

A Guide for Law Enforcement

**Conducting CPTED Risk Audits for Anti-terror
Infrastructure Protection**

By

**Gregory Saville
University of New Haven**

For

**The Police Executive Research Forum
1120 Connecticut Avenue, NW, Suite 930
Washington, DC 20036**

November 11, 2003

A Guide for Law Enforcement

Conducing CPTED Risk Audits for Anti-terror Infrastructure Protection

**Gregory Saville
University of New Haven**

Security and anti-terror protection protocols recommend that it is important to put into place a Critical Infrastructure Protection Plan in order to be prepared for major emergencies and terror attacks. The plan typically incorporates a section on threat warnings, response procedures, and assorted roles and responsibilities. These are mitigation strategies and they outline how to coordinate the response of agencies during and after a terror attack. The plan also incorporates the preventive and proactive measures an agency can take to improve the survivability of critical assets. Those are called remediation strategies.

There is a range of services available to law enforcement officials regarding incidents of terrorism. They include new technologies for mapping potential terror crime targets, methods for expanding partnerships for first responders, and conducting risk audits by identifying key individuals who may be involved in terrorist activities. This guide takes another approach by directing efforts toward protecting key infrastructure resources through the use of a CPTED risk audit.

The objective of this guide is to provide an outline for conducting Crime Prevention Through Environmental Design (CPTED) audits of critical infrastructures within your jurisdiction. The method recommended in this guide is compiled from an assortment of other CPTED evaluation and audit methods, however here it is specifically tailored to critical infrastructure for anti-terror prevention. This guide also suggests a process for implementing the audits and hereafter uses the generic term “auditors” to refer to the security and police personnel, facility managers, and other prevention practitioners who will implement this audit.

A preparedness plan should not be considered complete on the completion of a risk audit. Audits provide only one remediation strategy that can contribute to an overall Critical Infrastructure Protection Plan.

The guide is designed for use as a practical, hands-on manual. It is broken into four parts:

- ❑ Part 1 provides an overview of critical infrastructure protection as it relates to the problem of terrorism
- ❑ Part 2 introduces various versions of crime prevention through environmental design, more specifically 1st Generation CPTED, situational crime prevention, and 2nd Generation CPTED.

- ❑ Part 3 introduces the CPTED Risk Audit methodology. It shows how law enforcement officials can apply the Risk Audit for the protection of key infrastructure assets in each municipality.
- ❑ Part 4 lists resources. The final section is particularly useful for those agencies preparing, or updating, a Critical Infrastructure Protection Plan.

INTRODUCTION TO THE PROBLEM

It is important to recognize the reality of terrorism. As stated by a recent publication of the Office of Community Oriented Policing Services of the Department of Justice (COPS Office):

*The vast majority of communities will never directly experience a terrorist event. However, it is critical that public safety officials work to prevent the possibility of such an event taking place, as well as plan should such an unlikely event occur.*¹

In contrast to this reality is the fact that, while local places may have low risks of terror attack, the complexity of global affairs makes even the most remote community interconnected to global events. This reality was highlighted in papers presented to the Joint Economic Committee, Congress of the United States.

*Social, economic and environmental problems are worsening in many parts of the world. And diffuse and asymmetrical nuclear, biological, chemical, cyber and terrorist threats are emerging at the same time that distinctions between what is domestic and what is foreign are blurring.*²

This guide provides a strategy for assessing some of the critical infrastructure risks due to terrorism within any jurisdiction. There is already a range of services available to law enforcement officials regarding terrorism³. They include new technologies for mapping potential terror crime targets, methods for expanding partnerships for first responders, and identifying key individuals who may be involved in terrorist activities. This guide takes another approach by using the latest thinking in crime prevention through environmental design to protect key physical infrastructure resources.

¹ Chapman, Robert et al. *Local Law Enforcement Responds to Terrorism: Lessons in Prevention and Preparedness. COPS Innovations*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing, 2002. Pp. 20. It is available on-line at www.cops.usdoj.gov

² Oslund, Jack. "National Security: The Definitions Landscape." In the 107th Congress, 2nd Session, Joint Committee Print, *Security in the Information Age; New Challenges, New Strategies*. Compendium of Papers Submitted to the Joint Economic Committee of the Congress of the United States. May, 2002. This is available at the U.S. Government Printing Office, www.bookstore.gpo.gov.

³ A good description of many of those resources is included in Chapman, et al cited above.

Focusing on physical assets and property protection does not imply that protection against personal victimization is unimportant. To the contrary, there are already excellent resources available for assessing interpersonal risk and some are listed in part four of this guide.

In addition, there is also a hidden benefit from the crime prevention concept known as the diffusion of benefits. Because this guide aims to help local officials enhance the safety of key assets, it is equally likely that any attack deterred at one of these sites will most certainly save lives in and around that facility. This will indirectly benefit the community in a number of ways beyond protecting the physical asset.

Finally, unlike other anti-terror publications in recent years, this guide deals exclusively with prevention, not first response nor investigation. For those topics there are a host of other resources, some of which are cited in part 4.

PART 1 – CRITICAL INFRASTRUCTURE AND TERRORISM

Why preparedness?

Is it possible to prepare adequately for terror attacks? There is obvious benefit to assembling the important agencies to coordinate responses during the first critical moments of an attack. Indeed, most emergency plans dedicate a significant portion of their content to responses. But how does preparation for response compare with preventing the event?

Unlike prevention of crime, prevention of terror events is relatively new. Even the definition of terrorism is unclear. For example, the U.S. Department of State indicates there is no universally agreed upon definition. The Federal Bureau of Investigation uses the following definition:

The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives⁴.

That does not indicate whether the terror is domestic or international. Neither does it clarify the differences between violence against persons and destruction of property. Therefore, it is important to specify the scope of this document; this guide deals with destruction of property, specifically critical infrastructure, through either domestic or international terrorism.

As for prevention, do protective measures provide complete protection against terrorism? That is unlikely. But it is likely that such measures can reduce the impact of a potential

⁴ Jane's Information Group. *Jane's Facility Security Handbook*, Alexandria, Virginia: Jane's Information Group: June, 2000. p.6. For more information on the Jane's Information Group contact: info@janes.com or Phone 703-683-3700.

threat. They can also provide opportunities for the apprehension of terror suspects prior to the event.

Do protective measures displace risks?

In crime prevention the answer is, “not necessarily” (Hesserling, 1996). In a majority of cases displacement is rarely one for one, and often the overall harm is reduced. In terrorism there is no research to know with certainty. It seems probable that dedicated and resourceful terrorists can switch targets. But it is very likely that strengthening infrastructures and potential displacement targets throughout a jurisdiction can minimize the potential harm.

What are critical infrastructures?

In recent years there has been a growing list of what is considered a critical infrastructure⁵. This guide varies from others in a few important ways. It deals only with physical asset protection from destruction or disruption⁶. These comprise local infrastructures identified in the National Strategy for The Physical Protection of Critical Infrastructure and Key Assets published by the White House (2003). These assets include:

1. Agriculture and food
2. Water, including Dams
3. Public Health
4. Emergency services
5. Defense industrial base
6. Telecommunications and information systems (computers)
7. Energy, including nuclear power plants
8. Transportation
9. Banking and finance
10. Chemical industry and hazardous materials
11. Postal and shipping
12. Government facilities
13. Commercial key assets
14. National monuments and icons

Focusing on physical assets and property protection does not imply that protection against personal victimization is unimportant. To the contrary, there are already excellent resources available for assessing interpersonal risk and they are listed in part three of this guide.

⁵ Motleff, John et al. Critical Infrastructures: What Makes an Infrastructure Critical? *Report for Congress*. Washington, DC: Congressional Research Service. August, 2002.

⁶ In addition to the destruction of infrastructures during terrorist incidents, there is equally important harm that might be caused by the disruption of services. Disruption of service can have serious consequences, as evidenced by the massive eastern seaboard blackout in the summer of 2003 when 50 million people went without power.

Examples of critical infrastructures include terror targets that affect both property and persons. This was the case in the domestic terrorism event at the Murrah Federal Building in Oklahoma City. Further, terrorists can disrupt critical infrastructures while targeting the people who use them. This was the case of the sarin nerve agent used by domestic terrorists in the Tokyo subway attack in 1995, or the anthrax attacks on postal stations and government offices by unknown assailants in the U.S.

Specific examples

In each jurisdiction these infrastructures will be different. What follows is a guideline for the kinds of structures that represent each of the infrastructures:

Agriculture and food	Food distribution centers and processing plants
Water, including Dams	Sources of water supply systems such as dams, reservoirs, holding facilities, water cleaning and treatment plants; mechanisms that provide for civilian and commercial water delivery such as pumping stations.
Public Health	Hospitals; medical laboratories
Emergency services	Police and fire stations; emergency coordination and control centers
Defense industrial base	Military bases; armory's
Telecommunications and information systems	Computer facilities supporting any of the other critical infrastructures; television and other communications transmitting and receiving stations
Energy, including nuclear power plants	Generating stations; power transforming facilities; processing and storage facilities for gas and oil
Transportation	Airports; bus and train stations; bridges and tunnels
Banking and finance	Major commercial and banking facilities; exchange boards and trading houses
Chemical industry and hazardous materials	Chemical production, processing and storage facilities; biological medical and research laboratories; explosives and weapons production, storage, and sales facilities
Postal and shipping	Postal offices; shipping and container facilities
Government facilities	Government offices
Commercial key assets	Major commercial production facilities such as mines and factories
National monuments and icons	Major national monuments such as historic sites

Do we know what kind of attacks terrorists will use?

