EDITOR’S COMMENT

**This is a collection of papers focusing on hotels as soft terrorism targets. It aims to mobilize those involved in hotel industry to proceed to necessary hardening measures that will fortify their infrastructures, guests and personnel. Because the unexpected always happens and the targeted hotel does not have to be in a hot zone! It could be your hotel and it can happen today!**

# Soft Targets Back in Focus

**By Scott Stewart (Stratfor -** Vice President of Analysis)

Source:http://www.stratfor.com/weekly/soft-targets-back-focus

From time to time, I will sit down to write a series of analyses on a particular topic, such as the fundamentals of terrorism series last February. Other times, unrelated events in different parts of the world are tied together by analytical threads, naturally becoming a series. This is what has happened with the last three weekly security analyses -- a common analytical narrative has risen to connect them.

First, we discussed how the Jan. 16 attack against the Tigantourine natural gas facility near Ain Amenas, Algeria, would result in increased security at energy facilities in the region. Second, we discussed foreign interventions in Libya and Syria and how they have regional or even global consequences that can persist for years. Finally, last week we discussed how the robust, layered security at the U.S. Embassy in Ankara served to thwart a suicide bombing.

Together, these topics spotlight the heightened and persistent terrorist threat in North Africa as well as Turkey and the Levant. They also demonstrate that militants in those regions will be able to acquire weapons with ease. But perhaps the most important lesson from them is that as diplomatic missions are withdrawn or downsized and as security is increased at embassies and energy facilities, the threat is going to once again shift toward softer targets.

### Soft Targets

Obviously, individuals desiring to launch a terrorist attack seek to strike the highest-profile, most symbolic target possible. If it is well known, the target can magnify the terror, especially when the operation grabs the attention of international media. Such extensive exposure not only allows people around the globe to be informed minute by minute about unfolding events, but it also permits them to become secondary, vicarious victims of the unfolding violence. The increased exposure also ensures that the audience affected by the operation becomes far larger than just those in the immediate vicinity of the attack. The attack on the U.S. diplomatic office in Benghazi and the killing of U.S. Ambassador Christopher Stevens led to months of media coverage that has included televised congressional hearings and fierce partisan and bureaucratic squabbles in the media. It was the terrorist equivalent of winning the lottery.

However, in the wake of terrorist attacks, increased situational awareness and security measures make successful attacks difficult to replicate. Targets become more difficult to attack -- what we refer to as hard targets. When this happens, attackers are forced to either escalate the size and force used in their attack, identify a vulnerability they can exploit or risk failure.

In the August 1998 attacks against the U.S. embassies in Nairobi, Kenya, and Dar Es Salaam, Tanzania, al Qaeda planners turned to the first option: a larger attack. They attempted to use large truck bombs to overcome the embassies' layered security. The embassies had decent perimeter security but lacked enough distance between the street and the buildings to protect them from a large blast. In both attacks, the attackers also tried unsuccessfully to get the bomb-laden trucks through perimeter security vehicle checkpoints to detonate them closer to the embassy buildings.

After those bombings, security enhancements made most diplomatic facilities more difficult to attack, leading militant groups to turn their attention to hotels. A strike on an international hotel in a major city can make almost the same kind of statement against the West as a strike on an embassy. Hotels are often full of Western business travelers, diplomats, intelligence officers and, not insignificantly, members of the media. This has made hotels target-rich environments for militants seeking to kill Westerners and gain international media attention without having to penetrate the extreme security of a hard target like a modern embassy.

But increased security is not the only factor that leads those wishing to conduct a terrorist attack to gravitate toward softer targets. For the better part of a decade, we have chronicled how the global jihadist movement has devolved from an organizational model based on centralized leadership and focused global goals to a more amorphous model based on regional franchises with local goals and strong grassroots support. For the most part, these regional franchises lack the training and funding of the al Qaeda core and are therefore less capable. This means franchise groups are often unable to attack hard targets and tend to focus on softer targets -- such as hotels or the U.S. ambassador while he is staying at a poorly protected office in Benghazi rather than at his residence in Tripoli.

### Changing Threats in North Africa

As hotels in places like Amman and Jakarta became harder to attack with large vehicle bombs, attackers began to smuggle in smaller devices to bypass the increased security. There was also a trend in which attackers hit restaurants where Westerners congregated rather than the more secure hotels.

The same dynamic will likely apply today in the Sahel. We believe that the attack at the Tigantourine natural gas facility in Algeria was greatly aided by the complacency of the security forces. The attackers did not demonstrate any sort of advanced terrorist tactics or tradecraft. It would be very hard to replicate the attack on another energy facility in the region today due to increases in awareness and security. The increase in security will be compounded by the fact that al Qaeda in the Islamic Maghreb and its jihadist brethren in the Sahel lack sophisticated terrorist capabilities and have lost their bases in northern Mali. This means they will be hard-pressed to conduct a successful attack against a hard target.

Furthermore, having lost substantial quantities of men and materiel, and with French and African forces potentially interdicting their lucrative smuggling routes, these jihadist groups will be looking to refill their coffers. Kidnapping is a longstanding way for militant groups in the region to resolve precisely these issues. Although they have lost control of the towns they captured in northern Mali, these groups will continue to pose a threat of kidnapping over a wide swath of North Africa.

### Turkey and Lebanon

While the jihadist militants in Syria are currently fixated on attacking the Syrian regime, there is nonetheless a non-jihadist threat in Turkey -- and perhaps Lebanon -- that emanates from the Syrian intelligence and its proxy groups in the region. However, the Feb. 1 attack against the U.S. Embassy in Ankara demonstrated the limitations of the capabilities of one of those proxies, the Revolutionary People's Liberation Party-Front.

Carrying on the operational legacy of its parent organization, Devrimci Sol, the Revolutionary People's Liberation Party-Front aspires to conduct spectacular attacks, but its attacks frequently fizzle or fail. Successfully striking a hardened target such as the U.S. Embassy is beyond the group's capability. In fact, the group frequently botches attacks against softer targets, as in the attack against an American fast food chain outlet in May 2012 that failed when the explosive device malfunctioned.

The Revolutionary People's Liberation Party-Front's limited tactical capability supports the theory that the attack against the U.S. Embassy in Ankara was commissioned by the Syrian regime. The group has even failed in suicide bombings against Turkish police stations with far less security; it knew it was attacking something beyond its reach. But at the same time, the group's limited capability and the failure of the attack against the U.S. Embassy will likely result in a shift to softer targets if the Revolutionary People's Liberation Party-Front was acting at Syria's behest and the Syrians have asked for additional anti-American attacks.

As noted last week, Devrimci Sol conducted dozens of attacks against U.S. and NATO targets in Turkey during late 1990 and early 1991 at the behest of Saddam Hussein. The majority of these attacks were directed against soft targets such as U.S. corporate offices, nongovernmental organizations, hotels and restaurants. We believe these same targets are in jeopardy of attack by the Revolutionary People's Liberation Party-Front now.

Syria maintains a number of proxy militants in Lebanon, including Hezbollah. Hezbollah has its own calculations and may not be as willing as Syria's smaller proxy groups to act on Syria's behalf. Hezbollah maintains a far more sophisticated militant capability than these small groups and is able to attack hard targets, unlike the smaller groups. Therefore, if the Syrians commission a terrorist attack in Lebanon and Hezbollah does not help them, the attacks their proxy groups will carry out will be quite limited -- and will again focus on soft targets.

For the most part, soft targets are soft by their very nature. It is not only impractical to employ embassy-like security at a fast food restaurant, but it is inordinately expensive -- too expensive to be economically feasible for a business. Still, there are some simple and practical security measures that can be taken to make them slightly more secure and hopefully cause anyone planning an attack to divert their operation toward an even softer target.

Additionally, individuals living in or traveling to these places can and should practice good situational awareness, review their personal contingency plans and mentally prepare to respond to any crisis.

## Indicators of Suspicious Behaviors at Hotels

Source: http://publicintelligence.net/dhs-fbi-suspicious-hotel-guests/

Known or possible terrorists have displayed suspicious behaviors while staying at hotels overseas—including avoiding questions typically asked of hotel registrants; showing unusual interest in hotel security; attempting access to restricted areas; and evading hotel staff. These behaviors also could be observed in U.S. hotels, and security and law enforcement personnel should be aware of the potential indicators of terrorist activity.

Possible indicators of terrorist behaviors at hotels: The observation of multiple indicators may represent—based on the specific facts or circumstances—possible terrorist behaviors at hotels:

* Not providing professional or personal details on hotel registrations—such as place of employment, contact information, or place of residence.
* Using payphones for outgoing calls or making front desk requests in person to avoid using the room telephone.
* Interest in using Internet cafes, despite hotel Internet availability.
* Non-VIPs who request that their presence at a hotel not be divulged.
* Extending departure dates one day at a time for prolonged periods.
* Refusal of housekeeping services for extended periods.
* Extended stays with little baggage or unpacked luggage.
* Access or attempted access to areas of the hotel normally restricted to staff.
* Use of cash for large transactions or a credit card in someone else’s name.
* Requests for specific rooms, floors, or other locations in the hotel.
* Use of a third party to register.
* Multiple visitors or deliveries to one individual or room.
* Unusual interest in hotel access, including main and alternate entrances, emergency exits, and surrounding routes.
* Use of entrances and exits that avoid the lobby or other areas with cameras and hotel personnel.
* Attempting to access restricted parking areas with a vehicle or leaving unattended vehicles near the hotel building.
* Unusual interest in hotel staff operating procedures, shift changes, closed-circuit TV systems, fire alarms, and security systems.
* Leaving the property for several days and then returning.
* Abandoning a room and leaving behind clothing, toiletries, or other items.
* Noncompliance with other hotel policies.

# Airport Terror Announcements Now Being Played in Hotels

**By Paul Joseph Watson & Alex Jones**

Source: http://www.infowars.com/airport-terror-announcements-now-being-played-in-hotels/

Airport-style announcements encouraging Americans to “report suspicious activity” in the name of spotting terrorists are now being played in thousands of hotels across America as the Department of Homeland Security’s domestic snitch program expands.

As a result of the DHS’ partnership with media provider LodgeNet Interactive, “TV systems in more than 5,500 hotels began showing public service announcements that encourage anyone observing suspicious activity to immediately report it to the proper authorities. The videos are being shown on a free promotional and information channel that is part of LodgeNet TV systems and appears when the guest room TV is turned on.”

A DHS Hotel & Lodging Advisory flyer filmed inside a hotel in Orlando Florida lists, “visitor attitudes overtly concerned with privacy” as a sign of terrorism, as well as “denial of access to a room,” or guests who take photos and video footage.

Exactly what constitutes “suspicious activity” was also outlined in a previous Homeland Security PSA entitled ‘No Reservations – Suspicious Behavior in Hotels’, which encourages hotel employees and guests to be on the lookout for terrorists.

Banal activities such as paying for a room with cash, even if the individual presents ID, or being “nervous,” were characterized as a suspicious behavior indicative of terrorism by the DHS as part of the federal agency’s ‘See Something, Say Something’ campaign. The clips shows a hotel manager calling the police after a guest says he doesn’t use credit cards.

This is merely one example of a huge network of citizen snoops being recruited to spy on the American people, despite the fact that you are more likely to be killed by intestinal illnesses, allergic reactions to peanuts, bee stings, drowning in the bath, or accident-causing deer than by terrorists.

As we have documented, every historical example of such informant programs illustrates that they never lead to a more secure society, but instead breed suspicion, distrust, fear and resentment amongst the population. The only “benefit” that such programs have ever achieved is allowing the state to more easily identify and persecute political dissidents while discouraging the wider population from engaging in any criticism against the government.

Over the past few years, we have highlighted innumerable other examples of how the DHS and other federal agencies are turning the citizens against each other and in the process distracting them from a far bigger threat – corruption and malfeasance within government itself.

- Rental car companies and other retailers are now asking customers a laundry list of questions to ascertain whether they could be terrorists in response to a joint FBI and DHS bulletin which characterized activity such as paying with cash or being “overly concerned about privacy” as a potential indication of terrorism.

- Large cable television companies in the United States are training their employees to look for suspicious behaviorand report it to police under the guise of neighborhood watch initiatives that have their origins in a 2002 program named Operation TIPS. The program was supposedly nixed by Congress yet continues in a myriad of other forms under the auspices of the DHS, including programs that train garbage men to spot terrorists during their rounds.

- In July 2008, we reported on how hundreds of police, firefighters, paramedics and utility workers were trained and dispatched as “Terrorism Liaison Officers” in Colorado, Arizona and California to watch for “suspicious activity” which is later fed into a secret government database.

- An FBI advisory aimed at Internet Cafe owners as part of the Communities Against Terrorism (CAT) program instructs businesses to report people who regularly use cash to pay for their coffee as potential terrorists.

- Under the same program, the FBI also defines bulk buying of food as a sign of potential terrorism and encourages retailers to report such behavior to the authorities.

- DHS promotional videos for the ‘See Something, Say Something’ campaign have portrayed routine behavior as suspicious, including opposing surveillance, using a video camera, talking to police officers, wearing hoodies, driving vans, writing on a piece of paper, and using a cell phone recording application.

- During last year’s Super Bowl, the DHS trained thousands of fast food sellers and other vendors to spot terrorists under the “First Observer” program.

- As part of the ‘See Something, Say Something’ program, Walmart stores across the country play an Orwellian video message featuring Janet Napolitano which encourages shoppers to spy on their fellow citizens.

Watch a satirical video below illustrating the DHS snitch program in action, a skit that is too close to the truth for comfort.

***Paul Joseph Watson*** *is the editor and writer for Infowars.com and Prison Planet.com. He is the author of Order Out Of Chaos. Watson is also a host for Infowars Nightly News.*

# Terrorists still pose threats to hotels

**By Anthony C. Roman**

Source:http://www.hotelnewsnow.com/Articles.aspx/5571/Terrorists-still-pose-threats-to-hotels

“This blood will be a curse that will chase the Americans and their agents, a curse that will pursue them inside and outside their country”

(Credit: CNN.com)

The death of Osama bin Laden has raised the question: Are we safer in a post-bin Laden world?

It is not easy to make a clear-cut prediction. To understand the current risk to travelers and the hospitality industry, it is worth understanding the elements that lead to the death of bin Laden and its affect on Al-Qaeda’s ability to wage war and continue on its quest of terror.

During the Obama presidency, there was a quiet but important shift toward counterterrorism versus counterinsurgency. Simply put, improvements in human intelligence gathering, changes in military tactics, the development of new technology, and the honing of military special operations, have effectively eliminated or captured a substantive number of Al-Qaeda’s battlefield commanders and mid-level terror operatives globally. This has progressively diminished Al-Qaeda’s ability to wage war and terror during the past two years.

The recent raid that resulted in the death of Al-Qaeda’s ideological and military leader is significant not only tactically, but operationally. Tom Donilon, President Obama’s national security advisor reports “… a small college library of material was taken” from the bin Laden compound.

 This should provide a treasure trove of intelligence. The apparent conclusion would be that the ability to further reduce the risk of attacks in a post bin Laden world is excellent.

Does this mean our hotels and corporate centers are safer now? Like the problem, the answer is disturbing: Yes and no. It is clear Al-Qaeda’s ability to carry out large-scale, well-organized 9/11 style attacks has been successfully diminished. Their network is under serious threat as well.  But the analogy that a wounded creature is at its most dangerous may hold true here.

So what do we believe is the current threat against our industry, executives, transportation, and the world? It comes from three likely sources:

• The lone wolf: A radicalized individual who is moved to militancy because of bin Laden’s death.  
• Fringe terror cell: A loosely organized, low-level Al-Qaeda network cell that provides routine logistical support moves towards militancy.

• Sleeper cell: Well-trained, motivated militants prepared to lose their lives in a previously planned terror operation that is triggered into action by a specific sequence of events or command.

All three pose  serious threats to  porous, high-value targets that will have high concentrations of people, deep financial impact, and draw keen media attention—Al-Qaeda’s modus operandi.

Hotels and resorts pose attractive targets for these threats. A recent example is the Times Square bomber, who, if successful, would have devastated a major hotel and caused countless deaths and casualties. It would have had serious consequences for the hospitality industry and the economy of New York City. Ripple effects would have progressively spread worldwide.

Al-Qaeda may cite Americans as their target for revenge, but their history leaves no doubt, no one or business is really safe.

# Hotel protection strategy in a post-bin Laden world

Al Qaeda’s unprecedented success in attacking military, government, transportation and business targets with the aim of causing massive damage and casualties is not arguable. The question we must now face—and one I raised in part 1 of this series—is, “Are we safer in a post-bin Laden world?”

As previously outlined, we have with increasing success diminished Al Qaeda’s ability to launch large-scale attacks. All levels of the terrorist group have been disrupted in the absence of its leader. However, Al Qaeda continues to pose serious threats, including the Lone Wolf, the Fringe Cell and the Sleeper Cell (see part 1 for details). All three risks, in many ways, are more difficult for intelligence sources to detect and therefore to counter. Although now they are less likely to cause massive casualties, attacks by operatives from these three categories pose crippling risk to life, property and business operations.

The nature of terrorism is evolutionary. Al Qaeda will continue to adapt despite this serious setback. Splinter groups likely will form as a result of ideological, religious, tribal and geographical loyalties. Yes, the glue that has bound them may have been removed; nonetheless, their ideology lives and the result will remain the same. Attacks will continue until a socio-political solution is achieved. This will take a generation or more.

**Protection strategies**

In formulating a protection strategy for our business centers, hotels, resorts and executives, we should evaluate the nature of terrorist groups. They adapt to changing defensive strategies. They conduct surveillance of potential targets. They identify weaknesses. They thrive on targets that suffer terminal routine. They move against businesses that are administratively and logistically unprepared to detect, deter and prevent an attack.

The peculiar difficulties posed in detection and deterrence also are compounded by the risk that an attack may be launched from within the ranks of your employed staff or by the very guests you are trying to protect, as well as a visitor or seemingly random intruder.

Protection against these risks follows several fundamental principles which form a layered defense that considers: all administrative policies, procedures and protocols; the integration of risk management and security departments; and the prolific use of IT and security technology.

Some special areas of consideration are:

* employee and guest due diligence;
* risk management and security training;
* risk management and security protocols;
* IT department security compliance;
* software management of critical data flow—quantitative and qualitative;
* current generation security software and cameras with analytics; and
* special attention areas and items—outdoor perimeter; lobby; non-public access and obscure locals; boiler and machinery; storage area for flammables; and anywhere large groups congregate.

The preceding is not meant to replace an all-inclusive assessment. It touches on a number of limited but primary principles and areas that require attention in order to promote further evaluation of your facilities, to promote consideration of new protocols and to provoke thought and management discussion. The risk of maintaining the status quo is, by the nature of the threat, unthinkable.

***Anthony C. Roman*** *is the CEO of Roman and Associates, Inc. a global investigation and security & risk management program consulting firm based in the New York metropolitan area. He is the software designer of WEB TRAC©, a business and security risk management intelligent software program. This firm specializes in corporate, legal, and insurance investigation and security and risk management program consultation. Mr. Roman is a former Adjunct Instructor at the State University of New York Aerospace Department*.

|  |
| --- |
| How to protect your hotel from the threat of terrorism  **By Chris Phillips**  Source: http://www.bighospitality.co.uk/Business/How-to-protect-your-hotel-from-the-threat-of-terrorism  ***Chris Phillips****, a former head of the National Counter Terrorism Security Office (NaTSCO) and a consultant at Wilkinson Construction Consultants outlines how hotels and other hospitality businesses can protect themselves from a terrorist attack.* |

**Terrorism: the implications for hotel management agreements of events outside owners’ and operators' control**

Source: http://www.mayerbrown.com/publications/terrorism-the-implications-for-hotel-management-agreements-of-events-outside-owners-and-operators-control-03-02-2010/

Bombings and attacks on hotels in India, Indonesia and elsewhere are major concerns for hotel owners and operators alike. Quite apart from the obvious primary concern for staff and guest safety, terrorist events outside the control of an owner or operator present significant issues of risk allocation for both parties under hotel management agreements. This note identifies those provisions in hotel management agreements to which both owners and operators should pay particular attention when negotiating agreements in today's environment.

There needs to be legal certainty and fairness in how risk is apportioned between owner and operator. This particularly applies to significant provisions that deal with repair and restoration of the hotel, appropriation or forced alteration of a hotel, force majeure, guest liability, and insurance.

**Repair and restoration of a hotel**

Where a terrorist event has significantly damaged a hotel, one of the key questions a hotel owner will likely ask is, "Should I restore my damaged hotel or would it be better to start afresh with an entirely new class or even new type of property?" He or she may, however, be contractually bound to the operator to reinstate the hotel and accordingly have no opportunity to exercise his preference.

Under a management agreement the obligation on the owner to reinstate the hotel usually depends on the extent of the damage. Only if the costs of repair exceed a specified threshold, will the owner have the right to terminate the management agreement without payment of compensation to the operator and start again.

What is useful from an owner's perspective is to have another, lower, threshold which is applicable when the damage is not covered by insurance. The determination of both thresholds is a matter for the owner and operator to negotiate. The thresholds are usually defined by reference to the cost of repair and the expected duration of the repair works. Clearly having a low threshold, particularly for damage not covered by insurance, is very important for every owner. From an owner's perspective, it would be ideal if the owner has the discretion to decide whether to undertake the repair works based on whether it is economically feasible to do so. However, from an operator's perspective, there should be an objective threshold determining whether owner should repair the hotel.

If an owner does not repair and restore the hotel and the hotel management agreement is therefore terminated, there are two further issues worth considering: firstly, who is entitled to the insurance proceeds (if any), and secondly, whether the operator should have a right of reinstatement if the owner rebuilds a hotel after termination. An operator would argue that the insurance proceeds should be shared equitably between the parties, while an owner would argue that priority should be given to the owner's recovery of its investment.  It is quite common for the operator to have a right of reinstatement if the owner rebuilds a hotel of similar class and standard within 2 or 3 years after termination, but this period should not be too long.

In some cases, operators even ask for payment of compensation from the owner in the event of such termination. Owners often try to resist this or at least try to limit the amount of compensation payable to the operator by the amount of insurance proceeds recovered by the owner that represents operator's loss of income for business interruption.

**Appropriation and forced alteration of a hotel**

Although not directly relevant to terrorist events, there is always a possibility that a hotel becomes appropriated by a government or an army. In such a situation, an owner will generally have the right to terminate the management agreement without payment of compensation to the operator if the hotel is taken for a long period of time, often 12 months.

If the length of “appropriation” is shorter than the specified period, the owner will normally be obliged to repair and reinstate the hotel after the “appropriation” unless there is an excessive cost of repair, as discussed above.

There is also a question as to whether the term of the contract should be extended in such circumstances by the period of "appropriation".

In Hangzhou, China, there were reports that the local authorities might impose an order on the Shangri-La to remove the top few stories of its hotel to meet new height restrictions as part of Hangzhou's drive to attain UNESCO heritage status.

This would amount to a partial appropriation and should also be dealt with in the management agreement by providing a right to terminate if the appropriation makes it commercially or practically impossible to operate the remaining portion of the hotel as a hotel of the same class and standard.

The issue of who is entitled to any appropriation awards should also be considered. The principles discussed above in respect of entitlement to insurance proceeds for repair and restoration of a hotel apply to this issue.

**Force majeure**

Force majeure may be regarded by some as a boring boilerplate provision. Yet in the aftermath of a terrorist attack (or other major incident) it can become key to the operation of the whole agreement.

Following a terrorist attack, hotels in a city, country or even region may experience difficult trading conditions. Hotel operators may well struggle to meet their performance tests. Whether this will trigger performance termination will depend on how the force majeure clause is drafted.

