Designing For Homeland Security (6/22/04)

By Randy Atlas Ph.D., AIA, C.P.P. Counter Terror Design Inc.

Terrorism represents a real threat for our society and to our peace of mind. The attacks on the World trade Center and the Pentagon, the Oklahoma City bombing, the World Trade Center Bombing, the firebombing in the New York subway, the toxic gas attack in Japan’s subway, the derailment of the Amtrak Train in the Arizona desert, are now forever etched as terrorism landmarks in our memory. However, the face of terrorism is undergoing systemic changes as the level of terrorist sophistication increases with the availability of knowledge and materials to carry out these acts of violence.

Access. Knowledge about bombs and terror has proliferated to a point that virtually any terrorist or criminal can easily acquire the information to build anything from a pipe bomb to a nuclear bomb, or develop killer toxins to carry out their particular transgressions. Timothy McVeigh, who blew up the Oklahoma City Courthouse, stated in an interview shortly after his arrest, that he picked the courthouse because ‘it was more architecturally vulnerable”. Who would have thought that a rental truck and a load of manure could be so deadly? What can the public and government agencies do to be effective in diminishing the threats and losses to persons, information, and property? How do you reduce the opportunity for and fear of crime in the built environment and improve the quality of life? The answer: Crime Prevention Through Environmental Design (CPTED).

This article addresses how to reduce the threats and vulnerabilities in the built environment by changing how we design and use space.

The targets of terrorism in the future will be cities, utility companies, government buildings or agencies, technology companies, and high profile corporate entities. New Technology has made the infrastructure of America more vulnerable to sabotage, especially disruption of communications and information systems, which have the same net result as a bomb going off.

On September 11, 2001 it took but a few moments to breach the airport security systems, and shatter America's confidence in "flying the friendly skies." The 9/11 Tragedy was the combined failure of intelligence (information, and at least four attempts to deny access of the hijackers into the United States by U.S. Customs), the failure of security systems and protocol, and the failure to properly train security personnel. The airport security systems, overseen by the Federal Aviation Authority and the security industry, have ignored years of known and obvious defects. How could passengers pass through security screening, X-ray equipment, ID checks and then breach the cockpit doors otherwise? The terrorists did not need to beat the airport security system, but rather took advantage of the system as it existed. These individuals probably watched screeners and tested the security to see what they could get away with. Flight protocol called for pilots to cooperate with hijackers if the lives of passengers or crew were at stake. That might have allowed terrorists to gain easy entry to the cockpit, and do something that none of the pilots expected: fly the jets, and then deliberately crash them. What ended in horrific acts of terror started with ordinary breaches of security and street level crime.

Increased security from this point forward will be expensive, inconvenient, and time consuming. For example, the cockpit doors were designed to be broken relatively easy in the event of an accident. At the present however, pilots see the doors as the last line of defense, and must be strengthened to protect the flight crew.

On a recent flight to Australia, I observed the flight attendants had blocked the isles with the food carts to prevent persons from moving between the class sections and gaining access to the cockpit. On another flight I was forced to take off my shoes to go through weapon screening barefoot. No system can prevent all breaches, but a comprehensive and consistent approach will empower the security systems ability to catch potential criminals and terrorists with much greater certainty. The federal government has taken control over the thousands of airport screeners where they will be given background checks, drug tested, and presented with a consistent level of training. However, the effort is extremely labor intensive and focuses on only screening passengers of commercial airlines and their luggage. Cargo holds of planes, small private airports and planes, and shipping companies like Fe Ex and UPS are not screened to the same rigid standards. The approach is still not consistent or comprehensive. The focus is on grandmothers with tweezers and scissors, not dangerous cargo or chemicals in the belly of a jet.

