Literature review on design terror mitigation for facility managers in public access buildings

Sarel Lavy and Manish K. Dixit
Department of Construction Science, College of Architecture, Texas A&M University, College Station, Texas, USA

Abstract

Purpose – The purpose of this paper is to identify key risks that are posed to the security of a site and building perimeters in the first and second lines of defense against terrorism, and are relevant to facility managers.

Design/methodology/approach – A qualitative approach to the literature review was applied. This involved an extensive literature search of existing peer-reviewed research papers, as well as state and federal reports to mark crucial issues relating to the security of a facility. Strategies to deal with the critical issues pertaining to the security of a facility were reviewed, based on the literature.

Findings – The paper identifies major security risks suggested by the literature and lists strategies to address those risks. The paper also proposes recommendations made by the literature; their implementation may provide a higher level of security to key areas located in the first and second lines of building defense.

Practical implications – The site and building perimeter areas that offer great potential for avoiding and deterring terror attacks are often neglected in terms of security planning, which seriously hampers efforts to provide an enhanced level of security to the facility. The paper points out these areas and major security issues related to them, so they can be taken care of by design professionals as well as facility managers.

Originality/value – The paper provides a comprehensive and detailed review of various aspects tied to the security level of critical areas of the building and site perimeters that could be useful to facility managers of critical facilities.

Keywords Design, Terrorism, Facilities, Disasters, Property management

Paper type Literature review

Background

The target of terrorist groups is shifting from iconic buildings or structures to soft (unsecured and easily accessible) targets where a large number of people gather, like transportation systems and facilities, business and shopping centers, public spaces, schools, libraries, and hospitals (Decker, 2001; Gilbert et al., 2003; Fischer and Green, 2004; Sternberg and Lee, 2006). Then and Loosemore (2006a, b) assert that most buildings are subject to risk associated with:

• premises;
• personnel;
• equipment; and
• data, information, and knowledge.

Since facility managers are responsible for the management of the buildings within an organization, their duties often incorporate activities such as planning,
and managing its security. In fact, this aspect is becoming an increasingly important feature of facility management (Then and Loosemore, 2006a, b). It is, therefore, important to identify the potential areas of terror risks and to create measures to reduce or eliminate such risks.

This study involves an extensive literature review, including government documents, reports, peer-reviewed journals, dissertations, and other literary sources. The paper is limited to the analysis of site perimeters, space between site boundaries and the building, and building perimeters. Literature is analyzed in order to not only identify potential risks, but also to suggest recommendations to deal with security risks. Thus, the paper focuses on those parts in the literature on design terror mitigation that are relevant to the facility management community.

**Literature review**

Sternberg and Lee (2006) define facility as: “a large and complex human occupied structure,” and such structures may become the primary target for terrorist attacks because of their mass occupancy (Marshall, 2002). Elliott et al. (1992) discuss strategies that could protect built facilities from terror attacks, and they propose the following measures to ensure the security of a building protection through:

- structural improvements, such as provision of structural members, joints, and prevention of progressive penetration;
- legislation, codes, and standards, such as those governing setbacks, occupancy, material use, emergency preparedness, and standoff distance; and
- building arrangements in planning and design, such as orientation, façade, standoff distance, physical barriers, natural barriers, and camouflaging primary structural members.

Sagun et al. (2008) reveal that the design of the exterior façade, the site and its environment has an impact on the security level of a building, as these affect entrances, exits and circulation, which eventually govern the chances of forced vehicular entry into the site.

*The concept of crime prevention through environmental design*

Crime prevention through environmental design (CPTED) is a strategy used to provide protection to buildings and facilities and is based on the concept of deflecting crime and decreasing crime fear by thoughtful architecture and effective site design (Demkin, 2004; O’Shea and Awwad-afferty, 2009). The theory of CPTED has its roots in Newman’s (1972) work and Tim Crowe’s efforts (early 1990s) that integrated behavioral psychology and sociology of human behavior with architectural design (Demkin, 2004; Wenzel, 2007). Newman performed a study of large-scale public facilities, that was developed further by the criminologist Jeffery (1971), who established principles of CPTED (Coaffee and O’Hare, 2008; O’Shea and Awwad-afferty, 2009; Bishop, 2004; Wenzel, 2007). According to Bishop (2004), CPTED as a method does not affect people negatively because it neither supports the use of conventional barriers, nor does it create a bunker-like environment. Coaffee and Bosher (2008) reveal that CPTED connects to essential aspects of construction and sustainability as it incorporates the use of environmental features to ensure buildings’ security. The following principles of CPTED are suggested by the literature:
(1) **Territoriality.** Informing the public about the purpose, use and acceptable activities of the facility, so that facility spaces could be defined in territories by landscape features like level differences, pavement designs, shrubs, and low walls (Demkin, 2004; Wenzel, 2007; Bishop, 2004).

(2) **Access control.** Prohibiting strangers from accessing sensitive areas by means of a gatehouse or other barriers (Demkin, 2004; Wenzel, 2007; Bishop, 2004).

(3) **Surveillance.** Watching critical areas via natural views (provision of clear and unobstructed view), mechanical devices (using equipment like closed circuit cameras, motion detectors, and sensors), and operational devices (provision of security staff and personnel) (Demkin, 2004; Wenzel, 2007; Bishop, 2004).

(4) **Management and maintenance of site.** Keeping the site and buildings clean and clear with up-to-date maintenance of the building, its envelope, and its components (Bishop, 2004).

(5) **Community involvement.** Community support for discouraging criminal or terrorism activities (Carlson and Briggs, 1990; Demkin, 2004).

(6) **Compatible land use/adjacent land use.** The surrounding land uses, where its quality and type may adversely affect the security of the property (Bishop, 2004).

The above-mentioned principles are reflected in the line of defense concept, where campus areas from site perimeter to the building interior are discussed in detail.

**Protection strategies: lines of defense concept**

O'Shea and Awwad-afferty (2009) assert that the protection of a building can be viewed as having an “onion philosophy,” where the building and its premise are layered like an onion: the outermost layer represents less critical areas and marks the first layer of defense against any terrorist assault. Inner layers mark the increasing importance of the spaces, and the innermost layers serve as the most crucial area of the building.