Equally there may be hotel operators who continue to miss performance targets well after recovery. From an owner's perspective, it will be important that such an operator is not able to use a force majeure clause to excuse poor performance. From an operator's perspective, it is critical that it does not fail the performance test for reasons unrelated to its performance and that are not within its control.

Force majeure provisions might be used by either owner or operator and drafting need not favour one or the other. It is, however, important to ensure that there is complete clarity on what is included and when it will apply.

**Liability towards guests**

Hotel guests who are victims of terrorist attacks may bring claims of negligence against hotels which have suffered such attacks but, who is responsible for such claims, particularly where there is a gap in insurance coverage?

Hotel ownership will always involve the assumption of risk in relation to large personal injury claims. This liability may be direct. The operator will usually insist that the owner indemnifies them for most, if not all, risks.

Given the extent of possible claims, owners are advised to ensure they negotiate indemnity clauses so that these are fairly balanced with reasonable carve-outs of the indemnity they give operators and ideally with some form of reciprocal indemnity from the operator to the owner. Indemnities in relation to the negligence of the general manager and other key staff are particularly worth arguing for (although these are usually capped).

It is also preferable that owner and operator work together to ensure that reasonable care standards are met. This may include implementing appropriate security policies, providing crisis management training to all employees and regular reviews of how the hotel itself may be made more secure.

**Insurance**

Where there is a terrorist attack, the question of terrorism insurance becomes fundamental.

Owners are advised to consult their insurance brokers at an early stage and to explore the availability of terrorism insurance for the relevant market. Terrorism is typically excluded from most insurance policies, but in limited cases, may be written into the policy for an additional premium. In the absence of terrorist insurance, liabilities are likely to be borne entirely by the owner unless the hotel is located in a country where the government will step in to meet liabilities or provide other financial support.

In deciding the type and extent of insurance necessary it is always useful for the owner and operator to work together with their respective insurance brokers to agree on common ground. During the negotiation of management agreements, key issues often include who bears the cost of the insurance, what happens if one party invalidates the insurance and the consequences if a specific type of insurance is not available in a particular market.

**Conclusion**

Increasingly, hotels seem to be the unlikely victim of many events outside the control of both owner and operator. Although the likelihood that the above provisions are triggered is relatively small, the economic impact on owners and operators is great. A fair and well thought out management agreement needs to provide protection for the interests of both parties and to provide sufficient clarity to help both parties in the aftermath of such events.

## The Impact of Terrorism and Economic Shocks on U.S. Hotels

**By Cathy A. Enz Ph.D., Renáta Kosová Ph.D., and Mark Lomanno**

Source: http://www.hotelschool.cornell.edu/research/chr/pubs/reports/abstract-15481.html

Using data on 34,695 hotels from 2000–09, this study examines how the external shocks of the terrorist attacks on September 11, 2001, and the financial crisis of late 2008 affected aggregate occupancy, price (average daily rate), and revenue per available room (RevPAR) within the U.S. lodging industry. We found that the unexpected nature of these shocks did create fluctuations in occupancy and average daily rate, when controlling for the impact of other important hotel factors such as seasonality, segment, and hotel size, and for local economic factors. Although the industry was noticeably affected by the 2008 financial crisis, the impact of the 2001 attacks was both more negative and immediate in terms of drops in occupancy, ADR, and RevPAR. The isolated effects of the terrorist attacks were greatest immediately after the event, while the impact on hotel performance from the financial crisis worsened over time, with the most negative impact coming two months after the fall of Lehman Brothers. Exploring the differential impact of these shocks on various hotel segments revealed that higher-end hotels were more susceptible to their negative impact, but those hotels also made strong rebounds after four months. In contrast, limited-service midscale hotels were more negatively affected by the financial crisis than were midscale hotels that serve food and beverage. The reverse was true following the terrorist attacks.

►Register (free) at the end of the summary to gain access of full paper.

## Safety and Security in U.S. Hotels

**By Cathy A. Enz Ph.D.**

Source: http://www.hotelschool.cornell.edu/research/chr/pubs/reports/abstract-15092.html

An investigation of the physical attributes or features that signal safety and security in a sample of 5,487 U.S. hotels revealed significant differences in the distribution of these key amenities in various hotel price segments and geographical locations. Differences in these physical attributes were also found among hotels of various sizes, ages, and locations (e.g., urban, airport, small town). An analysis of hotel index scores across several different categories revealed an average safety-index score of 70 and a security index score of 64 out of a possible score of 100. Overall, luxury and upscale hotels, airport and urban hotels, large properties, and new hotels are most likely to maintain a high level of safety and security amenities. In contrast, old, small, and budget motels are the properties most challenged in providing those safety and security features.

►Register (free) at the end of the summary to gain access of full paper.

# New strategy will train shop and hotel managers to tackle terrorist threats

Source: http://www.guardian.co.uk/uk/2009/mar/24/anti-terror-al-qaida-weapons

Members of the public will be encouraged to confront people who "threaten democracy" while more shop and hotel managers will be trained to deal with terrorist threats, as part of the government's new anti-terrorism strategy to be launched today.

Contest 2, billed by ministers as the most comprehensive approach to tackling terrorism by any government in the world, will also outline the continuing threat from al-Qaida-inspired groups as well as putting renewed emphasis on the extreme risks from chemical, biological, radiological and nuclear weapons.

Speaking ahead of the launch, the home secretary, Jacqui Smith, said that there would be a greater emphasis on tackling terrorism through "civil challenge". She told Radio 4's Today programme: "Where people may not have broken the law but nevertheless act in a way that undermines our belief in this country, in democracy, in human rights, in tolerance, and free speech, there should be a challenge made to them, not through the law but through a civil challenge." She added: "We should argue back, we should make clear that those things are unacceptable. And I think that the vast majority of communities from all different religious and other backgrounds support those shared values and want to make that challenge." Smith denied that the move represented a switch in strategy but added: "It's tougher in defending the values that we share, values that terrorists seek to undermine when they attack us."

Smith said that 30,000 workers had been trained to help respond to a terror attack as part of the strategy, and said that programme would be extended to a further 30,000 people. The home secretary denied it amounted to "snooping". She said: "If terrorists want to target crowded places, the places where we live, work and play, I think it's right that we put in place, as we have done, a programme of training for the people that manage our shopping centres, pubs, restaurants, clubs and hotels. That's what we're doing to help people be vigilant of the threat from terrorism and to deal with a terrorist attack were it to happen. That's not about snooping, that's about the widest possible range of people helping to keep us safe in this country."

Experts have spent a year preparing the document to take into account lessons learnt from recent terror outrages such as the attacks in Mumbai last year, although there is not thought to be any intelligence of groups plotting to target hotels in the UK in the same way.

For the past six years, the Contest strategy has been divided into four strands – Prevent, Pursue, Protect and Prepare. These cover preventing radicalisation of potential terror recruits, disrupting terror operations, reducing the vulnerability of the UK and ensuring the country is ready for the consequences of any attack. The Prevent strand will face particular scrutiny after criticism that public money was not being well spent on discouraging extremism.

The strategy will include a section on preventing the radicalisation of Muslims. Writing in the Observer, Gordon Brown said the government's strategy was not just about training and equipping professionals, but also preventing people from becoming radicalised and better informing the public so everyone would become more vigilant.

"The approach we are taking tackles the immediate threat through the relentless pursuit of terrorists and disruption of their plots, builds up our defences against attacks and our resilience to deal with them," he said. He also said that it also "addresses the longer term causes ‑ understanding what leads people to become radicalised, so we can stop the process".

A Home Office spokesman said the new paper would take account of the way the terror threat has evolved and how the authorities were learning lessons from events.

The terrorism threat level, set by the Joint Terrorism Analysis Centre run by the security services, has since July 2007 been "severe", which means that future terrorist attacks are highly likely but not thought to be imminent.

By 2011, Britain will be spending £3.5bn a year on counter-terrorism. The number of police deployed on counter-terror work has risen since 2003 from 1,700 to 3,000, while the security service MI5 has doubled in size over the same period. Between 2001 and 2008, almost 200 people have been convicted of terror-related offences.

Securing High-Risk Hotels

**By John J. Strauchs, CPP**

Source: http://www.securitymanagement.com/print/9976

There is an old saying favored by terrorists: “Why attack the mighty lion when there are so many sheep to be had?” That mind-set, shared by many violent extremists, explains why terrorists attack soft targets—especially hotels and resorts.

Since 9-11, there have been at least 62 attacks against hotels [1] in 20 different countries. Among major recent examples are the 2008 assaults on the Oberoi Trident and Taj Mahal Palace hotels in Mumbai, India, in which 71 people were killed and more than 200 injured. During the same year, the Marriott in Islamabad, Pakistan, was reduced to rubble by a dump truck filled with explosives. At least 54 people were killed and 266 injured. In 2009, suicide bombers attacked the Jakarta, Indonesia, Marriott and Ritz-Carlton hotels. Nine people died there and 53 were wounded.

In the face of this type of threat, property owners, architects, and engineers responsible for lodging properties must find ways to balance their desire to make guests feel welcome with their need to keep guests as safe as possible.

While many security experts would agree that the most effective terrorism countermeasures for a hotel or resort are administrative and operational, also important is the ability of architects and engineers to mitigate risk in the design process.

**Think Creatively**

A combination of innovation and rational planning at the architecture and engineering (A/E) design phase can yield cost-effective solutions that will help mitigate the risk of a terrorist attack. For that creative process to occur, however, those in charge must be open to the possibilities. They must fight institutional cynicism and avoid risk-assessment methodologies that stifle innovation and nudge architects and planners toward expensive one-size-fits-all strategies. An unfortunate example of the latter is that every U.S. federal courthouse is now mandated to have virtually the same level of security [2]regardless of whether it is in Bangor, Maine, or in midtown Manhattan.

During the A/E design concept stage, architects and engineers should work with security professionals to develop a series of likely security scenarios and possible design responses ranging from basic security countermeasures to high concepts. These should be discussed with the facility owners and adjusted based on their preferences, goals, andbudget constraints.

Some, or even most, of the high concepts may be impractical for most sites, but each should be carefully evaluated. Similarly, with regard to innovative proposals, none should be dismissed out of hand. It is too easy to miss innovative opportunities if new ideas are perfunctorily discounted or if, at first glance, something seems to be unrealistic because it has never been attempted or doesn’t conform to conventional thinking. Even an idea that is ultimately deemed unworkable can potentially contain the germ of a new approach, but the idea has to be vetted for that seed to be discovered.

These deliberations must include discussions about designing against and responding to bomb blasts and armed attacks. An overarching goal is to create effective countermeasures to these threats. The challenge is to do so without negatively affecting the facility’s aesthetics or inconveniencing guests.

**Bombs**

Three primary categories of bomb threats should be addressed: improvised explosive devices (IEDs); vehicle-borne improvised explosive devices (VBIEDs); and walk-in suicide bombers wearing explosive vests. The input of a qualified blast engineer should be sought when designing these countermeasures.

In all of these cases, a primary consideration is collapse mitigation. During the Oklahoma City bombing in 1995 [3], half of the building crumbled within minutes of the detonation of the 5,000-pound truck bomb and caused an estimated 80 percent of the fatalities. Beams, girders, and columns should be carefully designed to prevent a sudden progressive collapse.

As a simplified example of this type of structural failure, the loss of an exterior column should not result in the upper levels immediately giving way. The building connections can be engineered so that even after a major explosion within the facility, the structure will survive long enough to allow occupants to evacuate.

The facility should be hardened at vulnerable, critical, and high-risk locations, especially areas where security and life-safety systems are vulnerable. In the security command center and throughout the hotel, electronic systems supporting security operations should be designed to survive a detonation. Adequate sources of emergency electrical power should also be incorporated into the design.

Designers should consider the use of pressure-release walls to direct blast overpressures away from areas where there would normally be a lot of people. (Overpressure is the pressure caused by the explosion that is over and above the normal atmospheric pressure. That is what constitutes the bomb blast or shock wave. At a certain level, it can shatter glass [4]. At another level, it can cause catastrophic organ failure and instant death.) They should also carefully consider where emergency assembly areas will be outside of the hotel following either an interior or exterior blast. These areas may be the planned location for a delayed secondary detonation, either by another bomb or by a suicide bomber—a recent evolution of terrorist tactics. To help defend against this, all possible post-primary incident assembly points should be away from areas with a lot of glass.

The building’s windows, frames, and walls can be designed to withstand higher PSI (pounds per square inch) loads on the basis of a blast analysis. The amount of glass in exposed facades should be reduced or the orientation of glazed areas changed to minimize the effects of blast overpressures.

Glass shards cause the majority of injuries during a bombing. Laminated glass is the preferred glazing to reduce shards. It should be used for all glazing, especially at vulnerable locations, such as external walls near streets where a truck bomb could be parked. This type of special glass consists of layers of glass held together by interlayers of sticky materials like polyvinyl butyral.

Another way to mitigate the risk of shards is to cover windows on the inside with window treatments, such as blast curtains. Film appliqués can also be applied to prevent or minimize flying shards by retaining the shards on the film. This is, however, the most expensive option because the film must be periodically replaced due to normal wear and tear.

**Setback**

Outside, there should be as great a distance as possible between the facility and the likely positioning of VBIEDs, because the overpressure or blast shock wave gets weaker as it travels. Known as “setback” or “stand-off,” the importance of this distance to mitigate the effects of explosions cannot be overstated, but it is equally important to acknowledge its limitations.

It is not widely publicized that setback standards and guidelines are usually based on comparatively small explosive-charge weights. The U.S. federal government restricts revealing the amount of TNT-equivalent explosives used to calculate minimum acceptable setback distance, therefore, it cannot be revealed here. It must suffice to say that it is a low figure. As a result, private-sector enterprises meeting these setback standards in good faith can be operating under a dangerous false sense of security.

The setback distances [5] required to adequately protect against large bombs can be great. For example, a safe setback for a large truck filled with 4,000 pounds of explosives may be more than 900 meters (or slightly more than half a mile). The attack on the Islamabad Marriott involved at least one ton of explosives and large charge weights have been employed by terrorists in other attacks, such as 10,000 pounds in the attack against the Khobar Towers in Saudi Arabia in 1996.

As noted, the idea of the setback is to put the building out of the range of the explosive blast or shock wave as much as practical. The effects of explosive overpressure are calculated on the basis of the inverse of the cube of the distance apart. Because the value is cubed, the destructive effects of a blast lessen exponentially as distance increases. Therefore, every meter of setback is vitally important. This said, such massive setbacks are unrealistic for many project sites, especially in dense, urban environments.

Optimal setback is rarely achievable, but other design elements can help to mitigate the risk. All vehicle ingress and egress routes, including the delivery and loading dock, trash pickup area, and guest and visitor parking locations should be planned to minimize the effect of VBIEDs. If possible, roadways that are perpendicular to the hotel should be blocked because of the high speed an approaching vehicle could attain. A location where vehicles can be inspected should be established at a safe distance. The distance between this vehicle control point and hotel entry points should be as great as possible.

Another facet of the design should be a hardened and protected post from which armed security officers can monitor the vehicle control point without likelihood of being entirely suppressed during an attack. Yet another part of the plan might be to subtly design vehicle entry control points that “lock-in” vehicles while they are being inspected and the driver’s credentials are being examined.

Designers should avoid creating underground parking beneath the hotel. For the possible consequences, we only need look to the 1993 attack on the World Trade Center when a 1,336-pound truck bomb was detonated below the North Tower, beneath the lobby of the Vista Hotel. If an underground garage can’t be avoided, robust columns and thicker upper floor slabs in parking areas should be used and connections made more ductile. Beyond design would be policies and procedures that control access to the garage as well as monitor for suspicious activity.

None of this has to appear to guests and visitors as overwhelming security. For example, hotel staff drivers at the control point could take over arriving vehicles, including those of guests who have chauffeurs. This can be presented as a service while it simultaneously allows security to carefully inspect the vehicles and to control their movement. It also allows the hotel to control all vehicles entering underground parking. This practice was implemented by the Vista Hotel following the 1993 New York City World Trade Center bombing. Most guests welcomed the valet parking and being treated like VIPs and only a few recognized it as an antiterrorism countermeasure.

**Armed Attack**

The architecture and engineering design process can mitigate the risk of armed attacks using many of the same countermeasures applied to bomb threats. There are, however, some critical additional design criteria to address this specific threat.

The property boundary should be studied to discover any feature that might enhance or hinder both terrorists and counterterrorism response forces. These features may include bodies of water; natural barriers such as boulders, hedges, and bushes; and topographic features such as hills or culverts. One high-concept idea to assist counterterrorism forces is to include secret entrance routes from the perimeter, as well as interior passages, for use in a terrorist hostage taking.

Additionally, the A/E design plan can include thermal imaging cameras to view heavily foliated areas of the perimeter as well as to monitor the status of vehicles parked close to the property. These thermal cameras can monitor the temperature of the engine compartment to detect whether a vehicle has been there many hours or was recently parked. This technique was effectively used by the World Trade Center before 9-11.

**Barriers**

Barriers and other design features can be used to prevent vehicles from crashing through the perimeter. Any barriers should be matched to the likely weight and speed of the attacking vehicle. The highest rated barriers—for example, those that have earned a K12 certification from the U.S. Department of State—are expensive and not needed if the only vehicles that could possibly access the area are less than 15,000 pounds in weight or if they could not attain a speed of 50 miles per hour due to the design of the roads leading to the facility. Robust overhead physical barriers can also be designed to prevent large trucks from entering areas intended only for passenger vehicles.

**Vents**

A flexible HVAC design can be used both for quarantine and for venting contaminants. HVAC air intakes should be placed either high on exterior walls or on the roof to make it more difficult for a terrorist to use those openings to carry out a chemical or biological attack. Airtight smoke dampers should be designed to allow security to remotely shut down or change air circulation.

**Water**

Potable water systems should be protected and fire water storage should be tapped in a way that preserves enough water for fire suppression but also allows for emergency potable water. Enhanced protection of fire system controls can be provided so that an alarm is annunciated if attackers attempt to shut down sprinkler and fire detection systems. On-site fuel storage should also be protected.

**Covert features**

A high-concept idea is the use of concealed remote-control security doors to allow certain areas of the hotel to either lock out invading terrorists or to lock them in to prevent them from reaching other guest areas. Another is to install entirely concealed video cameras with audio capabilities to allow responders to view the actions and movements of any persons who have taken over the hotel and are holding hostages.

**Countersurveillance**

Whether the plot calls for a VBIED [6] or an armed attack, terrorists usually spend many weeks, if not months, carrying out surreptitious surveillance and rehearsals beforehand. Terrorists use both fixed and mobile positions to watch the intended target. To possibly gain forewarning, static posts can be designed for use by hotel security officers trained to recognize such surveillance [7]. If this is not possible, dedicated CCTV cameras with analytic software can be used to monitor contiguous areas that may be used by terrorists for surreptitious surveillance. Security could also use automated vehicle license plate reader cameras and intelligent video analytics to spot vehicles that repeatedly drive by the property.

**Line of sight**

Designers should avoid convoluted designs for the face of the building and for interior corridors and entrances. Each hidden alcove, kink in a corridor, and recess in exterior walls might require a video camera at an average installation cost of $5,000 or more. Moreover, security guards are more effective when they have an unimpeded line of sight and can view clean, clear areas.

Hotels will remain terrorism targets for the foreseeable future. But with creative design and careful planning, they can mitigate the risk without ruining the lodging experience that guests seek.

***John J. Strauchs, M.A., CPP****, owned and operated a professional security and fire protection engineering firm for 23 years before starting his current private practice. Strauchs helped develop the U.S. Department of State, Office of Diplomatic Security, Antiterrorism Assistance training program for foreign law enforcement agencies. He is a member of the ASIS International Council on Hospitality, Entertainment, and Tourism.*

# Hotels Become a Favorite Target for Terrorists

Source: http://www.securitymanagement.com/news/hotels-become-a-favorite-target-terrorists-006186

Terrorist attacks against hotels have become more frequent and deadly since the events of September 11, 2001, says a private intelligence firm.

In a 12-page report, STRATFOR looked at the number of hotel attacks eight years before 9-11 and the number eight years after. It found that the bulls eye on foreign hotels catering to Westerners has grown significantly. Since 9-11, there have been 62 attacks against hotels in 20 different countries as opposed to 30 attacks in 15 different countries in the 8 years prior to it.

There are many reasons why jihadists have increasingly sought out hotels as targets, the private intelligence firm explains. First, the 9-11 attacks led many governments and militaries to "harden" the security around their installations and critical infrastructure. This has led terrorists to seek new, softer targets—crowded, poorly guarded public or semi-public facilities.

Hotels, because of their congestion, openness, and minimal security, "are the quintessential 'soft targets,'" according to the report. "They have fixed locations and daily business activity that creates a perfect cover for preoperational surveillance." Moreover, the hotel industry's ultra-competitive business environment makes hotel managers worry about inconveniencing its patrons with additional security measures they will find cumbersome.

Hotels also serve up two types of targets jihadists favor: Westerners and the indigenous local elite, which are frequently looked upon as collaborators with the West or apostate regimes. By attacking a linchpin of any tourism-based economy, terrorists know they can inflict tremendous economic pain, such as the November 2008 Mumbai attacks and the 2002 Bali nightclub bombings. It also doesn't hurt that hotels are places where men and women indulge themselves in each other, dancing, and drinks—all contrary to the Koran, STRATFOR reports.

Another related reason the firm believes hotels have come under greater attack is the changing nature of the jihadist threat. Radicalized and inspired by 9-11 and the wars in Afghanistan and Iraq, "grassroots jihadists" that have no contact with core al Qaeda or other professional jihadist networks have created their own jihadist organizations capable of conceiving and executing their own attacks. Because they lack resources, planning capabilities, and operational experience, these more amateur jihadists gravitate toward softer targets, such as hotels, according to the report.

STRATOR also discovered attacks against hotels have grown exponentially more lethal. There have been six-and-a-half times more people killed in terrorist hotel attacks since 9-11, while the injury rate has grown six-fold as well.

Improvised explosive devices (IEDs) are the most popular and deadly method of attack. The IEDs have been either hidden in cars or trucks or strapped to a bomber's body. But since security upgrades have been effective at stopping vehicle-borne IEDs, terrorists have directly strapped bombs to their bodies more and more since 2005. The latest attacks occurred in Jakarta, Indonesia, when two suicide bombers detonated themselves inside the adjacent JW Marriott and Ritz-Carlton hotels, killed nine and wounded 42.

"These attacks using what are essentially human smart bombs, capable of moving around and through security measures, have proven to be very deadly," the report says.

But the most infamous and deadly hotel attack came last November, when terrorist commandos stormed the Oberoi and Taj Mahal Palace hotels, killing 71 and wounding 200. "This incident," the report warns, "showed how an active-shooter situation carried out by well-trained militants can cause more casualties than some [vehicle-borne IEDs]."

The report recommends hotels undertake a vulnerability assessment to determine where their weaknesses are. If certain facilities sit inside a high-threat area, hotels should consider increasing the standoff distance between the hotel and vehicular traffic, bolstering their static security surveillance around the hotel's property, and consider adopting a protective surveillance program, which STRATFOR says "is the best means of interdicting hostile actions."

Explosive Testing of Window Systems – the Underlying Double-Standard

**By Kenneth W. Herrle, P.E., and Larry M. Bryant, Ph.D.**

Source:http://www.securitymanagement.com/article/explosive-testing-window-systems-underlying-double-standard?page=0%2C0

**Introduction**

As terrorist bombings have become more frequent worldwide, mitigation techniques for such hazards have become commonplace in the design and construction of occupied facilities. Window design, in particular, has seen major changes in recent years largely due to the significant hazards posed by flying glass fragments. Historically, many building occupants who are seriously injured or killed in blast events received their injuries due to flying glass fragments from the building’s exterior window systems. This potential hazard has prompted many federal agencies to mandate explosive testing to pre-qualify window systems prior to being installed in their facilities.

