hotel groups (one vice president of corporate security, one global director of global security, three regional directors of security, four group directors of security and four chief security officers), three represented international security systems companies and three were international security advisors/consultants.

For the first stage of the NGT process (individual idea generation) the participants were sent the terrorist attack cycle as presented in this paper and six scenarios of hotel terrorist attacks, based on real cases across the spectrum of terrorist groups and modes of operation. They were asked to list a set of physical, technical and operational security measures (maximum of five in each category) that would potentially avert each attack. They were then invited to attend a workshop in London (UK) to share and refine their ideas with fellow-professionals. Due to time constraints and various engagements of the participants, three such workshops -with 6, 5 and 8 participants- had to be organized between December 2008 and November 2009. By the time the workshops were organized, the industry experienced the Islamabad Marriott bombing and the Mumbai attacks and, therefore, these two scenarios were also taken into consideration. The workshops were facilitated by experienced moderators, assisted by the author.

For the second stage of NGT (idea sharing) during the workshops, the participants were asked to engage in a round-robin session where they had to discuss and record the measures and actions they had put on their lists during the first stage of the study. The third stage (group discussion) aimed at ensuring that the meaning and rationale of each measure was understood by the group, not to evaluate or judge its merits. Some similar or redundant measures were identified and consolidated. Reasons why some others should

remain distinct were also suggested. In this stage, the participants were also asked to link the proposed measures to particular stages of the two models (six-stage security function and terrorist attack cycle). The fourth and final stage of the NGT process (voting and ranking) aimed to aggregate the judgments of the participants, in order to determine the relative importance of the proposed measures and actions. The process concluded with a brief discussion to evaluate the procedure and the outcome.

4. Findings and Discussion

The discussion transcripts and the votes and rankings were analyzed and compared qualitatively by security function component and proposed measure/action separately. The most voted measures were then consolidated to produce a 'baseline' anti-terrorism strategy. In order to ensure the reliability of the analysis, the author and the workshop moderators performed the same analysis of the results independently by reading, sorting and classifying the participants' proposed measures by each component of the security function. The resulting classifications did not show significant differences from each other. To further ensure reliability with a test-retest check, the three moderators were invited to perform the same task for a second time, four weeks later. The analyses resulted in 82% agreement, much higher than the prescribed level of acceptance for exploratory research, which is "in the order of 0.6" (Easterby-Smith *et al.*, 2002, p. 135).

The outcomes of this analysis are presented following the six-step security function presented earlier in this paper:

4.1. Detect

In contrast with the Sandia model (Daneels, 2000) which focuses more on adversary detection when the attack begins, the participants emphasized terrorist detection from the stage of 'intelligence activities' throughout the 'dry-run' stage of the TAC suggesting a series of counter-surveillance actions. The rationale behind this was that in order for an attack to be planned, the 'intelligence unit' of the terrorist cell will conduct surveillance and reconnaissance over long periods of time in order to identify patterns and vulnerabilities in security processes, points of entry (and possibly escape), etc. Later, at the operational planning stage, operatives will conduct reconnaissance to familiarize themselves with the hotel and perhaps even 'dry-runs' of the attack to test the security levels of the property (Drake, 1998; Fussey, 2011). All these activities offer opportunities for detection and the participants suggest that essential actions to accomplish this are:

1. A robust, comprehensive suspicious incident reporting ("See something – Say something") and analysis program that involves every employee of the hotel at every level. According to a participant *"suspicious are all behaviors seemingly normal but out of context –such as a guest wearing a raincoat in a sunny day"*. Another suggested that security officers should be *"vigilant for 'four sames': same type of people, in the same place, at the same time of day, doing the same activity."*
2. Dedicated, trained in behavioral analysis counter-surveillance team which will be able to detect suspicious activities and analyze reported incidents.

3. Installation and 24/7 use of video surveillance in the hotel exterior and public areas, operated by properly trained console officers (although concerns about budgets to support this action were also expressed).
4. Use of loitering detection software to alert hotel security when individuals remain in an area for prolonged times or are perhaps looking to 'tailgate' members of staff or guests to access/controlled or restricted areas of the hotel.

When it comes to the detection of an actual attack, most participants suggested that intrusion detection measures in the hotel's perimeter would be useful but perhaps unrealistic for some hotel security budgets. Silent duress alarms (hidden finger or foot switches) were recommended for, mainly, the front office and back-office entrance.

Of particular interest to some participants was the scenario of an attack by grassroots-operatives (also known as 'lone wolves' since they operate on their own). It was argued that while such individuals should, in theory, be more difficult to identify through a counter-surveillance program, their lack of skills in pre-operational surveillance makes them more vulnerable to detection than the better-trained 'intelligence units' of organized terrorist groups.