Persons watching the horror live on TV were surprised and shocked that the World Trade Center buildings collapsed. The Towers, built in 1972-73 were 110 stories tall, and experienced progressive collapses similar to that caused by an explosion to the Murrah Federal Building in Oklahoma in 1995. The two plane crashes into the Towers destroyed columns and floors on several stories, which transferred excessive loads to the remaining structural columns. Explosions and raging fire weakened the remaining columns, which were already overloaded. The original design had provided for the structural strength to withstand a Boeing 707, which is a smaller plane with a much lower fuel capacity than the planes used on September 11th. The design of the Towers was substantial enough to withstand the impact of the jets without toppling instantly. Even with huge gaping holes, the remaining columns were strong enough to hold up the structure long enough for 20,000 people to escape. The jet fuel released a much higher heat than paper or plastic burning, which might be the contents of a normal office fire. Fire suppression systems in the Towers did not include foam sprinklers that could deal with the jet fuel fires. Both of the crashed jets were fully fueled for transcontinental flights, literally making them “flying bombs”.

Fireproofed steel loses half its strength when it reaches 1100 degrees F, and fails rapidly after 1600 degrees F. The temperatures inside the building were estimated to be over 2000 degrees. The steel columns, weakened by fire, finally buckled, and the floors they supported dropped on top of each other in a “pan caking” action. Each falling floor overburdened the columns and floor below, causing the buildings to tear themselves down (Architectural Record. October, 2001. Pp. 24-26). Designers agree that few structures short of a missile silo, no matter what their height, can endure such aggressive attacks.

Environmental design might not have been able to prevent to tragic events of September 11, but the design of our public and private space does relate to safety and security through planning for: crowd behavior in high-density environments; way finding and design of escape routes; placement and type of building security features; design for high risk environments; and effective design of the built environment providing the building users with less stress, less confusion, and less opportunity to be a victim of a crime. (Environmental Design Technical Group News, September 2001)

With all of the catastrophic effects of terrorism in the past, and the huge potential for damage in the future, acts of terrorism are relatively infrequent. The overall damage of these horrific acts of terror to society is less than loss of life and property from ordinary street crime. The societal damage from guns and drugs far exceeds the damage from any bomb, yet the perceived threat is much greater from terrorism than say robbery or mugging.

Changes. As the roles of the security designer and the architect are redefined for the 21st century, the first step in designing against crime and terrorism is to assess the threats and vulnerabilities. The initial step is to evaluate the tangible and intangible assets that are to be protected. Usually the assets of our buildings are (PIP), PEOPLE (users and employees), INFORMATION, and PROPERTY. The threats are the potential for losses of the assets. The vulnerabilities are the weaknesses, shortcomings, or perception of risk of attack by the actuality of crime or terrorism.

The question arises is there really a difference designing against terrorism or designing against crime and workplace violence? What is the chance or likelihood that our private or public sector buildings would be victims of an act of terrorism? The perceived level of threat is much greater than the actuality, seeing as the incidence of terrorism in the United States is still extremely low. The probability of becoming a victim of a robbery, burglary, auto theft, assault, or murder has already affected how most of us live our lives on a day-to-day basis so what effect will the threat of terrorism produce?

An example of increased awareness is the threat of workplace violence. Workplace violence is closely related to terrorism in its level of predictability. Yet, with all of the assaults at the post office, or office buildings, the frequency is increasing at an alarming rate. The threat is just waiting for an opportunity to surface with the next job termination or downsizing. Bombings are one of the most traditional ways to commit acts of terrorism. Knowing the tools of the terrorist helps identify where security needs to be strengthened. Acts of terrorism can also manifest themselves in arson, skyjacking, kidnapping, assassination, hostage taking, armed assaults, and bio-chemical attacks (Security Watch, Bureau of Business Practice. Newsletter, Oct. 2001, p.4)

The threat of terrorism is more marketable for social change than ordinary street crime. For decades efforts have been made to have a national security code, or security ordinances as part of state or national building codes. Sadly these efforts have fallen on deaf ears. Efforts to have criminals serve their actual sentence, or truth in sentencing, has collapsed under the weight of prison overcrowding and construction and budget moratoriums. Terrorism has been the vehicle for change, in an otherwise stuck universe of crime prevention. For example, President Clinton in June of 1995 mandated basic standards of security for all federal facilities. The mandate states that each federal building shall be upgraded to the minimum, security standards recommended for its audited security level by the Department of Justice. President Bush in November 2001 signed a bill federalizing airport security screeners and anti-terrorism legislation that empowers law enforcement and the military to take preventative actions.