Explosive testing can reveal deficiencies in both new technologies and improperly designed window systems, in addition to providing valuable data for improved analytical methods and software validation.  Such tests can also provide:

* Proof of novel concepts
* General product validation
* Project-specific validation for a particular design loading and performance level
* Data for the development, improvement, and refinement of products, and analytical tools and methods

Because these tests provide real-world results, the explosive test bed has become a ‘proving ground’ for both newly-developed hazard mitigation technologies and project-specific designs.  An explosive testing project typically begins by determining the test objectives, selecting the test method to be used, and determining the applicable test standard required for the project.  Unfortunately, either through misinterpretation or ill-intent, compliance with selected test standards has been slowly falling by the wayside. Such practices can unknowingly compromise the validity of a test series. A basic level of knowledge regarding explosive testing and test standard provisions can help test sponsors ensure the efficiency and validity of their test series and keep them from falling victim to unscrupulous or unknowledgeable test providers. Manufacturers of blast mitigation window systems and products, who are typically the sponsor of many of these types of explosive tests, would achieve great benefit from knowledge of test procedures and test standard provisions. However, such knowledge can also prove useful for project managers, facility managers, designers, architects, and engineers who must make decisions regarding the use of tested systems in facilities with blast mitigation requirements.

**Test Standards**

Currently there are two independent test standards for explosive testing of window systems in the U.S. Both have their own specific markets:

* U.S. General Services Administration (GSA) Test Standard (GSA-TS01-2003)
* Used by the GSA and other non-Department of Defense (DoD) agencies who comply with the ISC Security Design Criteria
* Available at no cost from the GSA (http://www.oca.gsa.gov/ [1])
* ASTM Test Standard (ASTM 1642-04)
* Widely used by some DoD components
* Available for purchase from ASTM (http://www.astm.org/ [2])

At this time, universally accepted blast test standards in the U.S. only exist for window systems.  Accepted blast test standards have yet to be developed for other façade elements such as doors and walls.

**Test Standard Overview and Compliance – The Double Standard**

Both the GSA and ASTM test standards were developed to ensure an adequate measure of standardization and quality assurance in the testing of window systems.  Each standard contains the following general provisions:

* A listing of terms and definitions associated with the explosive testing of window systems
* Performance Criteria/Hazard Ratings
* A listing of test requirements, which include:

1. Allowable test methods (shock tube or high-energy explosive arena testing)
2. Blast load and explosive charge requirements
3. Test site and reaction structure requirements
4. Data collection and documentation requirements
5. Test specimen requirements
6. Test report requirements

With many similarities between the two, testing to either standard can typically be accommodated at the same test site through modifications of the test setup.  Unfortunately, with such similarities, distinctions between these two test standards have become increasingly blurred as test providers have slowly been intermixing differing components of each standard.  In addition, failure to include mandatory test requirements has become more commonplace.  Such behavior violates the protocol outlined in either test standard and has the potential for invalidating test results for unsuspecting test sponsors.

Fortunately, test sponsors can take precautions during pre-test planning to help protect the integrity of their test series.  The following recommendations can prove helpful in doing so.

For starters, the test sponsor should obtain a copy of the selected test standard prior to testing and become familiar with its requirements.  As part of the familiarization, distinction should be made between "test options" and "test requirements."  Test requirements are typically accentuated in the standards by phrasing such as “must,” “shall” and “as a minimum.” Each of these items must be accounted for in the tests, whereas test options do not.  For an explosive test to meet a selected test standard, all test requirements specified in the standard must be met.

The test sponsor should ensure that the test method being used meets the objectives of the test. For example, if the objective is to verify that the tested windows meet a specific GSA Performance Condition, it is unacceptable to perform the test using the ASTM Test Method. Conversely, if the test windows must meet a specific ASTM Hazard Rating, testing performed using the GSA Test Method is unacceptable.  In short, differing test methods and performance ratings cannot be intermixed; they are exclusive of one another.

Although explosive tests can be configured to meet both the ASTM and GSA test standards, there are numerous differences between these two methods that must first be addressed.  Several differences in test requirements between these two standards include:

* Interior high-speed photography requirements: Although the ASTM Test Method allows the use of high-speed video, it is not necessary for meeting the test method requirements. The GSA Test Method, on the other hand, requires that, as a minimum, interior high-speed video be recorded for each test specimen.
* Pressure gauge requirements (both number and location): The ASTM Test Method requires the use of three reflected pressure gauges mounted on the exterior of each test structure and use of a free-field exterior pressure gauge located near one of the test structures. The GSA Test Method, on the other hand, requires the use of two reflected pressure gauges mounted on the exterior of each test structure and the use of at least one interior pressure gauge located inside of each test structure (or inside of each partitioned volume).
* Requirements specifying the minimum number of test samples: The ASTM Test Method requires testing of a minimum of three samples for each blast load environment plus disassembly and measurement of a fourth sample. The GSA Test Method does not specify a minimum number of test samples (one is typically used), or that sample disassembly is required.

While these are just a few of the differences between the two test standards, they are provided as a starting point for the test sponsor to assure that the test provider is conducting the test in compliance with the correct test standard. The test standard selected for the project should be consulted for the full listing of requirements that must be met.

Prior to testing, the test sponsor should make an inquiry with the test provider regarding the adequacy of the test structures planned for the test. If the test structures do not meet the requirements, the validity of the test results may be questioned. The test sponsor should assure that all test structures are fully enclosed (on all sides) to prevent infill loads, and that the response limits of the test structures will be in adherence with the selected test standard when exposed to the target blast loads. Questions regarding acceptable test structure response limits should be raised if the test structures are constructed of materials such as wood or lightweight metal sheeting, as these materials are not commonly used in blast-resistant construction.

If multiple window units are tested side-by-side in the same test structure, make sure that provisions have been made to distinguish between the glass fragments generated by each window unit. This can be accomplished by using a different color glass for adjacent window units, or by physically segmenting the test structure into individual compartments to avoid fragment intermixing. Also be on the lookout for items that may affect the response of the window systems such as test structure framing components located directly behind window mullions or items located directly behind the window that may obstruct fragment flight.

An additional item that may compromise the validity of an explosive test, and should be addressed during pre-test preparations, is the failure to meet the minimum blast load requirements specified for the test. Typically, window systems are tested to meet a specific set of criteria which consist of load requirements for both pressure (psi) and impulse (psi-msec).  These load requirements are minimum baseline values for meeting the criteria. Post-test reporting of sub-baseline test loads as having met the baseline requirements, based solely on the rationale that the loads are within a specific percentage of tolerance, is unacceptable. Tests that do not meet or exceed minimum baseline values (both pressure and impulse) have not met the specified test criteria, and the validity of the test results in such cases is often challenged. Prior to testing, the test sponsor should verify with the test provider that the target test loads are expected to be either met or exceeded, and the test sponsor should request proof that similar loads have been achieved on previous tests.  Standard blast load calculations assume that the explosive event takes place at sea level and that the reflecting surface of the target structure is infinitely large. When calculating charge weight and standoff combinations for explosive tests, adjustments must be made for both the altitude of the test site (if not at sea level) and clearing effects on smaller test structures. Failure to do so will result in blast loads that are lower than predicted.

Both test standards provide a list of required items that must be included in the test report as a minimum.  The test sponsor should verify with the test provider that all test report requirements will be met.  Omission of any of the required items is in violation of the test protocol and compromises the integrity of the report.

**Test Objectives**

Prior to arranging for explosive testing, the final test objective must be decided.  Generally, there are two major categories of test objectives:

* Proof testing
* Data collection

Although these objectives have differing ultimate goals, they share many common benefits.  For example, although the ultimate goal of a proof test is to obtain a “pass/fail” rating for a given specimen and load combination, data collected from the test is also useful for other purposes, such as development and validation of analytical methods and software, as well as improvement of a tested product.  Such additional benefits may include:

* High-speed video footage for analyzing the time-dependent response of window systems
* Pre-test and post-test photographs and measurements for analysis/comparison of response between tested window systems, including failure modes and details

For example, high-speed video of the specimens during a test has been very useful in determining actual sequence and modes of failure in complex systems.  Such documentation has also allowed development and validation of analytical models. For example, the bite response model currently implemented in the national standard WINGARD series of window blast analysis programs evolved from test observations.

Similarly, testing conducted for the primary purpose of collecting data may also provide a “pass/fail” rating as a byproduct of the test.

**Test Methods**

Explosive testing is typically performed in either shock tubes or in large-scale, open-air arenas.  Shock tube testing is generally less expensive but is not as realistic as open-air tests.

**Shock Tube Testing.** During shock tube testing, the test specimen is mounted at the end of a structural tube.  A pressure pulse, generated at the opposite end of the tube from the test specimen, travels down the tube and impacts the test specimen.  Pros and cons of shock tube testing include:

Pros:

* Less expensive than large-scale arena testing when testing only a few samples
* Readily reproducible loads
* Can be conducted quickly

Cons:

* Generally limited to one specimen per test
* Generally limited to relatively small test specimens
* Difficult or impossible to achieve realistic open-air blast waveforms (typically the positive phase impulse may be too high and negative phase effects cannot be consistently replicated)
* Difficult to obtain high-quality video footage of the response

In general, shock tube testing can be a useful tool for conducting expedient, inexpensive snapshots of the hazard mitigation potential for small specimens.  However, a full-scale specimen will most likely have to undergo open-air testing to receive true validation within the government and commercial markets.

**Large-Scale Arena Testing**

Large-scale arena testing is conducted on an outdoor test bed using actual high-energy explosives and full-scale test specimens.  The pros and cons of large-scale arena testing include:

Pros:

* Large size (often full-scale) specimens may be evaluated.
* Multiple specimens may be evaluated simultaneously, reducing overall cost per specimen.
* Replicates actual explosive environments, resulting in realistic blast loading that includes both positive and negative phase.
* High quality video footage of the response is typically obtained, providing good scientific data, as well as dramatic marketing/demonstration video.

Cons:

* More expensive than shock tube testing when testing only one or a few samples.
* Adjustments to the test structure and/or charge size may be required to avoid reduced impulse due to clearing effects when using smaller test structures.
* May require longer lead times in test planning.
* Some variability in results due to real-world environment.

In general, large-scale arena testing allows documentation of a real-world response of multiple, full-scale test samples in an actual, high-energy explosive environment and generally provides more validity in both the government and commercial markets than shock tube testing.

Both the ASTM and GSA test standards allow the use of either shock tube or large-scale arena testing.

**Additional Suggestions**

Several additional suggestions that are not in either the ASTM or GSA test standard, but should be used by the test sponsor to help insure a successful test series include:

* Performing a pre and post-test walkthrough/inspection of the test setup with the test sponsor. During this inspection, be sure to check for correct installation of the test windows and be on the lookout for anything that may be out of place or doesn’t look correct. Be sure to alert the test sponsor of any concerns.
* Being prepared for the unexpected. Anomalies sometimes happen in explosive testing, so it’s best to know this before hand. In addition, many test sponsors arrive at the test bed with preconceived expectations of what should happen and how their product should perform. Please be aware that the purpose of the explosive test is to determine the real-world response of the window system (what really happens). Some test items perform better than expected, some perform worse, and some perform just as expected.
* Taking time to make sure that everything in the test setup is correct before proceeding with the test. Explosive testing is very expensive and there is only one chance to get it right. Do not rush.
* Shipping extra test samples to the test site. Window samples are sometimes damaged during shipment. In tests using multiple window systems, shortage of one window equates to loss of a tested system and a resulting higher per-unit test cost.
* Being sure to ask plenty of questions and expect the test provider to provide sufficient answers.

Additional measures can be taken to ensure compliance with test standards, but test sponsors must be aware that due to the complex nature of explosive testing, data, high-speed photography, or other critical test items may not perform as intended due to unforeseen circumstances.  Test providers should utilize a high level of quality control to mitigate the risk, but there is no guarantee that the testing will always perform as desired.

**Conclusion**

Although explosive testing of window systems can provide a significant contribution toward protecting the occupants of constructed facilities, caution must be exercised to assure that all goals and requirements of the testing are met.  With careful planning, well-informed decisions can be made which should lead to an efficient, productive, and valid explosive test series.

# From Jericho to Jersey Barrier

**By Richard Kessinger, CPP**

Source: http://www.securitymanagement.com/article/jericho-jersey-barrier

The ancient city of Jericho is described on one biblical Web site as surrounded by a great earthen rampart with a stone retaining wall at its base that was imposingly high and topped by a thick mudbrick wall. It was considered a formidable barrier that presumably gave the city great peace of mind. Unfortunately for the inhabitants, it was never tested for resistance to trumpets.

Vehicle barriers are for today's businesses what city walls were millennia ago. They represent a first line of defense against potentially devastating car-bomb attacks, which remain one of the most common and lethal weapons of choice for terrorists. If improperly designed, however, a vehicle barrier system may fail to prevent the intrusion of a threat vehicle. Great care must, therefore, be taken when selecting and designing this element of a security program.

The following overview of the proper process for the selection, placement, and installation of vehicle barriers can help companies avoid costly mistakes. The main considerations include a threat and risk assessment, an effective/appropriate design, and barrier selection.

**Risk assessment**

One of the first steps in the design process of a vehicle barrier system is a threat and risk assessment of the target facility. The assessment should be conducted by a security consulting or engineering firm that has experience in protecting structures from the explosive-vehicle threat and that has performed assessments at facilities similar to the site being evaluated. An independent consultant with no affiliation with a vehicle barrier vendor or manufacturer should conduct the initial assessment. However, the consultant should seek assistance from a manufacturer or its representative during the design phase, to assist in the planning and design of the vehicle barrier system for that facility. The consultant should also have professional certifications such as the Certified Protection Professional (CPP) and should be able to supply references that can be contacted by the contracting facility.

The assessments should determine whether the facility is a potential target for terrorists. Some potential targets include national or local symbols such as monuments and buildings, and symbols of capitalism, like companies identified with Wall Street.

The consultant should include the following in the analysis: a description of any threats to the facility, including threats with a low probability of occurrence but high consequences, like the 9-11 attacks; the identification of assets requiring protection and an assessment of their potential vulnerabilities; and a cost estimate of both direct and indirect losses that could result from the destruction of or damage to these assets. The consultants should also offer recommendations on countermeasures to reduce these vulnerabilities.

A bomb-blast analysis should also be included. The blast analysis uses physical inspections and computer modeling to assess the structure's vulnerability to a blast, and it offers recommendations on protective measures.

Security directors can use the threat and risk assessment report as supporting documentation when they go to senior management to request funding of their physical protection program. The report should include an analysis of the cost of countermeasures versus the potential cost of leaving the risks unmitigated.

**Design**

Once the threat level for the facility is identified and funding for the physical protection plan is in place, the design process for the vehicle barrier system can begin. The security consultant, the engineering firm, and the vendor should assist the security director with this part of the process.

Site survey. The first part of the design phase is the site survey and layout of the barrier system. The survey should use a scaled map that shows the terrain and identifies the location of structures, roads, and the property's perimeter. Based on this map, distances between the perimeter and the facility, the potential angles of approach to the target, and the maximum speed attainable by a vehicle can be analyzed. This information will help to identify the required levels of protection needed along the perimeter line. A traffic-flow study should also be conducted at the roadway entrances to see what effect vehicle-barrier systems would have on traffic entering the site.

Because force from an explosion decreases rapidly with distance, the most effective protection from an explosive- vehicle threat is a maximum setback zone. The setback zone, also known as the "standoff distance," is the distance between the vehicle bomb and the target building. For example, if the facility is 100 feet from an accessible location where a terrorist could park or drive a bomb-laden vehicle, then 100 feet is the standoff distance.

Vehicle barriers should be placed as far from the building as possible to ensure the maximum standoff distance from a bomb-laden vehicle. In one case the author worked on, building managers were planning to upgrade security by installing vehicle barriers around the perimeter of the building. However, they planned to place the barriers only seven feet from the building's façade. After the author made the point that a large car bomb could destroy a reinforced concrete wall from that standoff distance, they agreed to move the barriers to the curb line, which was 40 feet from the building.

Maximum footage is always desirable, but rarely practical in areas where real estate is valuable. In an urban environment, 12 feet--the distance from the curb to the face of the facility--may be the maximum achievable standoff distance. That's not ideal, but the placement of barriers at the curb may establish a physical and psychological deterrent. The barriers will also prevent a moving vehicle from penetrating the building and help to minimize any damage that could be inflicted by a stationary-vehicle bomb. Even at this reduced standoff distance, depending on the size of the bomb and design of the structure, a vehicle barrier may be sufficient to prevent partial or total collapse of the structure.

**Barrier ratings**

The next step in the design phase is selecting the type of barrier that will stop a defined threat vehicle. Because barriers are created to withstand a variety of vehicles and situations, the potential threat vehicles should be identified before choosing the barrier type.

To determine the proper barrier, the designer must determine the threat vehicle's kinetic energy (the force with which the vehicle will hit an object). A mathematical equation using the threat vehicle's total weight and speed determines this energy. An effective barrier must have the ability to absorb the energy of the impact and transmit that energy to its foundation.

To determine whether the barrier will resist the level of threat, it is important to determine whether the product has been crash-tested or has been put through a computer analysis that demonstrates its performance capability. The Department of State and the Department of Defense have developed certifications based on their crash-testing processes that are used to determine these standards. Certification levels are based on how far a vehicle of a given weight will penetrate a barrier at 30, 40, or 50 miles per hour.

The Department of State uses K and L ratings for their certification levels. The K level defines the speeds of a vehicle that the barrier is able to withstand. The L level indicates maximum allowed penetration of the barrier by the vehicle or its major components on impact. The vehicle used in the tests weighs 15,000 pounds. (@ Go to www.securitymanagement.com to see a table that illustrates the K- and L-level ratings used by the State Department.)

In one case, the author had a client with three access roads that led into the facility. To simplify the equipment purchase, the client planned to order the same threat-level barriers for each entrance. At the two access roads for which the barriers were designed, vehicles had to make 90-degree turns to enter the building, significantly reducing any vehicle's potential speed and ramming power. The third access point, however, was opposite a long straight road that could allow a large vehicle to increase its speed and ramming power before reaching the barrier. The proposed barrier could not meet the threat level of the third access point.

It was recommended that the company redesign the third entrance to slow potential threat vehicles or that it purchase a higher threat-level barrier. The company chose to purchase a higher threat-level barrier, which proved more cost effective than redesigning the access point.

**Barrier types**

Many types of barriers and combinations of barriers can be used to provide the best possible defense. Barriers can be active or passive, fixed or movable, and they may be categorized by their form into the following categories: bollards, wedges, crash beams, sliding gates, and portable barriers. Less effective and often misused barrier options include Jersey barriers, planters, and fencing.

Active and passive. Vehicle barriers are categorized as either active or passive. Active barriers require some action either by people or equipment to be raised and lowered or moved aside to permit vehicle ingress and egress. These systems include barricades, bollards, beams, and gates that are operated manually, pneumatically, or by hydraulic power units. Sand-filled dump trucks or heavy construction equipment can be used as a temporary active barrier. Active barriers should be used at locations such as a driveway, a parking lot, or a loading dock entrance and should be located as far from the building as practical.

A passive barrier, on the other hand, has no moving parts. Examples include bollards, guardrails, ditches, large reinforced concrete planters, hardened trashcans, benches, water fountains, walls, raised planting beds, earth berms, boulders, and Jersey barriers. Passive barriers should be used along the perimeter line. It makes sense to use active barriers at entrances and passive barriers surrounding the rest of the facility.

Project designers should make sure that the barriers do not obstruct pedestrians or emergency vehicles. The local fire department should be consulted to ensure that the barrier would not impede firefighters' access to the building. It is also important for a facility with a standoff distance of more than 60 feet to create an easy access route to the building for emergency and maintenance services.

Fixed or movable. Depending on how they are made and used, both active and passive barriers can be fixed or movable. A fixed barrier is one that is permanently installed or requires heavy equipment to move or dismantle it. Examples of these include hydraulically operated wedge-type barrier systems or bollards set in concrete foundations.

A portable or movable barrier system is one that can be relocated from location to location. This type of barrier may also require heavy equipment to move. Hydraulically operated, sled-type barrier systems or Jersey barriers are typical examples.

Bollards. Bollards are metal posts that are embedded in a concrete foundation at a depth of four feet. These are the most versatile type of barrier and can be fixed or movable. Retractable bollards can be operated manually or automatically with a hydraulic pump unit. Spaced three to four feet apart, bollards do not obstruct pedestrian traffic and can be aesthetically pleasing. To blend with any environment, they can be equipped with a cast sleeve of aluminum, bronze, or stone. Logos and crests can also be incorporated into the sleeves.

A fixed and installed bollard may range in cost from $1,000 to $4,000. The price depends on the threat level and architectural enhancements that are required. A retractable 3-bollard system raised and lowered by a hydraulic power unit costs between $50,000 and $88,000 installed. As with the fixed bollard, the exact price depends on the threat level, architectural enhancements, and operating system requirements.

Wedge barriers. Wedge barriers are rectangular steel plates that rise from 24 to 38 inches from the surface of the road at a 45-degree angle. This barrier system can be surface mounted, so as not to interfere with buried utilities. It can also be installed completely below the roadway. This barrier, equipped with a hydraulic power unit for automatic operation, costs between $24,000 and $80,000 installed, depending on the threat level and operating system required.

It is important to choose the type of barrier best suited for the building's conditions. A former client of the author's planned to use bollards at the entrance to an underground parking garage that was being designed for a new office building. The bollards were to be installed at the top of the ramp before the security checkpoint. This design created a problem because the security officer would have to lower the barrier before he or she could check the driver's identification, defeating the purpose of the system and creating a vulnerability in the building's security.

Because of the limited space in the garage, the author recommended a surface-mounted wedge barrier that would be located just beyond the security checkpoint. With this design, the officers could check the driver's identification and carry out vehicle searches while keeping the barrier intact. The author worked with the building's architect to incorporate the barrier in the ramp design.

Crash beams. Crash beam barriers have hydraulic drop arms that are equipped with a 1-inch steel cable and are supported by concrete footings placed on both sides of the road. The drop arm can be raised to allow vehicle access. When in the closed position, the arm and cable lock into the concrete footing on the opposite side of the roadway, preventing a vehicle from penetrating the barrier.

This type of barrier system should be used at semiactive or inactive access roads because the process of opening and closing the barrier can be lengthy due to its design. Operated manually, this type of barrier can cost between $16,000 and $36,000 installed. When the barrier is equipped with a hydraulic power unit for automatic operation, the cost increases to between $24,000 and $49,000 installed.

Sliding gates. The sliding gate uses a cantilever or linear gate design. When in the closed position, the gate leaf locks into steel buttresses that are embedded in a concrete foundation on both sides of the roadway. These gates can be architecturally designed to match any facility's environment and can cost between $34,000 and $72,000 when installed with a hydraulic power unit.

Portable systems. Portable barriers are the most recent addition to the family of barriers. These barrier systems require no roadway excavation and can be assembled and made operational in less than four hours. They are either crash-beam or wedge barriers, equipped with steel buttress boxes that can be filled with sand or concrete to limit movement if a vehicle hits the barrier. Some of the wedge-type barriers are equipped with wheels that can be removed after the barrier has been towed into place.

A number of these barriers also have State Department crash ratings. There is a drawback to this design, however. When hit by vehicles, these barriers move. Therefore, placement and standoff distance must be carefully assessed before installing this type of barrier, which costs between $34,000 and $64,000 installed when equipped with a hydraulic power unit.