4.2. Deject

In short, 'deject' is about making all the other measures visible, so that the potential attackers perceive the particular property presents unacceptable risks for the group. All participants recognize the importance of this component, especially in relation to the target selection stage of the attack cycle but also at the later stage of 'dry-runs'. One participant suggested that "*the entire baseline anti-terrorism strategy is about deterrence; this is the foundation for everything else we do as security professionals*". The participants did not propose any deterrent-specific measure but proposed the following generic strategies:

1. High visibility of all measures which may lead the potential attackers to conduct longer surveillance, deeper reconnaissance and perhaps multiple dry-runs exposing themselves more to detection or to remove the hotel from their list of potential targets.
2. Build in randomness and unpredictability in certain security procedures such as in the frequency, timing and routes of security patrols, car checks, metal detector screening, luggage checks, etc.
3. Develop strong relations with local community through a comprehensive and genuine social responsibility program. For example, a jihadist group may opt out to attack a hotel (or a hotel chain) which has strong ties with the Muslim community and openly shows respect to fundamental Muslim beliefs. Such an attack might cause adverse effects in the credibility and ideological argumentation of the terrorist group.

Several participants noted that high visibility of security measures can be an issue for hotel guests. Indeed, Feickert *et al*. (2006) in a survey of 930 hotel guests, found that although hotel guests generally appreciate the existence of security measures, most guests dislike any intrusive security efforts such metal detectors, the obvious presence of an

armed guard, and checking guests' identification against law enforcement records. On the other hand, Grosskopf (2006) in two studies of 240 people in a non-hotel environment found that the respondents felt 3-6 times less vulnerable to theft, battery and sexual assault in areas having a visible security presence, whereas only a minority of respondents considered areas with a highly visible security presence to be unfriendly (6%), uninviting (12%) or uncomfortable (13%). Perhaps the answer to this issue would be a balanced approach, with the visibility of security measures to vary according to the risk level of the area where the hotel is located.

4.3. Protect

As discussed earlier, this is the component which attracted most of the proposed measures focusing mainly at the physical protection of the hotel. The majority of the respondents related this component with the dry-run, asset deployment and attack stages of the TAC.

The 'devalue' element was quite controversial in terms of measures and actions. A significant number of participants strongly argued that the devaluation of a hotel as a target should not be part of a baseline anti-terrorist strategy and should only be activated in higher threat conditions. Nevertheless, the participants proposed the following actions:

1. Layered blast protection system with blast film on windows as a priority (reinforced external concrete walls in the perimeter as a second step).
2. Review of publically available information on the hotel (especially the Internet) and removal of anything that could be used by potential attackers (although everyone admitted that GoogleEarth cannot be removed).
3. At elevated threat conditions removal or covering of company's logos from external display and abandon flag policy (especially flags of nations labeled as 'enemies' by the potential attackers).

Measures related with the 'deny' and 'delay' elements referred mainly to control of movement in the perimeter and the interior of the property:

1. Perimeter access control measures (barriers and bollards, maximum possible stand-off distance) including CPTED (e.g., large pots, cement stanchions) for controlled flow of pedestrians and vehicles towards the hotel.
2. Develop in collaboration with local law enforcement a vehicular parking plan providing adequate stand-off (at least 30 meters) next to and around the hotel as well as a control policy for vehicles approaching the premises or intended for the hotel's parking space, including undercarriage and the cab.
3. Design access control program with public, semi-public (not accessible to the general public without an escort, e.g., sales and marketing or banquets and conferencing offices), controlled (e.g., elevators requiring specific keys, parking lots) and restricted areas (e.g., HVAC rooms, HAZMAT/chemicals' storeroom, electrical, boiler and pump rooms). The program should also specify access control points in these areas and access credential procedures (e.g., swipe cards, badges, etc.).

4. In collaboration with local fire authorities installation and use of deployable barriers such as motorized operable walls, roll down grilles or deployable doors to contain movement of attackers as part of the hotel's 'active shooter' program.
5. Availability of weapon and explosive detectors (including sniffer dogs), millimeter wave scanners (for whole body imaging) and X-ray machines for elevated threat conditions.