*First line of defense.* The perimeter of the premises is the first line of defense, the protective layer that prohibits terrorists’ forced entry, which provides a shield against shooting, protects from thrown stones or hand grenades, and screens against blast from explosive charge (Eytan, 2002; FEMA, 2003b, 2007; Demkin, 2004; Reid, 2005; Little, 2004). Federal Emergency Management Agency (FEMA, 2003b) suggests that the first line of defense must be located as far as possible from the building, and must be designed and maintained to prohibit the forced entry of large-scale weapons and explosive laden vehicles. Furthermore, controlled access, deterrence and delay could prove to be vital elements of a building protection strategy (FEMA, 2003b). Following are three aspects to be considered as the first line of defense:

(1) **Deterrence through planning.** Building planning and site design can effectively take care of most security related measures. Access points at an angle to the approaching street can significantly reduce the impact and velocity of a terrorist vehicle trying to ram into the building (FEMA, 2003b). Vulnerable areas such as parking garages must be kept away from buildings; in cases of high-risk facilities, it is extremely vital to provide offsite parking (FEMA, 2003a, b; Then and Loosemore, 2006b). Public areas, such as front lobbies or reception areas that are unsecured, should preferably be detached from the main building as these areas are subject to greater risks (FEMA, 2003a; Elliott et al., 1992).
(2) **Barriers.** Barriers could provide additional security by physically or psychologically prohibiting vehicular or pedestrian traffic inside the site and building. The area located between the site perimeter and the building must introduce barriers to the forced entry of vehicles toward the building and occupied areas; these barriers could be landscaped elements like embankments, terraced gardens and surfaces, water bodies, fountains, statues, free-standing columns, planters, shrubs, and trees (FEMA, 2003b, 2007; Coaffee and O'Hare, 2008; Coaffee and Bosher, 2008; Holtorp, 1994; Stewart, 2008). FEMA (2003b) describes two types of barriers to deter and delay terrorist entry to the site or to the building’s occupied areas: passive and active. Passive barriers are fixed and mostly constructed in place, and they can significantly lower the chances of forced high-speed entry. Placement of rough surfaced planters along pavement, concrete filled steel pipes, bollards, and a continuous reinforced concrete knee wall are recommended as extremely effective. Active barriers are operable barriers like crash beams, crash gates, surface mounted plate system, retractable bollards, and rotating wedge systems, and they can provide enhanced security to the building and to its premise.

(3) **Standoff – a vital security measure.** The impact of an explosion or blast weakens as distance from it increases, thus it is essential to determine and provide as much distance as possible between the potential location of an explosive and the building. This distance, called standoff, can provide tremendous protection, if public and vehicle access is kept sufficiently away from the building’s occupied areas (Elliott *et al.*, 1992; Demkin, 2004; O’Shea and Awwad-afferty, 2009; Bishop, 2004; FEMA, 2003b, 2007; Little, 2004; Lange *et al.*, 2005; Holtorp, 1994; Stewart, 2008; McClure *et al.*, 2004; Coaffee and Bosher, 2008).

**Second line of defense.** The second line of defense refers to the building envelope, which incorporates the external walls and roofs. This second layer further protects against forced entry and blast impacts and shields primary structural members, like columns and beams, from being exposed to explosion (Eytan, 2002; FEMA, 2003b, 2007; Demkin, 2004; Reid, 2005; O’Shea and Awwad-afferty, 2009). Following are three aspects of the second line of defense:

(1) **Form and shape of building envelope components.** Can potentially aggravate or alleviate the impact or damage due to terror attacks. Plain geometry with minimal or no ornamentation can substantially reduce the impact of an explosion or blast as ornamental components could result in flying debris during the explosion. Complicated geometry with reentrant corners, concave surfaces, and projections could trap the blast waves and aggravate the impact, as well as buildings shapes, like “L”, “U”, “T”, or “H” (Then and Loosemore, 2006b; Elliott *et al.*, 1992; FEMA, 2003a, b). The staggering back form of buildings and pitched roofs can cause blast wave shedding, and can reduce the magnitude of damage (Elliott *et al.*, 1992; Then and Loosemore, 2006b; FEMA, 2003a, b; Holtorp, 1994).

(2) **Air tightness of envelope.** A critical aspect, as air leakage could contaminate the interior environment substantially (FEMA, 2003a). McClure *et al.* (2004) warn that a leaky building envelope with improperly fixed doors and gaps all around windows could pose serious risks.
(3) **Glazed surfaces and window design.** One of the greatest risks in any explosion comes from flying debris containing building parts, glass, furniture, engine, and vehicle parts, which, while flying at high velocity, can severely injure people. Out of all the materials, glass poses the most serious risk because of it is commonly used and is relatively weak, brittle and can hardly resist plastic deformation (FEMA, 2003a, b; Cormie and Sukhram, 2007; Smith, 2002; Elliott *et al.*, 1992). Dislodged glass splinters and sharp edged shards can fly at high speed to greater distances, severely injuring, and even killing people (Smith, 2002; Elliott *et al.*, 1992; Then and Loosemore, 2006b; FEMA, 2003a, b, 2005; Cormie and Sukhram, 2007; McClure *et al.*, 2004; Holtorp, 1994; Stewart, 2008; Little, 2004). Using laminated glass, thermally tempered glass and wire reinforced glass can provide considerable protection from fragmented glass, since they break in cubical fragments or arrest fragments. Fragment retention films or shatter resistant films can be used on the inner surfaces of window or glazing glass to arrest flying glass pieces (FEMA, 2003a, b; Holtorp, 1994; Smith, 2002; Elliott *et al.*, 1992; Stewart, 2008).