Less effective options. Not every barrier provides a defense in the sense of protecting against vehicle intrusion. For example, Jersey barriers are passive barriers that can give a false sense of security at a facility because of their size and mass.

Originally designed as highway dividers to stop vehicles approaching at a maximum angle of thirty degrees, they were not designed to be a high-speed vehicle-arrest system. Even if placed correctly or linked together, the usefulness of Jersey barriers is at best limited. If improperly placed, they may not counter the threat at all. This option should only be considered a temporary security measure, never a permanent solution.

Planters are another type of passive barrier often used incorrectly. Although aesthetically pleasing, they must be large, heavy, and constructed with reinforced concrete to be effective--otherwise, they are simply a psychological deterrent. Planters also require proper placement and should be anchored to the ground for maximum strength. Landscaping in and around the planter is also important because improper planting material could actually aid the terrorist by providing concealment of a small explosive device.

Perimeter fencing is not an obstacle to vehicle penetration and should not be considered adequate protection. Like the other barriers discussed, however, fortified fences may deter a minor attack. Installation of two 3/4-inch cables attached to anchors set in concrete foundations at both ends can be a cost-effective method for reinforcing a fence against the threat of penetration by lightweight vehicles.

**Environment**

It is important for planners to consider the climate and geography of the barrier site. For instance, in cold climates, hinges, hydraulics, or barrier surfaces may require heaters and snowmelt systems to resist freezing temperatures and snow and ice buildup. In warm climates the barriers may require protection from excessive heat and humidity. In urban areas barriers may require protection from dirt and debris. Similarly, along coastal areas the barrier may need protection from salt water, sand, and a high water table. The water table should be analyzed before installation to determine whether a sump pump or surface-mounted barrier should be installed.

**Safety**

Active vehicle barriers can cause serious injury, and the installation of safety devices is recommended to prevent activation either by operator error or equipment malfunction. Vehicle loop detectors should be used to prevent the barrier from being accidentally raised in front of or under an authorized vehicle.

Warning signs, audible alarms, and traffic-safety paint should mark the presence of a barrier and make it visible to oncoming traffic. Red and green traffic signals should be installed and operated in conjunction with the barrier. The red signal should go on as the barrier begins to rise, and the green signal should illuminate only when the barrier is down. In addition, pedestrian traffic must be channeled away from the barrier by using sidewalks, landscaping, or fencing.

In one case, the author had a client who refused to install a traffic light in conjunction with the barrier because, he said, it would have cost too much and would not have been aesthetically pleasing. Even though the author stressed that the light was a safety issue, management refused to install it.

After one month and a number of vehicle accidents, the client decided to install traffic lights. Because the lights were not included in the original design, the barriers had to be retrofitted, which cost the company more than if the light had been part of the original installation. The company is also facing possible litigation from persons who were involved in accidents before the light was added.

Other functional considerations. Frequently used perimeter entrances may require a pneumatic or hydraulic control system designed for repeated opening and closing. These barriers can be operated from a staffed entry-control station or from a remote location, using CCTV and remote controls.

If the barricades are not under continuous observation, then tamper switches should be installed to the hydraulic pump unit doors to ensure that the barrier system is continuously controlled. These switches should be connected directly to the central alarm station so that security can monitor the barriers around the clock. To make the system more redundant in high-security applications, the barrier should be controllable from both the entry-control station and from another secure location within the facility.

Barriers must be capable of operating continuously and handling the facility's normal traffic flow with minimal maintenance and downtime. A barrier should take between 3 and 12 seconds to move from a full down position to a full up position to satisfy security requirements and control normal traffic flow.

The barrier should also have an emergency operation feature that is capable of raising the barrier to the up position in a shorter time period--0.6 to 3.0 seconds is the accepted standard, depending on the barrier size. Backup generators or manual override provisions are also needed to ensure continued operation of active vehicle barriers during power failure or equipment malfunction.

**Installation**

Installation is one of the most critical steps in the design and implementation phases and must be well planned to avoid problems that can result in high maintenance costs. It is important to select a barrier manufacturer that has assembly experience, has developed an operations history of its products, and hires an outside company to regularly conduct tests and create comprehensive reports of its products. The selected barrier company should ideally have been in business for at least three years and should have a strong track record in the design and installation of vehicle barrier systems. It should also offer a warranty for its products.

Most manufacturers will resolve problems that arise in their barrier systems if they install them or a company that has been certified by them installs them. In addition, the manufacturer should certify the installers and technicians used.

**Maintenance**

Planning for barrier maintenance must start during the design phase. Manufacturers should provide the purchaser with wiring and hydraulic diagrams, maintenance schedules, and procedures for their systems. They should also provide barrier maintenance support in the form of training and operation manuals. In addition, the vendor should have an inventory of spare parts available to maintain any of its barrier systems in operation.

Maintenance contracts are available from most manufacturers and are recommended to ensure proper operation of the barrier and to provide assurance that the barrier will function as intended. These contracts should include inspection, adjustment, cleaning, pressure checks on hydraulic systems, and replacement of worn parts.

**Operator training**

Training for security officers operating active vehicle barriers is strongly recommended to help prevent serious injuries, litigation, and damage to vehicles and equipment. Most manufacturers offer client companies operator training for their systems, which should be planned for during the design phase.

Security directors should also develop written procedures for the normal and emergency operation of the system. These procedures should include instructions for keeping the barrier in the up position until a vehicle has been properly identified and provisions for allowing emergency vehicle access. Training should also include how to identify a threat vehicle and how to handle an attack situation. In addition, security officers should be trained in how to check truck manifests and make cargo inspections.

**Controlling costs**

Because of their moving parts, active barriers have higher installation and yearly maintenance costs than passive barriers. For semiactive or inactive entrances, a manually operated system may be the most practical and cost-efficient option.

Another cost-effective measure is to minimize the number of access points to the facility, thereby reducing the number of entrances requiring active barriers. Integrating traffic-calming features into the access route, such as medians and landscaped islands, or redesigning the access road to slow approaching traffic is another option; it allows for the use of a lower threat-level barrier, which in turn reduces the cost.

Barriers can be made more aesthetically pleasing with the help of landscape architects who can use everything from boulders to raised planting beds in the design. But aesthetics can add to the cost of the barrier system. Some passive barriers, such as planters, are intrinsically aesthetic, but their maintenance and upkeep can add an additional annual operating cost.

When estimating the costs of the barrier systems, security directors should make sure to include all ancillary expenditures, such as the creation of an access road and the addition of an entry-control station, vehicle inspection area, turnaround lane, and lighting. They should also make sure that the project plan is not cutting corners for the sake of cost savings. As the earlier example about the traffic light illustrated, savings at the expense of safety will cost the company more in the long run.

Vehicle barriers are not a total solution and should be integrated with other security components and options such as fencing, CCTV, and access control systems to provide a comprehensive protection plan. But when properly selected, installed, maintained, and operated, barriers can raise the deterrence factor for a facility and lower its risk of becoming the victim of a vehicular attack.

**Richard Kessinger, CPP**, is currently a lead physical security specialist with the United States Capitol Police. Formerly, he was a security consultant for a number of years following a 20-year career in law enforcement. He has been involved with the application and installation of barrier systems at government and private sector locations. He is a member of ASIS International.

# San Diego Law Enforcement Warns that Hotels Could Be Used For Bomb-making Labs

Source: http://www.securitymanagement.com/news/san-diego-law-enforcement-warns-hotels-could-be-used-bomb-making-labs-008745

What do a slow cooker, a pack of coffee filters, and a chemical peel have in common? Probably nothing, unless you're in the illegal bomb-making business.

In a bulletin dated from March, but published yesterday (Wednesday, July 13) by Public Intelligence, the San Diego Law Enforcement Coordination Center (SLECC) warns that a combination of those and other household items could indicate the presence of a mobile bomb-making lab. Overseas cases have increased, the bulletin warns. Whether that means the trend will move to the United States is not known, but already there was the case of Najibullah Zazi, who booked a suite in New York city to make peroxide-based explosives, notes the bulletin. Luckily, he was caught before he could do anything with them.

Hotels are ideal for illegal labs – be it for meth or bomb making – because they provide an inexpensive and low-profile place to set up a mobile operation.

Often terrorists are working with various chemicals in rudimentary labs, so the compounds are often unstable. Hotel rooms allow them to set up labs fairly close to their targets without detection. Proximity to targets helps decrease travel time, which in turn decreases chances for premature detonation.

In addition to the Zazi case, the report provides other examples of terrorists using hotels to assemble bombs, including Lors Doukaiev, who was injured when a bomb he was assembling in his Denmark hotel room detonated.

It helps if nonsecurity personnel, such as hotel staff, are also trained to look for signs of suspicious guest activity, because security personnel are "limited in number,” Elinor Garely, a travel writer and business management professor at the City University of New York told Security Management in 2009 on hotel security (**Ensuring an Uneventful Stay**, April 2009).

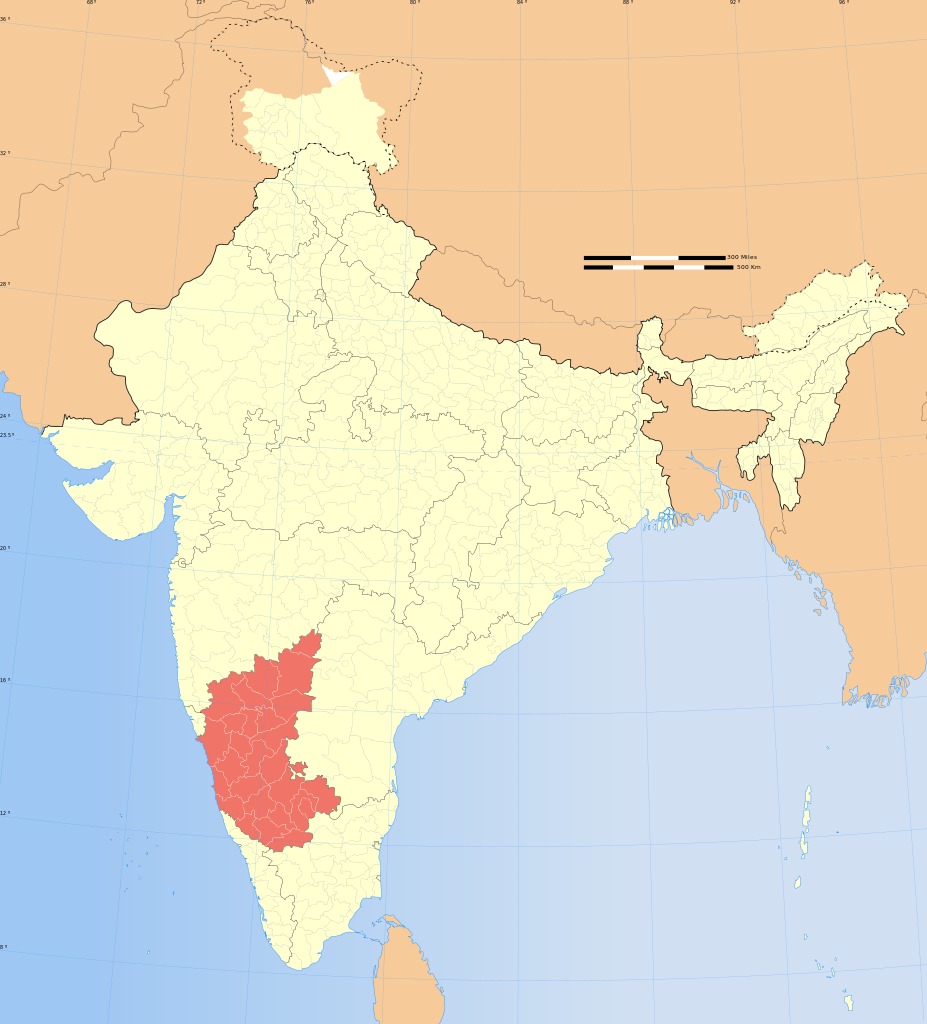
“Housekeeping staff should be trained to notice anything out of the ordinary in guest rooms,” the article states.

Some indicators of terrorist activity in hotels are requests for specific rooms or floors in hotels, unusual interest in hotel staff operating procedures, refusal of housekeeping services for long periods of time, extending departure dates one day at a time for long periods of time, and leaving the property for several days at a time and then returning.

# Indian Mock drill: Terrorists attack city hotel, kill security guard!

Source: http://www.deccanherald.com/content/301603/mock-drill-terrorists-attack-city.html

**In a daring 26/11 type attack on a city hotel early in the morning, the terrorist shot dead a security guard and entered two rooms and held the tourists hostage, here on Friday (Dec 2012).**

The early morning attack took everyone by surprise and shock as the gun shots were heard in the quiet precincts of the hotel just opposite the Karnataka Police Academy.

After killing the security guard the terrorists held the tourists hostage and send their demands to the police from the hotel.   
The police on hearing about the attack rushed to the spot and very successfully nabbed the terrorists. People heaved a sigh of relief at the quick action of the Mysore city police and the Commando force.

Was the action that unfolded true? No it was just a mock exercise to test the preparedness of the city police and the commandoes. Those were a witness to this event heaved a sigh of relief and there were faint smiles on their faces on learning the purpose of the drill.

Four NUS commandoes wearing the uniform of terrorists entered the JR Fortune Palace hotel located on the Mysore-Bangalore road and shot the security guard and his body was lying there till the police arrived. Later, his body was shifted after an ambulance was called for post mortem.

All this looked so real that it was just like a terrorist attack. After killing the security guard, they formed two teams and entered the rooms of the hotel. While in one room there was a couple, in another there was a family of four. Even though the tourists panicked they were taken into confidence and thus all of them cooperated for the mock exercise.

The terrorists told the police that if their demands were not met, they would kill the hostages one by one and later sent their demands list. In the whole exercise 30 NUS personnel had participated. Also 50 City Chaudoin force and 300 local police were involved in the operation.

The police themselves including city police commissioner Sudhir, SPY R Dixil, in charge deputy commissioner Dr Ajay Namaqualand and other high ranking officers were caught by surprise as they were totally unaware of the operation. The while exercise went on for five hours and finally there was a sense of relief among everyone present.

# 5 pressing hotel security concerns for 2012

Source: http://www.hotelnewsnow.com/Articles.aspx/7229/5-pressing-hotel-security-concerns-for-2012

Anticipating risk in the hotel security field is an imprecise art—one that’s grown increasingly difficult with the introduction of new technologies, regulations and global threats. But when asked for the areas of top concern for 2012, the usual suspects still top the list: information-technology breaches and terrorism, hoteliers said.

Yet, the reasons each appears on hoteliers’ to-do lists are changing. IT professionals now face new challenges brought on by the prolific use of cloud technologies and mobile devices.

Even though hotel security professionals and government agencies have quelled fears so successfully that travelers are less sensitive to potential threats, anti-terrorism efforts still face an emerging risk from complacency.

The result is a field that requires more focus than ever before, said Darrin Pinkham, VP of information technology for The Woodlands, Texas-based Benchmark Hospitality Group, which manages 26 properties throughout the United States.

“Security is getting harder and harder. We’re spending more and more money on it, and that’s at every level,” he said.

Hoteliers interviewed for this report recommended focusing on the following five areas during 2012:

**1. IT**

The hot-button issue within the realm of hotel-information technology is mobile and cloud technology.

“In general most mobile devices that are used for business remain unprotected, including lack of any password, let alone a complex password,” said Anthony Roman, founder and CEO of Lynbrook, New York-based hotel security company Roman & Associates. “Rarely do we find that any business using smart mobile technology has any encryption on it whatsoever. Even less than that do we find that there are written policies and procedures relative to the securing and protection of mobile devices, technology and the information continued within them.”

Amplifying the problem is the sheer number of devices, he added. A company could have tens of thousands of smartphones or laptops in the field at any given point—each a potential gateway to hackers and other criminals.

A good place to start to shore up those gaps in protection is with the Payment Card Industry’s Data Security Standard, which includes 12 “biblical” principles critical for any hotelier, Pinkham said. Though PCI DSS focuses specifically on the way hotels collect and store payment information, its requirements—which are getting stricter—will help shield hoteliers against other breaches as well.

Pinkham also recommended resources from Hospitality Financial and Technology Professionals and Hotel Technology Next Generation.

But IT protection goes beyond PCI DSS. Data security protection must include end-to-end management that takes a more comprehensive approach, said Ulf Mattsson, chief technology officer for Protegrity, a Stamford, Connecticut-based data security provider.

“We need to think more than compliance. We need to look at cost and benefit and how it’s supports the business,” he said. “The core principle is to provide end-to-end data protection so you are not just patching.”

Tokenization, which replaces sensitive data with an arbitrary value, is one such end-to-end solution, he said.

**2. Terrorism**

Ironically, one of the main reasons terrorism tops the list is because it has become less of an issue in recent years, sources said.

“It makes it a little bit harder to get things done because people are like, ‘Terrorism? That’s 10 years ago,’” said Chad Callaghan, security consultant for the America Hotel & Lodging Association.

Stressing diligence requires a delicate touch, however, Callaghan said. Hoteliers need to keep their staffs and travelers mindful of possible threats, but they don’t want to scare them.

Roman is a strong proponent of integrated risk management, “a concept in which all hotel business management departments including the executive level integrate with each other to assess corporate wide risk, from IT, to security, to business,” to combat terrorism and other security threats.

The process requires constant communication and the sharing of best practices, often through appropriate software and IT software, he said.

Callaghan and the AH&LA are taking a more industry-wide approach, stressing diligence from the executive level downward.

The association also supports education among travelers. During November, it revived its “If You See Something, Say Something” campaign along with the Department of Homeland Security.

“Don’t assume that you don’t need to continue to fund your security effort at your hotel,” Callaghan said. “And also initiatives like the ‘see something, say something’ campaign become very important as well.”

**3. Skimmers**

A related threat is that of “skimmers,” or devices that catch credit card numbers when consumers use them for payment. The problem primarily is contained to the restaurant industry, but Callaghan is concerned it could spread to hotels.

“It’s not an easy thing to stop,” he said. “You have to go investigate. You have to be aware of complaints about a particular outlet. Once you have that, you can back into it and find out who the workers on duty were at that point.”

Skimmers typically require an “inside man” or worker who swipes a credit card through a device before processing the payment. These are usually not hardened criminals, Callaghan said; they’re just “opportunists.”

The best prevention measure is to have an investigative team or third party on hand and making that known to employees, he said.

“If you have the capability of having an investigations team or using a third party, having people aware that this is something available and out there … just the fact that people know that you have the capability to do that will keep honest people honest,” he said.

**4. Liability and insurance fraud**

These two related issues can double, triple, quadruple and quintuple corporate insurance premiums in the blink of an eye, Roman said.

“The greatest business risk, as I see it … is insurance fraud. And it’s the most expensive,” he said.

It can include claims as small as a guest seeking a free room for stubbing his toe in the shower to extreme cases involving prolonged entanglements with worker’s compensation, Roman said.

“Liability” as a general label refers to hoteliers being held liable for the acts, which are often criminal, of third parties, the AH&LA’s Callaghan said.

A recent high-profile example involves ESPN reporter Erin Andrews, whose privacy was violated when a stalker filmed her changing in her guestroom through a peephole. Andrews in December filed a US$10-million lawsuit against a Marriott hotel in Nashville and the convicted stalker.

Whether frivolous or not, such cases are costly because they have to be defended and often settled, Callaghan said. “I don’t see that abating at all.”

He advised hoteliers to educate themselves on the issue, consulting with an attorney, if necessary.

“Sometimes hotel operators live in a little bit of a fantasy world when it comes to liability,” Callaghan said.

**5. Security as taboo**

“Security” still is something of a taboo in the global hotel industry, said Paul Moxness VP for corporate safety and security at The Rezidor Hotel Group, a Brussels-based hotel management company, with more than 400 hotels and nearly 90,000 rooms in its portfolio.

Not only is it a topic that might give some guests the jitters, but it’s one many hoteliers fear is akin to Pandora’s box—once it’s opened, all the problems will be released. The truth is just the opposite, Moxness said. If security becomes a permanent and prominent part of day-to-day operations, it’s more likely hoteliers will be better able to address it.

“It’s like a little kid that can’t sleep because there’s a tiger in his closet or a lion under his bed, but if you turn the light on, you’ll find that it’s not there,” he said.

Hoteliers need to do a better job of “turning on the light” by talking about security openly and regularly at staff and association meetings, Moxness said. Hotel executives should insist their GMs make security a priority.

“It has to be from the top down,” he said.

# If you see something, say something

Source: http://www.hotelnewsnow.com/Articles.aspx/6895/AHLA-DHS-If-you-see-something-say-something

This year, millions of leisure and business travelers will check-in to a U.S. hotel or motel.  In doing so, they will support a travel and tourism industry that employs more than 1.7 million U.S. hotel workers and generates more than $127 billion in annual sales.  America’s hospitality industry is not just a vital engine for job growth and sustainment; it is also a critical part of our nation’s economy.  Importantly, it is also a valuable partner in protecting our nation’s security.

This week, the Department of Homeland Security, the American Hotel and Lodging Association, LodgeNet, and some of our nation’s largest hotel chains announced a new partnership that will significantly expand the “If You See Something, Say Something™” campaign.

As part of the partnership we are launching this week, a fifteen second PSA will begin airing at more than 5,400 hotels nationwide, appearing on the “Welcome Channel” in nearly 1.2 million hotel rooms in all 50 states.  Its message is simple and clear: if you see something that doesn’t look right – an unattended bag or package, a person behaving in a suspicious manner, a vehicle that seems out of place – report it to the authorities.

The “If You See Something, Say Something™” campaign, which began in New York City under the Metropolitan Transportation Authority, encourages individuals, communities, and businesses to stay alert and report suspicious activity to state or local law enforcement authorities.

Time and again, we have seen the value of public vigilance in thwarting terrorism and crime, including foiled plots against Times Square in May 2010, an MLK day parade route in Washington state last year, and more recently, the Ft. Hood Army Base.  Each of these plots could have ended differently – and tragically – had someone not reported suspicious activity to authorities.

