

FM 3-19.30

(Formerly FM 19-30)

Physical Security



Headquarters, Department of the Army

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

Chapter 2

The Systems Approach

Commanders must ensure that appropriate physical-security measures are taken to minimize the loss of personnel, supplies, equipment, and material through both human and natural threats. Commanders commonly exercise those protective responsibilities through the provost marshal (PM) and/or physical-security officer and the force-protection officer. The force-protection officer must coordinate with several different agencies to complete his mission. For example, the Army's Intelligence and Counterintelligence Program (see Appendix C) provides information that will be used to complete the unit's crisis-management plan (see Appendix D).

PROTECTIVE SYSTEMS

2-1. The approach to developing protective measures for assets should be based on a systematic process resulting in an integrated protective system. The protective system focuses on protecting specific assets against well-defined threats to acceptable levels of protection. The system is organized in-depth and contains mutually supporting elements coordinated to prevent gaps or overlaps in responsibilities and performance.

2-2. Effective protective systems integrate the following mutually supporting elements:

- Physical protective measures, including barriers, lighting, and electronic security systems (ESSs).
- Procedural security measures, including procedures in place before an incident and those employed in response to an incident. (These include procedures employed by asset owners and those applied by and governing the actions of guards.)
- Terrorism counteraction measures that protect assets against terrorist attacks.

2-3. The following determinations are made when considering system-development procedures:

- The resources available.
- The assets to be protected.
- The threat to those assets.
- The risk levels applicable to those assets.
- The applicable regulatory requirements for protecting the assets.
- The applicable level of protection for those assets against the threat.
- Additional vulnerabilities to the assets (based on the threat).

SYSTEMS DEVELOPMENT

2-4. AR 190-51, DA Pamphlet (Pam) 190-51, and Technical Manual (TM) 5-853-1 are useful tools for developing protective systems using the systems approach. The key to applying these tools successfully is to use a team approach. A team may include physical-security, intelligence, and operations personnel; the installation engineers; and the user of the assets. It may also include representatives from the multinational, host-nation (HN), and local police as well as the regional security office from the embassy.

ASSETS

2-5. Protective systems should always be developed for specific assets. The goal of security is to protect facilities and buildings and the assets contained inside. The risk-analysis procedure in DA Pam 190-51 is used to identify assets. This procedure is applied to all mission-essential or vulnerable areas (MEVAs) according to AR 190-13. It represents the majority of assets with which DOD is commonly concerned. These assets include—

- Aircraft and components at aviation facilities.
- Vehicle and carriage-mounted or -towed weapons systems and components at motor pools.
- Petroleum, oil, and lubricants (POL).
- Controlled medical substances and other medically sensitive items.
- Communication and electronics equipment; test, measurement, and diagnostic equipment (TMDE); night-vision devices (NVDs); and other high-value precision equipment and tool kits.
- Organizational clothing and individual equipment stored at central-issue facilities.
- Subsistence items at commissaries, commissary warehouses, and troop-issue facilities.
- Repair parts at installation-level supply activities and direct-support (DS) units with authorized stockage lists.
- Facilities-engineering supplies and construction materials.
- Audiovisual equipment, training devices, and subcaliber devices.
- Miscellaneous pilferable assets (not included above) and money.
- Mission-critical or high-risk personnel.
- General military and civilian populations.
- Industrial and utility equipment.
- Controlled cryptographic items.
- Sensitive information (included in TM 5-853-1, but not included in DA Pam 190-51).
- Arms, ammunition, and explosives (AA&E).
- Installation banks and finance offices.

RISK LEVELS

2-6. DA Pam 190-51 provides a procedure for determining risk levels—assessing the value of the assets to their users and the likelihood of

compromise. These factors are assessed by answering a series of questions leading to value and likelihood ratings.

2-7. Asset value is determined by considering the following three elements:

- The criticality of the asset for its user and the Army as a whole.
- How easily the asset can be replaced.
- Some measure of the asset's relative value.

2-8. The relative value differs for each asset. For some assets, the relative value is measured in terms of monetary cost.

2-9. The likelihood of the threat is assessed for each applicable aggressor category by considering the asset's value to the aggressor, the history of or potential for aggressors attempting to compromise the asset, and the vulnerability of the asset based on existing or planned protective measures.