**Third line of defense.** The interior areas and inner envelope form the third layer of protection that provides enhanced security against terrorist activities (Eytan, 2002; FEMA, 2003b, 2007; Demkin, 2004; Reid, 2005; O’Shea and Awwad-afferty, 2009). Employing technology and manpower, and planning and demarcating restricted and unrestricted areas could protect interior areas effectively, using technologies like closed circuit television (CCTV) systems, sensors, electronic and mechanical locks, and computerized access controls (Demkin, 2004; Reid, 2005). Furthermore, limited access to some areas could be assured by an effective security zoning that divides area into unrestricted, controlled, and restricted zones (Demkin, 2004). Unsecured areas, like loading docks, lobbies, retail areas, mailrooms, and garages must be designed and placed in isolation or away from core building areas that are occupied; these unsecured areas could be placed on the edge of the building or at lower levels to provide further protection to the main building (FEMA, 2003b). The placement and design of interior elements like blinds, frames, furniture, and equipment seriously influence the security level of the building interior, as these can easily turn into flying debris during the blast (FEMA, 2003b).

This study deals with the site perimeter, the space between site boundaries and the building, and the building envelope, which include site and building components such as vehicular and pedestrian circulation, surface parking and perimeter, utility systems, and building envelope. This paper aims to study current literature on design terror mitigation in order to:

- identify terror risks associated with the buildings; and
- suggest possible measures/recommendations as to reduce or eliminate risks.

**Research methods**

For the purpose of this study, the qualitative research approach was chosen to collect, summarize, and interpret the data. In qualitative research, data are collected from different sources and evaluated in hierarchy to form new concepts and theories (Holliday, 2007). The data collection should be completed objectively and as comprehensively as possible for later interpretation purposes (Silvermann, 2000). Wolcott (2001) summarizes the significant implications of qualitative research:
• It involves structuring multiple-choice criteria into a hierarchy.

• It assesses the importance of considered criteria with respect to the major concerns of the study.

• It involves both subjective and objective evaluation measures, thus reducing bias results in decision making.

• The nature of this type of research is exploratory and open ended. Specifically, literature analysis involving peer-reviewed journal articles, dissertations, selected government and private organization documents, and reports is implemented in this study.

As stated earlier, limited research has been conducted on facility managers’ responsibilities to act or to prepare in case of a terror attack. The following benefits are identified, considering the implications of the qualitative research approach:

• Multiple organizations’ guidelines are studied. These guidelines state issues related to terror mitigation, and therefore, it will possibly help to identify the hierarchy of problems associated with these attacks.

• Objective measures, based on the literature study, can be provided.

• Based on the study, exploratory recommendations may guide facility managers to reduce the vulnerability of their buildings to terror attacks.

Based on the literature, security strategies are driven by concerns about the operation of safe business; safety of staff, people, and security systems; and management, education, and supervision of the FM department’s staff. Guidelines relating to security techniques, stated by FEMA, CPTED, the American Institute of Architects (as viewed by Demkin, 2004), and other state or federal organizations are chosen for the purpose of this study because of the following reasons:

• they are all federally recognized and/or sponsored organizations;

• they update databases related to security and safety on a regular basis; and

• they incorporate details and strategies, as developed by other federally recognized organizations, such as the Critical Infrastructure Protection, Defense Threat Reduction Agency, Operationally Critical Threat, Asset, and Vulnerability Evaluation, and the Office of Emergency Preparedness.

Peer-reviewed journal articles, security reports from building consultants, books, and reports from overseas organizations are also included in order to attain a holistic literature review.

Data related to the identification of risks, identification of consequences based on risks, and formation of strategies were collected from the guidelines provided by literary sources mentioned earlier, which refer to terror mitigation methods and techniques. Furthermore, the following concerns were of prime importance while collecting the information related to terror mitigation identifying:

• methods and techniques within the scope of work of facility managers;

• facility design and security planning criteria where facility managers play an important role during the operation and maintenance phases; and
post construction technological security and safety issues related to management and operations of facilities, and to the public safety.

Four components of a facility were characterized as, vehicular and pedestrian circulation, surface parking and perimeter, utility systems, and building envelope. These components are related to the first and second lines of defense mentioned in the literature section. The purpose of choosing these four components was to cover the security aspects of site perimeter and building envelope of a facility in relation to terror attack, as these components could prove to be vital in governing the security level of a facility. As stated earlier, this study focuses on the areas around the proximity of a building, where the initial contacts with terrorists are made in a terror attack. FEMA (2003a), CPTED (2005) and Demkin (2004) have identified certain factors that govern the defensive nature of the facility. For this study, three aspects are identified, which are explored further in greater depth: site planning and building design, security planning, and surveillance of the building. Site planning and building design refer to the location of the facility in dense urban areas, entries and circulation, placement of activities, shape and form, and elements and materials used for construction. The security planning is studied in terms of the provision of required standoff distance and physical barriers. The surveillance of the building is reviewed in terms of site monitoring, site lighting, and site signage.

Findings
The results are arranged in three tables that focus on the first two lines of defense, namely:

(1) Site perimeter, described in terms of circulation, parking and other perimeter areas, and utility areas.

(2) Building envelope. Three aspects of building planning are studied and presented for each of the four components mentioned earlier that are:

- planning and design of a building and its site;
- security planning; and
- surveillance on site and within the building perimeter.

Findings are presented in the form of potential risks identified by the literature in order to identify critical areas that need to be considered by facility managers.

Risks and measures related to site planning and building design
Table I summarizes potential risks based on the location of the facilities, or the distance of activities from and within the facilities. Five parameters of site planning and building design are studied:

(1) facilities located in dense urban areas;
(2) entries and circulation;
(3) placement of activities;
(4) shape and form; and
(5) elements and materials used for the construction.
<table>
<thead>
<tr>
<th>Location of facility: in dense urban areas</th>
<th>Vehicular and pedestrian circulation</th>
<th>Surface parking and perimeter security</th>
<th>Utility systems</th>
<th>Building envelope</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Traffic routes with heavy traffic loads in urban areas are prone to terror attacks. Identification of threat/hazard is less likely, due to traffic (vehicles and pedestrians) from and to the site in an emergency; rescue operation after the attack is difficult (FEMA, 2003a; Demkin, 2004, Savitch, 2005; Bishop, 2004; Then and Loosemore, 2006b; Alberson, 2004; Katzman, 2005; Steinhauser, 2003; Reid, 2005)</td>
<td>(2) Insufficient setback from the perimeter allows more vehicles to gather at the same place, disturbing individual screening (FEMA, 2003a; CPTED, 2005; Jreissati, 2003; Atlas, 2008; GAO, 2008; FEMA, 2005)</td>
<td>(3) Absence of protection to incoming utility systems along the perimeter walls will give a target point to disrupt services (FEMA, 2003a, b, 2005; Demkin, 2004)</td>
<td>(4) Compact but tall structures with high occupant density and designed primarily with glass and metal possess target potential and risk of more damage, due to flying debris and taller structures (FEMA, 2003a, b, c, 2005, 2007; Eytan, 2002; Byfield, 2006; NCDPI, 2008)</td>
<td></td>
</tr>
<tr>
<td>Entries and circulation</td>
<td>(5) No alternative route to divert traffic in case of an emergency. Terrorists may initiate an attack during the peak time, where vehicular and pedestrian traffic are greater than average. Possibility to target sensitive areas in the facility (FEMA, 2003a; Demkin, 2004). More entries could adversely impact the security level of the facility (FEMA, 2003b, c, 2005; Schneider, 2006; Vale, 2005; Lange et al., 2005; BNIM Architects, 2005; NCDPI, 2008)</td>
<td>(6) Owing to having a single entrance, curbside parking and parking along the perimeter walls, which are relatively far from buildings, are commonplace. Therefore, these situations are ideal for terrorists to prepare an attack and act, as they are not observed (FEMA, 2003a, b, c, 2005; Demkin, 2004; CPTED, 2005; RealPAC, 2005; Atlas, 2008; MIOSHA, 2003)</td>
<td>(7) Secured utility areas near the main route will become a first target. Thus, services might be interrupted and terrorists could distract attention and plan an attack elsewhere in the facility (FEMA, 2003a; Demkin, 2004; CPTED, 2005; Atlas, 2008; BNIM Architects, 2005; Garcia, 2003)</td>
<td>(8) Restrict number of entries to the building to a minimum; control and prohibit access through window locks, deadbolts for doors, internal hinges, and forced and covert entry proof window designs. Consider separating entries for different users (FEMA, 2003a, b, c, 2005, 2007; ASIS International, 2008; BNIM Architects, 2005; McClure et al., 2004; GAO, 2008; McCamley, 2001; Demkin, 2004)</td>
</tr>
</tbody>
</table>

Table I. Threats and measures related to site planning and building design
Threats and measures | Vehicular and pedestrian circulation | Surface parking and perimeter security | Utility systems | Building envelope  
---|---|---|---|---  
Placement of activities | (9) Critical areas with high occupancy are possible targets and are prone to attacks if placed in close proximity to major traffic routes and unsecured public areas (FEMA, 2003a, b, c, 2005, 2007; BNIM Architects, 2005) | (10) The building’s main activities and services could be targeted easily if positioned near surface or underground parking (FEMA, 2003a, b, c, 2005, 2007; National Crime Prevention Council, 2003) | (11) Utility areas are usually not secured. They have a great potential for unauthorized entry, and should be detached from the main building (FEMA, 2003a, b, c, 2005, 2007; BNIM Architects, 2005) | (12) Occupied areas and major activities, if placed on the perimeter of the building, could be prone to acts of terror (FEMA, 2003a, b, c, 2005, 2007; Elliott et al., 1992)  
Shape and form (planning aspect) | (13) Straight and focused roads are risky, considering the possibility of forced entry and chances of ramming an explosive laden vehicle into the building (NCDPI, 2008; FEMA, 2003b, 2007; BNIM Architects, 2006) | (14) Low visibility areas with improper or difficult surveillance could be risky (FEMA, 2003a, b, c, 2005, 2007; BNIM Architects, 2005; Lismore City Council, 2000; National Crime Prevention Council, 2003) | (15) N/A | (16) Building perimeter and envelope, if planned in a shape and form that enhances their vulnerability, could be damaging (Then and Loosemore, 2006b; Elliott et al., 1992; FEMA, 2003a, b, c, 2005, 2007; Holtorp, 1994)  
Elements and materials used | (17) Barrier free roads on campus are riskier as they may enable the ramming of vehicles straight into the main building (Schneider, 2006; ASIS International, 2008; BNIM Architects, 2006; Coaffee and Bosher, 2008; Katzman, 2005, FEMA, 2003b, 2007) | (18) Cluttered and unrestricted parking areas could pose greater threat to the building (FEMA, 2003b, 2007; Eytan, 2002; National Crime Prevention Council, 2003; McCamley, 2001) | (19) N/A | (20) Building materials like glass, metal, plastics, wood, and other decorative items could turn into flying debris easily and could be more damaging (Smith, 2002; Elliott et al., 1992; Then and Loosemore, 2006b; FEMA, 2003a, b, 2005; Connolly and Suldram, 2007; McClure et al., 2004; Holtorp, 1994; Stewart, 2008; Little, 2004)
These risks are studied with respect to vehicular and pedestrian circulation, surface parking and perimeter security, utility systems, and building envelope.

**Risks and measures related to security planning**

Table II summarizes possible risks based on the security planning aspect. Two parameters are studied:

1. standoff distance; and
2. physical barriers.

**Risks and measures related to surveillance of the building**

Table III summarizes possible risks based on the building surveillance systems. Three parameters are studied:

1. site monitoring;
2. site lighting; and
3. signage systems showing location of sensitive areas.

**Literature recommendations for security strategies**

Based on the identification of terror risks, as described above, security strategies were developed in order to assist facility managers’ preparations for such an emergency. The security strategies are categorized into the following five categories:

1. vehicular and pedestrian circulation;
2. surface parking and perimeter security;
3. utility systems;
4. building and envelope; and
5. miscellaneous.

The following recommendations are presented in the same order as risks are presented in the tables.

**Vehicular and pedestrian circulation.** The following recommendations were collected from the literature on security strategies relevant to vehicular and pedestrian circulation:

- In case of an emergency, vehicles can act as temporary physical barriers, and be placed at intersections for signaling or directing traffic. Furthermore, an evaluation of the amount of traffic and its flow should be done periodically in order to monitor problems related to traffic control (FEMA, 2003a; Demkin, 2004; CPTED, 2005) (item 1 in Table I).

- If possible, one-way circulation of vehicles within the premises should be designed to allow personnel to adequately monitor suspicious activities of vehicles and people (FEMA, 2003a; Demkin, 2004) (items 1 and 5 in Table I).