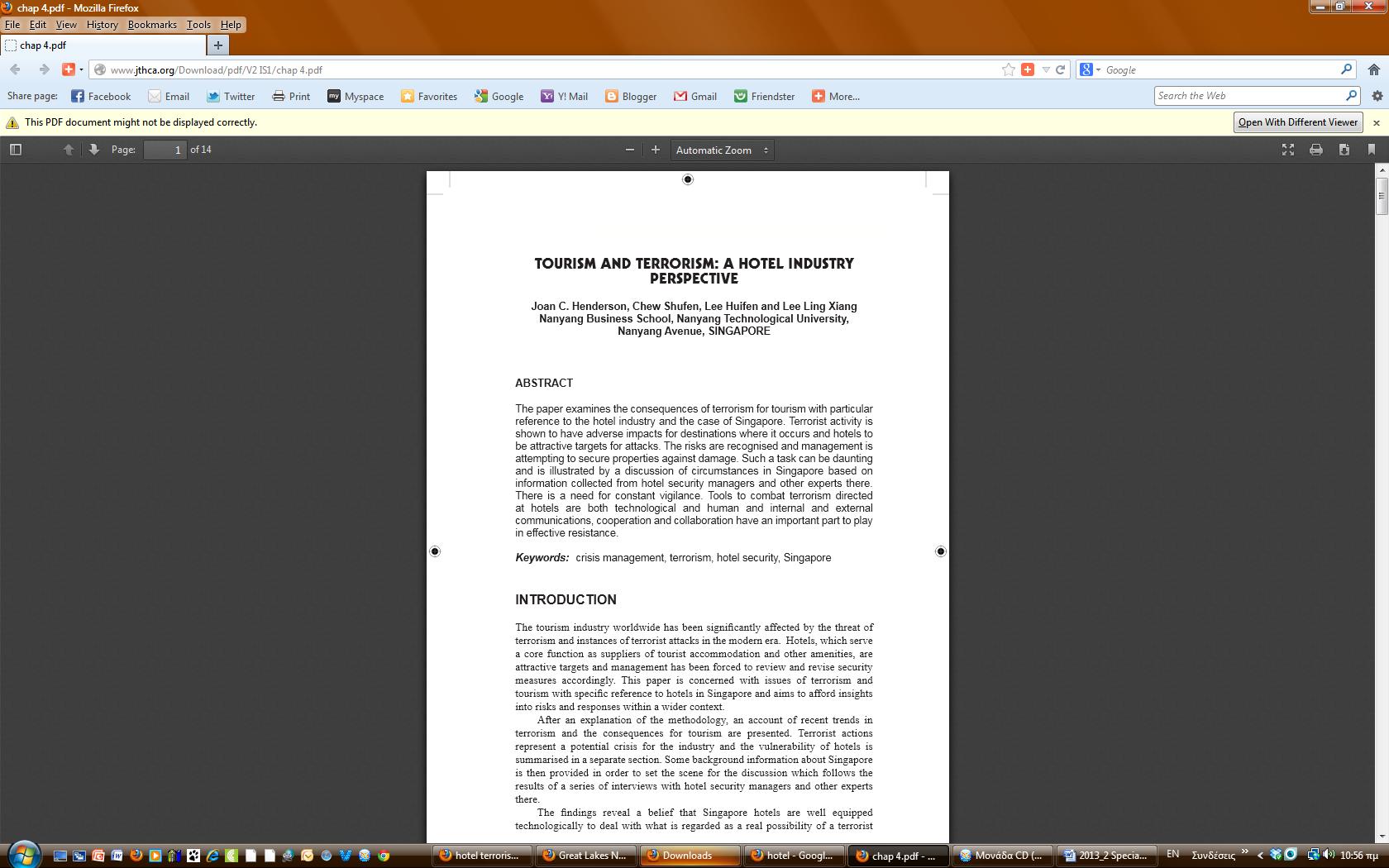
The “If You See Something, Say Something™” campaign is another way that DHS and the hospitality industry are working together to keep our nation and economy safe.   The American Hotel and Lodging Association and DHS have been working together over the past year to offer threat briefings to the hospitality industry and create a web-based training tool for employees.

As part of this collaboration, we have developed and distributed public education materials to help the hotel industry manage security at their facilities and encourage hotel employees to identify and report suspicious activities and threats.

In addition, over the past year, DHS and some of our nation’s largest hotel chains have partnered to expand enrollment in Global Entry, a trusted traveler program that offers low-risk, security-vetted air travelers streamlined processing upon arrival to the United States. Through this program, which is currently available at 20 U.S. airports, average wait times for international travelers have gone down 70 percent, with more than 75 percent of those enrolled in the program passing through customs in under five minutes.  Since the program’s inception, several hotel chains have held Global Entry enrollment events to encourage their executives and employees to join, while others have promoted it to corporate clients and members of their loyalty programs.

Finally, because we know that disasters can strike at any time in any place, the Federal Emergency Management Administration has partnered with the hotel and lodging industry to develop a set of PSAs that promote travel safety and disaster assistance for hotel guests.  During the devastating spring tornadoes, these videos ran in more than 50,000 hotel rooms, and during Hurricane Irene they reached individuals in over 420,000 hotel rooms.

Through efforts like these, we can engage all sectors of our community, including the millions of guests that stay at hotels each year, in our homeland security efforts.  Each of us has a role to play in helping to keep America safe and we thank you for doing your part.

Source: http://www.jthca.org/Download/pdf/V2%20IS1/chap%204.pdf

# Deadliest Terrorist Attacks on Hotels worldwide

Source: http://www.buzzom.com/2010/02/deadliest-terrorist-attacks-on-hotels-worldwide/

The terrorism is one menace that has disrupted the whole world. In reality, no country is completely free from terrorism, as its either home-born or imported from outside. Call it religious extremists shaping out young minds to combat their presumed enemies, politicians playing their dirty games or people trying to get over their material woes over night, terrorism has only harnessed death, misery, agony and remorse. People propagate the glory of sacrifice in the name of religion and swamp the lives into dogmatic and limited vision of the world. Fighting for territories and shedding innocent blood, these inhumane beings have laid down many innocent lives just to satisfy their personal motives. The history holds account of the most deadly terrorist attacks and their blood thirsty missions that are a blot on the human race. So lets take a look at some of the most lethal and fatal terrorist attacks on the hotels that once again present the grim prospect for the future of the mankind.

**King David Hotel (1946)**



The King David hotel was opened in 1932 as the first ever modern, luxury one in Jerusalem that hosted the royals. However after the invasion of the British Forces in Palestine and Transjordan, the southern wing of the Hotel became the administrative and military center for the British Military Command. The attack that took place on July 22,1946 was made in vengeance for the British Operation Agatha (Raid of Jewish Agency and arrest of 2500 Jews). The blast was ordered by Menachem Begin, the leader of the Jewish underground military organization **Irgun Tsvai-Leumi**. Irgunists planted a bomb in the basement of the main building of the hotel and the blast caused the collapse of the western half of the southern wing of the hotel that oused the Mandate’s intelligence records about Irgun, the Hagana, Lehi,  and other Jewish paramilitary groups. A total of 91 people were killed and 45 people were injured. Out of the casualties, most of them were civilians that included 28 British, 41 Arab, 17 Jewish, and 5 other. The blast was regarded as the pivotal moment in the Middle East history.

**Netanya Bombing (Park Hotel Passover attack 2002)**

On March 27, 2002Palestinian Islamic socio-political organization Hamas carried out a suicide bombing at the Park Hotel in Netanya, Israel, during a Passover seder. A Palestinian suicide bomber walked into the dining room of the hotel, in the center of the city, and detonated an explosive device. The deadliest attack against the Israelis claimed 30 lives and left 140 injured. Hamas claimed that the attack was specifically designed to disrupt the impetus from a recently announced peace initiative of the Saudi Arabian government at the Beirut Summit. Abbas al-Sayed the mastermind behind the attack was later arrested and  punished with 35 life sentences for each murder victim and additional time for those who were wounded.



**Canal Hotel (2003)**

In the afternoon of August 19, 2003, the Iranian UN headquarters in the Canal Hotel in Baghdad, became the target of the terrorist attack by a suicide bomber driving a truck full of explosives. At least 22 people, including the United Nations’ Special Representative in Iraq Sérgio Vieira de Mello were killed and 100 others were left wounded in the tragedy. The bombing was followed on September 22, 2003, by another car bomb outside the Canal Hotel after which 600 UN staff members withdrew from Iraq.

**Sinai bombings (2004)**

This bombing incident points to three bomb attacks that targeted tourist hotels in the Sinai Peninsula, Egypt. Thedarkness of the October 7, 2004 fell upon the people at the Hilton hotel at Egypt’s Taba resort when a truck drove into the lobby of the Taba Hilton and exploded killing 31 people and leaving 159 injured. When that was not enough to bruise the memories of the Egyptians, two more bombings after some time intervals, one at the Moon Island resort and Baddiyah camp jolted the Egyptian government. The total count of deaths reached 35 while 171 were left wounded.

**Amman bombings** **(2005)**

The 2005 Amman bombings were another planned series of bomb attacks in three famous hotels in Amman, Jordan that included the Grand Hyatt Hotel, the Radisson SAS Hotel, and the Days Inn.the three simultaneous attacks were carried out by 4 Iraqi suicide bombers before 9 am o n November 9, 2005.

The 35 years old Ali Hussein Ali al-Shamari detonated his explosive belt in the middle of a Jordanian-Palestinian wedding reception in the Radisson SAS hotel’s main ballroom that killed over 30 people and injured dozens. This was followed by second blast happened about 500 m at the Grand Hyatt Hotel lobby that killed 7 employees and the Syrian-American movie producer Moustapha Akkad and his daughter Rima.the last explosion took place at the Days Inn entrance where the 23 years old Safaa Mohammed Ali detonated himself, killing three members of a Chinese military delegation. The bombings killed a total of 63 people and 115 others were injured. Hours after the attack Al-Qaeda in Mesopotamia claimed the responsibility via internet.

**Islamabad Marriott  Hotel(2008)**

The five-story, 258-room hotel turned to dust and ashes when a dump truck filled with explosives, detonated in front of the Marriott Hotel in the Pakistani capital Islamabad on 20 September 2008.the explosion caused a natural gas leak that set the top floor of the hotel on fire and slowly spread to the entire hotel. Killing at least 54, injuring at least 266 the explosion left a  deep crater in the pavement outside the hotel. While the major casualties were Pakistanis, five foreign nationals were reported as dead and fifteen others as injured.

**Taj Mahal Hotel and Oberoi Trident, Mumbai (2008)**

This was one of the most tragic incidents in the history of terrorist attacks on India that shattered the lives of many families. While the 2008 Mumbai attacks were more than ten coordinated shooting and bombing attacks across Mumbai, the two hotels, the Oberoi Trident, the Taj Mahal Palace & Tower, were amongst the locations targeted by the Pakistani terrorists apart from the  Chhatrapati Shivaji Terminus, Leopold Cafe, Cama Hospital (a women and children’s hospital) and the Jewish-owned Nariman House. Initially a fire raged inside the Taj, with the dome of the luxury hotel billowing smoke. It was reported that the terrorists had been throwing grenades from the roof earlier. Approximately 450 people were staying in the Taj Mahal Palace and Hotel at the time of the seizure, and another 380 in the Oberoi. 32 staff and guests were killed during the 3-day siege at the Oberoi Trident and several injured at the Taj Mahal Hotel.



**Jakarta Bombings(2009)**

Indonesia’s worst terrorist attack in four years killed 9 people and left 53 wounded when explosions ripped through two hotels , the JW Marriott and the Ritz-Carlton on 17 July 2009. The attacks were carried out by two suicide bombers, who had checked into the hotels as paying guests several days earlier. The twin attacks were regarded as attempts to destabilize the country after presidential elections that had taken place a week ago.

# King David Hotel bombing

Source: http://en.wikipedia.org/wiki/King\_David\_Hotel\_bombing



The **King David Hotel bombing** was an attack carried out on July 22, 1946 by the militant right-wing Zionist underground organization the Irgun on the British administrative headquarters for Palestine, which was housed in the King David Hotel in Jerusalem. 91 people of various nationalities were killed and 46 were injured.

The hotel was the site of the central offices of the British Mandatory authorities of Palestine, principally the Secretariat of the Government of Palestine and the Headquarters of the British Forces in Palestine and Transjordan. The attack initially had the approval of the Haganah (the principal Jewish paramilitary group in Palestine). It was conceived of as a response to Operation Agatha (a series of widespread raids, including one on the Jewish Agency, conducted by the British authorities in the British Mandate of Palestine) and was the deadliest directed at the British during the Mandate era (1920–1948). The explosion caused more casualties than any subsequent bombing carried out in the Arab-Israeli conflict.

The Irgun planted a bomb in the basement of the main building of the hotel, under the wing which housed the Mandate Secretariat and a few offices of the British military headquarters. Warnings were sent by telephone, including one to the hotel's own switchboard, which the hotel staff decided to ignore, but none directly to the British authorities. A possible reason why the warning was ignored was that hoax bomb warnings were rife at the time. From the fact that a bomb search had already been carried out, it appears that a hoax call or tip-off had been received at the hotel earlier that day. Subsequent telephone calls from a concerned *Palestine Post* staff member and the police caused increasing alarm, and the hotel manager was notified. In the closing minutes before the explosion, he called an unknown British officer, but no evacuation was ordered. The ensuing explosion caused the collapse of the western half of the southern wing of the hotel. Some of the inflicted deaths and injuries occurred in the road outside the hotel and in adjacent buildings. Controversy has arisen over the timing and adequacy of the warnings and the reasons why the hotel was not evacuated.

## Background

### Motivation for the bombing



Zionist leaders arrested in Operation Agatha. Left to right: David Remez, Moshe Sharett, Yitzhak Gruenbaum, Dov Yosef, Shenkarsky, David Hacohen, Halperin.

The Irgun committed the attack in response to Operation Agatha, known in Israel as "Black Saturday". British troops had searched the Jewish Agency on June 29 and confiscated large quantities of documents which contained incriminating information about the Agency´s involvement with violent acts. The intelligence information was taken to the King David Hotel, where it was initially kept in the offices of the Secratariat in the southern wing. In order to destroy the documentation, the Irgun therefore determined to destroy that wing of the hotel.

### Hotel layout

In plan form, the six-storey hotel, which was opened in 1932 as the first, modern, luxury hotel in Jerusalem, had an I-shape, with a long central axis connecting wings to the north and south. Julian's Way, a main road, ran parallel and close to the west side of the hotel. An unsurfaced lane, where the French Consulate was situated and from where access to the service entrance of the hotel was gained, ran from there past the north end of the hotel. Gardens and an olive grove, which had been designated as a park, surrounded the other sides.

### Government and military usage

In 1946, the Secretariat occupied most of the southern wing of the hotel, with the military headquarters occupying the top floor of the south wing and the top, second and third floors of the middle of the hotel. The military telephone exchange was situated in the basement. An annexe housed the military police and a branch of the Criminal Investigation Department of the Palestine Police.

Rooms had first been requisitioned in the hotel in late 1938, on what was supposed to be a temporary basis. Plans had already been made to erect a permanent building for the Secretariat and Army GHQ, but these were cancelled after the Second World War broke out, at which point more than two-thirds of the hotel's rooms were being used for government and army purposes.

In March 1946, British Labour Party MP Richard Crossman gave the following description of activity at the hotel: "private detectives, Zionist agents, Arab sheiks, special correspondents, and the rest, all sitting around about discreetly overhearing each other." Security analyst Bruce Hoffman has written that the hotel "housed the nerve centre of British rule in Palestine".

### Previous attacks

Amichai Paglin, Chief of Operations of the Irgun, developed a remote-controlled mortar with a range of four miles which was nicknamed the V3 by British military engineers. In 1945, after attacks using the mortar had been made on several police stations, six V3s were buried in the olive grove park south of the King David Hotel. Three were aimed at the government printing press and three at the hotel itself. The intention was to fire them on the King's birthday, but the Haganah learned about the plan and warned the British through Teddy Kollek of the Jewish Agency. Army sappers then dug them up. On another occasion, members of an unknown group threw grenades, which missed, at the hotel.

## Preparations for the attack

### Planning

The leaders of Haganah opposed the idea initially. On July 1, 1946, Moshe Sneh, chief of the Haganah General Headquarters, sent a letter to the then leader of the Irgun, Menachem Begin, which instructed him to "carry out the operation at the 'chick'", code for the King David Hotel. Despite this approval for the project, repeated delays in executing the operation were requested by the Haganah, in response to changes unfolding in the political situation. The plan was finalized between Amichai Paglin (Irgun alias 'Gidi'), Chief of Operations of the Irgun, and Itzhak Sadeh, commander of the Palmach.

In the plan, Irgun men, disguised as Arabs, except for Gideon, the leader, who would be dressed as one of the hotel's distinctive Sudanese waiters, would enter the building through a basement service entrance carrying the explosives concealed in milk cans. The cans were to be placed by the main columns supporting the wing where the majority of the offices used by the British authorities were located. The columns were in a basement nightclub known as the Régence. In the final review of the plan, it was decided that the attack would take place on July 22 at 11:00, a time when there would be no people in the coffee shop in the basement in the area where the bomb was to be planted. It would be possible to enter the hotel more easily at that time as well.

It would have been impossible to have planted the bomb in the Régence any later than 14:00 because it was always full of customers after that time. The timing was also determined by the original intention that the attack should coincide with another, carried out by the Lehi, on government offices at the David Brothers Building. However, that attack, codenamed "Operation Your Slave and Redeemer", was canceled at the last moment. The Irgun said details of the plan were aimed at minimizing civilian casualties. Irgun reports allegedly included explicit precautions so that the whole area would be evacuated. This led to recriminations between the Haganah and Irgun later. The Haganah said that they had specified that the attack should take place later in the day, when the offices would have been emptier of people.

### Warnings

Rear of the hotel, 1931

Since the bombing, much controversy has ensued over the issues of when warnings were sent and how the British authorities responded. Irgun representatives have always stated that the warning was given well in advance of the explosion, so that adequate time was available to evacuate the hotel. Menachem Begin, for example, writes that the telephone message was delivered 25–27 minutes before the explosion. It is often stated that the British authorities have always denied that a warning was sent. However, what the British Government said, five months after the bombing, once the subsequent inquest and all the inquiries had been completed, was not that no warning had been sent, but that no such warning had been received by anyone at the Secretariat "in an official position with any power to take action."

American author Thurston Clarke's analysis of the bombing gave timings for calls and for the explosion which he said took place at 12:37. He stated that as part of the Irgun plan, a sixteen year old recruit, Adina Hay (alias Tehia), was to make three warning calls before the attack. At 12:22 the first call was made, in both Hebrew and English, to a telephone operator on the hotel's switchboard (the Secretariat and the military each had their own, separate, telephone exchanges). It was ignored. At 12:27, the second warning call was made to the French Consulate adjacent to the hotel to the north-east. This second call was taken seriously, and staff went through the building opening windows and closing curtains to lessen the impact of the blast. At 12:31 a third and final warning call to the *Palestine Post* newspaper was made. The telephone operator called the Palestine Police CID to report the message. She then called the hotel switchboard. The hotel operator reported the threat to one of the hotel managers. This warning resulted in the discovery of the milk cans in the basement, but by then it was too late.[[4]](http://en.wikipedia.org/wiki/King_David_Hotel_bombing#cite_note-tclarke81-4)

Some Israeli observers have claimed that the British ignored the warning calls because they assumed that the hotel was so heavily guarded that any attack would be futile. Begin claimed in his memoirs that the British had deliberately not evacuated so that they could vilify the Jewish militant groups.

Kind David Hotel (today)

### Leaks and rumours

Shortly after noon Palestine time, the London UPI bureau received a short message stating that 'Jewish terrorists have just blown up the King David Hotel!'. The UPI stringer who had sent it, an Irgun member, had wanted to scoop his colleagues. Not knowing that the operation had been postponed by an hour, he sent the message before the operation had been completed. The bureau chief decided against running the story until more details and further confirmation had been obtained. There were other leaks.

## Execution

The perpetrators met at 7 am at the Beit Aharon Talmud Torah. This was the first time they were informed of the target. The attack used approximately 350 kg (770 lb) of explosives spread over six charges. According to Begin, due to "consultations" about the cancellation of the attack on the David Brothers Building, the operation was delayed and started at about 12:00, an hour later than planned.

After placing the bombs, the Irgun men quickly slipped out and detonated a small explosive in the street outside the hotel, reportedly to keep passers-by away from the area. The police report written in the aftermath of the bombing says that this explosion resulted in a higher death toll because it caused spectators from the hotel to gather in its south-west corner, directly over the bomb planted in its basement. The first explosion also caused the presence in the hotel of injured Arabs who were brought into the Secretariat after their bus, which had been passing, was rolled onto its side. The Arab workers in the kitchen fled after being told to do so.

During the attack, two Irgun casualties occurred, Avraham Abramovitz and Itzhak Tsadok. In one Irgun account of the bombing, that by Katz, the two were shot during the initial approach on the hotel, when a minor gunfight ensued with two British soldiers who had become suspicious. The Irgun did not explain how the group would have been able to move 350 kg of home-made explosives into the hotel with the guards already alerted. In Yehuda Lapidot's account, the men were shot as they were withdrawing after the attack. The latter agrees with the version of events presented by Bethell and Thurston Clarke and is more credible. According to Bethell, Abramovitz managed to get to the taxi getaway car along with six other men. Tsadok escaped with the other men on foot. Both were found by the police in the Jewish Old Quarter of Jerusalem the next day, with Abramovitz already dead from his wounds.

## Explosion and aftermath

The explosion occurred at 12:37. It caused the collapse of the western half of the southern wing of the hotel. Soon after the explosion, rescuers from the Royal Engineers arrived with heavy lifting equipment. Later that night, the sappers were formed into three groups, with each working an eight hour shift. The rescue operation lasted for the next three days and 2,000 lorry loads of rubble was removed. From the wreckage and rubble the rescuers managed to extract six survivors. The last to be found was D. C. Thompson, 24 hours after the building had collapsed. He appeared to be more or less unhurt, but later died due to shock.

91 people were killed, most of them being staff of the hotel or Secretariat: 21 were first-rank government officials; 49 were second-rank clerks, typists and messengers, junior members of the Secretariat, employees of the hotel and canteen workers; 13 were soldiers; 3 policemen; and 5 were members of the public. By nationality, there were 41 Arabs, 28 British citizens, 17 Palestinian Jews, 2 Armenians, 1 Russian, 1 Greek and 1 Egyptian. 46 people were injured. Some of the deaths and injuries occurred in the road outside the hotel and in adjacent buildings. No identifiable traces were found of thirteen of those killed. One of the dead was Yulius Jacobs, an Irgun sympathizer.

# Tel Aviv map-plain.pngSavoy Hotel Attack

Source: http://en.wikipedia.org/wiki/Savoy\_Hotel\_Attack

The **Savoy Hotel Attack** was a terrorist attack by members of the Palestine Liberation Organization against the Savoy Hotel in Tel Aviv, Israel, on 4-5 March 1975.

## The attack

At 11:00 p.m. on the night of 4 March 1975, eight Palestinians in two teams landed by boat on the Tel Aviv beach at the foot of Allenby Street. Shooting and throwing grenades, they took over the Savoy Hotel near the center of the city. The guests were taken hostage. The Palestinians threatened that if Israel did not release 20 Palestinian prisoners within four hours the hostages would be executed.

Early the next morning, the Israeli counter-terrorism unit *Sayeret Matkal* stormed the hotel, killing seven of the perpetrators and capturing one. Five hostages were freed, while eight were killed. Three soldiers, including former Sayeret Matkal commander Uzi Yairi, were also killed.

A few hours after the rescue operation, the ship that had transported the militants was captured on the high seas by the Israeli Navy, and its crew was arrested.

## Perpetrators

The Palestinian operation was planned by Abu Jihad.

Members of the Savoy cell included Musa Juma al-Tallka, the sole survivor, Muhammad Mashala, Hader Muhammad, Ziad Talk al-Zrir, Musa Awad, Muhammed al-Masri, Abu al-Lel, and Ahmed Hamid, who were all killed by the Israeli troops. The bodies of those killed were released by the IDF in May 2012.

Initial Palestinian planning had called for an attack against the Israeli tourist city of Nahariya, yet the team was apparently unable to locate the city on the night of a previous attempt, two months earlier. The operation's objectives were then changed to the Manshiya Neighborhood Youth Club and the Tel Aviv Opera Building. The contingency plan in case the original targets could not be located was to select any nearby populated buildings as targets. This resulted in the Savoy Hotel raid, as it was the only illuminated building on the street.

### Recent Developments

In August 2012, it was reported that the Ramallah municipality approved the construction of a mausoleum to honor the eight Palestinians who were involved in the attack (the vote was initially reported by the PA daily newspaper Al-Hayat Al-Jadida and subsequently translated into English by Palestinian Media Watch). The decision to build the mausoleum coincides with the return of the perpetrators' remains, which were among the bodies of 91 Palestinian terrorists repatriated to the Palestinian Authority in June 2012 as an Israeli good-will gesture.



