Journal of Infrastructure, Policy and Development (2019) Volume 3 Issue 1.
DOI: 10.24294/jipd.v3i1.1118

ORIGINAL ARTICLE

Enhancing building security for embassies along the Maritime Silk Road against terrorist attacks

Chun-Lin Liu[1*] and Jeslin Quek[2]

[1] *K&C Protective Technologies Pte. Ltd.*

[2] *Fyfe Asia Pte. Ltd.*

ABSTRACT

Embassies are important buildings, involving the diplomatic image of a country's government in another foreign country. Given the rising tensions between countries, either political, economic, religion or war, attacks on embassies have been increasing in recent years. Thus, it is evident that appropriate measures are to be taken to reduce the potential impact of an attack. The paper discusses the measures in enhancing building security of embassies. The principles for Security Planning and Design are discussed, followed by an introduction to a systematic security risk assessment framework. The framework is evaluated regarding the potential security risk posed by an attack against elements of the mega infrastructure using explosives. Further options to increase the security of embassies are also explored to reduce the risk of a potential attack. A security-enhanced building, planned and constructed well to specifications, can provide benefits to the client, including greater cost advantage and increase of value for the structure.

Keywords: *mega public infrastructure; security risk assessment; threat; vulnerability; terrorist attack*

1. Introduction

Since the 911 terrorist attack, numerous risk-assessment studies pertaining to attacks with explosives and cost-efficiency analyses related to the development of security strategies in reducing such risks have been carried out worldwide. Incidents of terrorist attacks on hotels and consulates in Pakistan are presented in **Table 1** and **Table 2**.

The beginning of global terrorist networks represents a challenge to diplomatic missions and international business. Traditionally conceptualized as a type of political risk in conflict areas, terrorism has evolved in recent years. The global terrorist networks that dominate the international scene today have different motivations, strategies and tactics than their secular and ethnic-separatist predecessors. This paper observes the incidents of terrorist attacks on hotels and consulates in Pakistan.

ARTICLE INFO
Received: March 5, 2019
Accepted: May 17, 2019
Available online: May 30, 2019

***CORRESPONDING AUTHOR**
Chun-Lin Liu,
K&C Protective Technologies Pte. Ltd.,
125A Lorong 2, Toa Payoh #02-132, Singapore 311125;
liu.chun.lin@kcpt.com.sg

CITATION
Liu C-L and Quek J (2019). "Enhancing building security for embassies along the Maritime Silk Road against terrorist attacks". Journal of Infrastructure, Policy and Development, 3(1): 115-128. doi: 10.24294/jipd.v3i1.1118.

1.1 Causes of attack

Pakistan has been a frontline state in the war on terror since the tragic events of September 11, 2001. Pakistan has lost thousands of lives since joining the war on terror in the form of both soldiers and civilians and is going through a critical period. However, many areas of Pakistan are becoming terror-free. Suicide bombs are commonplace in Pakistan, whereas they were unheard of prior to 9/11. The Taliban have been in the doldrums in recent years in Pakistan, but other small separatist groups are resurging.

The China-Pakistan Economic Corridor (CPEC) requires an attention for China's security concerns, especially those stemming from its restive western region of Xinjiang. Beijing has sought to clamp down on Xinjiang's ethnic Uighur community and has met political violence with an expanded security presence and the push for economic development schemes. These efforts implicate Pakistan because Uighur militant groups, such as the East Turkestan Islamic Movement (ETIM), have sought refuge in the Pakistan-Afghanistan border areas, where they have established links with al-Qaeda and the Taliban in Afghanistan and Pakistan. In addition, the Baloch Liberation Army (BLA) is an insurgent group engaging in a violent conflict with the Pakistani military forces for the "liberation" of Western Baluchistan province. China recognizes BLA and ETIM as persistent threats that are committed to targeting China and attacking Chinese interests inside Pakistan.

Date	**Hotel**	**Tactic**	**Casualties**	**Collateral damage**	**Asset Accessibility**
8th May, 2002	Sheraton, Karachi	Suicide bomber caused an explosion, destroying a Pakistan Navy bus outside the hotel	At least 14 killed, more than 20 injured	Beyond 1-km radius	Open access, unrestricted parking
20th Sep, 2008	Marriott, Islamabad	A truck bomber carrying about one ton of explosives blew the truck up at the gate	At least 53 killed 266 injured	2/3 of building caught fire	Open access, unrestricted parking
9th June, 2009	Pearl-Continental Hotel, Peshawar	Three terrorists forced their way into the parking lot and blew up an explosive-laden truck	At least 11 killed 55 injured	Partial collapse of hotel	Open access, unrestricted parking