There is no way to be certain. Terrorists can modify tactics as easily as targets. However, based on past experience, we can categorize potential attacks into the following general topics.

- Assassination
- Armed assault
- Bombings
- Arson
- Hijacking
- Hostage-taking

Kidnapping
Product contamination
Cyber-terrorism
Weapons of mass destruction (WMD)⁷

These categories are not exhaustive, nor are they mutually exclusive. For example, in the 9/11 attacks, terrorists combined aircraft hijacking and used planes as bombs. Obviously, it is crucial that intelligence services provide law enforcement with adequate information regarding the potential kinds of attacks terrorists might use so they can be incorporated into risk audits.

For the purpose of infrastructure protection only the following are used below:

1. Bombings (including “dirty bombs”)
2. Arsons
3. Product contamination and
4. WMD.

The other forms of attack pertain directly to violence against persons, not property.

In addition, WMD pertain here primarily to biological or chemical weapons. Due to the overwhelming destructiveness of even low yield nuclear weapons, it is doubtful that any current form of CPTED is an appropriate strategy for prevention. However, some CPTED strategies may help in an indirect way, such as speeding up the identification of suspicious activities and items.

PART 2: CPTED – AN EVOLVING CRIME PREVENTION IDEA

Crime prevention is often thought of as the intersection of three different pathways, each with strengths and weaknesses. The first is motive reduction. That deals with the underlying motives that lead people to commit crime: social conditions, poverty, and as in many terrorist acts, politics.

Another pathway is the legal and justice system. Law enforcement and the presence of security are examples.

The third pathway is opportunity reduction. That is the place and time where the actual criminal act takes place. This is where CPTED emerges.

CPTED is an acronym for a well-established crime prevention program called Crime Prevention Through Environmental Design. Criminologist C. Ray Jeffery wrote a book

⁷ Jane’s Information Group. *Jane’s Facility Security Handbook*, Alexandria, Virginia: Jane’s Information Group: June, 2000. p.20-29. There is no way to know all possible terrorist methods as they continually change. This list provides only an overview.

using the term CPTED (pronounced sep-ted) in the early 1970s. CPTED is also attributed to architect Oscar Newman from his 1972 book *Defensible Space*. Newman showed how opportunities for crime in public places could be minimized through the proper design of the physical environment.

First Generation CPTED: Physical protection

CPTED works by bringing people together in common purpose to take ownership of an area. This will help to let offenders know they cannot act with impunity. This is called a sense of territoriality of a place. It increases the risk, and the perception of risk, that offenders will be caught or prevented from committing their intended illegal act. There are four basic strategies that accomplish that task:

- ❑ Natural surveillance;
- ❑ Access control;
- ❑ Territorial reinforcement; and
- ❑ Image⁸.

The prevention specialist, urban designer, or architect can apply each of these strategies in a number of different ways to reduce crime opportunities. For example, natural surveillance can be achieved in convenience stores by clearing away the advertising on store windows, enhancing the lighting, and placing the cash register in a clear visible location. Robbery suspects are less likely to rob stores with impunity knowing their chance of being seen by passers-by and police patrols in stores where these strategies have been used.

This early version of CPTED, now called 1st Generation CPTED, specifically deals with opportunity reduction. From the 1970s and 1980s it was taught to law enforcement and crime prevention officers across the country. Today, many municipalities use at least a few different forms of 1st Generation CPTED in their planning, such as proper lighting and beautification programs.

The four basic strategies are applied in the following ways:

Natural surveillance

Natural surveillance increases visibility of legitimate property owners and residents. It uses design features to increase the visibility of a property or building. Many potential criminals are unlikely to attempt a crime if they are at risk of being seen.

Natural surveillance happens in many ways, for example by positioning windows towards outside activity areas. The landscaper encourages natural surveillance through proper trimming and placement of trees and shrubs. The facility manager encourages it through

⁸ Saville, Gregory. Urban design and community-building for preventing crime. In Corina Brito and Tracy Allen (Eds.), *Problem-Oriented Policing: Crime-Specific Problems, Critical Issues and Making POP Work – Volume II*, Washington, DC: Police Executive Research Forum. 1999.

good lighting⁹. In the case of infrastructure protection, lighting for clear visibility and good color rendition, as with metal halide lighting, is preferable to the yellowish sodium lighting used for non-security, functional purposes, such as roadway lighting.

There is a difference between the natural surveillance described above, and other forms of mechanical (CCTV) and organized (patrols) surveillance. Natural surveillance provides a permanent, and non-intrusive, method for keeping watch of an area. Mechanical and organized forms may be necessary, such as in underground parking lots. However, they are considered after first examining opportunities for natural surveillance.

Access control

Access control restricts access into and out of properties through the use of a limited number of entranceways to buildings and neighborhoods. It places entranceways in areas where legitimate users of the space can easily monitor who enters and exits. It decreases opportunities for criminal activity by denying criminals easy access to potential targets.

Access controls include using cement jersey barriers on properties and roads adjacent to critical infrastructures. This can help keep potential car bombers away from vulnerable locations. They also include internal controls such as securing doors to mail rooms, computer rooms, elevator controls and boiler rooms when not in use. All these areas are particularly sensitive to terrorist attack.

Access controls have a long history in CPTED and have had many successes. For example, robbery offenders are less likely to rob stores with impunity knowing their ease of escape is limited and there are greater chances of being seen by passers-by or police. This strategy, as well as better management and requirements for clear sightlines, was successfully applied in Florida and is now part of the Florida Safe Streets Act¹⁰.

Territoriality

Designing a place with territorial “markers” (such as signs) shows it belongs to a person or group. This can be an effective method to help distinguish a property between anonymous public versus private space. This is also known as the hierarchy of space. It is the difference between the public street, where offenders can easily travel unnoticed, and the private space where they cannot. Creating semi-public and semi-private spaces helps send a message of “ownership” to would-be offenders¹¹.

⁹ Atkins, S., S. Husain, and A. Storey. The Influence of Street Lighting on Crime and Fear of Crime, *Crime Prevention Unit Paper* 28. London: Home Office. 1991.

¹⁰ This was first documented in Florida. See: Duffala, Dennis. “Convenience Stores, Armed Robbery, and Physical Environmental Features”. In *American Behavioural Scientist*, Vol. 21:495-97. 1976. For more recent research see Bellamy, L. “Situational Crime Prevention and Convenience Store Robbery”. In *Security Journal*. Vol. 7 (1), pp. 41-52, April 1996.

¹¹ MacDonald, J.E. and R. Gifford. Territorial cues and defensible space theory: the burglar’s point of view. *Journal of Environmental Psychology*. 9:193-205. 1990

For example, landscapers can install outdoor planters, low walls and fences, and decorative gateways to demarcate semi-private areas at a critical infrastructure such the front property of an office. This can encourage employees to take note of visitors walking in that front area and report it to security.

Territoriality can also be used to demarcate different parking areas for employees and visitors. Anyone entering the employee parking area is more likely identified. Marking clear territorial zones can also be used to keep parking at least 300 feet away from vulnerable locations in case of car explosions.

Image

A well maintained home, building, or property demonstrates that someone cares and could be watching. This will reinforce the territorial influence that legitimate users and owners have over that place, and that can deter the crime opportunities for offenders¹². A positive image can also be enhanced by clean-up campaigns and proper building maintenance. Well-maintained lawns and elimination of any graffiti or broken windows on commercial buildings can also enhance image.

One limitation to 1st Generation CPTED is that it was only applied to street crimes such as robbery and burglary and it uses primarily architecture to reduce opportunities.

That has now been expanded in two significant ways. Situational crime prevention, championed by Professor Ronald Clarke, adds significantly to the repertoire of 1st Generation CPTED. Many, in fact, now consider CPTED to be a component of the situational approach. Additionally, 1st Generation CPTED has been expanded into what is now called 2nd Generation CPTED.

Situational Crime Prevention

Situational crime prevention tackles many forms of crime opportunity, not simply those found in physical places. Situational prevention uses a variety of different strategies to reduce crime, three of which are selected for use here:

1. Increase the criminals effort to commit crime
2. Increase the risks the criminal will be caught
3. Reduce the rewards criminals get from crime

¹² For two recent studies on this see: Cousins, L. Ethnographic Windows on Urban Disorders, in *Journal of Contemporary Ethnography*. Vol. 27 (2), pp. 278-284, July 1998, and; Smith, M. Assessing Vandalism Cues in an Experimental Setting: A Factorial Design Involving State of Repair, Presence of Graffiti, Target Vulnerability, and Target Suitability, in *Dissertation Abstracts International, A: The Humanities and Social Sciences*. Vol. 57 (4), pp. 1857-1859, Oct. 1996.

