FM ENCORE

1st Quarter 2019

SAFETY & SECURITY

PROTECTING PUBLIC VENUES

FROM VEHICLE RAMMING ATTACKS WITH CPTED

By Randy Atlas Ph.D. FAIA, CPP, and Steve M. Crimando, CHPP

Public venues are attractive magnets for people activity, and a very inviting location for acts of crime and terrorism. Public venues, regardless of form or shape, are considered in the security arena as soft targets, because they are so difficult and costly to secure and protect. There are many approaches to protecting public venues, and one of the most reasonable and reliable among these are the concept of crime prevention through environmental design, or CPTED.

Crime Prevention Through Environmental Design (CPTED) is defined as a multi-disciplinary approach for reducing crime through urban and environmental design, and the management and use of built environments. CPTED strategies aim to reduce victimization, deter offender decisions that precede criminal acts, and build a sense of community among inhabitants, so they can gain territorial control of areas and reduce opportunities for crime, and the fear of crime.

Since motor vehicles are so commonplace, and people are generally comfortable around them, it can be difficult to fully appreciate the incredibly destructive nature of vehicle ramming attacks and their capacity for creating mass casualty events. Vehicles have also been used by attackers to breach security around buildings with locked gates, and then initiating bombing or shooting incidents. These tactics are not new and date back to the early 1970's.

Although vehicle ramming attacks represent only a small fraction of the overall number of casualties from terrorist attacks worldwide, the ease of execution combined with the difficulty in detecting or deterring such attack, has made this attack method very effective and easy to implement. Attacks on large public gatherings and venues, using weapons as common and accessible as cars and trucks, can have a very chilling effect on the legitimate user population. The goal for the terrorist is to create a climate of fear and distrust, and when every car or truck on the street can potentially be used as a weapon the constant and pervasive fear that ensues aligns well with the terrorist's agenda.

Architects worry about the fortress mentality of security professionals while security professionals are concerned about the failure of architects to include security elements in the design of buildings from the ground up to protect against these kinds of threats and vulnerabilities. The conflict is not over whether to include security equipment in the building design; rather the conflict lies between a building's openness on the one hand and the reasonable control of access to it on the other.

Making a building secure, when it was not originally designed to be secure, is an expensive proposition. Architects have to sacrifice much more of a building's openness in retrofitting for security than would be the case had the building been designed for security from the outset. Protection and operating expenses are greater than they need to be because of a lack of forethought during the design of a facility. This condition is particularly evident in many of today's buildings, where modern design and materials can result in facilities and infrastructure that are especially vulnerable.

The commission of an offense is the result of a multistage decision process that seeks out and identifies, within the general environment, a target or victim positioned in space and time. The environment emits many signals or cues about its physical, spatial, cultural, legal, and psychological characteristics.

An individual motivated to commit a crime or act of terror uses cues learned from experience and observed in the environment to locate and identify victims and targets. CPTED is a crime-environment theory based on the proposition that the appropriate design and application of the built and surrounding environment can improve the quality of life by deterring crime and reducing the fear of crime. Security and crime prevention practitioners should have a thorough understanding of CPTED concepts and applications in order to work more effectively with local crime prevention officers, security professionals, building design authorities, architects and design professionals, and others when designing new or renovating existing buildings.

PRACTICAL REALITIES

Theory holds, then, that altering the conditions that provide the opportunities for criminal behavior can curb crime. While this may be eminently sensible, great financial resources are required to alter the conditions. After a building has been constructed and put into use, the anticipated cost of physically changing it tends to overwhelm the anticipated benefits of crime reduction.

Even in new construction projects, owners and investors are reluctant to commit the extra funds required to incorporate the physical features called for in the crime prevention through environmental design theory.