REGULATORY REQUIREMENTS

2-10. The risk level is the basis for determining the required protective measures for assets covered in AR 190-51. For each asset type, there may be physical protective measures, procedural security measures, and terrorism counteraction measures. These measures are specified by risk level. The measures identified in AR 190-51 are the minimum regulatory measures that must be applied for the identified threat level. The minimum regulatory measures for AA&E are based on the risk category established in AR 190-11.

ANTITERRORISM/FORCE-PROTECTION CONSTRUCTION STANDARDS

2-11. In accordance with DOD Instruction 2000.16, the commanders in chief (CINCs) have developed standards for new construction and existing facilities to counter terrorism threat capabilities within the area of responsibility. These construction standards have specific requirements for such measures as standoff distance, perimeter barriers, building construction, and parking. The DOD construction standard provides for minimum standards that must be incorporated into all inhabited DOD structures regardless of the identified threat. These standards provide a degree of protection that will not preclude the direct effects of blast but will minimize collateral damage for buildings and people and will limit the progressive collapse of structures. These standards add relatively little cost, may facilitate future upgrades, and may deter acts of aggression. (All services have adopted common criteria and minimum standards to counter antiterrorism/force-protection [AT/FP] vulnerabilities and terrorism threats.) Protection to identified threat levels is described in the following paragraphs. Physical-security personnel must be familiar with the CINC and DOD AT/FP construction standards because these standards may affect elements of physical-security plans and how individual facilities are secured.

THREAT IDENTIFICATION

2-12. The threat must be described in specific terms to help determine the assets' vulnerabilities or to establish protective measures. This description should include the tactics that aggressors will use to compromise the asset (weapons, tools, and explosives are likely to be used in an attempt). For

example, the threat might be described as a moving vehicle bomb consisting of a 4,000-pound vehicle containing a 500-pound explosive. Another example would be a forced-entry threat using specific hand, power, or thermal tools. These types of threat descriptions (called the design-basis threat) can be used to design detailed protective systems to mitigate the attacks. TM 5-853-1 and DA Pam 190-51 contain procedures for establishing design-basis threat descriptions in the format described above. These procedures can be used together or separately. Threats listed in the TM will be summarized later in this chapter. When using the TM as a lone source or in conjunction with DA Pam 190-51, the following actions occur:

- When the TM process is used alone, the user goes through an identical process to that in DA Pam 190-51 up to the point where the risk level would be determined. In TM 5-853-1, the value and likelihood ratings are used differently than in DA Pam 190-51. The likelihood rating is used to determine the weapons, tools, and explosives that will be used by a particular aggressor in carrying out a specific tactic. In this procedure, higher likelihood ratings result in more severe mixes of weapons, tools, and explosives. The assumption is that the more likely the attack, the more resources the aggressor is likely to use in carrying out the attack.
- When the procedure in TM 5-853-1 is used in conjunction with the results of the DA Pam 190-51 risk analysis, the likelihood rating is taken directly from the risk analysis and applied as described above.

LEVEL OF PROTECTION

2-13. The level of protection applies to the design of a protective system against a specified threat (for example, a bomb, breaking and entering, pilfering, and so forth). The level of protection is based on the asset's value rating from either DA Pam 190-51 or TM 5-853-1. The level increases as the asset's value rating increases. There are separate levels of protection for each tactic. TM 5-853-1 provides detailed guidance on how to achieve the levels of protection, and Chapter 3 of this manual provides a summary of the levels of protection as they apply to various tactics.

VULNERABILITIES

2-14. Vulnerabilities are gaps in the assets' protection. They are identified by considering the tactics associated with the threat and the levels of protection that are associated with those tactics. Some vulnerabilities can be identified by considering the general design strategies for each tactic described in TM 5-853-1 and as summarized in Chapter 3 of this manual. The general design strategies identify the basic approach to protecting assets against specific tactics. For example, the general design strategy for forced entry is to provide a way to detect attempted intrusion and to provide barriers to delay the aggressors until a response force arrives. Vulnerabilities may involve inadequacies in intrusion-detection systems (IDSs) and barriers. Similarly, the general design strategy for a moving vehicle bomb is to keep the vehicle as far from the facility as possible and to harden the facility to resist the explosive at that distance. Vulnerabilities may involve limited standoff

distances, inadequate barriers, and building construction that cannot resist explosive effects at the applicable standoff distance.