- If possible, the number of vehicular access points to the site and building must be minimized in order to reduce the possibility of terror attacks (FEMA, 2003b, c, 2005; Schneider, 2006; Vale, 2005; Lange et al., 2005; BNIM Architects, 2005; NCDPI, 2008) (item 5 in Table I).
<table>
<thead>
<tr>
<th>Threats and measures</th>
<th>Vehicular and pedestrian circulation</th>
<th>Surface parking and perimeter security</th>
<th>Utility systems</th>
<th>Building and envelope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standoff distance</td>
<td>(1) The route between traffic origin and destination may be affected in case of devastating damage to the facility; even additional routes are affected badly in a hazard (FEMA, 2003a; CPTED, 2005; Savitch, 2005). There should be sufficient standoff distance between the vehicular roads and the buildings or main occupied areas of a facility (Coaffee and Bosher, 2008; BNIM Architects, 2005; NCDPI, 2008)</td>
<td>(2) Absence of exclusive zone(s) within the site gives freedom to terrorists for close and multiple inspections on the security techniques and procedures. Lack of enough standoff between parking and the building could be damaging (FEMA, 2003a, b, c, 2005, 2007; Demkin, 2004; Jreissati, 2003; BNIM Architects, 2005)</td>
<td>(3) Utility systems with no or little standoff could pose risk of attack on occupied areas as these areas are mostly unsecured and unmonitored (FEMA, 2003a, b, c, 2005, 2007)</td>
<td>(4) Main building without standoff could be detrimental, as impact of terror attacks like blasts could be reduced with distance (FEMA, 2003a, b, c, 2005, 2007; Elliott et al., 1992; Demkin, 2004; O’Shea and Awwad-afferty, 2009; Bishop, 2004; Little, 2004; Lange et al., 2005; Holtorp, 1994; Stewart, 2008; McClure et al., 2004; Coaffee and Bosher, 2008)</td>
</tr>
<tr>
<td>Physical barriers</td>
<td>(5) Straight and barrier free roads are prone to attacks that ram explosive laden vehicles into buildings. Internal roads should be provided with physical barriers in such a fashion that they welcome visitors and occupants but keep potential vehicle threats away (FEMA, 2003b, 2007; Coaffee and O’Hare, 2008; Coaffee and Bosher, 2008; Holtorp, 1994; Stewart, 2008)</td>
<td>(6) Parking areas possess great risk of potential attacks, if located closer to the building. Physical barriers between surface parking and building, like level difference, walls, earth mounds, and bollards could provide additional security to the building (FEMA, 2003b, 2007; Coaffee and O’Hare, 2008; Coaffee and Bosher, 2008; Holtorp, 1994; Stewart, 2008)</td>
<td>(7) Utility penetrations, if not checked and sealed properly, could be risky (FEMA, 2003a, b, c, 2005, 2007; BNIM Architects, 2005; ASIS International, 2008)</td>
<td>(8) An easily approachable and barrier free building is a more likely target of terror attacks (FEMA, 2003a, b, c, 2005, 2007; BNIM Architects, 2005)</td>
</tr>
</tbody>
</table>
### Threats and measures related to surveillance of the building

<table>
<thead>
<tr>
<th>Threats and measures</th>
<th>Vehicular and pedestrian circulation</th>
<th>Surface parking and perimeter security</th>
<th>Utility systems</th>
<th>Building and envelope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site monitoring (natural, mechanical, and operational)</td>
<td>(1) If traffic monitoring systems are not placed at intersections, it will be difficult to respond to building alarm systems in an emergency. Furthermore, lack of electronic surveillance and screening of incoming vehicles could be a grave threat to building security (FEMA, 2003a, b, c, 2005, 2007; CPTED, 2005; GAO, 2008; McCamley, 2001; ASIS International, 2008)</td>
<td>(2) Absence of pullover lanes for inspection of random and suspect vehicles at entrances provides an opportunity to enter deep into the site. Inadequate detection tools might not detect explosives in the lower part of a vehicle (FEMA, 2003a, b, c, 2005, 2007; CPTED, 2005)</td>
<td>(3) Absence of intrusion detection sensors and frequent manual surveillance might result in drastic problems, as terrorists may think they can act with no interruption, as no one is watching the utility systems (FEMA, 2003a, b, c, 2005, 2007; CPTED, 2005)</td>
<td>(4) Activities and circulation without constant monitoring pose risk to the building (Demkin, 2004; Wenzel, 2007; Bishop, 2004; O'Shea and Awwad-afferty, 2009; Carlson and Briggs, 1990)</td>
</tr>
<tr>
<td>Site lighting</td>
<td>(5) Dark or improperly illuminated streets on site hold greater risk of terror attacks (FEMA, 2003a, b, c, 2005, 2007; Demkin, 2004; Reid, 2005; CPTED, 2005; McCamley, 2001; Lismore City Council, 2000; Zahm, 2007; BNIM Architects, 2005; ASIS International, 2008; NCDPI, 2008; McClure et al., 2004)</td>
<td>(6) Parking areas are potential hiding places for threat vehicles, and thus need illumination (FEMA, 2003a, b, 2007; Demkin, 2004; CPTED, 2005; Then and Loosemore, 2006b; BNIM Architects, 2005; Harris et al., 2002; ASIS International, 2008; Katzman, 2005; NCDPI, 2008; National Crime Prevention Council, 2003)</td>
<td>(7) Utility areas like loading docks, storage, trash areas, and employee entries could possess great potential for terror attacks, if they are not well illuminated (FEMA, 2003a, b, c, 2005, 2007)</td>
<td>(8) Lack of illumination on the building perimeter could result in difficult surveillance and easy terror attacks (FEMA, 2003a, b, c, 2005, 2007)</td>
</tr>
<tr>
<td>Signage</td>
<td>(9) Internal roads with improper or no signage are almost certain to have unauthorized entries. However, signage may provide information about the location of critical buildings and occupied areas of the facility; thus, signage should be minimized (FEMA, 2003a, 2007; Demkin, 2004; CPTED, 2005; BNIM Architects, 2005; NCDPI, 2008; National Crime Prevention Council, 2003)</td>
<td>(10) Non-segregated parking with no or little signage could be confusing and thus risky (FEMA, 2003a, 2007; Demkin, 2004; NCDPI, 2008; Katzman, 2005; BNIM Architects, 2005)</td>
<td>(11) Utility areas are prone to unauthorized entry (FEMA, 2003a; Demkin, 2004; BNIM Architects, 2005)</td>
<td>(12) Critical areas with signage identifying them could be targeted easily (FEMA, 2003a, b, c, 2005, 2007; BNIM Architects, 2005)</td>
</tr>
</tbody>
</table>
• Critical areas possessing high occupancy should be kept away from major traffic arteries of the site by providing unsecured and public activities in between (FEMA, 2003a, b, c, 2005, 2007; BNIM Architects, 2005) (item 9 in Table I).