The unique contribution of situational prevention is that it still uses opportunity reduction. However, it goes beyond the strategies of architecture and planning. It is applied in the following ways:

Increase the effort needed to commit crime

Target hardening includes using physical barriers like special locks or shielded doors. Strategies include spot welding door hinges to prevent easy removal. It also includes devices that can make targets more difficult to attack such as using reinforced protective glass to prevent robbery in banks and post offices.

Deflecting offenders is another strategy in this category. This includes closing off a street where a vulnerable target is located, as law enforcement currently practices around of the White House to protect against terrorist bombings.

In critical infrastructures this could mean examining the routes used to transport hazardous materials. If nearby roads can carry large transport trucks with flammable or explosive tanks next to a critical infrastructure (trucks that can be hijacked), it may be time to examine whether these trucks can be deflected to another location.

Controlling the tools of the offender includes removing all sharp metal objects that might be used by terrorists as weapons in aircraft.

Vulnerable critical infrastructures include HVAC areas (heating, vents, air conditioning). Air intakes on the roof or ground provide easy opportunities for chemical or biological attack (CB). Controlling HVAC locations, such as placing them high on vertical walls out of reach, can make it more difficult for terrorists. Another HVAC vulnerability in this category is air exhausts with electric fans. If the electric motor direction is accessible for tampering, it can be reversed making the air exhaust vulnerable to CBs.

Increase the risks the offender will be caught

Methods of formal surveillance. While 1st Generation CPTED promotes better sightlines and lighting for natural surveillance, it is occasionally necessary to use formal methods of surveillance. These include closed circuit television systems and one-way mirrors in critical areas (as used by Custom's officers at borders). Organized security and police patrols are other ways to enhance surveillance.

Another example of organized surveillance is establishing zone controls within the perimeter of a critical infrastructure. For example, placing security stations, such as kiosks, in vulnerable locations can provide security personnel with better opportunities to keep watch. There are many tools for formal surveillance and there is significant evidence that it works to reduce crime opportunities¹³.

¹³ DiLonardo, Robert L. "The Economic Benefit of Electronic Article Surveillance," In *Situational Crime Prevention: Successful Case Studies*, Vol. 2 (Ed. Ronald V. Clarke). Guilderland, NY: Harrow and Heston. pp. 122-131. 1997.

Reduce anonymity. Reducing anonymity in an area like a building or school can help those who belong recognize those who do not. This can be accomplished with technical devices, such as security access cards in airports. However, it is much more effective if those who belong in a place actually know each other personally.

Instructing security staff to frequently interact with staff, employees, and visitors in a positive fashion, will enhance security. If employees and security knows everyone's name, they will also know when outsiders are in their midst.

Reduce the rewards offenders get from crime

Concealing or removing targets. One way of concealing theft targets is to cover or remove valuable items inside parked vehicles. This way thieves cannot see the benefit of breaking into the auto. Another way to conceal targets is to remove identifying markings from courier trucks transporting valuable items. This can reduce in-transit robberies.

Deny benefits. In recent years there have been a number of examples where prevention personnel have evaluated the benefits gained by offenders. By removing those benefits they have had great success¹⁴. One example is on the New York City subway system where graffitiists were denied the chance to see their work when a new program of immediate car cleaning was put into place.

2nd Generation CPTED: Encouraging the social to protect the physical

Early versions of CPTED have been taught to law enforcement and crime prevention officers across the country. Since 1996 an international association, the International CPTED Association, has promoted expanding the CPTED approach (see www.cpted.net). The latest modification to CPTED is called 2nd Generation CPTED¹⁵.

Second Generation CPTED focuses on the place where crime happens. But it draws on some of the social factors to build a sense of community. It employs strategies that bring people together in common purpose to let offenders know they cannot act with impunity. It strengthens relationships between people in a place and reduces the anonymity between them.

In modern parlance, this is called "capacity building". Second Generation CPTED employs four strategies:

¹⁴ DiLonardo, Robert L. and Ronald V. Clarke. 1996. "Reducing the rewards of shoplifting: An evaluation of ink tags." *Security Journal*, Vol. 7 (1): pp. 11-14.

¹⁵ Cleveland, Gerry and Gregory Saville. "Introduction to 2nd Generation CPTED". *CPTED Perspectives*. Vol. 6 (2). 2003. pp. 3-7. Available from the International CPTED Association at www.cpted.net.

Social cohesion

When people work and live together in a positive social climate they have more opportunities to collaborate for preventing crime. For example, reducing the anonymity between employees and customers in a workplace makes it difficult for offenders from outside to act with impunity.

Opportunities for social cohesion can emerge from teaching communication skills and conflict resolution strategies. It can involve programs to mobilize people to work together on social activities. There is ample evidence that when people share a sense of cohesiveness where they work and live they are more likely to participate in preventive programs to protect that place¹⁶

Connectedness

Not only is it important to build positive relations between people in a particular place, but it's also important to enhance communications between groups within that place, and groups outside as well. This connectedness between groups is an ideal way to pool resources and solve problems, particularly if they involve crime problems¹⁷.

Connectedness can apply to infrastructure protection by establishing formal rapport between business, cultural, and community groups and law enforcement or security officials. Consider, for example, the September, 2002, arrests of al-Qaeda suspects in Buffalo where police praised the Muslim community for helping in the investigation.

Community culture

Part of feeling a sense of place and caring about participation is related to culture. This does not necessarily mean a group needs to share a religious or ethnic background to share community culture. In fact community or organizational culture can emerge from any kind of shared activity.¹⁸

The community culture strategy brings people together not for work, but for social activities and for entertainment. It helps to develop a sense of pride and place history.

¹⁶ Rabrenovic, G. *Community Builders: A Tale of Neighborhood Mobilization in Two Cities*. Albany, NY: SUNY Press. 1996. See also Checkoway, B., and J. Finn. *Young People as Community Builders*. Ann Arbor, Mich.: Center for the Study of Youth Policy, University of Michigan. 1992.

¹⁷ Spicer, Valerie and Jean Prince. "Showdown at the Playground: A Community Confronts Drug and Disorder Problems in a Neighborhood Park." In Melissa Reuland, Corina Sole Brito and Lisa Carroll (Eds.). *Solving Crime and Disorder Problems*. Washington, DC: Police Executive Research Forum. 2001.

¹⁸ Oldenburg, Ray. *The Great Good Place: Cafes, Coffee Shops, Community Centers, Beauty Parlors, General Stores, Bars, Hangouts and How They Get You Through The Day*. New York: Paragon House. 1989.

Events can include scheduled barbeques, musical events, and participating in fund raising for charities.

The advantage to this is that a strong sense of community culture will support all the other CPTED strategies. It will encourage compliance with local rules, especially if breaking them means putting the community or its property at risk. A community in which all share a sense of pride and history is much easier to protect.

Neighborhood threshold

All areas, workplaces, and communities need a healthy balance in diversity and ideas in order to protect themselves from crime¹⁹. The concepts of balance and diversity are what is called threshold. For example, too many abandoned homes in a small area can act as a magnet for drug dealers and transients, and that can turn a neighborhood into a crime hotspot²⁰. Such an area will have unbalanced land uses and can be at risk of tipping into disorder.

Another way of looking at threshold is within an organization. If a local company has only a few employees responsible for security on the property, others in the organization will spend little, if any, time contributing ideas for prevention. It is far more effective to provide all employees with whatever relevant information possible (without compromising security) regarding potential risks, and give them an opportunity to participate in infrastructure protection. This builds a much larger critical mass of ideas to produce more effective suggestions. A threshold of diverse ideas can tip a company towards more effective preventive strategies.

PART 3 – IMPLEMENTING A CPTED AUDIT FOR CRITICAL INFRASTRUCTURE PROTECTION

The CPTED principles above provide the auditor with the conceptual framework for using the tailored model described below. Note that this model is modified from others that CPTED practitioner's use. However none of those CPTED strategies were created specifically for the purpose of critical infrastructure protection related to terrorist threats.

CPTED practitioners use a variety of audit tools for evaluating the risks on sites. Traditionally they have been called CPTED security reviews or site assessments. Most have been checklists where practitioners look at design features and check off a list whether the feature seems to satisfy CPTED principles²¹. Some are highly quantitative

¹⁹ Saville, Gregory. "Searching for a neighborhood's crime threshold." *Subject to Debate*. Vol. 10(10): 1-6. Washington, DC: Police Executive Research Forum Publication. 1996.

²⁰ Spelman, William. "Abandoned Buildings: Magnets for Crime?" *Journal of Criminal Justice*, Vol. 21:481-95. 1992.

and employ detailed numerical scales for ranking one feature over another²². One example is the School Environmental Design Assessment form used to evaluate the CPTED aspects of schools²³

Another quantitative CPTED risk assessment model is that of Chief Inspector Phil McCambly of the New South Wales police in Australia. He constructed a context based CPTED risk assessment tool for his architectural master's thesis and tested it over a number of months. One of his findings was that the complexity of the evaluation instrument resulted in less accurate findings with untrained or inexperienced evaluators. Training became an essential part of the model, which has now evolved into the Safer By Design program. In 2001 the government introduced legislative guidelines obliging municipalities to minimize crime opportunities by using the Safer By Design program.