PROTECTIVE MEASURES

2-15. Where vulnerabilities have been identified, protective measures must be identified to mitigate them. AR 190-13, AR 190-51, DA Pam 190-51, and TM 5-853-1 are effective tools for developing protective measures. The key to effective development of protective systems is a partnership between physical-security personnel and the installation engineers. Appendix E of this manual discusses information for office security, which should be listed in the physical-security plan (see Appendix F). Appendix G discusses personal-protection measures.

THE INTEGRATED PROTECTIVE SYSTEM

2-16. Protective systems integrate physical protective measures and security procedures to protect assets against a design-basis threat. The characteristics of integrated systems include deterrence, detection, defense, and defeat.

DETERRENCE

2-17. A potential aggressor who perceives a risk of being caught may be deterred from attacking an asset. The effectiveness of deterrence varies with the aggressor's sophistication, the asset's attractiveness, and the aggressor's objective. Although deterrence is not considered a direct design objective, it may be a result of the design.

DETECTION

2-18. A detection measure senses an act of aggression, assesses the validity of the detection, and communicates the appropriate information to a response force. A detection system must provide all three of these capabilities to be effective.

2-19. Detection measures may detect an aggressor's movement via an IDS, or they may detect weapons and tools via X-ray machines or metal and explosive detectors. Detection measures may also include access-control elements that assess the validity of identification (ID) credentials. These control elements may provide a programmed response (admission or denial), or they may relay information to a response force. Guards serve as detection elements, detecting intrusions and controlling access.

2-20. Nuclear, biological, and chemical (NBC) detection systems must be used to measure and validate acts of aggression involving WMD. NBC detection systems should also be used to communicate a warning.

DEFENSE

2-21. Defensive measures protect an asset from aggression by delaying or preventing an aggressor's movement toward the asset or by shielding the asset from weapons and explosives. Defensive measures—

- Delay aggressors from gaining access by using tools in a forced entry. These measures include barriers along with a response force.
- Prevent an aggressor's movement toward an asset. These measures provide barriers to movement and obscure lines of sight (LOSs) to assets.
- Protect the asset from the effects of tools, weapons, and explosives.

2-22. Defensive measures may be active or passive. Active defensive measures are manually or automatically activated in response to acts of aggression. Passive defensive measures do not depend on detection or a response. They include such measures as blast-resistant building components and fences. Guards may also be considered as a defensive measure.

DEFEAT

2-23. Most protective systems depend on response personnel to defeat an aggressor. Although defeat is not a design objective, defensive and detection systems must be designed to accommodate (or at least not interfere with) response-force activities.

SECURITY THREATS

2-24. Security threats are acts or conditions that may result in the compromise of sensitive information; loss of life; damage, loss, or destruction of property; or disruption of mission. Physical-security personnel and design teams must understand the threat to the assets they are to protect in order to develop effective security programs or design security systems. Historical patterns and trends in aggressor activity indicate general categories of aggressors and the common tactics they use against military assets. Aggressor tactics and their associated tools, weapons, and explosives are the basis for the threat to assets.

THREAT SOURCES

2-25. There are many potential sources of threat information. Threat assessment is normally a military-intelligence (MI) responsibility. MI personnel commonly focus on such security threats as terrorists and military forces. Within the US and its territories, the Federal Bureau of Investigation (FBI) has primary responsibility for both foreign and domestic terrorists. The FBI, the US Army Criminal Investigation Command (USACIDC [CID]), and local law-enforcement agencies are good sources for physical-security personnel to obtain criminal threat information. Coordinating with these elements on a regular basis is essential to maintaining an effective security program.

THREAT CATEGORIES

2-26. Security threats are classified as either human or natural. Human threats are carried out by a wide range of aggressors who may have one or more objectives toward assets such as equipment, personnel, and operations. Aggressors can be categorized and their objectives can be generalized as described below. (See DA Pam 190-51 and TM 5-853-1 for more information.)

Aggressor Objectives

2-27. Four major objectives describe an aggressor's behavior. Any one of the first three objectives can be used to realize the fourth. These objectives include—

- Inflicting injury or death on people.
- Destroying or damaging facilities, property, equipment, or resources.
- Stealing equipment, materiel, or information.
- Creating adverse publicity.