Table 1. Selected terrorist attacks on international hotels in Pakistan since 2002 (Bonner, 2002; Gall, 2008; Khan & Masood, 2009)

Date	Hotel	Tactic	Casualties	Collateral damage	Asset Accessibility
14th June, 2002	US Consulate, Karachi	Suicide truck bomber detonated outside the consulate	At least 11 killed 50 injured	Part of consulate's perimeter wall destroyed	Restricted access
2nd March, 2006	US Consulate, Karachi	Suicide car bomb equipped with explosives crashed into diplomat's car	At least 4 killed 52 wounded	Burning cars and trucks	Open access at nearby hotel parking lot
2nd June, 2008	Danish Embassy, Islamabad	Suicide car bomb exploded outside embassy	6 killed, more than 20 injured	Significant structural damage to structure and nearby buildings	Restricted access
23rd Nov, 2018	Chinese Consulate, Karachi	Three heavily-armed suicide bombers attempted to infiltrate the consulate	4 killed	Terrorists unable to infiltrate; minimal damage	Restricted access

Table 2. Selected terrorist attacks on international consulates/embassy in Pakistan since 2002 (Khan & Vick, 2002; Naqvi, 2006; Perlez & Shah, 2008; Elmer, 2018)

2. Principles for Urban Security Planning and Design for embassies

The probability of attacks on embassies are on the rise and, thus, it is essential for Security Planning and Design to be reviewed and conducted regularly. The following principles play a major role in Security Planning and Design (Liu *et al*., 2012; Liu, 2018):

2.1 Access and connectivity

Secure places balance the need for access control with connectivity and circulation. Security can be compromised if the following scenario is/are present for an embassy:

- No power to control who can enter a development
- Numerous uncontrolled escape routes from an area are present
- Insufficient access for emergency vehicles
- Easy, anonymous access to targets, buildings and plots
- Conditions where pedestrian routes have poor lighting, are indirect and segregated from traffic

2.2 Structure and spatial layout

Risk and conflict are considered in the design of embassies. Security can be compromised if the following scenario is/are present:

- Unclear designated use of space
- The usage of the space is underused and rundown
- Assembly of Conflicting user groups in a same location
- Public spaces are unnoticed
- Areas of concealment and entrapment exist

- Places at risk of vehicle attack do not benefit from a stand-off

2.3 Ownership

Occupants and users will have a sense of ownership and responsibility in secured places. Security can be compromised if the following scenario is/are present:

- Inability to determine whether the space is public or private
- Private space is open to the public
- Limited common interest or supervision for a space
- Offenders unfearful of being seen or reported

2.4 Surveillance

Appropriate levels of surveillance will be present in secured embassies. Security can be compromised if the following scenario is/are present:

- Surveillance and privacy could not achieve a balance point
- The balance between surveillance and the need for shading is not achieved
- Offenders unfearful of being seen or reported
- There is limited natural surveillance of the public area
- Active surveillance systems are not installed at vulnerable areas
- Insufficient lighting

2.5 Physical security

Secure places are appropriately and proportionately protected. Security can be compromised if the following scenario is/are present:

- Physical security is not appropriate or proportionate to risks
- Physical security components does not serve usage
- In ability to achieve defense in depth
- No risks assessed when determining physical security needs

3. Risk assessment

With the concepts of Security Planning and Design in place, a risk assessment is then conducted. The authors incorporate qualitative and quantitative measures from the US Federal Emergency Management Agency's (FEMA) risk assessment model. The model comprises the evaluation of risk after factoring the threat, vulnerability and asset impact ratings. The process of the risk assessment is shown in **Figure 1** below (Liu *et al*., 2012; Liu, 2018).

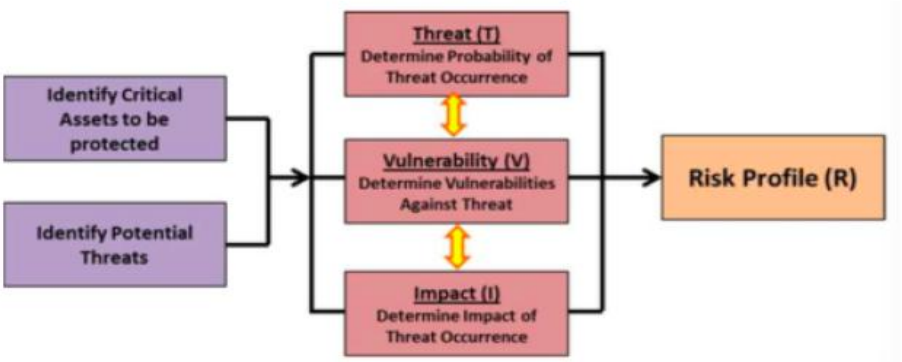

Figure 1. Process of risk assessment.