Prior to the U.S. Marshals Service conducting a vulnerability assessment, there were no government-enforced standards for security at federal buildings. The Marshals Service building security study developed 52 standards, primarily covering perimeter security, entry security, interior security, and security technology planning. Each federal building was rated within the five levels, with level I being minimum security and level V being a defense plant or nuclear facility. Most courthouses with multi-tenant, multi-story buildings are considered level IV and require shatter resistant glass, controlled parking, 24 hour CCTV monitoring and videotaping, x-ray weapon and package screening, and a photo identification system.

Pursuant to basic minimum, security standards being ultimately important, the federal government has now established a minimum standard of care for federal buildings. In the private sector, the American Society of testing materials Premise's Liability Committee was disbanded by lobbying pressures for developing minimum, security guidelines for multi-tenant residential housing environments. Presently, there is an effort to resurrect the effort with the National Fire Protection Association. The NFPA regulates fire protection and life safety requirements and security is definitely considered part of a life safety issue.

The threat of premises liability litigation is what has driven the major organizations from Hotel and Motels Associations, shopping center associations, retail store association, and builder associations to try and block all efforts of developing minimum standards. A legal and physical benchmark puts essentially, all of corporate America on notice to make their buildings safe against crime, not just safe against the remote occurrence of fire. Insurance companies are strongly supporting standards they can measure a business against, and reduce their losses to have less payout. The auto industry created the momentum for reduction of auto theft by redesigning locking systems, installation of alarm systems, improved driver training, and redesign of car stereos to resist theft (removable faceplates). Responsible car owners now realize discounts in their premiums because of the inclusion of security features and minimum standards.

Planning. Designing without security in mind can lead to lawsuits, injuries, and expensive retrofitting with protection equipment, and the need for additional security personnel. If not properly planned for and installed, that equipment can distort important building design functions, add to security personnel costs, and result in exposed unsightly alarm systems or blocked doors and windows.

Treating security as an afterthought increases the cost and obtrusiveness of security features when construction is completed. Whether the threat is from terrorism or street crime, or workplace violence, the increased threat of premises liability litigation will be the strongest driving elements for change. Where common sense fails, and building codes obscure, where management executives overlook, the slap of premises liability is driving building owners and managers to make the necessary safety and security improvements. Large judgments are striking fear into the hearts of building owners and managers as much as any act of terrorism.

The media covered the recent acts of terrorism for weeks with unrelenting enthusiasm. The personal dramas of terrorist attacks unfolded piece by piece. However, the secretary raped in a school, or the nurse attacked in a hospital parking lot barely makes the back page of the local section of the paper. The commonness and greater frequency of murder, rape, assault, and robbery is only newsworthy if someone famous is involved, or the crime is particularly heinous. The numbness to the high frequency of street crime does not motivate our politicians, insurance companies, building and zoning officials, or design professionals to make change or improve the quality of life. The actuality is that terrorism is much more marketable for the media to motivate politicians to create change in the security field, develop standards, and make changes in our physical environment to resist criminal behavior.

CPTED is the effective use and design of the built environment to reduce the opportunity and fear of predatory stranger-to-stranger crime. CPTED uses a multi-tiered approach to increase the effort needed to commit the crime, to increase the risks of being detected while committing a crime, to reduce the rewards for committing the crime, and to remove the excuses for inappropriate behavior. The strategies for achieving these goals include using natural access-control, natural surveillance, legitimate activity support, management and maintenance strategies, and territorial boundaries. Adequate security planning, CPTED, and defensible space planning are parts of the comprehensive security planning process as compared to a target-hardening or fortressing reaction to criminal incidents.