# Mumbai terror attacks similar to Savoy Hotel attack: Israeli terror expert

Source:http://indiatoday.intoday.in/story/Mumbai+terror+attacks+similar+to+Savoy+Hotel+attack:+Israeli+terror+expert/1/21480.html

Eight terrorists land on a beach from a mother ship, walk into a busy hotel in the centre of town firing AK-47s, throwing grenades. Sounds familiar? If Israel is grieving the death of its eight citizens in the November 26 attacks in Mumbai, its terror experts cannot help regard it with a sense of déjà-vu. The attacks were a near repeat of the Savoy hotel attacks of March 1975 carried out by the Palestine Liberation Organisation (PLO).

On the night of March 4, 1975, two teams of eight Palestinian terrorists landed on Tel Aviv beach in rubber boats. Shooting and throwing grenades, they captured the Savoy Hotel near the centre of the city. The Palestinians threatened to kill their hostages if the authorities did not release 20 Palenstinian prisoners within four hours.

Early next morning, an Israeli commando from Sayeret Matkal stormed the hotel, killing seven militants and capturing one. Five hostages were freed and eight were killed. Three soldiers, including former Sayeret Matkal commander Uzi Yairi were also killed.

"One cannot ignore the similarities between the Savoy attack and the resent Mumbai attack," says Colonel (retd) Jonathan Fighel of the International Policy Centre for Counter-Terror, Israel.

Fighel echoes the sentiment of terrorism experts across the world who were shocked by the sorry state of India's counter assault teams. "From what I have seen on TV, it looks as the assault forces were not equipped with special typical counter terror arms, clothing, night vision, laser viewfinder, ballistic shields, special helmets with communication devices," Fighel says.

The Israeli strategy in hostage barricade situation inside the borders of Israel is to stabilise the situation, buy time through engaging a negotiation team to contact the terrorists and seek for peaceful solution for their surrender, while preparing a special force for tactical operational capabilities to storm the target (building, plane, train, ship) in a very pin point surgical fashion with the clear operational instructions to kill all terrorists and rescue as much hostages as can.

"I really don't know what the operational tactics in Mumbai were so it is difficult for me to comment. I don't know if a negotiating process even started, who conducted it, was it connected and integral part of the operational military assault team?" Fighel asks.

Here's how the Israeli's followed up the Savoy attack. A few hours later the ship that transported the attackers was captured and its crew were taken prisoner. The Palestinian operation was masterminded by Abu Jihad (Khalil Ibrahim al-Wazir) who on April 16, 1988, was assassinated at his home in Tunis, apparently by Israeli commandos. Seven terrorists were killed and the only survivor Muhammad Mashala was captured.

# 2003 Marriott Hotel bombing

Source: http://en.wikipedia.org/wiki/2003\_Marriott\_Hotel\_bombing

The **2003 Marriott Hotel bombing** occurred on 5 August 2003 in Mega Kuningan, South Jakarta, Indonesia. A suicide bomber detonated a car bomb outside the lobby of the JW Marriott Hotel, killing twelve people and injuring 150. Those killed were mostly Indonesian, with the exception of one Dutch businessman, one Dane, and two Chinese tourists. The hotel was viewed as a Western symbol, and had been used by the United States embassy for various events. The hotel was closed for five weeks and reopened to the public on 8 September.

## Prelude

Two weeks prior to the bombing, there was a tip call to senior Indonesian police officers from a militant captured during a raid in Semarang that two carloads of bomb-making materials were heading to the capital, Jakarta. During the raid, the police also discovered some drawings outlining specific areas in the city for possible attacks.

## The explosion

A Toyota Kijang, bought on 20 July 2003, from a Jakarta businessman for 25.75 million rupiah was loaded with explosives and driven through the taxi stand in front of the Marriott Hotel. The vehicle stopped briefly in front of the lobby and CCTV cameras show a security guard approaching the vehicle, briefly speaking to the driver. The security guard then turns and a detonation can be seen. It is still not clear if the explosion was accidental, set off by remote detonation or a timer exploding prematurely. If the vehicle had kept a course heading straight for the lobby the damage would undoubtedly have been more severe. The blast radius was visible along the shattered windows of nearby buildings. According to Indonesian police, one of the ingredients in the car bomb contained the same chemicalused in the deadly 2002 Bali bombing. The bombs in both cases were made of the same mixture of explosives, mobile phones were used as detonators, and the attackers had tried to scrape off the identification numbers from the vehicle bombs.

The severed head of Asmar Latin Sani, aged 28, and from West Sumatra, was later found on the fifth floor of the building, The head was identified by two jailed members of the Jemaah Islamiah group who said they had recruited him.

Investigators uncovered the charred remains of a battery used to power the bomb and said it was similar to the ones used in a series of bombings against Christian churches on Christmas Eve 2000, in which 19 people were killed.

The attack came two days before a verdict in the trial of the Bali nightclub bombers. Al Qaeda claimed responsibility for the attack and the perpetrators are known to have trained in al Qaeda training camps in Afghanistan and Pakistan.

## Investigation

Six days after the atrocity on 11 August al-Qaeda claimed responsibility, via the Arab media Al Jazeera, and singled out Australia for special attention. The statement said

|  |  |  |
| --- | --- | --- |
| **“** | This operation is part of a series of operations that Dr Ayman al-Zawahiri has promised to carry out. [It is] a fatal slap on the face of America and its allies in Muslim Jakarta, where faith has been denigrated by the dirty American presence and the discriminatory Australian presence". | **”** |

Jemaah Islamiyah (JI), an organisation affiliated with al-Qaeda, is alleged to have carried out the bombing. The al-Qaeda link has been backed by Indonesia's Minister of Defense, Matori Abdul Djalil who said the Marriott bombers had trained with al-Qaeda in Afghanistan and Pakistan. *"Each one of them has special abilities received from training in Afghanistan and Pakistan,"* Matori Abdul Djalil said on 11 August 2003. He also claimed that the bombers were linked to a group of people arrested in the eastern Indonesian town of Semarang during July 2004 and are alleged to be members of Jemaah Islamiah.

*"There are many more Jemaah Islamiah members on the loose in Indonesia ... Because of this I am sure that JI is behind all of this,"*

On 5 May 2006 the International Crisis Group released its "Asia Report No 114" entitled *Terrorism in Indonesia*. It described the events leading up the attack;

The trigger for the Marriott bombing came in December 2002, when Indonesian police stepped up the hunt for Jemaah Islamiah members while investigating the 2002 Bali bombings. Toni Togar, a JI member based in Medan, North Sumatra, was nervous, because his house stored all the explosives left over from JI's 2000 Christmas Eve bombings. He contacted Noordin Mohammed Top to tell him he was going to throw them out. Noordin previously was part of the team that carried out the Christmas Eve bombings which was led by Hambali and included Imam Samudra and many of the other 2002 Bali bombers. He told Togar to hold on as he "saw good materials being wasted".

Abu Bakar Bashir approved of Hambali's activities, and Toni Togar was selected to take part in the new bombing plot. Hambali had already set a precedent for a secret team pursuing jihad on its own. This was in part because he controlled the separate funding from al-Qaeda. In January 2003, Muhammad Rais, Noordin and Azahari Husin moved to Bengkulu, where a group of JI members lived, including Asmar Latin Sani, who became the Marriott suicide bomber. The next stages of the operation took place in February 2003 when the explosives were transported from Dumai to Bengkulu via Pekanbaru,

Azahari secured the detonators with a new team member, Masrizal bin Ali Umar. also known as Tohir, another Pondok Ngruki graduate and a Luqmanul Hakiem teacher who was a close friend of Rais. After the explosives safely reached Bengkulu as unaccompanied baggage on an intercity bus, they were stored at the house of Sardona Siliwangi, another Ngruki student and JI member. At the time, Sardona, who was working with Asmar Latin Sani, opened a bank account in March 2003 to facilitate financial transactions for Noordin.

In late April 2003, Mohamed Ihsan also known as Gembrot and Idris, who was involved in the 2000 Christmas Eve bombings transported the explosives again. In May, he and Toni Togar, robbed a bank in Medan on 6 May to raise funds for the project. "Ismail", a Luqmanul Hakiem student who had previously worked with Rais and Noordin in the shock absorber repair shop in Bukittinggi, then received an email from Noordin asking him to pick up some packages from a man in Dumai. Ismail obliged, and the package turned out to be cash in Australian dollars, sent by Hambali via a courier.

A book that appears based in part on transcripts of Hambali's interrogation says Hambali arranged for A$25,000 to be sent: A$15,000 for operational expenses, A$10,000 for Bali bomber families. Conboy, op. cit., p. 229. Hambali's younger brother, Rusman Gunawan, who was arrested in Karachi in September 2003, testified Hambali had secured a promise of A$50,000 from an Noordin on how to bring the cash from Dumai to Lampung.

On 4 June 2003, in Lampung, the final team was put together: Noordin, Azhari, Ismail, Asmar Latin Sani, and Tohir. Noordin assigned the tasks and explained that he was in charge, Azhari was field commander and Ismail his assistant. Asmar and Tohir would be in charge of renting the house, buying the vehicles and getting the explosives to Jakarta. Asmar had agreed to be the suicide bomber. When they got to Jakarta, they split into two teams to survey four possible targets. Azhari and Ismail examined the Marriott and a Citibank branch; Noordin and Tohir looked at the Jakarta International School and the Australian International School. Eventually they decided on the hotel because of the American brand name and the fact that it was easy to reach. The bombing took place on 5 August.

They all drove back to Blitar with 25 kilograms of potassium chlorate and ten kilos of sulfur for bomb making, as well as a pistol and ammunition. Not long afterwards, another operative delivered 30 extra kilograms of TNT.

Around this time a pamphlet was circulating in jihadist groups that was a translation from Arabic into Indonesian of an article that first appeared in the al-Qaeda on-line magazine Sawt al-Jihad. Entitled "You Don't Need to Go to Iraq for Jihad", it was written in 2003 by a Saudi jihadist, Muhammad bin Ahmad as-Salim.

## Suspects

* Hambali: Riduan Isamuddin, is being held at Guantanamo Bay detention camp, since his August 2002 arrest in Thailand. He is accused of masterminding the 2002 Bali Bombing as well as the Marriott blast. According to interrogation reports, Hambali was undergoing plans to develop biological weapons, in particular Anthrax. Hambali, was al Qaeda's main connection in South East Asia, and was apparently trying to open an *"Al Qaeda bio-weapons branch plant"* in either Malaysia or Indonesia. He told investigators he had been *"working on an Al Qaeda Anthrax program in Kandahar,"* Afghanistan.
* Dr. Azahari Husin, a former university lecturer, was also known as the "Demolition Man" because of his bomb-making skils, and used a mobile phone to detonate the Marriott bomb and included ingredients similar to other Indonesian blasts. According to Indonesian police, "If Azahari did not make the bomb, then its creator was following his manual."
* Noordin Mohammed Top was suspected of helping finance the Bali blast and helping build the Marriott bomb. Noordin is a Malaysian citizen.
* Muhammad Rais was convicted in May 2004 of violating anti-terrorism laws in connection with the attack. Rais transported the explosives from various towns to Jakarta, where they were used in the bomb. He was sentenced to seven years in prison for his role. "*"We saw the Marriott attack as a message from Osama bin Laden,""* Rais said at his trail.
* Rusman Gunawan alias "Gun Gun" was sentenced in October 2004 to four years jail for *facilitating and aiding terrorism*. In particular he was found to have transferred the money (in Australian dollars) that was ultimately used to finance the Marriott bombing. He and six other Indonesian students were arrested during raids in Pakistan. He trained at the Al Ghuraba training camp in Afghanistan. In 2002 while he attended university in Pakistan, he took over as the "intermediary" for e-mail messages between al-Qaeda and Hambali, who at the time was hiding in Cambodia.
* Mohammed Nazir Bin Lep is one of Hambali's key lieutenants. and like Hambali is being held at the Guantanamo Bay detention camp. He allegedly transferred the al Qaeda funds used for the bombing and knew of Jemaah Islamiah plots to launch attacks elsewhere in South East Asia. The CIA claims he was to be a suicide bomber for a "second wave" of al Qaeda attacks targeting Los Angeles.
* Gempur Angkoro, alias Jabir, is al-Ghozi's cousin and was one of Top's most trusted men; he, was killed in a raid on 29 April. Jabir personally assembled the Marriott bomb, and the bombs used in the 2004 Jakarta embassy bombing. *(Jakarta Post, 2 May).*
* Sardona Siliwangi, was the first person to be sentenced for the Marriott attack. He had been *"legally and convincingly"* proven guilty of an act of terrorism, during his trial in the town of Bengkulu on the island of Sumatra, and sentenced to ten years in prison. Siliwangi had stored at his Bengkulu home, six cartons of explosives left by the suicide operative Asmar Latin Sani. The explosives were later moved to the South Sumatra town of Lubuk Linggau before being taken to Jakarta on the island of Java.
* Air Setyawan, Luthfi Haidaroh and Urwahr were all arrested in the Central Java city of Surakarta on 26 July 2004 by Indonesia's Detachment 88 anti-terrorist squad, which is trained and equipped by the United States and Australia.
* Yazid Sufaat

## Al-Qaeda connection

Stuart A. Levey, the Under Secretary for Terrorism and Financial Intelligence in the United States, believes that the 2002 Bali bombing, and the Marriott Hotel bombing were financed by smuggling $30,000 in cash for each attack from al-Qaeda to allied terrorists in Asia. By contrast, the 9/11 Commission estimated the 11 September 2001 attacks cost between $400,000 and $500,000 over two years—at least some of which was deposited in foreign accounts and accessed by the plotters in the USA.

The Vice President of the United States Dick Cheney said.

Hambali went to the training camps in Afghanistan that they ran back in the '90s, subsequently received funding from al Qaeda, went back then to Indonesia, and was behind some of the major attacks there. So you've got this sort of home-grown, but nonetheless affiliated, extremist operation going now in Indonesia. You'll find the same thing if you go to Morocco, where they had the attack in Casablanca; in Turkey, Istanbul, and so forth.

It was the simultaneous presence at al-Qaeda camps in Afghanistan by militants from across South East Asia that facilitated many of the personal relationships that exist between JI and members of other violent Islamist groups. These include the Moro Islamic Liberation Front, a secessionist movement fighting for a Muslim homeland in the southern Philippines, as well as several other Indonesian, Malaysian and Thai groups. The weight of evidence suggests that although some JI personnel might be inspired by the larger global mystique of figures such as Osama bin Laden, the South East Asian group remains operationally and organisationally distinct.

## Effects

The main Jakarta stock-market index tumbled 3.1 percent after the attack and its currency, the rupiah, lost as much as 2 percent of its value against the US dollar.

Australia issued a warning for its citizens to avoid all international hotels in Jakarta after intelligence found the capital could be under the threat of further attacks. This warning is still in effect.

# 2008 Mumbai attacks

Source: http://en.wikipedia.org/wiki/2008\_Mumbai\_attacks

The **2008 Mumbai attacks** were twelve coordinated shooting and bombing attacks across Mumbai, India's largest city by members of Lashkar-e-Taiba, the Pakistan-based militant organisation. The attackers allegedly received reconnaissance assistance before the attacks. Ajmal Kasab, the only attacker who was captured alive, later confessed upon interrogation that the attacks were conducted with the support of Pakistan's ISI. The attacks, which drew widespread global condemnation, began on Wednesday, 26 November and lasted until Saturday, 29 November 2008, killing 164 people and wounding at least 308.

Pakistan has often used proxy terrorists groups to achieve its foreign policy goal, in this case highlighting the issue of jurisdiction over Kashmir.

Eight of the attacks occurred in South Mumbai: at Chhatrapati Shivaji Terminus, the Oberoi Trident, the Taj Mahal Palace & Tower, Leopold Cafe, Cama Hospital (a women and children's hospital), the Nariman House Jewish community centre, the Metro Cinema, and a lane behind the *Times of India* building and St. Xavier's College. There was also an explosion at Mazagaon, in Mumbai's port area, and in a taxi at Vile Parle. By the early morning of 28 November, all sites except for the Taj hotel had been secured by Mumbai Police and security forces. On 29 November, India's National Security Guards (NSG) conducted Operation Black Tornado to flush out the remaining attackers; it resulted in the deaths of the last remaining attackers at the Taj hotel and ending all fighting in the attacks.

Ajmal Kasab disclosed that the attackers were members of Lashkar-e-Taiba, considered a terrorist organisation by India, Pakistan, the United States, the United Kingdom, and the United Nations, among others. The Indian government said that the attackers came from Pakistan, and their controllers were in Pakistan. On 7 January 2009, Pakistan's Information Minister Sherry Rehman officially accepted Ajmal Kasab's nationality as Pakistani. On 12 February 2009, Pakistan's Interior Minister Rehman Malik asserted that parts of the attack had been planned in Pakistan. A trial court on 6 May 2010 sentenced Ajmal Kasab to death on all the 86 charges for which he was convicted. On his appeal against this verdict, Bombay High Court on 21 February 2011and Supreme Court of India on 29 August 2012 upheld his death sentence. Kasab was executed by hanging at Yerwada Jail in Pune on 21 November 2012.

### Taj Mahal Hotel and Oberoi Trident

Two hotels, the Taj Mahal Palace & Tower and the Oberoi Trident, were among the four locations targeted. Six explosions were reported at the Taj hotel – one in the lobby, two in the elevators, three in the restaurant – and one at the Oberoi Trident. At the Taj Mahal, firefighters rescued 200 hostages from windows using ladders during the first night.

CNN initially reported on the morning of 27 November 2008 that the hostage situation at the Taj had been resolved and quoted the police chief of Maharashtra stating that all hostages were freed; however, it was learned later that day that there were still two attackers holding hostages, including foreigners, in the Taj Mahal hotel.

During the attacks, both hotels were surrounded by Rapid Action Force personnel and Marine Commandos (MARCOS) and National Security Guards (NSG) commandos. When reports emerged that attackers were receiving television broadcasts, feeds to the hotels were blocked. Security forces stormed both hotels, and all nine attackers were killed by the morning of 29 November. Major Sandeep Unnikrishnan of the NSG was killed during the rescue of Commando Sunil Yadav, who was hit in the leg by a bullet during the rescue operations at Taj. 32 hostages were killed at the Oberoi Trident.

A number of European Parliament Committee on International Trade delegates were staying in the Taj Mahal hotel when it was attacked, but none of them were injured. British Conservative Member of the European Parliament (MEP) Sajjad Karim (who was in the lobby when attackers initially opened fire there) and German Social Democrat MEP Erika Mann were hiding in different parts of the building. Also reported present was Spanish MEP Ignasi Guardans, who was barricaded in a hotel room. Another British Conservative MEP, Syed Kamall, reported that he along with several other MEPs left the hotel and went to a nearby restaurant shortly before the attack. Kamall also reported that Polish MEP Jan Masiel was thought to have been sleeping in his hotel room when the attacks started, but eventually left the hotel safely. Kamall and Guardans reported that a Hungarian MEP's assistant was shot. Also caught up in the shooting were the President of Madrid, Esperanza Aguirre, while checking in at the Oberoi Trident, and Indian MP N. N. Krishnadas of Kerala and Gulam Noon while having dinner at a restaurant in the Taj hotel.

# Case Study: Reconnaissance for the Mumbai Attacks

# By Steve Young

Source: http://www.homelandsecuritynet.com/HSN/index.php?option=com\_easyblog&view=entry&id=125&Itemid=2

At approximately 2000 hours on November 26, 2008, two motorized inflatable boats containing five men, each belonging to the terrorist group Lashkar-e-Taiba, landed on the southern tip of the peninsula jutting into the Arabian Sea that is home to nearly twenty-one million citizens of Mumbai city, formerly known as Bombay.  Armed only with small arms (AK-47’s) and hand grenades, they proceeded up the peninsula conducting terrorist attacks.  By 0800 hours on November 29, Indian Rapid Action Force personnel, Marine Commandos, and National Security Guard forces had killed 9 of the attackers and captured Pakistani citizen Ajmal Kasab.

The terrorists had succeeded in killing at least 173 people and wounding at least another 300.  It was India’s worst terrorist attack in terms of casualties and is often equated by Indians with the September 11, 2001, attack suffered by the United States.

The Mumbai attack could be considered successful from a terrorist’s perspective. But what is most interesting from a tacticians or intelligence perspective was that target selection and surveillance were not conducted by any of the terrorist perpetrators, but by American citizen Daood Gilani, a.k.a., David Headley.

Born Daood Gilani on June 30, 1960, to his American mother, Sherrill Headley, and Pakistani father, Syed Saleem Gilani, Gilani grew up in Karachi, Pakistan, after his parents divorced.  Here, he reportedly became extremely nationalistic (Pakistani) and anti-Indian.  In his late teens he returned to the United States and lived with his mother in Philadelphia.  However, Gilani returned to Pakistan several times and delved into drugs. In 1988, German police arrested him in Frankfurt trying to smuggle two kilograms of heroin into the United States.  Gilani only served four years in prison after US Drug Enforcement Agency (DEA) agents offered him a deal to cooperate against his two partners. They were convicted and received heavier sentences.

In 1997, the DEA again arrested Gilani and he became a paid informant.  The DEA then assigned him to travel to Pakistan and consort with drug dealers.  However, he ran afoul of the law again and served an additional eight months in prison.  While in prison, Gilani allegedly became a devout Muslim and, apparently unknown to the DEA, an Islamic supremacist. In 2000, Gilani again traveled to Pakistan under DEA control, but, at the same time discovered Lashkar-e-Taiba (LET), a US-designated Foreign Terrorist Organization whose Islamist ideology and anti-Indian manifesto appealed to Gilani.  Eventually Gilani was introduced to LeT founder Hafiz Saeed, who recruited Gilani for the Islamist cause.  Unbeknownst to the DEA, Gilani made several additional trips to Pakistan during 2000 and early 2001 to meet with LeT operatives.

After September 11, 2001, the DEA had Gilani travel to Pakistan several times to search out Pakistani drug dealers and also infiltrate terrorist groups.  However, it is unclear how many of his Pakistan trips were actually sanctioned or paid for by the DEA.  Nevertheless, in February 2002, at the same time he was possibly working for the DEA, Gilani began attending LeT training camps.  According to information divulged as part of his plea agreement, Gilani received additional LeT training in August 2002 and in April, August, and December 2003.

Gilani’s activities between 2003 and 2006 are not well documented.  However, in January 2006, Gilani met Major Iqbal (likely an alias), a Pakistani representative of the Inter-Services Intelligence Directorate (ISI), who recruited Gilani to spy for Pakistan and to continue working with LeT.  In February 2006, Gilani flew to Philadelphia, Pennsylvania, where he began the process of changing his official name to David Headley (from his mother’s maiden name).  For a foreign spy, this was an important event because now Headley would be able to travel on his US passport as a tourist and his Westernized name would not raise any official suspicions about his international travel, especially when crossing the Pakistani border into India.   When he returned to Pakistan, Major Iqbal began training Headley for his surveillance duties in Mumbai.

**Target Selection**

According to his plea agreement, Headley made trips to Mumbai to conduct surveillance in September 2006, February and September 2007, and April and June 2008.  On each occasion, posing as a tourist, he took extensive videos that he delivered to his LeT and ISI handlers in Pakistan.  He did not learn of the planned assault from the sea until just before his April 2008 travel to Mumbai, when potential landing sites were discussed. After arriving in Mumbai in April 2008, Headley identified with GPS the various landing sites, traveling by boat to each one so he could further describe the sites upon his return to Pakistan.