Aggressor Categories

2-28. Aggressors are grouped into five broad categories—criminals, vandals and activists, extremists, protest groups, and terrorists. Hostile acts performed by these aggressors range from crimes (such as burglary) to low-intensity conflict threats (such as unconventional warfare). Each of these categories describes predictable aggressors who pose threats to military assets and who share common objectives and tactics.

- Criminals can be characterized based on their degree of sophistication. They are classified as unsophisticated criminals, sophisticated criminals, and organized criminal groups. Their common objective is the theft of assets; however, the assets they target, the quantities they seek, their relative efficiency, and the sophistication of their actions vary significantly. Vandals and activists may also be included under this category.
- Vandals and activists are groups of protesters who are politically or issue oriented. They act out of frustration, discontent, or anger against the actions of other social or political groups. Their primary objectives commonly include destruction and publicity. Their selection of targets will vary based on the risk associated with attacking them. The degree of damage they seek to cause will vary with their sophistication.
- Extremists are radical in their political beliefs and may take extreme, violent actions to gain support for their beliefs or cause.
- Protesters are considered a threat only if they are violent. Lawful protesters have to be considered, but significant protective measures and procedures are not normally needed to control their actions. The presence of extremists or vandals/activists at a peaceful protest increases the chance of the protest becoming violent.
- Terrorists are ideologically, politically, or issue oriented. They commonly work in small, well-organized groups or cells. They are sophisticated, are skilled with tools and weapons, and possess an efficient planning capability. There are three types of terrorists—CONUS, OCONUS, and paramilitary OCONUS.
 - CONUS terrorists are typically right- or left-wing extremists operating in distinct areas of the US.
 - OCONUS terrorists generally are more organized than CONUS terrorists. They usually include ethnically or religiously oriented groups.

- Paramilitary OCONUS terrorist groups show some military capability with a broad range of military and improvised weapons. Attacks by OCONUS terrorists are typically more severe.

2-29. Natural threats are usually the consequence of natural phenomena. They are not preventable by physical-security measures, but they are likely to have significant effects on security systems and operations. They may require an increase in protective measures either to address new situations or to compensate for the loss of existing security measures. They may reduce the effectiveness of existing security measures by such occurrences as collapsed perimeter fences and barriers, inoperable protective lighting, damaged patrol vehicles, and poor visibility. Natural threats and their effects relative to security include the following:

- Floods may result in property damage, destruction of perimeter fences, and damage to IDSs. Heavy rains or snowfalls may have similar effects even if they do not result in flooding.
- Storms, tornadoes, high winds, or rain may cause nuisance alarms to activate and cause damage to IDSs. They may limit the visibility of security personnel and may affect closed-circuit television (CCTV) systems. Winds may also disrupt power or communication lines and cause safety hazards from flying debris.
- Earthquakes may cause nuisance alarms to activate or may disrupt IDSs. They may also cause broken water or gas mains, fallen electrical or communication lines, and weakened or collapsed buildings.
- Snow and ice can make travel on patrol roads difficult, may delay responses to alarms, may impede the performance of IDSs, and may freeze locks and alarm mechanisms. Heavy ice may also damage power and communication lines.
- Fires may damage or destroy perimeter barriers and buildings, possibly leaving assets susceptible to damage or theft.
- Fog can reduce the visibility of security forces, thereby requiring additional security personnel. It may also increase the response time to alarms and reduce the effectiveness of security equipment such as CCTV systems.

Aggressor Tactics

2-30. Aggressors have historically used a wide range of offensive strategies reflecting their capabilities and objectives. These offensive strategies are categorized into 15 tactics that are specific methods of achieving aggressor goals (see TM 5-853-1). Separating these tactics into categories allows facility planners and physical-security personnel to define threats in standardized terms usable as a basis for facility and security-system design. Common aggressor tactics include—

- **Moving vehicle bomb.** An aggressor drives an explosive-laden car or truck into a facility and detonates the explosives. His goal is to damage or destroy the facility or to kill people. This is a suicide attack.
- **Stationary vehicle bomb.** An aggressor covertly parks an explosive-laden car or truck near a facility. He then detonates the explosives either by time delay or remote control. His goal in this tactic is the

same as for the moving vehicle bomb with the additional goal of destroying assets within the blast area. This is commonly not a suicide attack. It is the most frequent application of vehicle bombings.