Reluctance to design for security is related to more than dollars. Modern buildings strive to attain openness and free-flowing movement. Design ideas that constrain and restrict are not on the agendas of the owners and not in the minds of the architects. Security features are often seen as obtrusive and lacking in aesthetical value. It seems to not matter that the world is an increasingly less safe place to work and live. For a building to be made truly crime-resistant, security considerations must be in the architectural drawings from the very beginning. The drawings should reflect a comprehensive security perspective, one that takes into account the interrelationships between electronic security equipment, security officer services, and, most importantly, the routine and exceptional activities of the users of the building.

A combination of both active and passive defense measures may be necessary to mitigate vehicle ramming attacks risk, but necessarily prevent attempts at vehicular attacks. Passive measures include installing barriers, bollards, and buffers that would prevent a crowd strike, whether purposeful or accidental. These include passive and operable barriers such as rigid fencing that is properly anchored; other vehicles that are loaded with sand or stone to provide a flexible yet substantial barrier that can be quickly deployed as needed; stationary barriers such as walls, permanent bollards and other CPTED landscaped features; movable barriers such as the infamous Jersey Barriers or heavy anchored planters; operable barriers such as wedges or beam barricades, electrical, or hydraulic bollards.

Active measures are most effective when used in concert with passive measures. Active measures involve technical surveillance of high-risk areas by a combination of commercial, public, and police video surveillance sources, along with direct security guard stations and observation. The goal is to create situational awareness necessary to detect any useful indicators of a vehicular attack. This is accomplished by reconnaissance of potential target areas, and rehearsals of threat activities. The surveillance becomes critical to the identification of the suspect, crime scene reconstruction, and determination and defensibility of police response, and providing meaningful forensic evidence in the prosecution of the perpetrator.

Proper preparation by law enforcement and property management includes focusing on when the peak times the greatest number of people will be gathered; having awareness of sections of roadway where the driver can build up speed before veering into a crowd or building facade; the locations of bollards and barriers that afford victims few routes of escape; and choke points that will allow passage of their vehicle but cause panicked flight and potentially stampedes of persons trying to escape.

In addition to the loss of life and property, consequences that can flow from an improperly designed electronic system, there is the prospect of being held liable, both criminally and civilly. The governmental agencies that hold regulatory authority in matters affecting public safety are increasingly under pressure from society, generally to seek criminal prosecution when violations result in death or injury. Next, the extremely litigious nature of the security industry poses great potential loss in terms of compensatory and punitive awards and loss of reputation. A property owner or manager who makes security-sensitive design decisions without the input of a competent security professional is taking on a very large risk.

SECURITY AS A DESIGN REQUIREMENT

Architects and designers can make the greatest contribution to meeting a project's security objectives. Architects generally make the basic design decisions about circulation, access, building materials, fenestration, and many other features that can support or thwart overall security aims.

Building clients and design professionals are not the only ones concerned about security during the design process. Many jurisdictions require a security review by police as part of the building permit approval process, much the same as with fire safety requirements. Inspectors evaluate the plans for obvious spots where assaults, mugging, break-ins, and other crimes of opportunity may exist. Many jurisdictions have security ordinances that require certain lighting levels, and secure door and window designs and hardware.

All federal government buildings must comply with the GSA Security Standards from 1995, and relates the many security classifications of government buildings. If security is treated as one of the many design requirements, then the implementation and costs for such measures will be no more a burden to the project owners than fire safety features or landscaping requirements. The basic premise of security design is that proper design and effective use of the built environment can lead to a reduction in the incidence and fear of crime, and to an increase in the quality of life. The environmental design approach to security recognizes the space's designated or redesignated use -- which defines the crime problem – and develops a solution compatible with that use. Good security design enhances the effective use of the space at the same time it prevents crime.

The emphasis in security design falls on the design and use of space, a practice that deviates from the traditional. The traditional approach focuses on denying access to a crime target through physical or artificial barriers, such as locks, alarms, fences, and gates. This approach tends to overlook opportunities for natural access control and surveillance. Sometimes, the natural and normal uses of the environment can replace or work in harmony with mechanical hardening and surveillance techniques. An intelligent use of the environment will present three basic strategies: access control, surveillance, and territorial reinforcement.