More recent forms of CPTED risk assessments are designed around qualitative methods. The most well known example is the fear of crime perception survey called the Safety Audit developed in Toronto in the late 1980s²⁴. This survey instrument has a unique method in that, unlike many CPTED evaluations conducted by a CPTED consultant, the Safety Audit uses a group process. A number of community residents are gathered together by a facilitator who then conducts them to a site at nighttime and collects their perceptions of safety onto the audit form²⁵.

The safety audit has the advantage of collecting resident's perceptions and fears of crime in an area. The advantage of the more traditional CPTED checklist is that it is easier and quicker to administer. The question is whether they are effective in reducing opportunities for crime²⁶.

²¹ Van der Voordt, and Herman van Wegen. "The Delft Checklist on Safe Neighbourhoods", *Journal of Architectural and Planning Research*. 10(4):341-355. 1993.

²² Pascoe T. "CPTED a Risk Management Tool for the Future". Paper presented at the *2nd International CPTED Conference*. Dec 2-5, Orlando, Florida. 1997. See also Saville, G. "Assessing Risk and Crime Potentials in Neighborhoods", Paper presented at the 1st Annual Canadian CPTED Conference, Calgary, Alberta, October 30 - November 1, 1996.

²³ Schneider, Tod, Hill Walker, and Jeffrey Sprague. *Safe School Design: A Handbook for Educational Leaders: Applying the Principles of Crime Prevention Through Environmental Design*. ERIC Clearinghouse on Educational Management. Eugene, OR. College of Education, University of Oregon. 2000. Available from <http://eric.uoregon.edu>

²⁴ Wekerke, G.R. and Whitzman, Carolyn. *Safe Cities: Guidelines for Planning, Design, and Management*. New York: Van Nostrand Press. 1995.

²⁵ Ibid.

²⁶ There is considerable debate on this theme within the CPTED community. For example, see G. Saville, "Assessing Risk and Crime Potentials in Neighborhoods", Paper presented at the 1st Annual Canadian CPTED Conference, Calgary, Alberta, October 30 - November 1. 1996.

Research of this topic is sporadic. Perhaps the most important question for this guide is whether they have been developed specifically for anti-terror infrastructure protection. The simple answer is, with one exception, they have not. Given the discussion above about CPTED principles regarding infrastructure, it seems there are obvious advantages for a modified CPTED assessment in infrastructure protection. That is the approach used here.

Constructing a CPTED Terror Risk Matrix

The lessons from each of the audits described above are three-fold:

1. Strictly quantitative checklist approaches rarely capture the context of a particular environment. The Safer By Design program is an exception, though its complexity requires a training course in use of the model prior to implementation. Therefore, if critical infrastructure CPTED audits are to experience wide use they need to be straightforward and clearly designed.
2. None of the CPTED risk assessment models were specifically designed for critical infrastructure regarding terrorism. Many features from these models are adaptable to the matrix presented in the next section.
3. None of the risk assessment models incorporated the newer approach of 2nd Generation CPTED, since most of them evolved from older CPTED strategies. A new critical infrastructure CPTED audit needs to incorporate the state of the art in CPTED thinking. The model presented below does that.

Each CPTED strategy included in the discussion above was selected based on its applicability to the problem of critical infrastructure protection. Each strategy provides the auditors with guidelines for where and how a property might be assessed for security.

Drawing from the previous examples of CPTED risk assessment models it is possible to combine all these various prevention concepts into a list of 12 specific strategies²⁷.

1. Territoriality
2. Access control
3. Surveillance
4. Image/maintenance
5. Increase the effort to commit crime
6. Increase risks to criminal
7. Reduce rewards from crime
8. Reduce factors that provoke crime
9. Social cohesion
10. Connectedness

²⁷ This particular version is modified from an automated database program called the The Learning Matrix used to train prevention professionals and police officers in problem-based learning (PBL). It is described in more detail at www.capsr.com

11. Community culture
12. Threshold

It is then possible to compile four categories of potential terror attacks from Part 1:

1. Bombings (including “dirty bombs”)
2. Arsons
3. Product contamination and
4. WMD.

By placing the prevention strategies on one side of a chart, and the terror attack risks on another, it is possible to create a CPTED risk matrix for auditing a site.

TERRORISM RISK MATRIX

	ARSONS	BOMBINGS	PRODUCT CONTAMINATION.	WEAPONS OF MASS DESTRUCTION
Territoriality	A1	B1	P1	W1
Surveillance	A2	B2	P2	W2
Access controls	A3	B3	P3	W3
Image and maintenance	A4	B4	P4	W4
Increase effort to commit crime	A5	B5	P5	W5
Increase risks of getting caught	A6	B6	P6	W6
Reduce rewards from crime	A7	B7	P7	W7
Social cohesion	A8	B8	P8	W8
Neighborhood connectedness	A9	B9	P9	W9
Community culture	A10	B10	P10	W10
Threshold	A11	B11	P11	W11

Documenting findings within each cell

Note that each cell in the matrix is labeled, for example A1 and B2. Each cell represents a different evaluative category, for example A1 represents territorial factors related to arson at the particular site being audited. Cell B2 represents surveillance factors related to potential bombings at the site being audited.

To conduct a CPTED risk assessment audit of a site the auditor’s need to address each of the categories in the matrix and document the strengths and weaknesses of the site under audit. They can document their audit in whatever method appropriate for their particular organization or jurisdiction. For example, they can use the matrix categories to collect

field notes or jot notes onto laptop computers. These notes can then be transferred to a field report with recommendations for improvements.

Another method of documentation is to create forms that include each category on the matrix and then use those auditing forms to review the site. The most important factor is that each CPTED category on the side of the matrix is addressed and correlated to each risk category on the top of the matrix. That will ensure that a systematic methodology is applied throughout a jurisdiction.

The audit process: balancing security with diversity

Process is another important factor. In traditional CPTED assessments, a single CPTED practitioner walks around a site with a checklist in hand. This is a speedy way to collect information. Unfortunately one auditor cannot possibly know how all the various design features work. Even with interviews it is unlikely that a single person can incorporate enough diversity of experience into the audit process. An entire perspective is left out of this form of analysis: the perceptions of local people who work and live in the area.

A modification of this traditional approach is to supplement the audit with local surveys and interviews to record perceptions. The limitation of this is that it is difficult to gather detailed information about specific areas in a site and also surveys can take considerable time to administer.

The Toronto Safety Audit overcame this problem by utilizing a small group of people from the area, as well as CPTED experts, in the audit team. The team spent time walking around the site with the audit forms collecting information on problems and possible solutions. The strength of diversity on the team (the principle of threshold) provides a wide range of experience during the audits and that strengthens the quality of solutions.

An important process lesson from the audits, especially the Toronto Safety Audit, is that “team building” within the audit team is an essential reagent for effective terrorist prevention.

The terror risk matrix combines all these approaches.

The audit process: primary and secondary teams

In the first phase of the audit process the auditor selects two or three members of an audit team. They are called the primary team.

NOTE: All members of the primary team should possess security clearance. The data they collect should be kept confidential and secured by the lead auditor. The reason for this is obvious. If terrorists gain access to data on the physical infrastructure this will provide them with a dangerous advantage.

The primary team then conducts the audit using six categories of the matrix:

- ☑ Territoriality,
- ☑ Surveillance,
- ☑ Access controls,
- ☑ Increase effort to commit,
- ☑ Increase risks of being caught, and
- ☑ Reduce rewards.

Once collected, the data is kept confidential and is not brought to subsequent audits. The primary team then selects a half dozen other members including employees from the organization, residents from the local community, and other key stakeholders related to the infrastructure. This is the secondary audit team.

The secondary audit team then conducts the audit for the remaining categories of the matrix:

- ☑ Image and maintenance,
- ☑ Cohesion,
- ☑ Connectedness,
- ☑ Community/organizational culture, and
- ☑ Threshold.

When that data is collected the primary team reviews the information and prioritizes a list of recommendations for improvement at the site. The recommendations are presented to key decision-makers and others who are directly affected by the recommendations. These recommendations comprise remediation strategies for the Critical Infrastructure Protection Plan or, in it hasn't yet been developed, the first steps toward creating one.

Conducting audits

An audit requires a number of different research activities. Each activity will be entirely based on the critical infrastructure being audited. For example, in a power generating plant it will be necessary to determine *natural surveillance* opportunities. It may be necessary to interview staff on site to get their impressions.

It will also be necessary to review strategies that *increase risks* to potential terrorists, such as methods of formal surveillance. For that it will be necessary to examine the CCTV placement, television monitor quality, and review the security arrangements for using the equipment.

In addition to these research activities, it will also be necessary to do a series of walk-throughs of the site during the day and night. The number of walk-throughs depends on the size, configuration, and nature of the infrastructure. Generally, the team begins by mapping out on a diagram the site configuration. They then document on the map their auditing route. When the exterior portions of the site are complete, the team then does the same for the interior.