3.1 Identification of critical assets

Prioritizing and identifying an embassy's asset is important in order to distribute the required cost based on the greatest risk reduction. The assets are analyzed based on ranks in terms of redundancy and recovery plan, as shown in **Table 3**. As for embassies, critical assets may include legal documents, control rooms and vaults.

Ref No	Name of Asset	Description of Asset	Redundancy (Quantity & Readiness)	Recovery Plan (Repair/Replacement Cost & Time)
ASST01	Asset A	e.g. Production system...	e.g. 100% redundancy, but requires 2 hours lead time to fully activate.	e.g. $10,000-50,000/ $6 months
ASST02	Asset B	e.g. Emergency power supply	e.g. 1 no 2 cells on hot standby	e.g. < $200,000/ 3 months
ASST03	...	...	...	...

Table 3. Identification of critical assets

3.2 Identification of potential threats

Potential treats on an embassy will lead to damage and harm to the embassy and people. The main threat would be terrorist attacks, many of which are due to economic, religious or political reasons. Common attacks come from armed assailants, vehicle-borne improvised explosive devices (VBIED), unauthorized entry and improvised explosive devices (IED). Potential treats are assessed based on the following factors:

- Access to resources
- Knowledge/expertise
- History of threats
- Asset visibility/symbolism
- Asset accessibility
- Site population/capacity
- Collateral damage/distance to the building

3.3 Threat assessment

Threat assessment shall consider criminal threats and terrorist threats which the program may be exposed to for an embassy. The objective of conducting the threat assessment is to evaluate the

likelihood of occurrence of each threat. To determine the likelihood of occurrence of potential threats targeting the program, the following seven factors are assessed for each potential threat, with an overall score assigned to each parcel. The seven factors include: (a) Access to resources, (b) Knowledge/expertise, (c) History of threats, (d) Asset visibility/symbolism, (e) Asset accessibility, (f) Site population/capacity and (g) Collateral damage/distance to the building.

3.4 Vulnerability assessment

Vulnerability is defined as any weaknesses that can be exploited by an aggressor to make an asset susceptible to damage. A vulnerability assessment is prepared based on identified assets that can be affected by potential threats. A vulnerability assessment is an in-depth analysis of the functions of the key facilities/buildings, systems and site characteristics to identify the weaknesses, the sufficiency of existing security measures (baseline security measures), the lack of redundancy and the duration of operation recovery from an attack.

3.5 Impact assessment

Impact assessment is carried out to assess the consequences/impact of the probable occurrence of the various identified threats to the program. The assessment is based on factors including loss of life, injuries, loss or damage of key facilities/buildings within the parcels, loss of primary service (importance/duration), as well as impact on the economic, political and social well-being of the country/nation.

3.6 Parcel-wide risk assessment

Risk assessment is the process of defining and analyzing the dangers posed by potential threats to individuals, businesses, operations, industry and the country during various threat periods. Risk assessment consists of an objective evaluation of risk, in which assumptions and uncertainties are clearly considered and presented in this study. The primary complexity in risk assessment is that the measurement or evaluation of potential loss in terms of services and value, as well as the probability of occurrence of potential threats, can be very difficult to measure.

3.7 Risk profile

Risk is a function of threat assessment, vulnerability assessment and asset impact assessment. A total risk score is derived by multiplying the score assigned to the threat assessment, vulnerability assessment and asset impact assessment in accordance with the risk formula (Liu *et al*., 2012). The total score is then mapped into the table of quantitative risk profile/rating in Table 4, which is based on the likelihood of threat occurrence, the vulnerability of the facility against threats when they occur and the impact on the parcels after a threat occurrence.

Rating	Risk Level	Quantitative Risk Range
5	Very High	65 to 125
4	High	28 to 64
3	Medium	9 to 27
2	Low	2 to 8
1	Very Low	1 to 1

Table 4. Quantitative risk profile/rating table

We have included the results of the risk assessment, both before and after the implementation of a comprehensive Urban Security Planning and Design concept, which takes into consideration the following key elements:

- Environment – overall control of traffic and human movements
- Facility – city-wide smart perimeter security systems to monitor movements
- Human – the involvement of the community in security matters
- Engagement – reporting system on people entering the city and suspicious activities
- Operations – emergency planning and response to security situations

After a thorough understanding of the assessment, a Risk Rating for each asset against a specific threat is derived by multiplying the score assigned to threat assessment, vulnerability assessment and asset impact assessment in accordance with the risk formula:

$$Risk = T \times V \times I \tag{1}$$

where T = Threat Rating, V = Vulnerability Rating, and I = Asset Impact Rating.