• Roads must be designed in meandering fashion so as to prevent a speeding vehicle from ramming into the buildings (NCDPI, 2008; FEMA, 2003b, 2007; BNIM Architects, 2005) (item 13 in Table I).

• Placing objects and using materials properly can significantly reduce not only the risk but also the impact of terror attacks. For example, physical and psychological barriers can be placed to restrict and guide traffic on roads (Schneider, 2006; ASIS International, 2008; BNIM Architects, 2005; Coaffee and Bosher, 2008; Katzman, 2005; FEMA, 2003b, 2007) (item 17 in Table I).

• The route between traffic origin and destination may be affected in case of devastating damage to the facility; even additional routes are affected badly in case of a hazard (FEMA, 2003a; CPTED, 2005; Savitch, 2005). There should be sufficient standoff distance between the vehicular roads and the buildings or main occupied areas of a facility (Coaffee and Bosher, 2008; BNIM Architects, 2005; NCDPI, 2008) (item 1 in Table II).

• Internal roads should be provided with physical barriers in such a fashion that they are welcoming to visitors and occupants but keep away potential vehicle risks (FEMA, 2003b, 2007; Coaffee and O'Hare, 2008; Coaffee and Bosher, 2008; Holtorp, 1994; Stewart, 2008). Barriers should be used at an angle so that vehicles will not be able to gain speed before accessing buildings or sensitive zones. Moreover, to prevent direct or straight-line access of vehicles to sensitive zones, barriers should be placed on entry roads at these road intersections (FEMA, 2003a; Demkin, 2004; CPTED, 2005) (item 5 in Table II).

• Access and ways leading to sensitive areas should be controlled with detection systems, and should have minimum possible signs identifying their location. Signs should be placed, stating that the zone is under inspection and no one can enter without prior permission (FEMA, 2003a; Demkin, 2004; CPTED, 2005) (item 1 in Table III).

• Traffic routes must be illuminated with required level of light to improve surveillance and visibility (FEMA, 2003a, b, c, 2005, 2007; Demkin, 2004; Reid, 2005; CPTED, 2005; McCamley, 2001; Lismore City Council, 2000; Zahm, 2007; BNIM Architects, 2005; ASIS International, 2008; NCDPI, 2008; McClure et al., 2004) (item 5 in Table III).

• In public buildings, entrances should be marked specifically for site personnel, visitors, and public traffic. All the entrances should be equipped with security personnel to guide people, if necessary, and the entrances should always be lighted for fast and efficient inspection (FEMA, 2003a; Demkin, 2004; CPTED, 2005). Instead of detailed and descriptive information for buildings located within the facility, street addresses and building numbers should be provided. This will keep the information on sensitive areas, e.g. mailing center, loading docks, etc. available only to those who need to use it (FEMA, 2003a; Demkin, 2004) (item 9 in Table III).

Surface parking and perimeter security. The following recommendations were collected from the literature on strategies relevant to surface parking and perimeter security:
Curbside parking and parking along the wall could be minimized to avoid possible terror attacks. In order to inspect suspect vehicles, pullover lanes should be provided at each of the site entry gates. This will facilitate vehicle inspection before allowing them to park within the premises (FEMA, 2003a, b, 2003c, 2005, 2007; CPTED, 2005) (items 2 and 6 in Table I).

To minimize the effects of blasts caused by vehicle bombs, it is recommended to keep vehicle parking and service areas away from buildings and sensitive zones (FEMA, 2003a, b, 2003c, 2005, 2007; CPTED, 2005) (item 10 in Table I).

Parking and perimeter areas should be designed in shapes and forms that allow for maximum visibility and easy surveillance (FEMA, 2003a, b, c, 2005, 2007; BNIM Architects, 2005; Lismore City Council, 2000; National Crime Prevention Council, 2003). Depending on the site layout, the inspection areas should be designed so that one is located at the entry point and another one near the building envelope. This way, random checkup of suspect vehicles and individuals is possible without disturbing the routine operations of the building (FEMA, 2003a; Demkin, 2004; CPTED, 2005) (item 14 in Table I).

Physical and psychological barriers should be placed where they can restrict and guide traffic in between parking areas and other perimeter areas. Furthermore, walls and ceilings in parking areas should have light color finishes (FEMA, 2003b, 2007; Eytan, 2002; National Crime Prevention Council, 2003; McCamley, 2001) (item 18 in Table I).

Appropriate distance between parking and buildings should be provided. If the setback is insufficient, structural hardening of the external walls is necessary (FEMA, 2003a, b, c, 2005, 2007; Demkin, 2004) (item 2 in Table II).

Traffic obstacles and barriers, e.g. bollards, should be provided near entry control points in order to slow down traffic and allow the inspection of suspicious activities (FEMA, 2003a, b, c, 2005, 2007; Demkin, 2004) (item 6 in Table II).

In high-risk facilities, using manual and technological surveillance systems at each access point can control unauthorized access. This includes patrolling and inspecting individuals by using metal detectors, CCTV, and intrusion detection devices (FEMA, 2003a; Demkin, 2004; CPTED, 2005). The latest inspection and monitoring technologies (as approved by the appropriate authorities) should be provided in inspection areas (FEMA, 2003a; Demkin, 2004; CPTED, 2005) (item 2 in Table III).