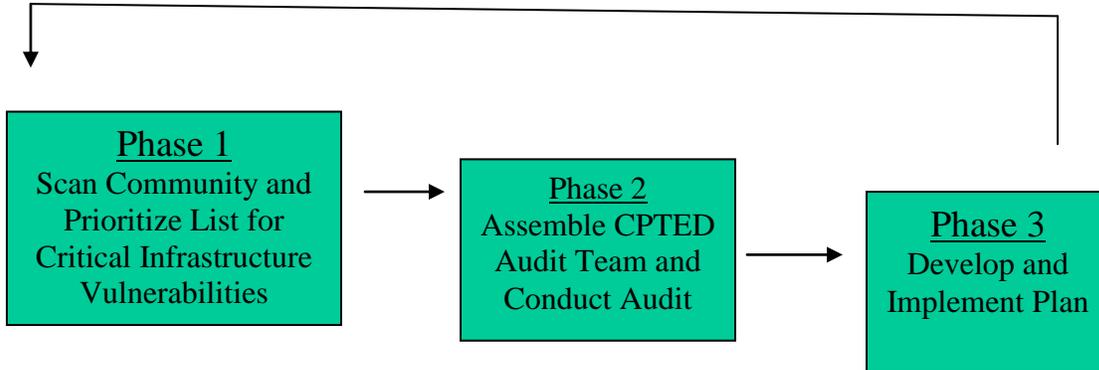
Using matrix cell prompts

Each cell of the matrix relates to a particular aspect of CPTED. The audit team should develop a series of questions to ask for each cell pertaining to the risks on the site. These questions become prompts the audit team can use to assess that critical infrastructure.

Territoriality	<input checked="" type="checkbox"/> How are vulnerable areas on site supervised or controlled by employees, and by security? <input checked="" type="checkbox"/> Are semi private areas demarcated to separate the private areas from the public?
Surveillance	<input checked="" type="checkbox"/> Are there adequate perimeter, rooftop, parking lot and passageway lighting? <input checked="" type="checkbox"/> Are there vision barriers that will hinder or help potential terrorists? <input checked="" type="checkbox"/> Are there good natural surveillance sightlines in public areas such as parking lots?
Access controls	<input checked="" type="checkbox"/> Are there adequate zone controls on entranceways such as passes for visitors? <input checked="" type="checkbox"/> Are passes collected and recorded on exit? <input checked="" type="checkbox"/> Is there a balance between security fencing and good visibility for security?
Image and Maintenance	<input checked="" type="checkbox"/> Are there adequate controls and cleaning of hazard materials on site, such as bio-waste storage? <input checked="" type="checkbox"/> Is the overall site well maintained and clean?
Increase effort to commit	<input checked="" type="checkbox"/> Are potential targets concealed or removed? <input checked="" type="checkbox"/> Do features on site provide opportunities for terrorist such as window boxes, flower pots, landscaping features where bombs might be concealed? <input checked="" type="checkbox"/> Is there hardening of vulnerable targets on site, such as protecting electrical systems, panel boards, circuit breakers and power relays from damage or bombings?
Increase risks of getting caught	<input checked="" type="checkbox"/> Are there CCTV and other formal surveillance mechanisms, such as security or police patrols?
Reduce rewards for crime	<input checked="" type="checkbox"/> Can potential targets on site be removed or concealed? <input checked="" type="checkbox"/> Are there any possible benefits to terror attack on site that can be denied?
Social cohesion	<input checked="" type="checkbox"/> Is there positive interaction between security/police and persons on site? <input checked="" type="checkbox"/> Are there security education and training programs for staff?
Neighborhood connectedness	<input checked="" type="checkbox"/> Do employees interact with visitors on site, do they speak to them, find out who they are? <input checked="" type="checkbox"/> Are neighborhood groups involved with the site in any positive way so they can help with security?
Community culture	<input checked="" type="checkbox"/> How is staff morale and how does it affect participation in infrastructure protection? <input checked="" type="checkbox"/> Do organizational social or recreational activities between employees contribute to a positive environment?
Threshold	<input checked="" type="checkbox"/> Do all employees, staff, or organizational members participate in infrastructure protection, or only a few? <input checked="" type="checkbox"/> Can security information about potential risks be employed to create a critical mass of organizational members who are committed to infrastructure protection?

The Planning Process

CPTED Risk Audit Planning Process



As with any Critical Infrastructure Protection Plan, there are a number of phases that help law enforcement agencies implement this audit process. Take note that the auditing process is not a one time event, but rather circles back to Phase 1. This is because the number of critical infrastructures may change in a jurisdiction and it will become necessary to institute on-going audits. Further, the infrastructures that are audited may themselves change in the span of a few years. They should institute a program of plan updates on a regular basis.

These phases are:

Phase 1 – Scanning the community for critical infrastructures and developing a priority list and time schedule for the audits.

In Phase 1 it is necessary to survey the community for the critical infrastructures that may be vulnerable. Some will be well known. Some will not. It is advisable to use the list provided in this guide as a starting place to identify sites.

There are also a few ideal resources that can assist. This includes computerized geographic information systems (GIS), such as crime mapping resources. Examples of these resources are included in the next section of this guide. One is the Information Collection and Automated Mapping program (ICAM) in Chicago.

Mapping programs allow the CPTED auditors to identify the geographic locations of critical infrastructures, adjacent properties, connected transport and roadway networks, and so forth. They provide an ideal birds-eye view of the community. If a community does not utilize crime mapping resources, most municipal planning and development offices also use GIS technology.

Once a list of infrastructures is compiled it will be necessary to develop a work plan by prioritizing each site and contacting the relevant stakeholders. In larger jurisdictions it may be more effective to create a training program for stakeholders at each site and have them conduct their own audits. This will depend on the size and nature of each community.

Phase 2 – Assemble a primary and secondary CPTED audit team and conduct the audits.

Assembling primary audit teams requires security clearances for the key personnel.

The members of the team, no more than 3 members with one leader, ideally should have CPTED training, or at a minimum some form of crime prevention and security experience. The team will also benefit from architecture and engineering experience

The secondary team will comprise a larger group consisting of members from the community, employees or staff representing the infrastructure, and local security and facility managers. This group will be no larger than a dozen people and the duration of its activities will depend on the size and scope of the infrastructure. It is likely these people will be volunteers, or will be assigned by the organization responsible for the infrastructure.

The audits themselves, described above, depend entirely on the size and scope of the infrastructure. Some may last no longer than a few hours. Others will require repeat visits over a period of weeks. Recall that the audit results will be presented for inclusion as remediation strategies in a larger Critical Infrastructure Protection Plan. If such a plan does not exist, the audits can represent the first steps in creating one.

Phase 3 – Develop and Implement the plan

The audits are for the purpose of helping protect critical infrastructure assets in a community. It may take many months to implement all the recommendations, depending on budgetary constraints. Other recommendations can be put in place immediately.

Implementation of a Critical Infrastructure Protection Plan is beyond the scope of this guide. It is sufficient to note there are many resources that outline the method for this process and they are included in the next section of this guide.

PART 4 - RESOURCES

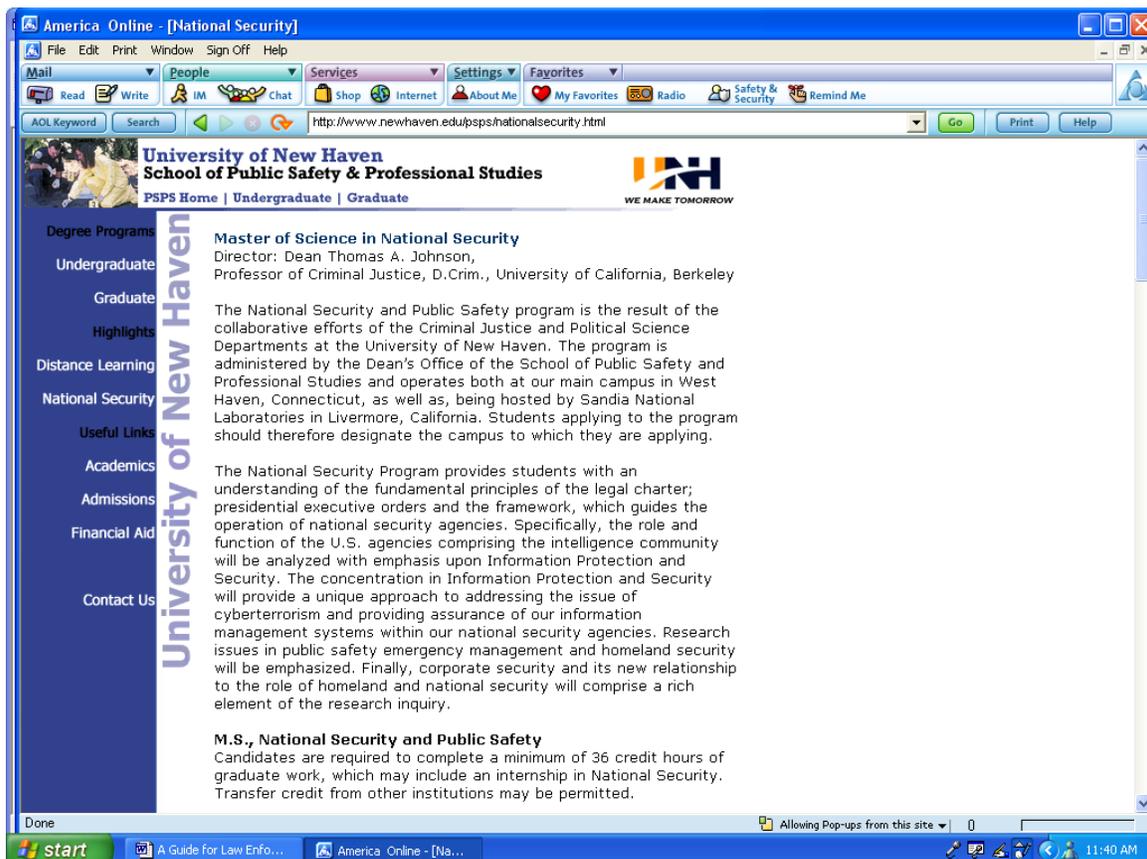
There are a few places where national security and anti-terror risk assessments are available. These include the following:

Training – CPTED and National Security

There are numerous locations where CPTED training is available. Many are described on the International CPTED Association website at www.cpted.net .