4. Conceptual approach to Urban Security Planning and Design

With information on the expected risk, Urban Security Planning and Design is then conducted. Five concepts are commonly used to underpin the concept of Urban Security Planning at the Parcel and Development Level, as shown in **Figure 2.**

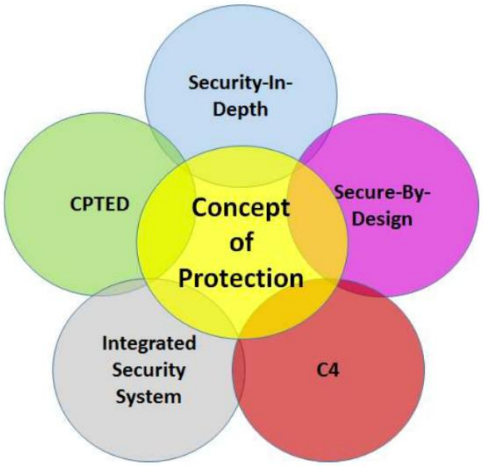

Figure 2. Model of concept of protection

4.1 Crime prevention through environmental design (CPTED)

CPTED is a security concept based on natural security strategies and environmental psychology. It benefits from traditional methods by having less cost. The fundamental strategies are territorial reinforcement, natural surveillance and natural access control.

Territoriality incorporates the use of physical design to create a sense of user ownership. The sense of ownership is felt by the users by designing an environment that defines personal or public space.

Natural surveillance encourages the design to ease visibility. For instance, placing the seats near windows improves vision on people entering the building. Installing more windows instead of walls gives outside information to the viewer.

Natural access control encourages the use of natural environment and landscape as barriers. Using natural access control for traffic calming, such as by planting trees close to the road edge, can provide a feel of road narrowing and thus making drivers reduce traffic speed (Prevatt, 1998).

4.2 Security in depth

Security is measured in layers, from the outermost layer to the protected asset. In order to reach the asset, the outer layers of security have to be breached. The separate zones also reflect the levels of security with increasing importance towards the deeper depths (Coole *et al*., 2012). **Figure 3** shows a diagram of the stages of security in depth.

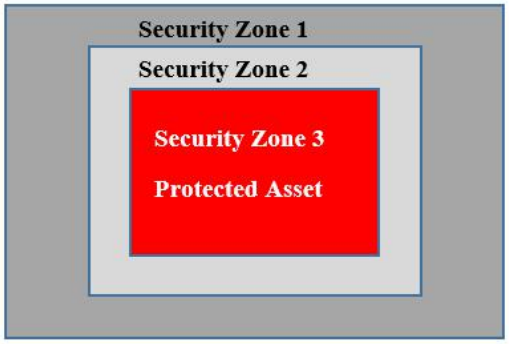

Figure 3. Stages of security in depth

4.3 Security by design

Security by design ensures that all security elements blend well with mechanical and electrical (M&E), civil, structural, geotechnical and architectural designs. With proper design at the early stage, the cost can be reduced from future retrofitting or additional changes after the building is completed.

4.4 Command, Control, Communication and Computer (C4)

C4 is an information system incorporating strategic and tactical systems. The functions are further explained below:

- Command: Functional exercise of authority to achieve a goal, such as enhancing security
- Control: Verifying the activity until the aim is achieved
- Communications: Achieving effective command by having the proper liaison implemented
- Computer: Connecting command, control and communication with newer technology and introduction of computer systems

4.5 Integrated security system

An integrated security system manages all physical and technological security aspects with a single graphical user interface. By combining CCTV, access control, intercoms, fire systems and all other related systems together, operations can be done more efficiently. The system leads to lower cost and reduction of manpower as all logs are automatically managed and recorded by the system.

5. Risk-mitigation measures

Risk mitigation is required to reduce the potential impact of an attack. Mitigation measures

may be achieved by technological, design or political measures. Appropriate measures should consider the cost factor of implemented measures, while achieving the required level of protection, in order to achieve a balance between cost and performance.

5.1 Retrofitting existing buildings to resist explosive threats

Existing buildings may often require retrofits for explosive threats based on changes in mission, occupancy or threat level. Conducting a threat, vulnerability and risk assessment is the first step in identifying the need to upgrade a conventionally designed building in order to protect its occupants and assets. This will identify the maximum credible threats and the associated hazards based on the site conditions, building layout, access control, structural framing and facade components.