Under this label, and as part of the 'deny' element, some participants brought up also the issue of employee vetting. The discussion on this topic was triggered by the fact that one of the perpetrators in the 2009 JW Marriott and Ritz-Carlton bombings in Jakarta (Ibrohim) was the florist for both hotels and that two more suspects arrested in the aftermath of the attack were also hotel employees (Amir Abdilah, was a former employee in the five-star Hotel Mulia and Yayan was a cook in the Grand Melia Hotel). While the difficulties of employee vetting were acknowledged in this discussion, it was agreed that it should be placed higher in the agenda of hotel security and human resources, especially for properties located in 'high risk' areas.

4.4. Deflect

This component is exclusively related with the attack stage. Although in some 'high risk' areas hotels employ armed security officers, the participants agreed that a baseline anti-terrorist strategy should not involve direct engagement of security or other personnel with the attackers. For this reason they suggested that the 'defend' element should be combined with the 'continue' and aim primarily at the protection of employee and guest lives and secondarily at the continuity of mission critical business processes. The measures and actions proposed under this component were:

1. Train security personnel on appropriate and acceptable response in the event of a terrorist attack using a number of scenarios (VBIED attack, suicide bomber attack, active shooter attack, etc.). Hotel's first responders should be trained in first aid, CPR and use of defibrillator.
2. Test effectiveness of evacuation planning and related signage and ensure that evacuation routes and assembly points are secure from potential adversary action. Establish policy by which current lists of employees and guests are stored in a central repository on a daily basis. Determine alternate accommodation arrangements for evacuees and establish liaison persons with local hospitals for the potentially injured.
3. Develop a "shelter-in-place" program for cases where evacuation is not possible, with meals ready to eat and drinking water, defibrillators and first aid kits.
4. Detailed property architectural plans should be kept up-to-date and shared with local authorities. Conduct joint drills and exercises on various terrorist attack scenarios with local 'blue light' services.
5. Identify business critical functions and develop continuity plans including contingencies for potential loss of critical utility services, with specified and appropriately trained plan owners.
6. Maintain a properly equipped 'cold' site to be used by the crisis management team as a command centre in emergency situations.

The issue of a possible RDD (radiological dispersal device) attack was also discussed in two of the three workshops as a result of the Litvinenko poisoning with polonium-210 at the Millennium Hotel, Grosvenor Square, in 2006. However, the eventuality of such an attack in a hotel was largely dismissed by the participants as it was noted that it would not have the massive impact that a terrorist group would desire. It was also argued that the materials required for a RDD are quite expensive to obtain and difficult to handle. One participant also noted that *"an RDD attack would be far more effective in places of large population concentration, such as a subway station not a hotel – remember the 1995 sarin gas attack in Tokyo by Aum Shinrikyo members?"* Participants therefore agreed that such eventuality should not be considered in a baseline hotel anti-terrorist strategy.

4.5 Connect

The 'connect' component has to do with the creation and maintenance of all those networks, both internal and external to the hotel, necessary for an effective security function. These networks are facilitating the flow of security-related information at all stages of the TAC. Internal communication networks transfer information generated by the property's surveillance and counter-surveillance processes thus enabling detection of terrorist operatives, notification about possible intrusion and infiltration of the property, emergency communication during an attack, etc.

1. Develop and keep up-to-date an emergency notification network (call tree) for the crisis management team, other key contact personnel, internal first responders and local emergency response teams. Test regularly emergency communication procedures and protocols.
2. Create contingency communication networks (satellite phones, pagers) for the event that primary communication channels (landline and mobile telephony, e-mail) become inoperable.
3. Assign responsibility for internal crisis communications to a dedicated person or team and generate 'canned' messages to be disseminated to the workforce at various levels of threat.
4. Provide effective and efficient connectivity for surveillance team and other personnel for suspicious incident reporting.

External communication networks refer to connections with the various hotel stakeholders such as guests, corporate accounts, suppliers, media, local and international community and sources of intelligence. As with internal communication, the responsibility for external communication should be assigned to a dedicated spokesperson or team. Different stakeholders will have different information needs. The workshop participants distinguished three types of external communication networks: marketing communication networks, social networks and intelligence networks.

Marketing communication networks are the networks used to restore the organization's public and market image and recover business back to normalcy after a crisis situation.

Normally these networks are created and maintained by the senior management team, the marketing team and the company's public relations professionals.

Social networks are those developed between the organization and members and leaders (political and religious) of the local community as part of its social responsibility program. Depending on the strength of connectivity between the various nodes in these networks, they can also provide important counter-surveillance information back to the hotel. As discussed earlier, a strong relationship with the local community may act as an ideological deterrent on a potential terrorist attack.