If possible, parking within the interior of a group of buildings should be restricted: only employee vehicles parking with identity cards should be allowed in these areas. Access to the interior of a group of buildings must be screened and monitored 24/7 (FEMA, 2003a; Demkin, 2004; CPTED, 2005). Preferably, parking lots are located within view of occupied buildings. Parking areas that are not in direct view of the buildings should be used by employees only (FEMA, 2003a; Demkin, 2004; CPTED, 2005) (item 2 in Table III).

Emergency communication systems should be provided in parking areas in well lighted and easily identifiable and reachable locations. These should have direct line to in-house FM department, police, emergency medical care, etc. (FEMA, 2003a; Demkin, 2004). An in-house communication system (directly monitored
Utility systems. The following recommendations were collected from the literature on security strategies relevant to utility systems:

- Incoming utility systems must be provided with adequate protection (FEMA, 2003a, b, 2005; Demkin, 2004). Underground utilities should be concealed after any repair and maintenance work (FEMA, 2003a, b, 2005, 2007; CPTED, 2005) (item 3 in Table I).
- Redundant utility systems should be designed for emergencies (FEMA, 2003a; CPTED, 2005) (items 3 and 7 in Table I).
- Redundant and backup utility systems should not be located within main systems or even run in the same chases (FEMA, 2003a; CPTED, 2005) (item 7 in Table I).
- Sensitive areas should be separate from loading docks and shipping and receiving areas by at least 50 feet (15 meters) (FEMA, 2003a; CPTED, 2005; NCDPI, 2008; BNIM Architects, 2005) (item 11 in Table I and item 3 in Table II).
- Trash receptacles should not be placed within the standoff zone of a building (FEMA, 2003a; Demkin, 2004) (item 3 in Table II).
- Utility penetration in all barriers should be properly checked and sealed, and all utility lines should be properly concealed, encased, and buried (FEMA, 2003a, b, c, 2005, 2007; BNIM Architects, 2005; ASIS International, 2008). All utility penetrations at the perimeter of the site should be secured and screened regularly in order to avoid access by an intruder; intrusion detection sensors can also be used (FEMA, 2003a; CPTED, 2005) (item 7 in Table II).
- Proper monitoring systems must be provided to watch utility systems and utility areas systems (FEMA, 2003a, b, c, 2005, 2007; CPTED, 2005) (item 3 in Table III).
- Utility areas like loading docks, storage, trash areas, and employee entries should be provided with required lighting, as these possess great potential for terror attacks because of unsecured activities (FEMA, 2003a, b, c, 2005, 2007) (item 7 in Table III).
• Signs identifying critical utility complexes should be minimized. In order to prevent unauthorized access, fencing can be placed along the side of the utilities main entrance (FEMA, 2003a; Demkin, 2004; CPTED, 2005; NCDPI, 2008) (item 11 in Table III).

*Building and envelope.* The following recommendations were collected from the literature on security strategies relevant to building and envelope:

• Tall structures must be designed considering structural failure in case of a terror attack, and must not be built with materials that cause more damage to the building and its surroundings (FEMA, 2003a, b, c, 2005, 2007; Eytan, 2002; Byfield, 2006; NCDPI, 2008) (item 4 in Table I).

• Attention must be paid to the entry points on the building perimeter as those are primary points of entry to the main occupied areas (FEMA, 2003b, c, 2005; Schneider, 2006; Vale, 2005; Lange et al., 2005; BNIM Architects, 2005) (item 8 in Table I).

• The building’s perimeter is prone to attack and damage, thus, public and unsecured areas must be provided on periphery of the main building while placing occupied areas in a central secured core (FEMA, 2003a, b, c, 2005, 2007; Elliott et al., 1992) (item 12 in Table I).

• The building’s façade and its form must discourage possible damage due to terror attacks, like blasts, by not providing concave curves, recessed areas, courts, re-entrant angles, or “L”, “U”, “H” or “T” shapes (Then and Loosemore, 2006b; Elliott et al., 1992; FEMA, 2003a, b, c, 2005, 2007; Holtopr, 1994) (item 16 in Table I).

• Building façades must not contain building materials that possess the potential to become flying debris during terror attacks like blasts (Smith, 2002; Elliott et al., 1992; Then and Loosemore, 2006b, FEMA, 2003a, b, 2005; Cormie and Sukhram, 2007; McClure et al., 2004; Holtopr, 1994; Stewart, 2008; Little, 2004) (item 20 in Table I).

• Buildings must be secured by providing the required standoff distance from the potential targets of terror attacks like vehicular roads, parking areas, site entry points, and utility areas (Coaffee and Bosher, 2008; BNIM Architects, 2005; NCDPI, 2008; FEMA, 2003a, b, c, 2005, 2007, 2008; Demkin, 2004; Jreissati, 2003) (item 4 in Table II).

• The building perimeter must be well equipped with natural mechanical and operational monitoring systems to facilitate surveillance, and must be properly lit to provide better visibility (FEMA, 2003a, b, c, 2005, 2007; CPTED, 2005; GAO, 2008; McCamley, 2001; ASIS International, 2008; Demkin, 2004; Wenzel, 2007; Bishop, 2004; O’Shea and Awwad-afferty, 2009; Carlson and Briggs, 1990) (items 4 and 8 in Table III).

*Miscellaneous security strategies.* Apart from the strategies listed above, the literature lists several more concerns that require special attention from a facility manager. Implementing the following additional strategies may improve the security systems and procedures of a facility:
Employees and support staff should be trained for emergencies and in how to assist those who need help (FEMA, 2003a, b).

The security measures should be evaluated in a periodic manner, and emergency evacuation plans involving outgoing traffic of employees, visitors, and incoming traffic of emergency service vehicles should be assessed (FEMA, 2003a, b; Demkin, 2004; CPTED, 2005).

Personnel should be encouraged to be aware and conscious of suspicious activities, like vehicles going around the campus, persons taking photographs or videotaping the site activities, unattended packages left around the building and site perimeter, and information-seeking visitors. Also, employees should be encouraged to report suspected activities in a timely manner to a responsible person. At the same time, training has to be provided for custodial and maintenance staff for identifying and handling of suspicious packages found on campus (FEMA, 2003b; CPTED, 2005).