The efficiency of the upgrades depends to a great extent on the structural details of the building, the aesthetics and functional impacts that may be tolerated. The cost of protective design and the impact of this protection on the structure may be minimized by using advanced analytical methods. These methods, developed over years of explosive testing and numerical simulations, enable the design team to focus resources on portions of the structure that most likely sustain damage and to minimize materials required to mitigate these hazards. The protective measures that may benefit most from these methods involve the designing of protective facade systems, the hardening of structures to resist the effects of progressive collapse and the retrofitting of existing structures.

5.2 Partnerships with stakeholders

Perhaps the most important step in countering the terrorist threat is to partner with stakeholders in both the government and the private sectors. Securing the perimeter in the areas where the threats are significant in number can be done by involving the law enforcement agencies and safety consultants in making the asset more resistant to attacks.

5.3 Building Information Modeling

Building Information Modeling (BIM) can be used as an integrative tool for building security. For example, interactive objects in 3D provide better understanding of vulnerabilities and better correlation with other design aspects such as building, site access, location, types of doors and windows, and structural design characteristics for blast- resistant design. BIM further enhances the integration among project team members, design disciplines and the various stages of a project in order to achieve the goal of a high-performance building. If properly maintained, BIM can provide complete, up-to-date information on the building and its systems throughout the building's service life.

5.4 Introduction of new security technologies

With the introduction of new technologies, damage from mob attacks can be reduced, while decreasing the need for local guard forces. One of the devices is known as the Long-Range Acoustic Device (LRAD). The device works by emitting directional high-energy waves to disperse the crowd. Using sound as a protection system reduces potential damage when compared to conventional methods, while effectively driving off unwanted crowds.

6. Risk-protection measures

Protective measures form the final component in the Security Protection Plan. The measures consist of four layers:

- Surrounding areas (1st layer of protection)
- Protection of the ground structures' perimeter (2nd layer of protection)
- Protection within the building compound (3rd layer of protection)
- Control of movements within the interior spaces and protection of critical assets (4th layer of protection)

6.1 Surrounding areas

Surrounding areas of the embassy refer to areas outside of the building perimeter. This is the first layer of protection which prevents further damage if successfully implemented.

The first layer mainly consists of proper monitoring and surveillance via Video Surveillance System (VSS). Electronic security systems, consisting of CCTV cameras linked to monitors, are closely observed by security officers at the Command Center. VSS functions to conduct and record surveillance of the focused ingress points in a sensitive region. For VSS to be effectively functional, proper lighting is essential. Strategic placement of lights can reduce the chances of criminal activities, while providing a better image for judgment. The basic level of lighting suggests that the human face be detected up to 10 meters in distance.

In operational terms, the security officer is responsible to report and detect any suspicious activity or personnel in the surrounding area. Should such events are found to be possible, the officer must conduct further investigation as a potential attack may occur. Regular patrol duties need to be conducted and unusual items or people recorded.

6.2 Protection of ground structures' perimeter

Barriers are a line of defense built along embassy property lines (Young, 2013). Vehicle barriers serve to prevent unauthorized vehicles from entering the building. Risks of Vehicle-Bourne Improvised Explosive Devices (VBIEDs) are common in recent years. These barriers have to be strategically located at least 30m away from an embassy building, based on Embassy Perimeter Improvement Concepts and Design Guidelines (US Department of State, 2011). This is to reduce the explosive forces from a vehicle blast to a minimal level.

The anti-ram barriers are designed based on a set of specific requirements and are given a crash rating. The barriers will then be designed based on the vehicle weight and speed of the attacker, as well as considerations of barrier penetration. Components of anti-ram barrier assessment are as shown below (US Department of State, 2011).:

- Identification of all potential vehicle approaches
- Determination of vehicle impact speed and angle of impact for each approach path
- Occupancy of adjacent properties
- Location of vehicle access points
- Availability of natural vehicle barriers
- Determination of potential setback distances
- Expectations for future site development

Aside from conventional K4-rated anti-ram barriers, other alternatives are also possible. The US Department of State's Bureau of Overseas Buildings Operations-Embassy Perimeter Improvement Concepts and Design Guidelines suggests other elements that can be used while presenting a better landscape for users. Hardened street furniture, retaining walls, integrated plant walls, decorative bollards, sculptural elements, moats and stabilized natural boulders serve as great alternatives.