Intelligence networks are purposefully developed for the collection of information on possible terrorist activity and determination of threat condition levels. Usually these are networks with local law enforcement, intelligence agencies and embassies. However, valuable information can be also collected by the media, and business intelligence providers. The latter can be private (contracted) sources (e.g., Control Risks Group, Hill and Associates, I-Jet Travel Risk Management, Jane's Information Group, Transecur) or private-public partnerships such as the Overseas Security Advisory Council (OSAC) in the US, the Dutch Counterterrorism Alert System and the under development Italian Observatory on National Security Matters.

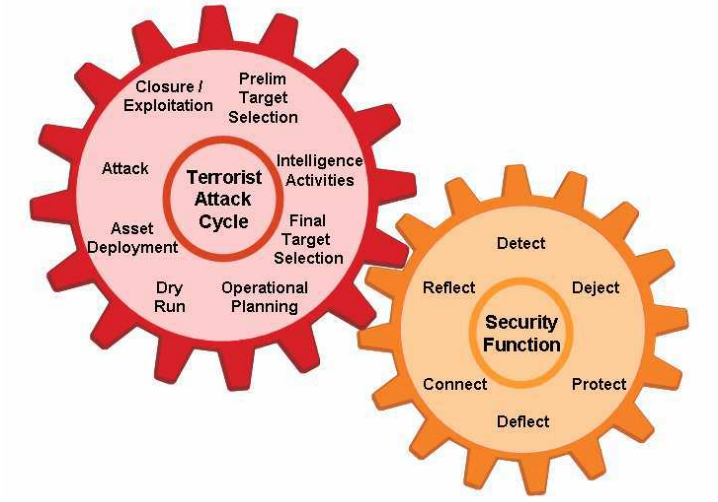
4.6. Reflect

The final building bloc of the baseline anti-terrorism strategy is the organization's and its security professionals' attitude towards continuous learning, self-evaluation and self-renewal. The participants showed remarkable consensus in this aspect as they almost unanimously agreed that the security function is dynamic and should continuously change. The actions and measures proposed for this last building block are as follows:

1. Reflect on why the particular property can be targeted by a terrorist group (symbolism, clientele, etc.). Consistently conduct vulnerability analysis to identify possible weaknesses that adversaries can exploit in order to successfully attack the property. Test and evaluate counter-surveillance effectiveness, possible ways of infiltration and exfiltration, effectiveness of protective physical, technological and operational counter-measures.
2. Develop an organization-wide security awareness culture where everyone is engaged in the protection and welfare of guests and workforce.
3. Create a security knowledge repository where new learning on terrorist activities, modes of operation and tactics as well as industry lessons from both failures and best practice will be stored.
4. New knowledge should be used for continuous review and updating of the hotel's security processes and measures as well as for training the people involved with the security function.
5. Anticipate possible adversary strategic, operational and tactical changes the property's current security practices may trigger and prepare countermeasures for these changes.

In the plenary sessions at the end of the three NGT workshops it became apparent that, although the identified six components of the security function can be used as the building blocks of a hotel's anti-terrorism strategy, the core of this strategy and the aim of every hotel security professional should be the disruption of one or more stages of the TAC. As noted by one participant *"…by the law of compounding probabilities, decreasing the chance of successfully completing one or more of these stages will exponentially decrease the chance of completing the entire attack cycle."* Therefore, the anti-terrorism strategy should always be viewed as inextricably linked with the TAC (Fig. 2).

Fig. 2 - A Six-Step Model for Anti-Terrorism Strategy in Hotels



5. Conclusions

The aim of this study was to develop and propose a baseline anti-terrorism strategy for hotels. Drawing from the generic crisis management literature (Drabek, 1985; Mitroff, 2005) the study showed that there is a need to expand the understanding of the security function from its classic approach of 'detect-deny-respond' (Garcia, 2001) to a model with six building blocks that can become the framework for the development of the strategy in question. Using this framework as a basis, a nominal group of nineteen hotel security professionals identified a series of measures and actions that can formulate a hotel's baseline anti-terrorism strategy with two dimensions: threat-based physical protection of employees, guests and hotel's critical assets (protect – deflect); and intelligence-led security tactics (detect – deject – connect – reflect). This new proposed two-dimensional approach differs from the current security practice because it emphasizes the role of the security function both before and in the aftermath of a terrorist attack and shifts the focus of the strategy from the passive protection of the target to the active disruption of the terrorist attack cycle (TAC). Although this general approach to anti-terrorism strategy is consistent with the generic models of crisis management, the study revealed two additional elements that are vital for the success of the strategy: the role of external networks in detection and recovery; and the need for security professionals to engage in a continuous 'mind-game' with potential adversaries and

implement dynamic anti-terrorism policies and practices which are constantly reviewed and updated, so that they are always 'one step ahead' of them. These two elements add a dimension of dynamism to the extant crisis management models which are often criticized as dominated by 'static' crisis management plans, normally developed and executed by 'authorized' members of the organization without the participation or involvement of external stakeholders (Robert and Lajtha, 2002; Takeda and Helms, 2006).