Can Crime Prevention Through Environmental Design (CPTED) make a difference in preventing acts of terrorism? Absolutely. CPTED emphasizes problem seeking before rushing into problem solving. CPTED starts with the threat and vulnerability analysis to determine the weakness and potential for attack. Attack from criminal behavior, or attack from terrorist activity only reflects a change in the level and types of threats. The process and challenges are the same. CPTED and Defensible Space planning are a planning process, as compared to fortressing or target hardening. When designing against crime, workplace violence, or terrorism the security consultant must resist the rush for quick answers.

What the CPTED process does is ask the questions about:

1) access control; choosing who and how people get onto your property and into your building;

2) natural surveillance; the ability to see without obstruction who are the legitimate and illegitimate users of the defined space;

3) territorial reinforcement; the ability to define the boundaries of what is public and what is private space, and the layers in between in order to create and encourage a sense of ownership and protectiveness by the legitimate users.

4) maintenance; Is the building maintained and service in a way that encourages legitimate behavior and keeps the spaces clean and used the way as designed and designated.

5) management strategies: Are there assigned and capable guardians that watch out and enforce the groundrules of legitimate behavior for that designated and defined function or purpose of hat building or space.

6) Legitimate activity support: Does the built environment support the kinds of activities and behaviors that the space or building was designed for and operated for?

The CPTED process provides a holistic methodology to meet the challenges of crime and terrorism with organizational methods (people - security staff, capable guardians), mechanical methods (technology- hardware, barriers, hardening), and natural design methods (architecture, design and circulation movement flow).

For example, if one of the outcomes of a threat analysis for a government building is the challenge of a truck bomb, and the goal is to distance a potential bomb from the building, then the CPTED approach would propose careful consideration of:

* Where is the parking placed?

* How does service delivery get screened and controlled?

* How do pedestrians flow into the building?

* How many entrances are there for the public, staff, and service?

* Is there one main entrance for the public?

* How much distance is the exterior path of travel from the street , pedestrian plaza, to the building facade?

* Do all four facades have setbacks from the street?

* What is the most appropriate bollard system or vehicular barrier system?

* Does bollards or planters create blind spots or sleeping places for homeless persons and street criminals?

* Does the threat exist from bicycles and motorcycles bombers, thus requiring a smaller net?

* Does surveillance from the building to the street remain unobstructed?

* Does landscaping and plantings remain unobstructed?

* Do barriers hinder accessibility by persons with disabilities?

* Where do private or public security forces patrol?

* Are security patrol patterns unobstructed and verified with a guardtour system?

* Is the structure of the building designed with structural redundancy?

* Does the building become a less appealing target by layers of buffer zones that make it more difficult for an intruder to reach the intended target?

* Has the structural components been designed to allow the decompression effects of an explosion?

* Are the window systems designed to protect against the threat of broken glass by using window film Mylar coatings, blast curtains, or blast resistant glazing materials?

* Does lighting around the property provide a uniform level of light to resist shadows or hiding places?

* Is there CCTV in places of extra ordinary activity to detect inappropriate behavior and record and monitor that activity?

* Does the building have a consistent and comprehensive weapon screening program for the building users, staff, and packages and mail?

* Does the property use security layering to create a sense of boundary of the property(site), the building, and specific points within the building?

* Does management and maintenance practices and policies support security operations , the use of security staff, monitoring devices, weapon screening procedures for people and property, screening of employees backgrounds, and physical upkeep of the premises?