Video became essential to the surveillance phase of the operation.  In fact, when doing his surveillance activities throughout the city, Headley frequently stayed at the Taj Mahal Palace Hotel, eventually a prime target, going on in-house tours and photographing and shooting surveillance videos.  By the time he finished his surveillance there, he had documented almost every square inch of the very large hotel. In addition to the Taj Mahal Palace Hotel, the final targets were the Leopold Café, the Chabad House Jewish Community Center, the Chhatrapati Shivaji Terminus (CST) Train Station, and the Oberoi-Trident Hotel.  The Oberoi was considered a target of opportunity because it had not been on Headley’s original list of potential targets; however he took an opportunity to video the hotel and it was eventually selected for the attack.

Why these targets were eventually selected is subject to speculation.  However, the fact that Mumbai has nearly twenty-two million people in one of the world’s most populated countries guarantees immediate publicity, which is what terrorist groups thrive on.  Without media coverage, the event would never get noticed, nor would the terrorist group’s political message be conveyed to the general public. The two hotels attacked are some of the largest in the city and traditionally host many foreigners.  We can assume these hotels were chosen for maximum casualties.  The Jewish community center appears to have been a target because of the traditional animosity between Muslims and Jews. The Leopold Café is a popular restaurant and bar hangout for foreigners.  Drinking and bars are against Muslim religious practices, so it is possible that the bar was chosen as a target because of its affront to Islam.  Finally, the train station was an excellent target because of the large number of Indian passengers frequently present in its terminal.

**The Attack**

All things look different at night, even to those familiar with the area in the daylight.  In the Mumbai case, attacking at night and originating from the sea inhibited Indian citizens and security services. It also provided a degree of concealment for the terrorists.  Having landed their inflatable boats at approximately 2000 hours on November 26, 2008, the attackers split into five groups of two and began their attacks.  At approximately 2130 hours, two persons, including Ajmal Kasab, attacked the Chhatrapati Shivaji Terminus (CST) Train Station.

By the time this assault ended at about 2245 hours, 58 people had been killed and 104 others wounded. Shortly after the attack, Kasab was captured alive, but his partner was killed by Indian security forces.   At approximately the same time as the CST was being attacked, the Leopold Café was attacked by 2 people.  Approximately 10 people were killed there.  Apparently the terrorists spent little time there, only spraying the Café with AK-47 fire before moving on to assist in the takeover of the Taj Mahal Palace Hotel and the Oberoi Hotel.

Meanwhile, the Chabad House Jewish Community Center, also known as the Nariman House, was taken over by two people, and residents of the center were held hostage.  During the second day of the attack, the five-story building was stormed by Indian commandos late in the evening of November 28. Both terrorists and a commando had been killed during the assault.  The terrorists also murdered Rabbi Gavriel Holtzberg and his wife Rivka Holtzberg, who was six months pregnant, along with four other hostages.

The sequence of events at the Taj Mahal Palace Hotel and Oberoi Hotel is less clear than  the other attack sites presumably because so many witnesses make for conflicting reports.  Nevertheless, it appears that the attacks on the two hotels were conducted nearly simultaneously and began at approximately 2300 hours on November 26.  Four terrorists assaulted the Taj Mahal and two assaulted the Oberoi.  The lobbies of both hotels and the hotel restaurants were assaulted first.  At least thirteen diners in the Oberoi were killed, including thirteen-year-old Naomi Sherr, who was having dinner with her father, who was also killed. Terrorists then made their way onto the various floors looking for targets of opportunity.

Why these targets were eventually selected is subject to speculation.  However, the fact that Mumbai has nearly twenty-two million people in one of the world’s most populated countries guarantees immediate publicity, which is what terrorist groups thrive on.  Without media coverage, the event would never get noticed, nor would the terrorist group’s political message be conveyed to the general public. The two hotels attacked are some of the largest in the city and traditionally host many foreigners.  We can assume these hotels were chosen for maximum casualties.  The Jewish community center appears to have been a target because of the traditional animosity between Muslims and Jews. The Leopold Café is a popular restaurant and bar hangout for foreigners.  Drinking and bars are against Muslim religious practices, so it is possible that the bar was chosen as a target because of its affront to Islam.  Finally, the train station was an excellent target because of the large number of Indian passengers frequently present in its terminal.

Indian security forces arrived first at the Taj Mahal Palace Hotel at approximately midnight on the November 26 and fought with the terrorists throughout the night, while evacuating as many hotel guests and staff as possible.  Fighting continued throughout November 27 and 28.   In the early morning hours of November 29, it was reported that the Taj was under the control of Indian security forces.  However, all terrorists were not accounted for and at 0730 hours, Indian commandos discovered the last remaining terrorist and shot him. It was not until 0800 hours on November 29 that the Taj Mahal Palace Hotel was secured, leaving 31 hotel guests and staff dead and approximately 250 survivors.

Security forces did not arrive at the Oberoi until approximately 0600 hours on November 27, and they immediately began to assault the building. The terrorists retreated to the upper floors and began detonating hand grenades, setting the roof on fire and trapping a number of hotel guests.  Fighting continued throughout the day and night of November 27, but by mid-morning of the 28th many hostages had been rescued.  At approximately 1500 hours, Indian security forces had killed both terrorists.  Approximately 30 hostages had been killed and 140 people rescued.

Many foreigners were killed in the five attacks, including 6 American citizens.  However, of the approximately 173 people killed during the 3-day attack, approximately 138 Indian citizens were killed, mostly at the train station, but also a number of Indian police and commandos

**Aftermath of the 26 November 2008 Mumbai Attacks**

It was not until Ajmal Kasab, the lone surviving terrorist, was interrogated by Indian Security Services that LeT and Pakistani involvement in the attack was determined.  Presumably the Pakistanis were not pleased that Kasab had been captured alive, because Pakistani support for the operation, although suspected, was then confirmed by the Indians.  Kasab was convicted of 86 counts of murder in an Indian Court and sentenced to death on May 6, 2010.   On April 25, 2012, his death sentence was upheld by the Indian Supreme Court.

In early April 2012, the US Government offered a $10 million reward for the capture of Hafiz Mohammad Saeed, founder of LeT.  The day following the announcement, Saeed gave a press conference in Pakistan’s capital, Islamabad, demonstrating his freedom of movement and quasi-official Pakistani government support.

As for David Headley, in 2010 the US Government accepted a plea deal after he pled guilty to all federal terrorism-related charges.  According to the terms of the plea agreement, the US Attorney General agreed not to seek the death penalty against Headley as long as he continued to cooperate with federal officials.  Interestingly, Headley’s sentencing has been deferred until after the conclusion of his cooperation. This latest twist regarding Headley’s sentencing allows Headley to remain in US custody indefinitely and avoid extradition to India, where he would likely face the death penalty.

***Dr. Young*** *is a former CIA Operations Officer of the Clandestine Service with tours in the Middle East and South Asia. He is currently the Coordinator for the Masters of Science in Security Studies at Sam Houston State University, in Huntsville, Texas.*

Hotel Security: Have the hotels learnt a lesson after 26/11?

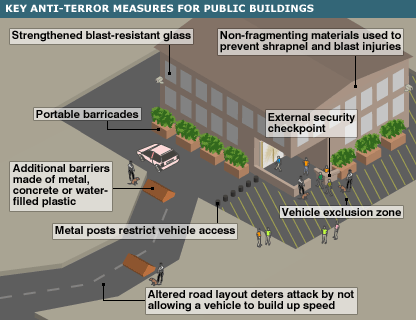
Source: http://www.moneylife.in/article/hotel-securityndash-i-have-the-hotels-learnt-a-lesson-after-2611/25969.html

****Hotel security in India is much tighter today. A visit to the Taj Mahal Hotel will make you aware that the hotel has become a fortress. The 26/11 terrorist attack when 166 people were killed in the twin attacks on the Taj Mahal Hotel and Trident Oberoi in Mumbai, have changed the perception of the hospitality sector regarding their vulnerability to such attacks and security incidents. I was recently staying at Hotel Keys in Thiruvananthapuram and was impressed by the security arrangements in the hotel. The instructions about fire safety were cogent and practical particularly the suggestion to crawl at the time of fire to avoid getting suffocated from smoke. Renjith Rajendranath, the Guest Service Manager-Front Office admitted that the 26/11 incident did push them to look more carefully at the security aspects in the design. The hotel came up after the incident.

However, Percival Edward, a security expert based in Bangalore, says that the actions taken by the hospitality sector post 26/11 were more of knee-jerk reactions. Installing security surveillance systems is not enough. Installing effective security surveillance systems coupled with creating awareness among the hotel staff by way of intensive training is what is needed. Another security expert Sathiya Seelan says that some of the hotels try to cut corners by installing fewer cameras than what is required. Much less attention is paid towards minor details like position of the cameras, the capturing and storage of images, training, retrieval of images, capturing moving objects with excellent precision and installing cameras in common areas like lobbies, reception, etc.

Though both Taj and Oberoi Trident have taken stringent measures to restore their premises and beef up the security, the same cannot be said about the others in the hospitality sector in India. Fire safety and security surveillance must go beyond the need to ‘comply’ and get a “No-objection” certificate from the fire department or the municipal authorities.

Worse is the fact that hospitality sector does not believe in regular annual maintenance contracts with the service providers. Says Chetan Nagappa who works for a security organization, “At the end of the day everything boils down to cost. The hotel authorities will remember the service providers only when there is a problem; when it comes to safety and security their primary intent is to save costs.”

A management trainee who briefly worked in a famous three-star hotel in Mumbai spoke to me on the condition of anonymity. She says, “It always surprises me that the hospitality sector spares no expense when it comes to providing world-class interiors with a terrific aesthetic sense; but when it comes to safety/security related issues, they believe that nothing will happen to them or their premises and so any money spent on security surveillance is considered an added burden.”

The hospitality sector should look at the consequences in the aftermath of an accident. How will it impact their brand? How long will it take to rebuild the hotel in case of property damage? Global insurance companies do talk about resilience—the ability to bring back a damaged property back to shape, but in India, the insurance companies seem to be more concerned about losses and claims. Our question is why not look at prevention through robust risk management and prudent underwriting norms?

The situation in some of the lesser known second-rung hotels is even more alarming. It doesn’t help that there is not a single designated authority to conduct periodic checks or audits. One is not sure if hotels have a disaster response plan in place.

Nagesh, a security expert based in Bangalore, feels that there are very few people who have realized the need to make their properties fail safe or security safe. He agrees that there are limitations that the hospitality sector faces in terms of fool-proof security measures. Security has always been on top of the agenda in five star hotels and high-end hotels, but the 26/11 incident has made them realize the importance of maintenance.

Nagesh regrets that other than these top-end hotels, the efforts of the mid-range and lower range hotels in the hospitality sector to improve the security measures are inadequate. Windsor Manor hotel in Bangalore refurbished their security surveillance post the 26/11 incident. He says that earlier hotels neglected maintenance but after 26/11 they have realized that maintenance is important too.

According to Nagesh, the mid-range and lower-end hotels install CCTVs only to comply with regulatory norms. He even adds that most of the five-star hotels are not aware of what they exactly need. So, the thinking of the hospitality sector has to change. The thinking should not be restricted to looking at the criteria required or meeting the norms. The need to install security systems under pressure from fire department or legal cell should be replaced with the need to enhance security surveillance to take care of their employees, guests, their properties and also the surrounding properties. The buildings adjacent to such hotels are also subject to collateral risks. This cannot be ignored.

# Canal Hotel bombing

Source: http://en.wikipedia.org/wiki/Canal\_Hotel\_bombing



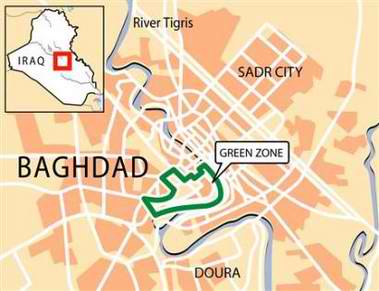
The Canal Hotel Bombing in Baghdad, Iraq, in the afternoon of August 19, 2003, killed at least 22 people, including the United Nations' Special Representative in Iraq Sérgio Vieira de Mello, and wounded over 100. The blast targeted the United Nations Assistance Mission in Iraq created just 5 days earlier. (The United Nations had used the hotel as its headquarters in Iraq since the early 1990s.) The attack was followed by a second bombing a month later which resulted in the withdrawal of the 600 UN staff members in Iraq. These events were to have a profound and lasting impact on the UN's security practices globally.

Abu Musab Zarqawi, a leader of the al-Qaeda terrorist organization, claimed responsibility for the blast.

## The bombing

In his book *The Prince of the Marshes*, Scottish writer Rory Stewart recounts his experiences at the Canal Hotel the day of the bombing.

I had wandered past the security point without anyone attempting to search me or ask my business. The Iraqis coming in and out of the compound were good-humored. I had said to my friend that things seemed pretty relaxed. She had replied that the special representative was proud that Iraqis could approach the UN building -unlike in the Green Zone, whose barriers were a half mile from the main offices. ... I went to the canteen, where I sat from ten until two in the afternoon, talking to local NGO staff who came in to eat and use the Internet. I particularly liked a Tunisian security advisor who had served in the Balkans and was worried about terrorists targeting the UN. I left at two, intending to return later in the afternoon to use the Internet. But when I came back at 4:30, a thick column of smoke was rising from either end of the building, families were screaming and pushing at a cordon of U.S. soldiers, and the woman who had served me my salad in the cafeteria was running toward us. In my brief time away from the building, a suicide bomber had driven his truck up beneath De Mello's office window.

The explosion occurred while Martin Barber, director of the UN's Mine Action Service (UNMAS) was holding a press conference. The explosion damaged a spinal cord treatment center at the hospital next door and a U.S. Army Civil-Military Operations Centre located at the rear of the Canal Hotel, and the resulting shockwave was felt over a mile away.

The blast was caused by a suicide bomber driving a truck bomb. The vehicle has been identified as a large 2002 flatbed Kamaz (manufactured in Eastern Europe and part of the former Iraqi establishment's fleet).Investigators in Iraq suspected the bomb was made from old munitions, including a single 500-pound bomb, from Iraq's pre-war arsenal.

The OCHA Humanitarian Information Centre (HIC) for Iraq (UNOHCI) was located directly beneath the office of Sérgio Vieira de Mello, the UN High Commissioner for Human Rights, and suffered a direct hit. Of the eight staff and one visitor in the office at the time, seven were killed instantly, but Sérgio Vieira de Mello and Gil Loescher were critically wounded and trapped in debris under the collapsed portion of the building. An American soldier - First Sergeant William von Zehle - crawled down through the collapsed building and worked to extricate the two men. He was joined later by another American soldier - Staff Sergeant Andre Valentine - and the two men spent the next three hours trying to extricate the two survivors without benefit of any rescue equipment. Loescher was rescued after having his crushed legs amputated by the soldiers, but Vieira de Mello died shortly before he would have been able to have been removed.

According to Abu Musab al-Zarqawi, de Mello was specifically targeted in the blast. The reason given by al-Zarqawi for targeting de Mello was that he had helped East Timor become an independent state (see the Indonesian occupation of East Timor). Zarqawi said that de Mello had participated in the unlawful removal of territory from the Islamic Caliphate and was therefore a thief and a criminal.

## Second bomb

The bombing was followed on September 22, 2003, by another car bomb outside the Canal Hotel. The blast killed the bomber and an Iraqi policeman and wounded 19 others, including UN workers. The second attack led to the withdrawal of some 600 UN international staff from Baghdad, along with employees of other aid agencies. In August 2004, de Mello's replacement, Ashraf Qazi, arrived in Baghdad along with a small number of staff.

# Kenya: Terror strikes on Paradise Hotel & plane

Source: http://www.dailymail.co.uk/news/article-149378/Terror-strikes-hotel--plane.html

Suicide bombers blew up a hotel full of Israelis in Kenya today (Nov 24, 2002), killing 15 people, minutes after missiles narrowly missed an Israeli airliner taking off nearby, in an apparently synchronized attack.

Israeli and Kenyan officials swiftly blamed the al Qaeda network, while the previously unheard-of "Army of Palestine" sent a claim of responsibility. Police said they were questioning two people seized near the scene of the hotel bomb.

Witnesses spoke of Israeli tourists and other survivors, streaked with blood and dust, staggering to the beach from the shattered Mombasa Paradise resort hotel and screaming for water after the attackers rammed a car bomb into the hotel lobby.

Police said three suicide attackers had killed themselves, nine Kenyans and three Israelis.

Israeli officials said two of the Israeli dead were children. Eighty people were wounded, Kenya's ambassador to Israel said.

Wreckage of the bombers' car was left 15 metres from the smouldering rubble of the entrance to the hotel, reported to be Israeli-owned and where most guests were Israeli.

"Around 7.30, we heard a massive explosion. The entire building shook," witness Kelly Hartog wrote on the Web site of Israel's Jerusalem Post newspaper.

"I saw people covered with blood, including children. Everyone seemed to be screaming. From the dining room we were herded out to the beach. There were no medics. People were screaming for water.

"I tried to occupy myself tending to the children. 'I want to go home,' they said. 'Where are my parents?'"

Minutes before the hotel blast, missiles were fired at an Israeli Arkia airliner carrying 261 passengers as it took off from Mombasa's airport.

"About two kilometres from the airport, two missiles were fired at the aircraft from a white Pajero (jeep) by some people who are suspected to be of Arab origin. Both missiles missed the aircraft," police spokesman Kimgori Mwangi said.

Ezra Gozlan, a passenger sitting at the back of the plane, said he saw a missile fly over the wing moments after take-off.

"All the wheels were in the air and then we heard the explosion. It (the missile) went about one metre above the wing," he said. The plane landed safely in Israel, escorted by Israeli air force jets.

"We spotted two white smoke trails passing us on the left side, from the rear to the front, and disappearing after a few seconds," pilot Rafi Marik said.

A Kenyan security source said it was believed the attackers used shoulder-borne missile launchers.

The hotel attackers were also described as of Arab appearance and also driving a four-wheeled-drive Pajero they had turned into a suicide bomb.

"Just after a group of tourists were brought to the hotel, I saw a white Pajero forcing its way into the gate," said a barman at a hotel across the road from the Mombasa Paradise, adding the attack happened at about 8.30am.

"It had three people of Arab origin and after it got to the reception area I heard an explosion."

Investigators said they did not rule out a link between the crash of a light plane which took off from Mombasa today, injuring at least seven, and the two attacks on Israelis.

Israeli and Kenyan officials were quick to accuse the al Qaeda network, blamed by Washington for the September 11 attacks last year on the United States that killed about 3,000 people and for the bloody 1998 truck bombings of U.S. embassies in Kenya and Tanzania that left 224 people dead.

If that judgment is correct, these would be the first direct attacks on Israelis by the fugitive Osama bin Laden's group.

"Indications are it is another wake-up call from hell by al Qaeda," said a senior Israeli diplomat. Nabil Abdel-Fattah, assistant director of the Cairo-based Al-Ahram Centre for Political and Strategic Studies, said the timing seemed to be aimed at coinciding with the Likud party leadership vote in Israel.

"It is to show the (Ariel) Sharon option, the Likud option, is not a solution to the Palestine problem," he said.

A statement faxed to Reuters in Beirut said however they were carried out by the "Army of Palestine" to mark the anniversary of the 1947 U.N. resolution partitioning Palestine between Arabs and Jews. There was no confirmation of the claim.

Bin Laden and his followers, forced into hiding by the U.S. campaign against their bases in Afghanistan after the September 11 attacks, were also suspected of involvement on the October 12 Bali bomb which killed 185.

U.S. officials said in June Sudanese authorities had arrested a suspected al Qaeda militant who claimed to have fired a shoulder-launched missile at a U.S. aircraft in Saudi Arabia.

The discovery of an empty but scorched launcher at the Saudi air base prompted the FBI to issue an intelligence alert that terrorists might try to shoot down an American commercial aircraft with shoulder-fired missiles.

Kenya's coastal region has a large Muslim population with traditional links to Saudi Arabia and Yemen.

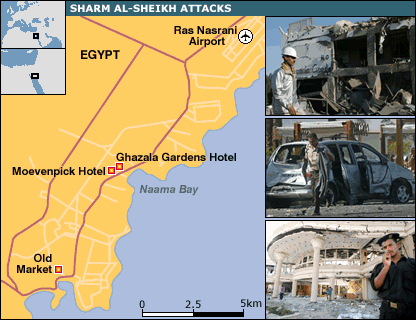
"We had similar attacks in 1998, the world including our friends have not helped us enough," Kenyan President Daniel arap Moi said. "We will do what we can to fight back."

# 2005 Sharm el-Sheikh attacks

Source: http://en.wikipedia.org/wiki/2005\_Sharm\_el-Sheikh\_attacks

The 2005 Sharm el-Sheikh attacks were a series of terror attacks on 23 July 2005, perpetrated by an Islamist organization, targeting the Egyptian resort city of Sharm el-Sheikh, located on the southern tip of the Sinai Peninsula. Eighty-eight people were killed, the majority of them Egyptians, and over 200 were wounded by the blasts, making the attack the deadliest terrorist action in the country's history.

The bombings coincided with Egypt's Revolution Day, which commemorates Nasser's 1952 overthrow of King Farouk. They were intended to hurt one of Egypt's most important vacation spots, a tourism capital that had billions of dollars invested in it, and achieved that goal as it was registered that many tourists vacated and there were numerous cancellations.

As a response, there were many arrests, especially of the Bedouin in the Sinai who allegedly aided the attack, and Egypt started erecting a separation barrier around the city, cutting it off from possible attacks and the nearby Bedouin community.

## Background

Historically, foreign tourists have been a common target of attacks dating back to the early 1990s. Militants have typically been motivated by a combination of Qutbism and opposition to the Mubarak government, and attacking foreigners including non-Muslims while hurting Egypt's tourist trade was seen as serving both goals.

The most bloody attack prior to the Sharm el-Sheikh bombings was the November 1997 Luxor massacre, in which 58 foreign tourists and four Egyptians died. In October 2004, a series of bomb attacks killed 34 people in Taba, also on the Sinai Peninsula. In April 2005 Cairo was hit by two days of terrorist violence, in which three foreign tourists were killed.

Unlike the October 2004 attacks, this attack does not appear to have been directed in particular against Israelis, for whom Sharm is a popular destination. However, one Israeli Arab was killed and another, Saneh Hussein, was injured.

## Explosions

The attacks took place in the early morning hours, at a time when many tourists and locals were still out at restaurants, cafés and bars. The first bomb blast, at 01:15 local time (22:15 UTC), happened at the Old Market bazaar in downtown Sharm el-Sheikh, killing 17 people, mostly Egyptians. The bomber had to abandon his truck bomb in the market because of a police roadblock. The second bomb was hidden in a suitcase and exploded outside the Moevenpick Hotel, killing six tourists. The final bomb was a truck bomb that was driven into the lobby of the Ghazala Gardens hotel, a 176-room four-star establishment in the Naama Bay area, a strip of beachfront hotels some 6 km from the town centre. About 45 people died in this blast.

The blasts were powerful, shaking windows miles away. Fire and smoke could be seen rising from the explosion sites.

## Casualties

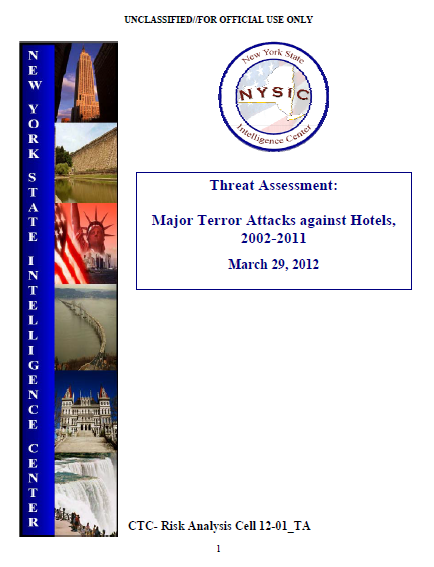
While the official government toll a few days after the blast was put at 64, hospitals reported that 88 people had been killed in the bombings.