From a practitioner's perspective, the implementation of a baseline anti-terrorism strategy will be influenced predominantly by the size and the budget of hotels. International hotel groups with multiple brands in their portfolio may opt to protect the higher end of their provision rather than the lower one. However, it should be noted that the terrorist threat is not lower for non-western-flagged, locally-owned hotels with lower profiles (3-star hotels) or guest houses. The 2010 attacks on the Park Residence and Hamid guesthouses in the heart of the most secure areas in Kabul debunked these arguments. Therefore, even smaller hotels will need to deploy some elements of this strategy allocating budgets based on the 'threat-based and intelligence led' principle.

Of course, this study has methodological limitations that need to be taken into consideration when evaluating the findings. The first limitation concerns the format of the NGT, which although quite structured and prescriptive, does not always allow the participants to put forward the reasons for their judgments and opinions. Also, some aspects of the process (such as the composition of the group or the procedure for aggregating votes and ranking) may influence the outcome to varying directions. A second area of concern is the way that the participants' professional backgrounds (e.g., police vs. military; operations vs. intelligence; loss prevention vs. risk management) and organizational cultures affect their views. The final concern is reliability, particularly as far as nominal groups are concerned. The strength of the NGT is that it provides a platform for in-depth discussion; however, this can also be its weakness since it can lead to non-representative and therefore unreliable, judgments.

It would therefore be interesting for future researchers to test these findings not only with a larger and more representative sample of hotel security professionals but also test these findings with hotel owners and operators, general managers, and law enforcement agents. Several other streams of research may be followed, building on the findings of this study in areas that hospitality and tourism scholars have identified as needing more in-depth exploration. In the context of the 'deject' stage of this study, for example, researchers could explore the extent to which the "labeling and framing" of specific anti-terrorism measures and strategies cause a positive or a negative effect on the guests' experience of the hotel. Ritchie, Tung and Ritchie (2011), for example, in their study of tourist experiences argue that most research focuses on the 'facts' of what happens rather than the interpretation that travelers are giving to those 'facts'. In the case of heightened security measures and policies, it would be interesting to explore hotel guests' interpretations of these measures and to identify ways to encourage guests to make sense of them with implications to branding, signage, promotional messaging, etc. Further, Harrington and Ottenbacher (2011), in their review of hospitality research on strategy and uncertainty suggest that studies should look at how strategic relationships between

hospitality and non-hospitality firms can be used to minimize uncertainty, a research question which could be contextualized within the 'connect' stage of this study, on the ways of creating and effectively operating internal and external intelligence and social and marketing communication networks for hotel security purposes.

References

Araña, J. E. and León, C.J. (2008). The impact of terrorism on tourism demand, *Annals of Tourism Research*, Vol. 35, No. 2, pp. 299-315.

Beirman, D. (2002). Marketing of tourism destinations during a prolonged crisis: Israel and the Middle East. *Journal of Vacation Marketing*, Vol. 8, No. 2, pp. 167–176.

Blake, A. and Sinclair, T. (2003). Tourism crisis management: US response to September 11. *Annals of Tourism Research*, Vol. 30, No. 4, pp. 813–832.

Broder, J.F. (2006). *Risk Analysis and the Security Survey*. 3rd edition. Oxford,UK: Butterworth-Heinemann.

Brown, G., and Giles, R. (1994). Resident responses to the social impact of tourism. In A.V. Seaton, C.L. Jenkins, R.C. Wood, P.U.C. Dieke, M.M. Bennett, LR MacLellan and R. Smith (Eds.), *Tourism: A State of the Art*, Chichester: Wiley, pp. 755–764.

Caplan, G. (1964). *Principles of Preventive Psychiatry*. New York: Basic Books.

Carlisle, D. (2007). Dhiren Barot: Was he an Al Qaeda mastermind or merely a hapless plotter? *Studies in Conflict and Terrorism*, Vol. 30, No. 12, pp. 1057-1071.

Carlsen, J.C. and Liburd, J.J. (2008). Developing a research agenda for tourism crisis management, market recovery and communications. *Journal of Travel and Tourism Marketing*. Vol. 23, Nos. 2/3/4, pp. 265-276.