ACCESS CONTROL This strategy embraces the tried and true custom of utilizing security guard forces, and the less understood and infrequently applied strategy of making use of terrain and spatial characteristics and natural circulation patterns. Mechanical safeguards, such as, locks and card key systems, can augment access control. The central objectives of an access control strategy are to deny access to a crime target and to create in the mind of the criminal a belief that an attack on the target will present personal risk.

SURVEILLANCE. A strategy based on surveillance is directed at detecting intrusion attempts, keeping an intruder under observation, and launching a response to an intrusion or an attempt at intrusion. A surveillance strategy can take advantage of terrain features, such as landscaping; building features, such as raised entrances; organized methods, such as patrolling; and electronic supplements, such as closed-circuit television.

TERRITORIAL REINFORCEMENT. The thrust of this strategy is that physical design can create or extend the sphere of influence naturally exercised by the users of the territory. The idea is that an individual's sense of proprietorship concerning a place of work or domicile can be enhanced and extended by conscious individual action and by cooperating with others in a variety of crime-suppressing activities.

THE ARCHITECT IS THE KEY

The architect is the key to opening the opportunities inherent in the crime prevention through environmental design approach (CPTED). The architect is the essential element in creating a structure that will work in tandem with the various CPTED strategies. However, to be effective in this regard, architect must be skilled in three areas:

DETERMINING REQUIREMENTS. Security needs must be determined early in the project's programming and problem-defining stage. The design team should analyze the designated purpose of how the space or building will be used. The designated purpose will be clear when designers examine the cultural, legal, and physical definitions of what the prescribed, desired, and acceptable behaviors are for that space. The space can then be designed to support desired behaviors and the intended function of the space. The design team should inquire about existing policies and practices, so that this information will be integrated in the programming process.

KNOWING THE TECHNOLOGY. Rapid and substantial advances in the technology of security systems make keeping up-to-date a challenge. Many construction projects, even those that may be seen as routine, will require the services of an architect knowledgeable in security principles and applications. An important competency is to understand and bring into existence the expressed needs of the security professionals representing a building's owner or manager. Within this competency is the ability to know when an expressed security need cannot be filled by a particular design idea and how to lead the security professional to an alternate idea. Construction management, usually for reasons of economy, will sometimes invite an electronic security system vendor to act as an unpaid security consultant in matters involving major design decisions. The problem in such an arrangement is that the vendor's expertise will be in manufacturing and selling a product, not in providing an unbiased consulting service. The vendor's design recommendations are likely to reflect what will be best for the vendor in the short term without regard for the building occupants in the long term. Experience has shown this to be a primary reason underlying the poor performance of electronic security systems. This is not to say that vendors should be excluded from contributing to the design, only that the design team for practicality and efficiency should critically examine their contributed ideas. Good sense dictates that all ideas, irrespective of source, be looked at from every perspective. The architect's best contribution to a project may be in providing a constructively critical analysis of security design concepts.

UNDERSTANDING THE IMPLICATIONS. Designs must integrate the complicated and sometimes conflicting goals of security and safety. The tendency to want to lock out the undesirables can create serious safety drawbacks in situations that require quick and unhampered egress. Space and function are variables hat must also be brought into balance with security objectives.

Security and safety needs can be integrated in a five-stage approach. First is the problem statement, which explores the users' needs and leads to the development of functional requirements. Second is developing the scope of work from the problem statement, client expectations, and staff available. This stage should lead to a signed contract. Third is the design and documentation of the building and systems. It is at this stage that most architects go through schematic design, design development, and construction documents. Stage four is the administration and supervision of construction, and stage five involves acceptance testing, training, and setting up the building for occupancy.

Randy Atlas, Ph.D. FAIA, CPP is president of Atlas Safety & Security Design Inc., and Steve M. Crimando CHPP, is a principal in Behavioral Science Applications.