The CPTED process and security threat assessment process would look at the following high risk targets:

- Engineering and back up power/ utility systems
- Mechanical, Ventilation and water treatment systems
- Communications systems including the computer facilities
- Supply and storage areas, including loading and receiving docks , warehouses, volatile substances or materials storage.
- Transportation facilities that include rail, bus, train, seaports, and airports.
- Human targets which can include political figures or CEO's, or casual observers to impact collateral damage such as school children or shoppers.
- Government, military facilities, chemical plants, explosives or volatile materials.

Summary. It is self evident that a lot of thought and money goes into making a building secure. However, an architect nor security director cannot change human nature, and a lot of criminal acts will be perpetrated in spite of the best-laid plans. Our built environment cannot be defended against every potential threat. No building security system could have prevented the act of terrorism of September11, or the bombing of our embassies, or courthouses. But there are many active steps that can be taken to reduce the opportunities and fears of crime and increase our awareness of the threats. Our goal is to design safe buildings that protect our assets of people, information, and property.

Security systems come in many varieties, but crime is not yet monolithic. Furthermore, it is ironic that the kind of crime that most people fear is not the kind that occurs most frequently. Stranger to stranger crimes--assault, murder, rape and robbery--are less common than white-collar crime. In fact, most criminals don't tote a gun. The terrorism of the 21st century will probably not be bombings, but industrial espionage, computer pilfering and destruction of records, as well as biological and chemical terrorism. The greatest threat to us on a day-to-day basis is from workplace violence and street crime. Designing against the threats of crime and workplace violence is going to greatly reduce the likelihood of acts of terrorism. It is all about controlling access and basic CPTED principles. Even terrorists have to make our buildings and assets accessible to carry out their crimes.

Architecture is unfortunately one of the least used pieces of the security puzzle to make public and private buildings safe and secure. CPTED and Defensible Space planning create the environment for better security by allowing natural surveillance and unobstructed visibility, controlling access to persons who belong on the property, preventing unauthorized access of persons onto the property, integrating the security technology into functional design and architecture, and allowing the legitimate building users to be your capable guardians for legitimate activity and deterrence of criminal activity.

Finally, environmental design can never eliminate crime completely because it does not attack root causes. Architectural security design may only be responsible for shifting the places where crime occurs. Yet, environmental control does go a long way toward making people feel better about their work and living environment, and that empowers people to act in a safer manor.

Architects and security professionals should avoid worry over events that they have no control over. Save your worry for that which you can control: good design, integrated security systems, competent training and staff, and keeping a watchful eye on your workplaces, living environments and residences.

REFERENCES

Architectural Record. October 2001. Pp. 24-26

Atlas, Randall. “Just when you thought it was safe to go back in the building.” Security Management, August 1998

Crowe, Tim. Crime Prevention Through Environmental Design 2nd edition Boston: Butterworth - Heinman, 2000.

Environmental Design Technical Group News, EDRA. September 2001.

Newman, Oscar. Defensible Space: Crime Prevention Through Urban Design. New York: MacMillan , 1973.

Security Watch, Bureau of Business Practice Newsletter, Oct. 2001, p.4

Werkerle, Gerda and Whitzman, Carolyn. Safe Cities: Guidelines for Planning, Design and Management. New York: Van Norstrand, 1995.

BIO: RANDALL I. ATLAS Ph.D.,AIA,CPP

Randall Atlas is President of Counter Terror Design Inc., and vice-president of Atlas Safety & Security Design Inc., in Miami , Florida. He is a registered architect in Florida and national accreditation with N.C.A.R.B., a certified protection professional (CPP) from the American Society of Industrial Security, and member of the ASIS Security Architecture and Engineering Committee, and received his doctorate of criminology from Florida State University. Dr. Atlas is a nationally recognized trainer and author on Crime Prevention Through Environmental Design (CPTED) for the National Crime Prevention Institute, the American Society of Industrial Security, and the American Institute of Architects. Dr. Atlas has been appointed to the Oklahoma City National Memorial Institute of the Prevention of Terrorism peer review panel. Dr. Atlas is a technical assistance consultant for HUD and has conducted CPTED surveys for housing projects around the country. He is a regular contributor to the Protection of Assets Manual, Access Control Magazine, Security Technology Magazine, and Security Management Magazine. For more information go to http://www.cpted-security.com or http://www.counterterrordesign.com