Clark J. (2008). Formulating strategic marketing direction for a second-tier convention center: the Hickory (North Carolina) Metro Convention Center. *Journal of Convention and Event Tourism*, Vol. 9, No. 2, pp. 148-160.

Coaffee, J. and Bosher, L. (2008). Integrating counter-terrorist resilience into sustainability. *Proceedings of the Institution of Civil Engineers: Urban Design and Planning* Vol. 1, pp. 75-83.

Coppola, D.P. (2006). *Introduction to International Disaster Management*, London: Butterworth-Heinemann

Cozens, P.M, G. Saville and Hillier, D. (2005). Crime prevention through environmental design (CPTED): A review and modern bibliography. *Property Management*, Vol. 23, No. 5, pp. 328-356.

Danneels, J.J. (2000). Methodology for improving the security of the water infrastructure. *Water Surety Workshop*. Albuquerque, N.M.: Sandia National Laboratories.

Delbecq, A.L., Van de Ven, A.H. and Gustafson, D.H. (1986). *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*. Middleton, WI: Green Briar Press.

Drabek, T.E. (1985). Managing the emergency response, *Public Administration Review*, Vol. 45, Special Issue: Emergency Management: A Challenge for Public Administration, pp. 85-92.

Drake, C.J.M. (1998). *Terrorist's Target Selection*, New York: St. Martin's Press, Inc.

Drakos, K., and Kutan, A. M. (2003). Regional effects of terrorism ontourism: Evidence

from three Mediterranean countries. *Journal of Conflict Resolution*, Vol. 47, No. 5, pp. 621–641
Easterby-Smith, M., Thorpe, R. and Lowe, A. (2002). *Management Research: An Introduction.* 2nd edition. London: Sage Publications.
Enders, W. and Sandler, T. (2006). *The Political Economy of Terrorism*. New York: Cambridge University Press.
English, R. (2009). *Terrorism: How to Respond*, Oxford: Oxford University Press
Formica, S. and Kothari, T. H. (2008). Strategic destination planning: analyzing the future of tourism. *Journal of Travel Research*, Vol. 46, No. 4, pp. 355-367.
Fox News (2005) Al Qaeda Addresses Muslim Deaths. FOXNews.com , Thursday 10 November, online: http:// www.foxnews.com/story/0,2933,175235,00.html (accessed 14 March 2011).
Fussey, P. (2011). An economy of choice? Terrorist decision-making and criminological rational choice theories reconsidered, *Security Journal*, Vol. 24, No.1, pp. 85–99.
Garcia, M.L. (2001). *The Design and Evaluation of Physical Protection Systems*. Oxford, UK: Butterworth-Heinemann.
Garcia, M.L. (2006). *Vulnerability Assessment of Physical Protection Systems*. Oxford, UK: Butterworth-Heinemann.
Gearty, C. (1996). *Terrorism*, Dartmouth, Aldershot: Ashgate Publishing Ltd.
Goertzel , T. G. (2002) Terrorist beliefs and terrorist lives . In Stout , C. E. (ed.), *The Psychology of Terrorism: Theoretical Understandings and Perspectives*, Vol. 1 . Westport, CT : Praeger , pp. 97 – 111 .
Grosskopf, K.R. (2004). *Strategies to devalue, deter, deny and defend (D4) terrorist targets: A study of physical, psychological and operation methods to protect buildings and critical infrastructure.* University of Pittsburgh: Center for National Preparedness.
Grosskopf, K.R. (2006). Evaluating the societal response to antiterrorism measures. *Journal of Homeland Security and Emergency Management*, Vol. 3, No. 2, pp. 1-9.
Gupta, D.K., Horgan, J. and Schmid, A.P. (2009), Terrorism and organized crime: a theoretical perspective, in Canter, D. (ed.), *Terrorism and Crime: A Multidisciplinary Perspective*. John Wiley and Sons, London.
Gurtner, Y.K. (2007). Crisis in Bali: Lessons in tourism recovery. In E. Laws, B. Prideaux and K. Chon (eds) *Crisis management in tourism*, Wallingford, UK: CABI, pp. 81- 97.
Harrington, R.J. and Ottenbacher, M.C. (2011).Strategic management: An analysis of its representation and focus in recent hospitality research, *International Journal of Contemporary Hospitality Management*, Vol. 23, No. 4, pp. 439 – 462.
Henderson, J. (2003). Managing the aftermath of terrorism: The Bali bombings, travel advisories and Singapore. *International Journal of Hospitality and Tourism Administration*, Vol. 4, No. 2, pp. 17–32.
Hennelly, B. (2008). How safe are hotels and other urban spaces? WNCY.Org. Available online: http://www.wnyc.org/news/articles/118764 (accessed June 14, 2011).
Israeli, A.A. and Reichel, A. (2003). Hospitality crisis management practices: The Israeli case. *International Journal of Hospitality Management,* Vol. 22, No. 4, pp. 353-372.
La Guardia, A. (2006). Target any white person: the chilling guidelines for Bali suicide bombers, *The Daily Telegraph*, Tuesday 4 July. Available online:

http://www.telegraph.co.uk/news/worldnews/asia/indonesia/1523064/Target-anywhite-person-the-chilling-guidelines-for-Bali-suicide-bombers.html (accessed June 14, 2011).
Lockyer, T. (2005). Understanding the dynamics of the hotel accommodation purchase decision. *International Journal of Contemporary Hospitality Management*. Vol. 17, No. 6, pp. 481-492.
Martin, G. (2009). *Understanding Terrorism: Challenges, Perspectives and Issues*. Sage Publishing, Thousand Oaks, CA.
McCormick, G.H. (2003). Terrorist decision making, *Annual Review of Political Science*, Vol. 6, No.3 (June), pp. 473-507.
McLoughlin, D. (1985). A framework for integrated emergency management, *Public Administration Review*, Vol. 45, No. 1, pp. 165-172.
Mitroff, I.I. (1988). Crisis management: cutting through the confusion. *Sloan Management Review*. Winter, pp 15-20
Mitroff, I.I. (2004). *Crisis Leadership: Planning for the Unthinkable*. John Wiley and Sons, Inc.
Mitroff, I.I. (2005). *Why Some Companies Emerge Stronger and Better from a Crisis: 7 Essential Lessons for Surviving Disaster*, New York: AMACOM.
Morral, A.R. and Jackson, B.A. (2009). *Understanding the Role of Deterrence in Counterterrorism Security*. Santa Monica, CA: RAND Corporation.
NCTC (2007). *Implementing recommendations of the 9/11 Commission Act of 2007*. Washington, DC: National Counterterrorism Center. Available online: http://www.nctc.gov/docs/ir-of-the-9-11-comm-act-of-2007.pdf (accessed December 22, 2010).
O'Connor, N, Stafford, M.R. and Gallagher, G. (2008). The impact of global terrorism on Ireland's tourism industry: an industry perspective, *Tourism and Hospitality Research*, Vol. 8 No. 4, pp. 351-363
Olsen, M.D. (1995). Issues driving change in the hospitality industry. Paper presented at the Caribbean Hotel Industry Conference, Caribbean Hotel Association. San Juan, Puerto Rico.
Paraskevas, A. (2008). Towards safer special events: A structured approach to counter the terrorism threat. In J. Ali-Knight, M. Robertson and A. Fyall (eds.) *International perspectives on festivals and events* (Advances in Tourism Research Series), London, UK: Elsevier, pp. 279-293.
Paraskevas, A. and Arendell, B. (2007). A strategic framework for terrorism prevention and mitigation in tourism destinations. *Tourism Management*, Vol. 28, No. 6, pp. 1560-1573.
Paraskevas, A. and Saunders, M.N.K (2012). Beyond Consensus: An Alternative use of Delphi Enquiry in Hospitality Research. *International Journal of Contemporary Hospitality Management*, Vol. 24, No. 6, pp. 907-924
Pearson, C.M. and Clair, J.A. (1998), Reframing crisis management, *Academy of Management Review*, Vol. 23, No. 1, pp. 59-76
Pearson, C.M. and Mitroff, I.I. (1993). From crisis prone to crisis prepared: a framework for crisis management. *Academy of Management Executive*, Vol. 7 No. 1, pp. 48-59.
Perry, R.W. (1985). *Comprehensive Emergency Management: Evacuating Threatened Populations*. Greenwich, CT: JAI Press