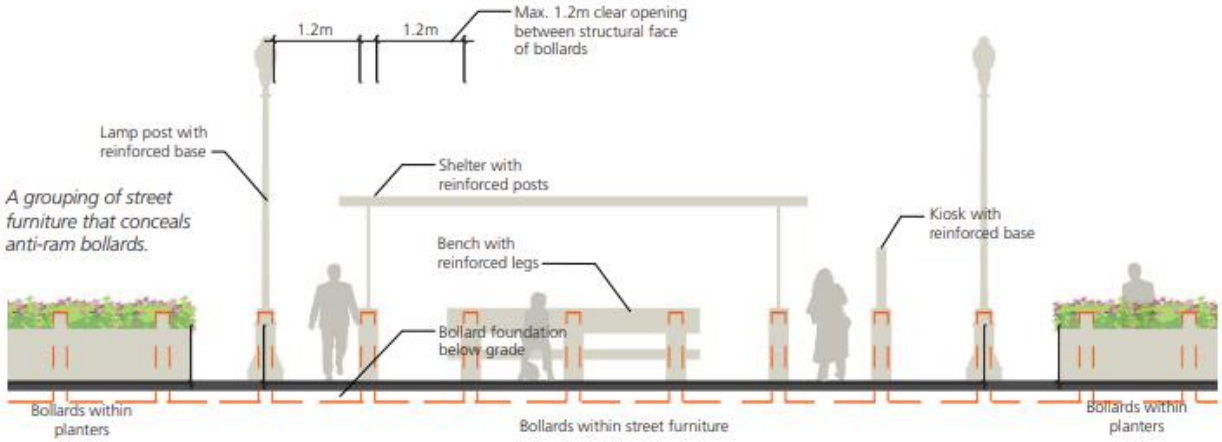

Figure 4. Furniture and posts with reinforced base serve as anti-ram barriers. (US Department of State, 2011)

Pedestrian barriers, on the other hand, prevent pedestrian intruders from entering the embassy. These barriers usually take the form of walls and fences. The walls and fences are designed based on requirements, such as whether to be opaque and to satisfy height requirements (US Department of State, 2011).

Aside from barriers, the protection of the guard house as the second layer of defense is also important. Several cases were documented whereby the security guard house was targeted by gunmen. In 1998, the US Embassy in Nairobi was targeted when terrorists triggered a bomb at the guard house after the guards refused to permit entry of the suspects. Structural hardening can be done to strengthen the structural integrity of the guard house against a blast. Blast-protected and bullet-proof windows should be installed for protection (Cooke, 2018).

Similar to the first layer of protection, perimeter areas should also be well equipped with proper surveillance systems. Intrusion detection systems such as step detectors and video motion detectors can assist in the detection of intruders. Step detectors alert the security officer when someone steps on the wall or places a ladder against it. Regular security patrol is required in the compound and around the parameter.

Every vehicle entering the embassy is made compulsory to undergo a thorough vehicle screening at the entrance of the internal driveway. An anti-crash barrier will be deployed to prevent forced entry of vehicles, facilitating the screening process. With the advancement in technologies, intelligent vehicle undercarriage scanners can be implemented to detect foreign objects and anomalies before vehicle entry.

6.3 Protection within building compound

Proper security monitoring, surveillance and patrol apply in the third layer of protection. As per the Secure Embassy Construction and Counterterrorism Act 1999, office facilities are required to be

constructed at least 100 feet from uncontrolled areas. This serves to protect the embassy from bomb blasts or other threats with the setback, as stated in "Diplomatic Security- Overseas Facilities May Face Greater Risks Due to Gaps in Security-Related Activities, Standards, and Policies" (United States Government Accountability Office, 2014). The standard also necessitates the use of blast-resistant construction techniques and materials. Examples of materials include reinforced concrete, steel and blast-resistant windows.

The proper positioning of car parks is required to minimize the potential risks of terrorism. Car parks should be located far from highly populated areas and critical assets such as the utility mains and the control room. Parking under the building or at access nearby should be avoided; if unavoidable, however, the hardening of the building against a blast should be done. The management of traffic flow and traffic queue is also an element to be considered when deciding the car park's location as stated in Guidelines for Enhancing Building Security in Singapore (Singapore Ministry of Home Affairs, 2005; 2010; 2018).