The majority of dead and wounded casualties were Egyptians. Among those killed were 11 Britons, two Germans, six Italians, four Turks, one Czech, one Israeli, and one American. Other casualties, dead and wounded, included foreign visitors from France, Kuwait, the Netherlands, Qatar, Russia, and Spain.

## Responsibility

A group calling itself the Abdullah Azzam Brigades was the first to claim responsibility for the attacks. On a website the group stated that "holy warriors targeted the Ghazala Gardens hotel and the Old Market in Sharm el-Sheikh" and claimed it has ties to Al-Qaeda.

The Egyptian government said that the bombers were Bedouin militants from the same group that carried out the bombings in Taba a year before. Arrested suspects claimed to have been motivated by the War in Iraq.



New York State Intelligence Center Threat Assessment: Major Terror Attacks against Hotels, 2002-2011

Source: http://publicintelligence.net/nysic-hotel-attacks/

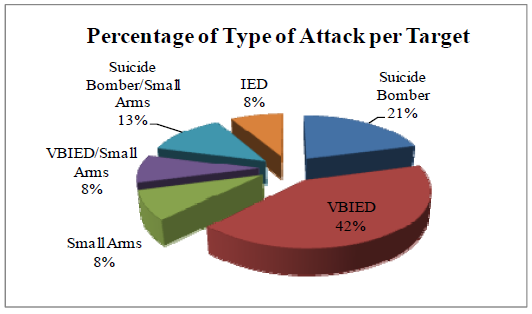
This product analyzes major terror attacks on hotels and provides a strategic-level assessment of the groups, tactics, and frequency of global terror attacks against hotels from 2002 – 2011. Additionally, the product identifies the deadliest types of attacks, comparing casualty counts and attack methods. The product was derived from media reporting and unclassified, for official use only sources.

Key Assumptions

Radical Islamic groups, including al-Qaeda and al-Qaeda linked groups continue to plan attacks against the West, including the United States (US). These groups view civilians as potential targets and will continue to use a variety of attack methods. Lack of information pertaining to a certain category in this report does not necessarily represent the absence of a threat. However, the frequency and tactic of attack analyzed in this report may indicate the most common vulnerabilities to an attack on the hotel sector.

**Executive Summary**

Since 2002 there have been 18 major terrorist attacks against hotels worldwide; a major attack is defined as an attack resulting in at least 10 casualties. During this time period there were no attacks against US homeland-based hotels. Groups with a connection to al-Qaeda carried out all but one of these major attacks.

* An attack on a hotel within New York State or the US would most likely follow the current predominant worldwide trend and utilize explosives or small arms.
  + Major attacks against hotels were primarily carried out using a military grade explosive; however, an explosive device constructed within the US would most likely use homemade explosives, such as triacetone triperoxide (TATP).
  + The use of small arms to attack a US-based hotel may be seen as a more viable option than trying to assemble a homemade explosive. Al Qaeda and their affiliates have encouraged Western-based radicals to use small arms to carry out attacks because of their ease of use and availability in comparison to building an explosive device.
* The likelihood of an al-Qaeda-inspired lone actor successfully attacking a hotel is low. However, lone actors in the US have shown an interest in targeting hotels previously. For example, Farooque Ahmed, arrested in April 2010, conducted pre-operational surveillance at a Washington, D.C. area hotel.
* A key leader or high-profile event/mass casualty opportunity was targeted in nearly 50% of the attacks, and represents a possible motivating factor for targeting.
* The most common tactic used against hotels is a vehicle-borne improvised explosive device (VBIED), accounting for 43% of the attacks analyzed in this report.

►**Read full report at:** http://info.publicintelligence.net/NYSIC-HotelAttacks.pdf

Bioterrorism: What Should Hotels Do to Reduce the Risk?

**By Carol J. Klitzke** (Apparel, Education Studies, and Hospitality Management

Iowa State University) **and Thomas Schrier** (Apparel, Education Studies, and Hospitality Management Iowa State University)

Source:http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1069&context=gradconf\_hospitality&sei-redir=1&referer=http%3A%2F%2Fwww.google.gr%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3Dinternational%2520hotel%2520terrorism%2520chronology%26source%3Dweb%26cd%3D39%26ved%3D0CGMQFjAIOB4%26url%3Dhttp%253A%252F%252Fscholarworks.umass.edu%252Fcgi%252Fviewcontent.cgi%253Farticle%253D1069%2526context%253Dgradconf\_hospitality%26ei%3Dq1U8UYeTHar07Aar1oHwBg%26usg%3DAFQjCNFjA6MRm6iTdM-zcAupb3XRey-urg%26bvm%3Dbv.43287494%2Cd.ZGU#search=%22international%20hotel%20terrorism%20 chronology%22

***ABSTRACT***

*The risk of a terrorist attack at any one hotel is low, but the consequences are dire, making it important for hoteliers to protect hotel guests and assets to the fullest extent possible. Terrorists cause fear and use violence to make their cause known. Biological weapons have the potential to harm larger populations than explosives, especially if released into the air, building ventilation systems, or water supplies. The types of hotels that are most at risk serve international customers, hold an iconic brand, or are owned by persons considered to be part of an “enemy” group. This study uses a Delphi method to poll hotel security managers about critical and feasible measures that hotels should take to prevent acts of bioterrorism. It is one of the first studies to investigate guidelines for bioterrorism in the hotel industry. As such this study can be used as a foundation for future research.*

# British hotels are vulnerable to Mumbai-style attacks, anti-terrorist officers warn

**By Christopher Hope** (Whitehall Editor)

Source: http://www.telegraph.co.uk/news/uknews/defence/5023968/British-hotels-are-vulnerable-to-Mumbai-style-attacks-anti-terrorist-officers-warn.html

Security services officials are also judging the threat against the UK to be at the "severe end of severe", just days before the G20 summit in London is due to begin.

The Daily Telegraph has learned that senior counter-terrorism officers are highly concerned about the possibility of attacks by terrorists using automatic weapons on major hotels and other public buildings.

This marks a change in the challenge posed to the security services, which have previously focused on preventing bombings.

The fears have been heightened by attacks by terrorists armed with pistols, grenades and assault rifles on eight sites including a luxury hotel in Mumbai last November, in which 173 people were killed and 308 injured.

The attacks have forced anti-terrorist officers to watch for any increase in small arms being smuggled into the UK through ports or remote airfields, where security is more lax.

Officials are also considering issuing guidance to the management of hotels, businesses and other buildings where people gather in large numbers about the best way to protect against terrorist attack.

Security sources have also told The Daily Telegraph that the threat of terrorist attack is now reckoned to be at the top end of "severe", the third of four risk levels which rate an attack "highly likely".

The only higher rating would be "critical" which means that an attack "is expected imminently".

The warning comes ahead of the planned launch of the new version of the Government's six-year-old "Contest" counter-terrorism strategy next week, which will include advice on how to protect buildings from attack.

"Contest Two" is also likely to raise concerns that the relentless focus on London is displacing the threat of terrorism away from the capital and towards other parts of the UK.

This fear is particularly relevant to the security plans for the Olympics in London 2012.

One official said the Home Office was "acutely aware" that the focus on securing London ahead of the Games could "displace attacks onto other parts of the UK".

The new strategy maintains the core focus on the four "Ps" - Prevent, Pursue, Protect and Prepare. However there will be a renewed emphasis on the "prevent" strand.

Officials are keen to identify and find ways of dissuading young Muslims from being radicalised and persuaded to become involved in terrorist activity.

The new strategy is also likely to address whether the security services are communicating the threat from terrorism to the public appropriately, amid fears that the warnings are being greeted with scepticism.

Chris Grayling, the shadow Home Secretary, said: "The Government is right that the horrific events in Mumbai have highlighted the need for a different strategy in counter-terrorism.

"No part of the UK is free from threat - and we know that terrorists want soft targets."

Patrick Mercer, chairman of the Commons' anti-terrorism sub-committee, added that he was concerned about the increased risk of attacks outside London.

The attempted suicide bombing of Glasgow airport with a car packed with propane canisters nearly two years ago showed how vulnerable the areas outside the capital are to a terrorist attack.

He said: "My greatest concern is that the regions should get the same level of attention as that which London does because that is where the terrorist will concentrate."

He also questioned whether spending £102million on the prevent strand over the past four years offered best value for money.

He said: "There is no doubt that a lot of work has been done but it has taken a long time to achieve what they have."

Mr Grayling added that there was "still not doing enough to tackle the problem of individuals and groups in the UK who are fostering the hatred and extremism that lies behind the terrorist threat".

The Home Office declined to comment on the record. However a Home Office source "strongly denied" that there was specific intelligence or concern about a Mumbai-style attack on hotels in the UK.

The source added: "We are always on alert. We are not just going to be relaxed and complacent. We are at this threat level. That is why we are going ahead with Contest Two."

## Hotel Security: Evolving Security Threats

Source: http://www.hotel-industry.co.uk/2011/06/hotel-security-threats/

**Ensuring the safety of your guests is of paramount importance and it is essential to have robust hotel security measures in place.**

**With threats evolving, we turn to Farina and Associates hotel security expert, Philip Farina, for up-to-date advice.**

### Hotel-industry.co.uk: What are the key security threats that UK hoteliers currently face?

**Farina:** It’s important to realise that UK hospitality organizations are exposed to various levels of man-made and natural risk. This may include: fire, weather, food poisoning and tampering, fraud, data theft and of course, the terrorism element, to name a few. An event against just one hotel property could send catastrophic ripple effects throughout our entire industry.

### Hotel-industry.co.uk: Has the nature of threats changed in recent years?

**Farina:** Yes, the use of technology, has greatly impacted how criminals can target hotels. For instance, instead of visiting a hotel to collect many pieces of information, a criminal can now scan the Internet pulling up specifics about room numbers, location to other areas of interest, the leadership team and photos of critical areas in the property. Using applications like Google Earth, a criminal can diagram the structure and their escape routes.

### Hotel-industry.co.uk: Do hoteliers often overlook the full impact of security threats?

**Farina:** Absolutely. Security in most hotels is falling way behind the curve ball when compared to many other industries. Due to the complexity of operations in running a successful hotel and the possibility of reputation damage, many potential risks and actual incidents are kept quiet and go unreported.

History has shown us that when an incident occurs at our hotel or resort and we have simply reacted or not properly prepared for it; the opportunity for catastrophic loss is greatly increased. These losses can include injuries and death as well as property, community and reputation damage. Security within hospitality is not cut and dry. An organisation that decides to install a few video cameras and add a security gate after an incident, is merely throwing money into an ever-growing fire.

### Hotel-industry.co.uk: Why is it important for hoteliers to partner with third-party companies and suppliers to improve hotel security?

**Farina:** Hoteliers should consider the utilisation of board-certified security consultants and vendors as they will have critical security insight about your property. Let’s face it, even the best employee security teams can become complacent and may only be able to view security from the inside out. While this has some benefit, it pales in comparison to a vendor who is experienced in hotel operations and qualified to analyse your property from the outside in or through the eyes of what would be a potential criminal.

The challenge for hotels is finding a vendor or consultant who can balance security and antiterrorism with customer service and convenience. Security in itself is black and white; hospitality on the other hand is an “open” environment and full of colour. Although this represents a challenging environment, only by blending these methodologies together effectively, can the organisation be successful in providing this heightened level of service to its employees and customers.

### Hotel-industry.co.uk: What steps can hoteliers take immediately to improve their hotel security?

1. **Conducting pre-employment screening checks and background investigations on all of their employees:**  
   The unfortunate truth within any organisation is that a large percentage of incidents occur due to the actions or inactions of current employees. Within the human resources community there is a saying: “garbage in, garbage out”. This means if you hire the wrong person who brings a questionable past onboard, there is a greater likelihood that problems and challenges can arise during their employment.
2. **Implementing Company-Wide Security Awareness programs:**

This empowers all of the employees (not just the security or loss prevention departments) within the company to become proactive and take part in the security of the hotel or resort.

1. **The 10-5 Rule:**

This procedure is taught to new employees through their orientation and existing employees through ongoing training. At 10 feet away, an employee makes eye contact with a guest and smiles. The employee then closes the distance and at 5 feet away, the employee engages the guest through conversation, offering to assist them or provide an answer. The last thing that a criminal desires is to be noticed and engaged by not one, but many employees. It can easily get criminals to re-think their choosing your hotel as a target. The Benefits: It provides the guest with a greater experience by showing true customer service at the time, increases the level of security at your property.

1. **The Creation or Revision of an Emergency and Evacuation Plan:**

Emergency and evacuation plans are proactive, working documents that should cover everything from a fire or natural disaster to the threat of an active shooter or terrorism event. They are designed to provide the safest avenue for the protection of your employees, guests and vendors. These plans should be updated at least semi-annually or whenever there is a turnover in any position of upper management.

### Rising extremism could threaten Maldives’ tourism industry: report

**April 5th, 2013**

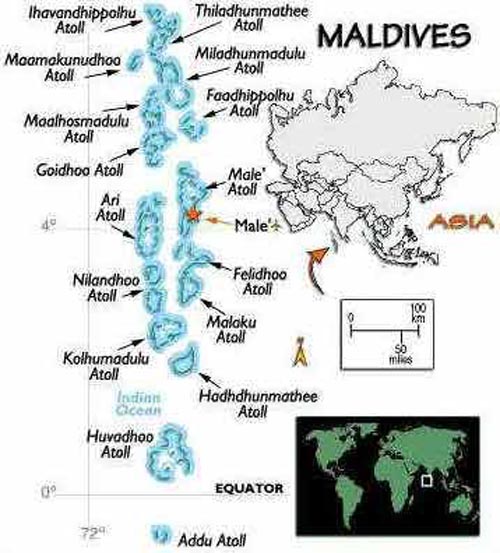
Source:http://www.terrorismwatch.org/2013/04/rising-extremism-could-threaten.html?utm\_source=feedburner& utm\_medium=email&utm\_campaign=Feed%3A+terrorismwatch%2FJTvK+%28Terrorism+Watch%29&utm\_content=Yahoo!+Mail

Religious conservatism and extremist violence have been increasing in the Maldives over the past decade, while incidents of Maldivians joining overseas jihadist groups are becoming more common, according to a report published in the Combating Terrorism Center (CTC) Sentinel, a publication based out of the West Point military academy in the US.

The article entitled The Threat from Rising Extremism in the Maldives, observes that growing religious extremism and political uncertainty could result in more violence and negatively affect the nation’s tourism industry, which would be “devastating” to the Maldives.

“This has coincided with a number of violent attacks on liberal activists and other citizens who have expressed outspoken support for moderate religious practices,” the report notes.

If current trends continue “extremist incidents may rise, with violence targeted against the country’s more liberal citizens,” it states.

According to the report, five key factors have contributed to the growing extremism and violence:

* the encouragement of “more hard line Islamist elements in the country” during the 30 year autocratic rule of former President Maumoon Abdul Gayoom;
* political uncertainty;
* an increasing number of people seeking education in foreign madrasas;
* grassroots radicalisation through civil society and political parties;
* escalating extremist incidents of violence and involvement with jihadist groups.

“The country has already suffered one terrorist attack targeting foreign tourists, and a number of Maldivians have traveled to Pakistan’s tribal areas to receive jihadist training. Moreover, evidence exists that jihadists tried to form a terrorist group in the country in 2007-2008,” the report states.

The study recommends that Maldivian political and religious developments be followed closely.

**Encouraging of hard line Islamic elements**

Islam was introduced to the Maldives in the 12th century and subsequent religious practices have been the “moderate, more liberal form of the religion”.

“Yet, during Gayoom’s three decade autocratic rule, the Egyptian-trained religious scholar enacted a number of measures that, at least inadvertently, encouraged more hard line Islamist elements in the country,” the report concluded.

“From imposing a ban on Christian missionary radio to apprehending migrant service providers for allegedly preaching and practicing their own religion, Gayoom’s regime initiated an era of state-backed religious intolerance and radicalisation in the Maldives.”

The Protection of Religious Unity Act, passed in 1994, mandated that no other religion but Islam could be practiced.

In 1996, Gayoom constituted the Supreme Council for Islamic Affairs, renamed the Ministry of Islamic Affairs in 2008, to preside over religious affairs in the Maldives.

“This body of clerics pressured the government to carry out moral and cultural policing of alleged “anti-Islamic activities”,” the report states.

For example, in 2008 the Ministry requested police “ban nightclubs and discotheques for New Year’s Eve celebrations because they were contrary to Islam”.

“By the end of Gayoom’s time in office in 2008, the dress code for women had grown increasingly conservative, and more and more men grew out their beards,” the report states.

Women now dress more conservatively with fewer brightly colored clothes. Instead they “increasingly wear black robes and headscarves and on more conservative islands such as Himandhoo, women wear black abayas and face veils,” it added.

**Political uncertainty**

The democratic transition “gave a greater voice to religious conservatives and those calling for the rigid implementation of Shari`a (Islamic law) in the Maldives,” states the report. “This became especially evident following the implementation of political reforms and the transition to multi-party democracy in 2008.”

The first democratic presidential elections in the Maldives were held in 2008, with Mohamed Nasheed defeating Gayoom in the second round with 54 percent of the votes.

However, the Nasheed administration was accused of defiling Islam by “promoting Western ideals and culture and restricted the spread of more austere Islamic practices,” the article notes.

This resulted in the December 2011 “Defend Islam” protests led by opposition political parties, religious groups, civil society organisations and thousands of supporters in the country’s capital, Male’.

These protests “unleashed a chain of events that culminated in a bloodless coup on February 7, 2012 that toppled the Maldives’ first democratically-elected government,” declared the study.

**Appeal of education in foreign madrasas**

Education in foreign madrasas has also contributed to growing extremism within the Maldives, with students “unwittingly attending more radical madrasas” and preaching these views upon their return.

“The offer of free education in madrasas in Pakistan and Saudi Arabia is widely acknowledged as a core means of radicalising Maldivians locally, with well-meaning parents sending their children off on scholarships to ‘study Islam’,” the report states.

Following the 2007 terrorist attack in Male’s Sultan Park, “Gayoom himself warned of this problem”.

“Maldivians are influenced by what is happening in the world. They go to Pakistan, study in madrasas and come back with extreme religious ideas,” the report quoted Gayoom as saying.

**Grassroots radicalization**

“The contemporary Maldivian political environment favors radical and political Islam taking root in Maldivian society, especially when political parties and civil society increasingly take refuge in religion,” the report states, citing Maldivian academic Dr Azra Naseem.

In 2010, new regulations prohibited “talking about religions other than Islam in Maldives, and propagating such religions through the use of any kind of medium.” The Ministry of Islamic Affairs published this legislation under the Protection of Religious Unity Act of 1994.

However, the report found that the “major force behind more austere religious practices in the Maldives is the Adhaalath (Justice) Party (AP), which has controlled the Ministry of Islamic Affairs, with Sheikh Shaheem Ali Saeed as its current minister”.

Given that the AP supports strict implementation of Shari’a Law, the party has “outspokenly argued that music and singing are haram (forbidden) and called for an end to the sale of alcohol at the country’s hundreds of luxury resorts,” said the report.

In February 2013, Saeed warned that “various Christian organisations and missionaries are strongly involved and active in our society because they want to ‘wipe out’ Islam from the Maldives”. He subsequently started a campaign against Christians and “Freemasons”, the report stated.

Two non-government organisations (NGOs), Jamiyyathu Salaf (JS) and the Islamic Foundation of Maldives (IFM), are considered religiously conservative Salafists who “work with the country’s political parties to further the cause of Islamism in the Maldives,” the report stated.

**Extremist incidents**

Extremists have directly targeted Maldivian liberal intellectuals, writers and activists, the study notes.  
“On January 3, 2011, assailants attempted to kill Aishath Velezinee, an activist fighting for the independence of the country’s justice system, by stabbing her in the back in broad daylight,” said the report.

Velezinee is a whistleblower that in 2010 identified members of the Judicial Service Commission (JSC) who were “conspiring with key political figures to hijack the judiciary and bring down the country’s first democratically-elected government,” the report added.

The study found that the Ministry of Islamic Affairs was “at least indirectly encouraged extremism” by initiating “crackdowns” on media outlets for anti-Islamic content.

The blog of prominent free speech and religious freedom campaigner, Khilath ‘Hilath’ Rasheed, was blocked in 2011. A month afterward, Rasheed’s skull was fractured when 10 men attacked him with stones during a peaceful rally he organised in Male’.

Rasheed was arrested a few days after the incident and jailed for 24 days for participating in the rally.

In June 2012, Rasheed was nearly killed “after extremists cut his throat open with a box cutter”.

“After the attempt on his life, Rasheed named three political leaders—Islamic Affairs Minister Mohamed Shaheem Ali Saeed, Adhaalath Party President Imran Abdulla and Jumhooree Party lawmaker Ibrahim Muttalib Shaheem – as being indirectly responsible for the attempt on his life,” the report states.

Later in 2012, the moderate religious scholar and lawmaker, Afrasheem Ali, was stabbed to death at his home in Male’. He was considered an Islamic moderate who was “outspoken in his controversial positions,” reads the report.

In February 2013, “a reporter for the Maldivian Democratic Party (MDP)-aligned Raajje TV station, Ibrahim ‘Aswad’ Waheed, was beaten unconscious with an iron bar while riding on a motorcycle near the artificial beach area of Male’,” the study added.

Previously, during the 2011 South Asian Association for Regional Cooperation (SAARC), protesters “intolerant toward other religious and cultural symbols” damaged monuments gifted to the Maldives by Pakistan, Bhutan, Sri Lanka.

Islamic radicals on February 7 2012 also vandalised archaeological artifacts in the National Museum that were mostly ancient Hindu and Buddhist relics, destroying 99 percent of the evidence of Maldivian pre-Islamic history.

**Jihadists**  
“In April 2006, a Maldivian national, Ali Jaleel, and a small group of jihadists from the Maldives attempted to travel to Pakistan to train for violent jihad in Afghanistan or Iraq,” the report reads.

While his first attempt was unsuccessful, Jaleel did eventually travel to Pakistan and “launched a suicide attack at the Inter Services Intelligence (ISI) headquarters in Lahore in May 2009.”

In September 2007, Islamic extremists committed a terrorist attack in the Maldives aimed at the tourism industry.

A bomb exploded in Male’s Sultan Park and wounded 12 foreigners. The three men arrested and later jailed for the bombing confessed that their goal was to “target, attack and injure non-Muslims to fulfill jihad,” states the report.

A month following the bombing, the investigation led to Darul-Khair mosque on Himandhoo Island. However, “some 90 masked and helmeted members of the mosque confronted police, wielding wooden planks and refusing to let the police enter,” said the report.

Although the Maldivian army eventually established control, “The stand-off resulted in a number of injuries, and one police officer had his fingers cut off.” In November, a video of the mosque confrontation was posted on the al-Qa’ida-linked alEkhlaas web forum by a group called Ansar al-Mujahidin with the message “your brothers in the Maldives are calling you,” the report states.

Evidence suggests that three Maldivian jihadists planned to establish a terrorist group in the country around 2007-2008 and send members for military training in Pakistan.

“At least one of these individuals did in fact travel to Pakistan, as Yoosuf Izadhy was arrested in Pakistan’s South Waziristan Agency in March 2009, along with eight other Maldivians,” states the report.

In 2009, then-President Nasheed warned that “Maldivian people are being recruited by Taliban and they are fighting in Pakistan,” quotes the report.

“Despite its reputation as an idyllic paradise popular among Western tourists, political and religious developments in the Maldives should be monitored closely,” the report concludes.

****

## 