An example is the Center for Advanced Public Safety Research at the University of New Haven where training is provided in both 1st Generation and 2nd Generation CPTED. It is described at www.capsr.com.

Also, the University of New Haven's School of Public Safety and Professional Studies, in partnership with Sandia National Laboratories in California, has created the first graduate program in National Security and Public Safety. The program is described at: <http://www.newhaven.edu/psps/nationalsecurity.html>

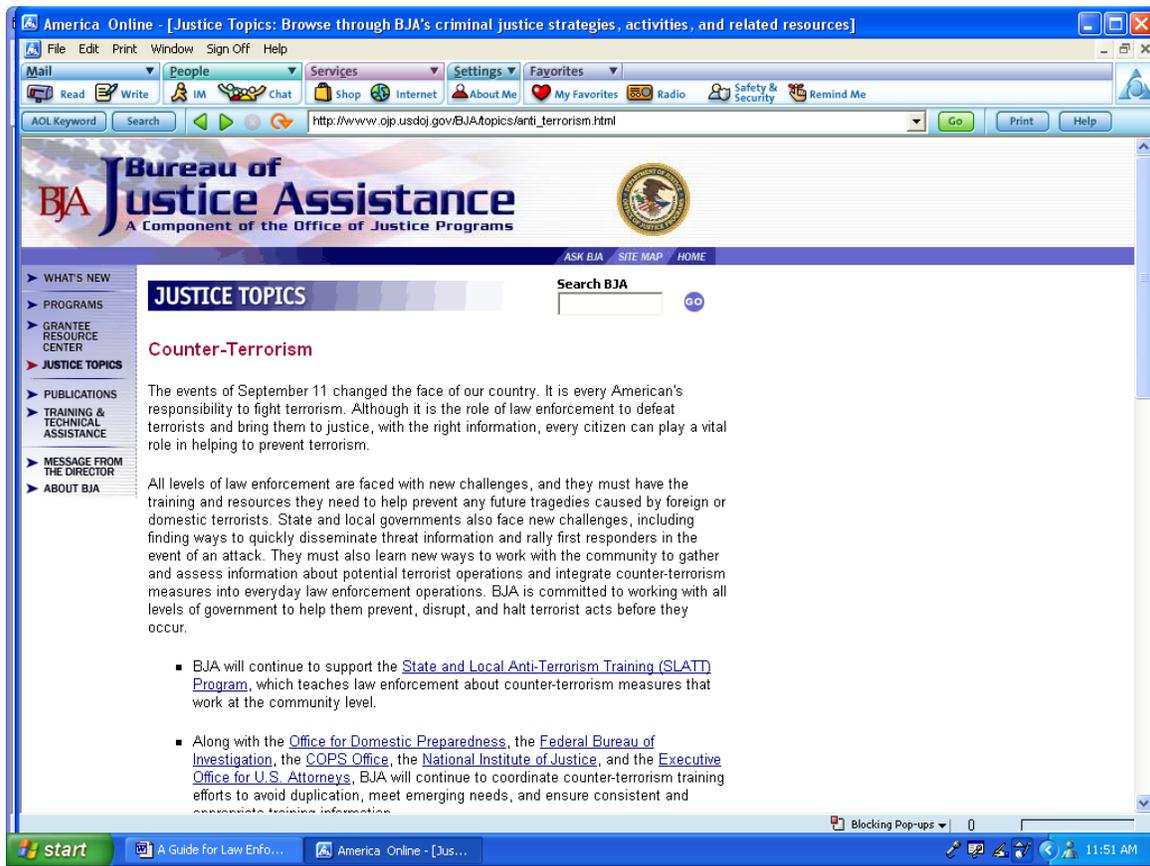


The screenshot shows a web browser window titled "America Online - [National Security]". The address bar displays the URL "http://www.newhaven.edu/psps/nationalsecurity.html". The page content includes the University of New Haven logo and the text "School of Public Safety & Professional Studies". A vertical navigation menu on the left lists "Degree Programs", "Undergraduate", "Graduate", "Highlights", "Distance Learning", "National Security", "Useful Links", "Academics", "Admissions", "Financial Aid", and "Contact Us". The main content area is titled "Master of Science in National Security" and lists the Director as Dean Thomas A. Johnson, Professor of Criminal Justice, D.Crim., University of California, Berkeley. The text describes the program as a collaborative effort between the University of New Haven and Sandia National Laboratories, focusing on information protection and security, cyberterrorism, and homeland security. It also mentions that candidates for the M.S., National Security and Public Safety program are required to complete a minimum of 36 credit hours of graduate work.

Training – Anti Terror Programs

The U.S. Bureau of Justice Assistance also promotes and sponsors a range of anti-terror training programs. They are outlined on their website:

http://www.ojp.usdoj.gov/BJA/topics/anti_terrorism.html



Training – Crime Mapping

There has been a proliferation of crime mapping resource centers and training programs in recent years.

One example of resources is the Information Collection and Automated Mapping program (ICAM) in Chicago.

It is located at <http://12.17.79.6/ctznicam/ctznicam.asp>



There are many examples of training programs. A small sample is:

Center for Advanced Public Safety Research, University of New Haven: www.capsr.com

Center for Applied Studies of the Environment (CAPSE) Crime Related Software
<http://www.geography.hunter.cuny.edu/capse/projects/nij/software.html>

CAPSE Mapping & Crime Analysis Bibliography
http://www.geography.hunter.cuny.edu/capse/projects/nij/crime_bib1.html

Crime Analysis and Crime Mapping Graduate Certificate Program
<http://www.cohpa.ucf.edu/crim.jus/map/Index.cfm>

Crime Mapping and Analysis Program (CMAP)

<http://www.nlectc.org/cmap/>

CrimeMap Tutorial

<http://www.icpsr.umich.edu/NACJD/cmtutorial.html>

International Association of Crime Analysts (IACA)

<http://www.iaca.net/>

International Association of Law Enforcement Intelligence Analysts (IALEIA)

<http://www.ialeia.org/>

Justice Technology Information Network

<http://www.nlectc.org/>

Mapping and Analysis for Public Safety (MAPS)

<http://www.ojp.usdoj.gov/nij/maps/>

Office of Community Oriented Policing Services (COPS)

<http://www.cops.usdoj.gov/>

Professional Certificate in Crime Mapping and Analysis

http://ocpe.gmu.edu/certificate_programs/crimemapping.html

Government Services and Clearinghouses

There are federal government sites where resources are available. The Office of Domestic Preparedness at the U.S. Department of Homeland Security provides helpful services.

The website is located at <http://www.ojp.usdoj.gov/odp/ta/overview.htm>.

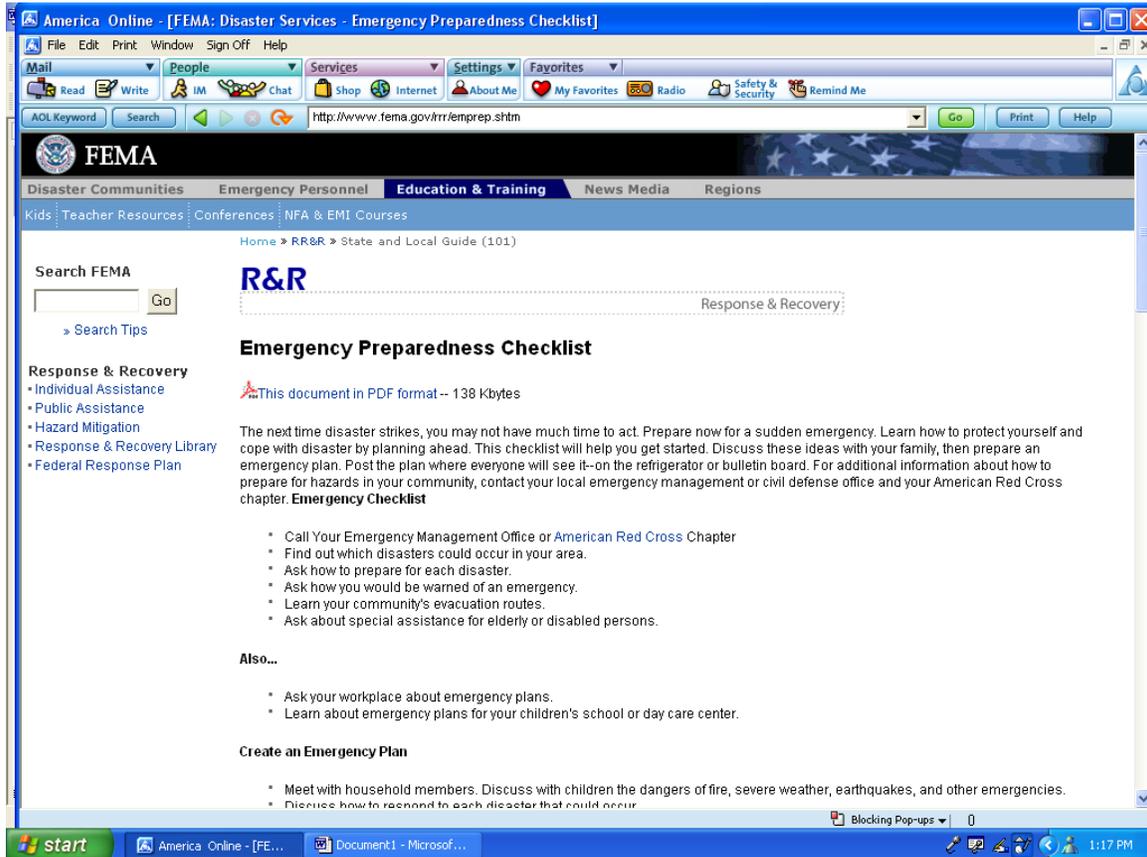
The screenshot displays a web browser window with the following elements:

- Browser Title Bar:** America Online - [Assistance in Preparedness Assessment from the Office for Domestic Preparedness Support]
- Address Bar:** <http://www.ojp.usdoj.gov/odp/assessments/definition.htm>
- Page Header:** U.S. Department of Homeland Security logo and a "THREAT ADVISORY ELEVATED" banner with the text "Significant Risk of Terrorist Attacks".
- Navigation Menu (Left):**
 - ODP Home
 - About ODP
 - What's New
 - Training and Technical Assistance
 - Equipment Acquisition Grants
 - Exercise Development & Support
 - State-Based Needs Assessments
 - Library
- Main Content Area:**
 - Section:** State Homeland Security Assessment and Strategy Process
 - Text:** ODP launched its Fiscal Year (FY) 2003 State Homeland Security Assessment and Strategy (SHSAS) process on July 1, 2003. As part of this effort, ODP has refined the SHSAS process that was originally established in FY 1999. The FY 2003 process will allow states and local jurisdictions to update their needs assessment data to reflect post-September 11, 2001 realities, as well as identify progress on the priorities outlined in their initial homeland security strategies. Furthermore, the refined process will serve as a planning tool for state and local jurisdictions, and will assist ODP and its partners in better allocating federal resources for homeland security.
 - Text:** Concurrent with the launch of the SHSAS process, ODP has also activated a revised Online Data Collection Tool. The Tool allows states and local jurisdictions to input data from the assessment section of the SHSAS online, without the need to develop complex systems to support the required data collection. The Tool also serves as the medium for each State Administrative Agency (SAA) to develop and submit a revised state homeland security strategy. The Online Data Collection Tool may be accessed through the following link:
<https://justice.ojp.usdoj.gov/dct>
- Image:** A photograph showing two individuals in blue uniforms, one with "FBI" on the sleeve, reviewing documents.

Government Services and Clearinghouses

Another excellent source of assistance is the Federal Emergency Measures Agency (FEMA) that also provides a basic emergency preparedness checklist.

This is available at <http://www.fema.gov/rrr/emprep.shtm>



The screenshot shows a web browser window displaying the FEMA website. The browser's address bar shows the URL <http://www.fema.gov/rrr/emprep.shtm>. The website's navigation menu includes "Disaster Communities", "Emergency Personnel", "Education & Training", "News Media", and "Regions". The "Education & Training" section is active, and the "R&R" (Response & Recovery) sub-section is selected. The main content area features a search bar, a "Search FEMA" button, and a "Go" button. Below the search bar, there is a "Search Tips" link. The "Response & Recovery" section is highlighted, and a list of links is provided: "Individual Assistance", "Public Assistance", "Hazard Mitigation", "Response & Recovery Library", and "Federal Response Plan". The "Emergency Preparedness Checklist" is the main focus, with a sub-section for "Response & Recovery". The checklist is presented as a PDF document (138 Kbytes) and includes the following text: "The next time disaster strikes, you may not have much time to act. Prepare now for a sudden emergency. Learn how to protect yourself and cope with disaster by planning ahead. This checklist will help you get started. Discuss these ideas with your family, then prepare an emergency plan. Post the plan where everyone will see it--on the refrigerator or bulletin board. For additional information about how to prepare for hazards in your community, contact your local emergency management or civil defense office and your American Red Cross chapter. **Emergency Checklist**

- Call Your Emergency Management Office or [American Red Cross Chapter](#)
- Find out which disasters could occur in your area.
- Ask how to prepare for each disaster.
- Ask how you would be warned of an emergency.
- Learn your community's evacuation routes.
- Ask about special assistance for elderly or disabled persons.

Also...

- Ask your workplace about emergency plans.
- Learn about emergency plans for your children's school or day care center.

Create an Emergency Plan

- Meet with household members. Discuss with children the dangers of fire, severe weather, earthquakes, and other emergencies.
- Discuss how to respond to each disaster that could occur.

References – Risk Assessment Information

In addition to these resources, there are a number of published studies and risk assessment documents for more general crime prevention. These include:

Ahlberg, J., & Knutsson, J. “The risk of detection.” *Journal of Quantitative Criminology*, 6, 117-130. 1990.

Brown, B. B., & Bentley, D. L. “Residential burglars judge risk: The role of territoriality.” *Journal of Environmental Psychology*. Vol. 13, pp. 51-61. 1993.

Felson, M. “Predicting crime potential at any point on the city map.” In P. Figlio, S. Hakim, & G. Rengert (Eds.), *Metropolitan Crime Patterns*. New York: Criminal Justice Press. Pp. 139-160. 1986.

Figlio, P., Hakim, S., & Rengert, G. (Eds.). *Metropolitan Crime Patterns*. New York: Criminal Justice Press. 1986.

Florida Center for Community Design & Research. *Safe Schools Design Guidelines: Recommendations for a Safe and Secure Environment in Florida's Public Schools*. Project No. 4950-33-10-056-LO. Tallahassee, FL.1993.

La Vigne, N. G., & Wartell, J. (Eds.). *Crime Mapping Case Studies: Successes in the Field (Volume 1)*. Washington, DC: Police Executive Research Forum. 1998.

La Vigne, N. G., & Wartell, J. (Eds.). *Crime Mapping Case Studies: Successes in the Field (Volume 2)*. Washington, DC: Police Executive Research Forum. 2000.

Pascoe, Tim. *Predicting the Targets of Household Burglars- Developing Risk-Based Models from a Case Study of Recent Experience in Redditch, United Kingdom*. Ph.D. Thesis. London: Cranfield University. 2000.

Ruehl, Gorden. *Creating Safer Schools*. Olympia, WA: Office of the Superintendent of Public Instruction. 1980.

Sanford, R. (1995). How to Develop a Tactical Early Warning System on a Small-City Budget. In C. R. Block, M. Dabdoub, & S. Fregy (Eds.), *Crime Analysis Through Computer Mapping*, (pp. 199-208). Washington, DC: Police Executive Research Forum.

Smith, M. “Assessing Vandalism Cues in an Experimental Setting: A Factorial Design Involving State of Repair, Presence of Graffiti, Target Vulnerability, and Target Suitability”, in Dissertation Abstracts International, A: The Humanities and Social Sciences. Vol. 57 (4), pp. 1857-A-1858-A, Oct. 1996.

Stoks, F. G. Assessing Urban Public Space Environments for Danger of Violent Crime - Especially Rape. Doctoral Dissertation, University of Washington. 1982.

Van der Voordt, and Herman van Wegen. "The Delft Checklist on Safe Neighbourhoods", *Journal of Architectural and Planning Research*. 10(4):341-355. 1993.

Waller, I., & Welsh, B. C., "Reducing Crime by Harnessing International Best Practice." *National Institute of Justice Journal*. Washington, DC: U. S. Department of Justice. Pp. 26-31. 1998.

Wekerke, G.R. and Whitzman, Carolyn. *Safe Cities: Guidelines for Planning, Design, and Management*. New York: Van Nostrand Press. 1995.

References – Responding and Investigating Terror Incidents

Chapman, Robert et al. *Local Law Enforcement Responds to Terrorism: Lessons in Prevention and Preparedness. COPS Innovations*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing. 2002. Pp. 20. Available on-line at www.cops.usdoj.gov

Charlotte-Mecklenberg Police Department. *ALERT: Advanced Local Emergency Response Team*. Prepared by Staff of the Charlotte-Mecklenberg Police Department, Charlotte, NC: Charlotte-Mecklenberg Police Department. 2002.

Goldfarb, Michael. *Protecting First Responders: A Reference Guide for Police Executives on Biological, Chemical, and Radiological Threats*. June 2003 discussion draft, Police Executive Research Forum, 2003.

International Association of Chiefs of Police. *Leading from the Front: Law Enforcement's Role in Combating and Preparing for Domestic Terrorism*. International Association of Chiefs of Police, 2001.