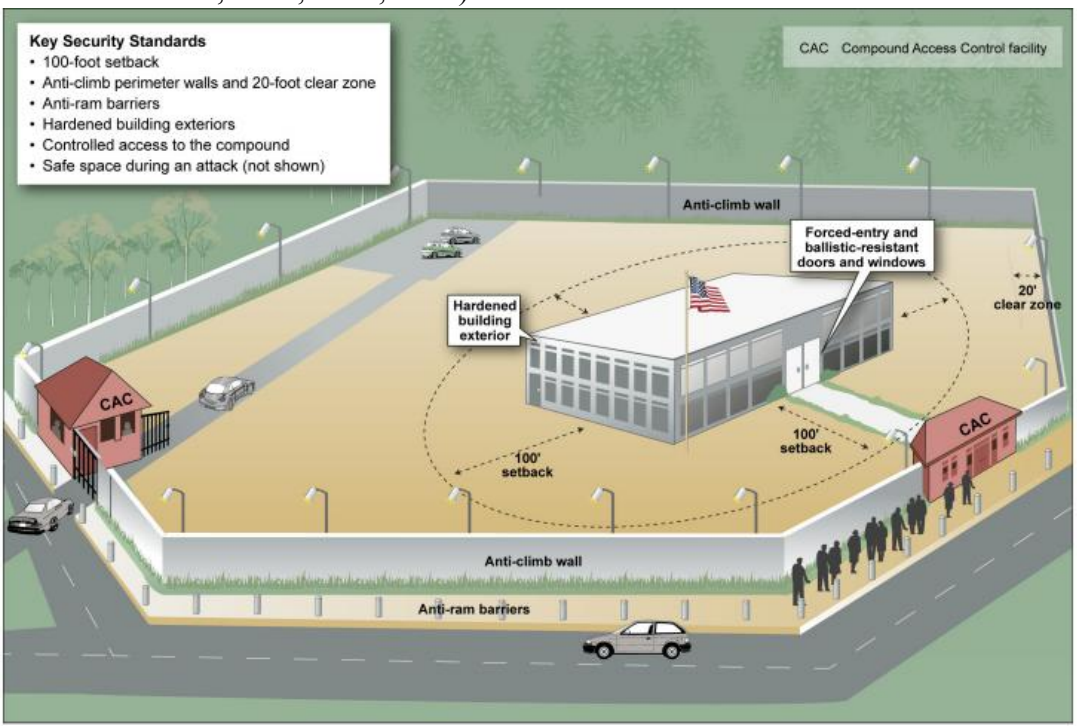

Figure 5. Key security measures at a notional embassy. (United States Government Accountability Office, 2014)

6.4 Control of movements within interior spaces and protection of critical assets

Access control of personnel from semi-restricted areas to restricted areas is required for the protection of the embassy. The CCTV coverage of the interior of buildings shall ensure the field of view for visual identification of personnel at fire escape staircase doors, lobbies, corridors, access doors to restricted and secured rooms, access to critical assets, M&E room access doors and office access doors.

Electronic access control systems (EACS), including card readers and electromagnetic locks, prevent the intrusion of unauthorized personnel by permitting authenticated-only entry for legitimate personnel in possession of valid access card. The principles of implementing an electronic access control system are in accordance to the security zoning demarcation. Access points (doors) from semi-restricted zone to restricted zone are secured by EACS.

Intrusion detection sensor and alarm systems can be used for intrusion detection. Among relevant examples are the Video Content Analytics (VCA) and Intrusion Detection System (IDS). Video Content Analytics are video motion detectors that detect movement on video signals transmitted from CCTV cameras. It allows early detection when intruders enter the restricted area. Intrusion Detection System in the form of magnetic contact (MC) or electromagnetic locking system, coupled with magnetic contact installed on doors, will trigger an intrusion alert if there is a forced entry. It will activate an alarm in the intrusion detection monitoring system at the Command Center. Security personnel will be alerted by the IDS alarm in the intrusion detection monitoring system to provide necessary response immediately.

7. Advantages

Typically, in our experience, incorporating Urban Security Planning and Design at the very beginning of the development of the program can result in the following advantages and benefits:

- Greater attractiveness to investors: Due to the increasing safety and security concerns globally, a world-class Urban Security Planning and Design of the program will make it more attractive to investors.
- Cost savings: Proper Urban Security Planning and Design can result in an overall reduction in security by design cost. For example, for a mega development with total developed land 1,084 km^2, the cost saving of security by design can be around 5%–7% of the total value of the development, which is $12.5bil–$17.5bil out of the mega development's total development value of $250bil.
- Increases development value: The program can command a premium for its mega development.

8. Conclusion

This paper further refines the threat ratings and assessment criteria and proposes a new security risk assessment methodology. The assessment result provides a more reliable and scientific reference for facility owners regarding the necessity of building resistance analysis and strengthening. A case analysis validates the security risk assessment methodology. Based on the security risk assessment criteria, facility owners and policymakers can quickly decide on whether a building requires protection and identify the threats that are of high risk and cause big losses from all the threats that the building is up against.