Critical issues that should be considered by facility managers

Based on the aforementioned discussion, the following is a list of topics that need the attention of a facility manager in order to provide safe and secured buildings:

(1) Site planning and building design:
   • issues associated with the impact of vehicular and pedestrian traffic in dense urban areas;
   • security of incoming utility systems to avoid unauthorized access;
   • vehicular and pedestrian traffic in the interior of a group of buildings within the campus;
   • critical areas of high occupancy, parking and utility areas, and special attention to the building envelope and to its perimeter areas;
   • potential areas of terror attack like straight roads, courtyards, re-entrant angles, recessed areas, parking areas, etc.; and
   • use of material and elements that could aggravate the impact of a terror attack.

(2) Security planning of the facility:
   • traffic circulation within the routes in the premises, leading to sensitive areas in the facilities;
   • maintenance and supervision of parking lots; and
   • maintenance of physical and psychological barriers, traffic calming devices, and other landscape based barriers.

(3) Building surveillance systems:
   • monitoring techniques of site and the building;
   • need to use different kinds of lighting systems during peak and non-peak hours and ensuring required illumination in areas like entrances, parking, utility, and vehicular roads; and
   • details provided on building signage to avoid unnecessary and uninspected access to sensitive areas.
Conclusions

One of the most crucial strategies suggested by the literature on the topic of design terror mitigation is to avoid and deter the terror attack before it reaches the main building. The first line of defense provides excellent opportunities to deter a terror attack. The second line of defense provides not only security to the core areas, but also holds potential for reducing damage due to such attacks. This paper resulted from a literature review study that was conducted from a point of view of a facility manager, as it identifies risks, presents literature recommendations, and suggests critical issues that the authors believe should be considered by facility managers in public accessed buildings.

This paper provides a list of 42 recommended items, based on an extensive review of literature, for four key areas of a facility: vehicular and pedestrian circulation, surface parking and perimeter, utility systems, and building and envelope. These four components of a facility represent various lines of defense suggested by previous research in the field of design terror mitigation. The first line of defense incorporates the areas between the boundary and the building, as represented in vehicular and pedestrian circulation, and surface parking and perimeter. The second line of defense is the building envelope and the perimeter areas, addressed by utility systems, and building and envelope. These four components are studied in terms of planning and design of the facility, security planning, and surveillance of the facility.

One of the most critical areas of a facility is the vehicular and pedestrian circulation that possesses potential for terrorist attacks because of the presence and the movement of vehicles and absence of restrictions. Explosive laden vehicle could be driven forcibly with intentions of ramming into the building and other occupied areas. Planning these areas with a security perspective, providing circulation routes with physical barriers to avoid forced entry, and categorizing and restricting certain circulation routes could effectively protect the facility from terror attacks.

Parking and perimeter zones are typically located in the vicinity of the main building, thus, they are prone to acts of terror. Surface parking areas must be segregated and located sufficiently away from occupied areas of the facility through the provision of standoff distance. Landscape design and site planning could be helpful in providing effective security by creating barriers in the form of interesting features of the site. The standoff between the site boundary and the building consists of the perimeter areas that need to be secured against terror attacks.

One prime target of terrorists is the utility system of a facility, which, if disrupted, could be more damaging to ongoing operations. A utility zone provides the opportunity to penetrate the building easily because of a low level of security and surveillance. Strategies like minimization of signage identifying critical utility areas, redundant utility systems, proper concealment of utility lines and increased surveillance could help provide a higher level of security to the facility.

The building envelope forms the second line of defense to the occupied areas of the building; as such, it must be designed carefully in order to minimize damage. Design of the envelope and selection of materials used in the envelope skin could control the impact of a terror attack on the building. The material must be placed along the building’s perimeter in such a way that it forms a cover to protect the building’s core areas.

This paper reviews and summarizes the literature available in the area of terror attack mitigation. It outlines potential risks, as well as a list of possible recommendations on how these risks can be effectively addressed. By concentrating
on the aspects that are relevant to facility managers of public buildings, this paper creates a rough draft which can be further developed in future and continuing studies. Although each building is significant and unique in terms of its characteristics, functions, and needs, it is still important that facility management teams be able to draw a security measures picture for the top decision makers.

References


BNIM Architects (2005), Security Design, Richard Bolling Federal Building First Impressions Project, BNIM Architects, Kansas City, MO.


Design terror mitigation


Lange, C., Decker, R., Wilson, P. and Chen, T. (2005), Smart Building Systems for Reducing the Vulnerability of Buildings to Chemical Biological and Radiological Attacks, The Institute of Infrastructure and Information Assurance, James Madison University, Harrisonburg, VA.

Lismore City Council (2000), Development Control Plan No. 43 – CPTED, Lismore City Council, Lismore.


NCDPI (2008), *Design of Schools to Resist Violent Attacks*, Division of School Support – School Planning, North Carolina Department of Public Instruction, Raleigh, NC.


**About the authors**

Sarel Lavy is a Faculty Member in the Department of Construction Science, which is one of four departments in the College of Architecture at Texas A&M University. He also serves as the
Associate Director of the CRS Center for Leadership and Management in the Design and Construction Industry. Dr Lavy graduated with a PhD degree in Civil and Environmental Engineering from the Technion – Israel Institute of Technology, and is a current member of the International Facility Management Association, the American Society of Civil Engineers, and the American Society for Engineering Education. Dr Lavy’s principal research interests are: facilities management in the healthcare and educational sectors, maintenance management, and performance and condition assessment of buildings. Sarel Lavy is the corresponding author and can be contacted at: slavy@arch.tamu.edu

Manish K. Dixit, LEED AP, M.Arch (Landscape Architecture), MSc (Construction Management) is currently enrolled for a PhD degree Program in Architecture at Texas A&M University. Mr Dixit has practiced for nine years as an Architect and Landscape Architect and worked on several residential, commercial and industrial projects in Central India. He has been associated, as a Guest Faculty, with institutions imparting undergraduate level education in Architecture in India for eight years. In addition, Mr Dixit is a LEED Accredited Professional and is a registered member of the Council of Architecture of India and the Indian Society of Landscape Architects.

To purchase reprints of this article please e-mail: reprints@emeraldinsight.com
Or visit our web site for further details: www.emeraldinsight.com/reprints