(BREAK OUT BOXES)

ISSUES THAT THE ARCHITECT SHOULD ADDRESS WITH THE SECURITY CONSULTANT

Site Planning

- Access

- Service delivery

- Circulation patterns

- Lighting quality and quantity

- Perimeter defense

Main Lobby

- Visitor control issues

- Building fire system location

- Reception/guard kiosk design and equipment provisions

- Architectural security barrier design--turnstiles, glass enclosures, reception areas, etc.

- Retail tenant security adjacent to lobby areas

- Development of unobtrusive CCTV surveillance

- Controlling access into emergency stairwells adjacent to the main lobby

- After-hours access control into the main lobby

- Alarm monitoring of perimeter doors

- Main lobby lighting

Parking Garage

- Valet or self parking

- Public, private, or mixed use

- Segregated parking levels

- Executive parking security

- Need for and use of CCTV surveillance system, emergency signaling system, intercom system, and guard tour system

- Lighting issues, including type of lighting and number of footcandles to be provided

Loading Docks

- Amount of vehicular traffic flow expected

- Impact, if any, on street traffic or pedestrian walkways

- Storage of package and materials

- Distribution of deliveries throughout the building

- Development of necessary CCTV surveillance and intercom systems

- Provision of remote door release controls

Emergency Stairwells

- Restricting access or allowing use by the public for interfloor traffic

- Communication provisions in stairwells

- Emergency exit alarm devices on doors

- Alarm monitoring of the stairwells

- Access control into and out of the stairwells

Miscellaneous

- Elevator bank access control and architectural design

- Communication provisions in elevator vestibules on individual floors

- Public washrooms

- Mail services

- Deliveries

- Security in mechanical areas

- Door hardware for telephone, electrical, and storage closets

- Security for fuel and water storage areas

- Roof access

- Tunnel or skyway connections to other nearby buildings

- Plaza security--issues related to landscaping, lighting, and use of unobtrusive surveillance systems

- Elevator cab communication devices

Building Tenant Security

- A comprehensive access control program to encompass elevator car access control requirements and individual floor access control measures

- Security measures for individual departments and operations that may have additional security requirements

- Executive floor security

- Receptionist workstations

- Boardroom or executive conference room access control issues

- Vestibule construction of freight elevator lobbies

- Console room design

- Secured storage areas, vaults, and safes within tenant space

- Closet space for security-related equipment

- HVAC and power requirements for security operations

Major Systems

- Fire and life safety

- Public address

- CCTV surveillance

- Access control

- Alarm monitoring

- Radio communication

- Emergency signaling

- Intercom

- Guard tour

- Door control

- Uninterruptible power supply

CPTED DESIGN GUIDELINES

- Place unsafe activities in safe areas where there is natural surveillance and supervision

- Design the exterior of a structure so it is hard to climb

- Minimize the number of exterior openings at or below grade

- Protect all building openings against entry or attack

- Provide for extra conduit for growth and changes

- Design walls to resist penetration by intruders possibly using cars, hand tools, explosion, etc.

- Provide sufficient space in the lobby or entry areas for verification, identification, and screening of users, i.e. sign-in desks, contraband detection equipment such as X-ray machines, and personal identification equipment.

- Provide adequate space for maintaining security equipment.

- Protect all utilities and control panels from disruption by unauthorized persons.

- Design elevators, stairways, and automated locking mechanisms not to compromise security during emergency evacuations.

- Design lighting for proper illumination in coordination with CCTV--reduce glare, increase view of field.

- Design perimeter to be well defined and supported by natural barriers such as landscaping, mechanical barriers such as walls, fences, buried sensors, motion sensors, proximity sensors, and by organizational methods such as guard patrol.