Acknowledgments

The authors would like to thank PhD student Hasan Saeed from the Department of Civil, Chemical, Environmental and Material Engineering, University of Bologna, for reviewing and providing his opinion on this paper.

References

Bonner R (2002). *At Least 14 Die in Attack on French Group in Pakistan* [online]. New York, USA; The New York Times. May 9, 2002. Accessed on: Jan 30, 2019. Available from: https://www.nytimes.com/2002/05/09/world/at-least-14-die-in-attack-on-french-group-in-pakistan.html

Cooke C (2018). *Remembering the 1998 Embassy Bombings* [online]. Washington, DC, USA: US Department of State. Aug 3, 2018. Accessed on: Jan 30, 2019. Available from: https://www.state.gov/m/ds/rls/284888.htm.

Coole M, Corkill J and Woodward A (2012). *Defense in Depth, Protection in Depth and Security in Depth: A Comparative Analysis Towards a Common Usage Language. Australian Security and Intelligence Conference.* Perth, Australia: SRI Security Research Institute, Edith Cowan University. https://doi.org/10.4225/75/57a034ccac5cd.

Ekmer K (2018). *7 killed in attack on Chinese consulate in Karachi claimed by local terrorist group*[online]. Hong Kong; South China Morning Post Publishers. Nov 23, 2018. Accessed on: Jan 28, 2019. Available from: https://www.scmp.com/news/asia/south-asia/article/2174655/gunmen-police-exchange-fire-near-chinese-consulate-pakistans

Gall C (2008). *Bombing at Hotel in Pakistan Kills at Least 53* [online]. New York, USA; The New York Times. May 9, 2002. Accessed on: Jan 30, 2019. Available from: https://www.nytimes.com/2008/09/22/world/asia/22islamabad.html

Khan I and Masood S (2009). *Militants Strike Hotel in Pakistan, Killing 11* [online]. New York, USA; The New York Times. June 9, 2009. Accessed on: Jan 28, 2019. Available from: https://www.nytimes.com/2009/06/10/world/asia/10peshawar.html

Khan K and Vick K (2002). *Bomber Hits U.S. Consulate in Karachi.* [online]. Washington USA: The Washington Post, June 15, 2002. Accessed on: Jan 28, 2019. Available from: https://www.washingtonpost.com/archive/politics/2002/06/15/bomber-hits-us-consulate-in-karachi/fc0ee347-591d-4b05-b40b-99139fafd1f7/?noredirect=on&utm_term=.1c3121b3e02d

Liu C (2018). *An Introduction to Urban Security Planning and Design.* 7th International Conference on Protection of Structures against Hazards. Hanoi, Vietnam, 29–31 Oct, 2018.

Liu C, Tan C-K, Fang Y-S and Lok T-S (2012). The Security Risk Assessment Methodology. *Procedia Engineering*, 43: 600–609. https://doi.org/10.1016/j.proeng.2012.08.106.

Navqi SM (2006). *Pakistan blasts kill U.S. diplomat* [online]. Georgia USA: Cable News Network, March 2, 2006. Accessed on: Jan 28, 2019. Available from: http://edition.cnn.com/2006/WORLD/asiapcf/03/01/karachi.blast/

Perlez J & Shah PZ (2008). *Embassy Attack in Pakistan Kills at Least 6.* [online]. New York, USA; The New York Times. June 3, 2008. Accessed on: Jan 28, 2019. Available from: https://www.nytimes.com/2008/06/03/world/asia/03pakistan.html

Prevatt JS (1998). *Crime Prevention Through Environmental Design (CPTED) and the Role of Facilities Planning in Force Protection.* Monterey, CA, USA: Naval Postgraduate School.

Singapore Ministry of Home Affairs (2005). *Enhancing Building Security.* Singapore: Ministry of Home Affairs.

Singapore Ministry of Home Affairs (2010). *Guidelines for Enhancing Building Security in Singapore (GEBSS).* Singapore: Ministry of Home Affairs.

Singapore Ministry of Home Affairs (2018). *Guidelines for Enhancing Building Security in Singapore.* Singapore: Ministry of Home Affairs.

US Department of State (2011). *Embassy Perimeter Improvement Concepts and Design Guidelines.* Washington, DC, USA: US Department of State, Bureau of Overseas Buildings Operations.

United States Government Accountability Office (2014). *Diplomatic Security- Overseas Facilities May Face Greater Risks Due to Gaps in Security-Related Activities, Standards, and Policies.* Washington, United States Government Accountability Office.

Young W (2013). *Embassy Security: From The Outside In.* Santa Monica, CA, USA: RAND Corporation.