U.S. Department of Justice. *Responding to Terrorist Victims: Oklahoma City and Beyond*. Washington, DC: Office for victims of Crime, U.S. Department of Justice, 2000.

Hutton, S.A., & Myrent, M. (1999, December). *Incident-Based Crime Analysis Manual: Utilizing Local-Level Incident Reports for Solving Crimes*. Chicago: Illinois Criminal Justice Information Authority.

Heuer, R. J. (1999). *Psychology of Intelligence Analysis*. Center for the Study of Intelligence, Central Intelligence Agency. Online. Available: <http://www.odci.gov/csi/books/19104/art1.html>

Additional reference material is on the Sandia National Laboratories website at:

http://techlibpac.sandia.gov:8101/ipac20/ipac.jsp?session=106AL7158K700.1583&menu=search&aspect=basic_search&npp=10&ipp=20&profile=pac&ri=1&source=134.253.163.7@%21horizon&index=.GW&term=terrorism+prevention&aspect=basic_search#focus

References: First Generation CPTED

- Angel, S. *Discouraging Crime Through City Planning, (Paper No. 75)*. Berkeley, CA: Center for Planning and Development Research, University of California at Berkeley. 1968.
- Clarke, R. V., & Mayhew, P. (Eds.) *Designing Out Crime*. London: H.M.S.O. 1980.
- Cooper-Marcus, C., & Sarkissian, W. *Housing As If People Mattered: Site Guidelines for Medium-density Family Housing*. Berkeley, CA: University of California Press. 1986.
- Crowe, T. D. An ounce of prevention: A new role for law enforcement. *FBI Law Enforcement Bulletin*, 57, 18-24. 1988.
- Crowe, T. D. *Crime Prevention Through Environmental Design*. Woburn, MA: Butterworth-Heinemann. 1991.
- Gallagher, Winifred. *The Power of Place: How Our Surroundings Shape Our Thoughts, Emotions, and Actions*. New York: Poseidon Press. 1993.
- Gardiner, R. A. *Design for Safe Neighborhoods: The Environmental Security Planning and Design Process*. Washington, DC: National Institute of Law Enforcement and Criminal Justice. 1978.
- Jeffery, C. Ray. *Crime Prevention Through Environmental Design*. Beverly Hills, CA. Sage. 1971.
- Newman, Oscar. *Defensible Space. Crime Prevention Through Urban Design*. New York. Macmillan. 1972.
- Plaster, Sherry and Stan Carter. *Planning for Prevention: Sarasota, Florida's Approach to Crime Prevention Through Environmental Design*. Tallahassee, FL: State of Florida Criminal Justice Executive Institute. 1993.

References: Situational Crime Prevention

- Bellamy, L. "Situational Crime Prevention and Convenience Store Robbery", in *Security Journal*. Vol. 7 (1), pp. 41-52, April 1996.
- Bell, J., & Burke, B. Cruising Cooper Street. In R. V. Clarke (Ed.), *Situational Crime Prevention: Successful Case Studies*. New York: Harrow & Heston. 1992.
- Clarke, R. V. Situational crime prevention: Theory and practice. *British Journal of Criminology*, 20, 136-147. 1980.
- Clarke, R. V. Situational crime prevention: Its theory basis and practical scope. In M. Tonry & N. Morris (Eds.), *Crime and Justice: An Annual Review of Research*, 4. Chicago: University of Chicago Press. 1980.
- Clarke, R.V.G. *Situational Crime Prevention: Successful Case Studies*. New York, NY: Harrow and Heston. 1992.
- Clarke, R. V., & Mayhew, P. Parking patterns and car theft risks: Policy-relevant findings from the British Crime Survey. In R. V. Clarke (Ed.), *Crime Prevention Studies: Vol. 3* (pp. 91-107). Monsey, NY: Criminal Justice Press. 1992.
- Cornish, D. B. The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (Ed.), *Crime Prevention Studies: Vol. 3* (pp. 91-107). Monsey, NY: Criminal Justice Press. 1994.
- Eck, J., Spelman, W. Thefts from vehicles in shipyard parking lots. In R. V. Clarke (Ed.), *Situational crime prevention: Successful case studies*. New York: Harrow & Heston. 1992.
- Heal, K., & Laycock, G. (Eds.) *Situational crime prevention: From theory into practice*. London: H.M.S.O. 1986.
- Hunter, R. D., & Jeffery, C. R. Preventing convenience store robbery through environmental design. In R. V. Clarke (Ed.), *Situational crime prevention: Successful case studies*. New York: Harrow & Heston. 1992.
- La Vigne, N. "Visibility and Vigilance: Metro's Situational Approach to Preventing Subway Crime", from U.S. Department of Justice, NIJ. 1997.
<http://www.ncjrs.org/pdffiles/166372.pdf>.
- Poyner, Barry. "Situational crime prevention in two parking facilities." *Security Journal*. 2:96-101. 1991.
- Saville, Gregory. Situational crime prevention as responsible urban design. *Plan Canada*. 36(2). Ottawa: Canadian Institute of Planners. Pp. 27-28. 1996.

References: Second Generation CPTED

- Adams, Don and Arlene Goldbard. 2001. *Creative Community: The Art of Cultural Development*. New York, NY: Rockefeller Foundation.
- Baba, Y., and D. M. Austin. 1989. Neighborhood Environmental Satisfaction, Victimization, and Social Participation as Determinants of Perceived Neighborhood Safety. *Environment and Behavior*. 21:763-80.
- Becker, F.D. "The Effect of Physical and Social Factors on Residents' Sense of Security in Multi-Family Housing Developments", in *Journal of Architectural Research*, Vol. 4(1). February, 1975.
- Bennet, R.R. and J. M. Flavin. 1994. Determinants of Fear of Crime: The Effect of Cultural Setting. *Justice Quarterly*. 11:357-81.
- Checkoway, B., and J. Finn. 1992. *Young People as Community Builders*. Ann Arbor, Mich.: Center for the Study of Youth Policy, University of Michigan.
- Gibson, Chris L., Jihong Zhao, Nicholas P. Lovrich, and Michael J. Gaffney. 2002. Social Integration, Individual Perceptions of Collective Efficacy, and Fear of Crime in Three Cities. *Justice Quarterly*. 19(3)537-564.
- National Institute of Justice. 1996. *Communities Mobilizing Against Crime: Making Partnerships Work*. Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.
- Oldenburg, Ray. 1989. *The Great Good Place: Cafes, Coffee Shops, Community Centers, Beauty Parlors, General Stores, Bars, Hangouts and How They Get You Through The Day*. New York: Paragon House.
- Rabrenovic, G. *Community Builders: A Tale of Neighborhood Mobilization in Two Cities*. Albany, NY: SUNY Press. 1996.
- Saville, Gregory. New tools to eradicate crime places and crime niches. In Steven Cooper (Ed.), *Perspectives: Criminology*. Irvine, CA: University of California Press. 2001.
- Saville, Gregory and Todd Clear. Community Renaissance with Community Justice. *The Neighborworks Journal*. 18(2): 19-24. 2000.
- Saville, G. and G. Cleveland. "2nd Generation CPTED: An Antidote to the Social Y2K Virus of Urban Design." Paper presented at the 3rd Annual International CPTED Conference, Washington, DC, December 14-16. 1998.
- Saville, G. "Displacement: A Nagging Problem for CPTED", Paper presented at the 2nd Annual International CPTED Conference, Orlando, Florida, December 3-5. 1997.

Saville, G. and Wong, P. "Exceeding the Crime Threshold: The Carrying Capacity of Neighborhoods", Paper presented at the 46th Annual Meeting of the American Society of Criminology, Miami, Florida, November 9-12. 1994.

Saint-Yves, Michele and Margaret Worth. Crime, Community, Environment, Art and Design. A CEAD and CPTED Preventive Partnership. Paper presented at the Conference on Safer Communities: Strategic Directions in Urban Planning. Australian Institute of Criminology and Victorian Community Council Against Violence, Melbourne. September. 1998.

Saville, Gregory and Todd Clear. Community Renaissance with Community Justice. *The Neighborworks Journal*. 18(2): 19-24. 2000.

Saville, Gregory, and David Wright. Putting Neighbours Back in the Neighbourhood: Strategies for Safety, Urban Design, and Cohousing. Paper presented at the 1998 Biennial Meeting of the Western Association of Sociology and Anthropology, Vancouver, British Columbia, Canada. 1998.

Saville, Gregory. Searching for a neighborhood's crime threshold. *Subject to Debate*. 10(10): 1-6. Washington, DC: Police Executive Research Forum Publication. 1996.

Schorr, Lisbeth B. *Common Purpose: Strengthening Families and Neighborhoods to Rebuild America*. New York, NY: Anchor. 1997.

Spelman, William. "Abandoned Buildings: Magnets for Crime?" *Journal of Criminal Justice*, 21:481-95. 1992.

White, Garland F. "Neighborhood Permeability and Burglary Rates". *Justice Quarterly*. 7(1):57-67. 1990.

Whyte, William. H. "Carrying Capacity", pp. 165-173. In (W. Whyte, ed.). *City: Rediscovering the Center*. Doubleday: New York. 1988.