Pizam, A. (2010). Hotels as tempting targets for terrorism attacks. *International Journal of Hospitality Management*, Vol. 29, No. 1, p. 1.
Pizam, A., and Smith, G. (2000). Tourism and terrorism: A quantitative analysis of major terrorist acts and their impact on tourism destinations. *Tourism Economics*, Vol. 6, No. 2, pp. 123–138.
Pratt, G. (2002). Terrorism and tourism: Bahamas and Jamaica fight back. *International Journal of Contemporary Hospitality Management*, Vol. 15, No. 3, pp. 192-194.
Radlauer, D. (2006). Rational choice deterrence and Israeli counter-terrorism. In: S. Mehrotra, D. Zeng, H. Chen, B. Thuraisingham and F.Y. Wang (eds.) Intelligence and Security Informatics, Proceedings of the *IEEE International Conference on Intelligence and Security Informatics*, San Diego, CA, May 23-24, Berlin, DE: Springer Verlag, pp. 609-614.
Richter, L. K., and Waugh, W. L. (1986). Tourism politics and political science: A case of not so benign neglect. *Annals of Tourism Research*, Vol. 10, No. 3, pp. 313–315.
Ritchie J.R.B., Tung V.W-S and Ritchie, R.J.B. (2011). Tourism experience management research: Emergence, evolution and future directions, *International Journal of Contemporary Hospitality Management*, Vol. 23, No. 4, pp. 419 – 438.
Rittichainuwat, B.N. and Chakraborty, G. (2009) Perceived travel risks regarding terrorism and disease: The case of Thailand, *Tourism Management*, Vol. 30, No. 3, pp. 410-418
Robert, B., and Lajtha, C. (2002). A New Approach to Crisis Management. *Journal of Contingencies and Crisis Management*, Vol. 10, No. 4, pp. 181-191.
Ruby, C.L. (2002), The definition of terrorism, *Analyses of Social Issues and Public Policy*, Vol. 2, No.1, pp. 9-14.
Schmid, A.P. and Jongman, A.J. (1988), *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*, Transaction Books, New Brunswick, NJ.
Schweitzer, J.A. (1987). *Computer, Business and Security*. Oxford, UK: Butterworth-Heinemann
Sheaffer, Z. and Mano-Negrin, R. (2003). Executives' orientations as indicators of crisis management policies and practices, *Journal of Management Studies*, Vol. 40, No. 2, pp. 573–606.
Shrivastava P. and Mitroff, I. I. (1987). Strategic management of corporate crisis. *Columbia Journal of World Business*, Vol. 22, No. 1, pp. 5–11.
Sönmez, S. F., Apostolopoulos, Y., and Tarlow, P. (1999). Tourism in crisis: Managing the effects of terrorism. *Journal of Travel Research*, Vol. 38, No. 1, pp. 13–18.
SPRING Singapore (2009). SS545: 2009 (ICS 03.080.30; 13.310) Singapore standard for hotel security. Available online: http://www.singaporestandardseshop.sg/data/ECopyFileStore/090813090414Preview%20-%20SS%20545-2009.pdf (accessed September 23, 2009).
Stafford, G., Yu, L. and Armoo, A.K. (2002). Crisis management and recovery: How Washington, D.C. hotels responded to terrorism. *Cornell Hotel and Restaurant Administration Quarterly*, Vol. 43, No. 5, pp. 27-40.
Stelter, L. (2009). Rating hotels based on security? Security Director News. Available online: http://www.securitydirectornews.com/?p=article&id=sd200909sNPNr (accessed December 12, 2009).

STRATFOR (2005). Vulnerabilities in the terrorist attack cycle. Available online: www.stratfor.com/vulnerabilities_terrorist_attack_cycle (accessed February 10, 2010).

Takeda, M. and Helms, M. (2006), Bureaucracy Meet Catastrophe: Analysis of the Tsunami Disaster and Implications for Global Emergency Governance, I*nternational Journal of Public Sector Management*, Vol. 19 No. 2, pp. 204-17.

Tierney, K.J. (1989). The social and community contexts of disaster. In R. Gist and B. Lubin (Eds) *Psychological Aspects of Disaster*, New York: John Wiley and Sons, pp. 11-39.

US DHS (2009). Surveillance detection training for commercial infrastructure operators and security staff course (SD CIKR). Washington, DC: US Department of Homeland Security.

Victoroff , J. (2005) The mind of the terrorist: A review and critique of psychological approaches . *Journal of Conflict Resolution* , Vol. 49, No. 1, pp. 3 – 42 .

Weaver, R., Silverman, B.G., Shin, H. and Dubois, R. (2001). *Modeling and Simulating Terrorist Decision-making: A 'Performance Moderator Function' Approach to Generating Virtual Opponents*, Center for Human Modeling and Simulation, online: http://works.bepress.com/barry_silverman/8 (accessed 15 June, 2011).

Wylie, I. (2001). He's Belfast's security blanket. *Fast Company Magazine* No. 53 (November), pp. 52-53.

Yechiam, E., Barron, G., and Erev, I. (2005). The role of personal experience in contributing to different patterns of response to rare terrorist attacks. *Journal of Conflict Resolution*, Vol. 49, No. 3, pp. 430–439.