- **Exterior attack.** An aggressor attacks a facility's exterior or an exposed asset at close range. He uses weapons such as rocks, clubs, improvised incendiary or explosive devices, and hand grenades. Weapons (such as small arms) are not included in this tactic, but are considered in subsequent tactics. His goal is to damage the facility, to injure or kill its occupants, or to damage or destroy assets.
- **Standoff weapons.** An aggressor fires military weapons or improvised versions of military weapons at a facility from a significant distance. These weapons include direct (such as antitank [AT] weapons) and indirect LOS weapons (such as mortars). His goal is to damage the facility, to injure or kill its occupants, or to damage or destroy assets.
- **Ballistics.** The aggressor fires various small arms (such as pistols, submachine guns, shotguns, and rifles) from a distance. His goal is to injure or kill facility occupants or to damage or destroy assets.
- **Forced entry.** The aggressor forcibly enters a facility using forced-entry tools (such as hand, power, and thermal tools) and explosives. He uses the tools to create a man-passable opening or to operate a device in the facility's walls, doors, roof, windows, or utility openings. He may also use small arms to overpower guards. His goal is to steal or destroy assets, compromise information, injure or kill facility occupants, or disrupt operations.
- **Covert entry.** The aggressor attempts to enter a facility or a portion of a facility by using false credentials or stealth. He may try to carry weapons or explosives into the facility. His goals include those listed for forced entry.
- **Insider compromise.** A person authorized access to a facility (an insider) attempts to compromise assets by taking advantage of that accessibility. The aggressor may also try to carry weapons or explosives into the facility in this tactic. His goals are the same as those listed for forced entry.
- **Visual surveillance.** The aggressor uses ocular and photographic devices (such as binoculars and cameras with telephoto lenses) to monitor facility or installation operations or to see assets. His goal is to compromise information. As a precursor, he uses this tactic to determine information about the asset of interest.
- **Acoustic eavesdropping.** The aggressor uses listening devices to monitor voice communications or other audibly transmitted information. His goal is to compromise information.
- **Electronic-emanations eavesdropping.** The aggressor uses electronic-emanation surveillance equipment from outside a facility or its restricted area to monitor electronic emanations from computers, communications, and related equipment. His goal is to compromise information.

- **Mail-bomb delivery.** The aggressor delivers bombs or incendiary devices to the target in letters or packages. The bomb sizes involved are relatively small. His goal is to kill or injure people.
- **Supplies-bomb delivery.** The aggressor conceals bombs in various containers and delivers them to supply- and material-handling points such as loading docks. The bomb sizes in this tactic can be significantly larger than those in mail bombs. His goal is to damage the facility, kill or injure its occupants, or damage or destroy assets. Appendix H addresses the actions to take when a bomb is suspected.
- **Airborne contamination.** An aggressor contaminates a facility's air supply by introducing chemical or biological agents into it. His goal is to kill or injure people.
- **Waterborne contamination.** An aggressor contaminates a facility's water supply by introducing chemical, biological, or radiological agents into it. These agents can be introduced into the system at any location with varying effects, depending on the quantity of water and the contaminant involved. His goal is to kill or injure people.

2-31. The aforementioned tactics are typical threats to fixed facilities for which designers and physical-security personnel can provide protective measures. However, some common terrorist acts are beyond the protection that facility designers can provide. They cannot control kidnappings, hijackings, and assassinations that take place away from facilities or during travel between facilities. Protection against these threats is provided through operational security and personal measures (see Appendices G and I), which are covered in doctrine relative to those activities and are under the general responsibility of the CID.

TACTICAL ENVIRONMENT CONSIDERATIONS

2-32. When determining the assets and threats, the same considerations should be given to the systems approach in the tactical environment as when in the cantonment area. The same process of determining the assets, their risk level, and any regulatory guidance apply. Identifying potential threats and the level of protection required for the assets are necessary. Commanders and leaders must also identify additional vulnerabilities and other required protective measures. Commanders are not expected to have the same physical protective measures due to the impact of resources, budget, location, and situations.

2-33. Commanders must consider the various tactics used by aggressors and use their soldiers' abilities to counteract these tactics. Considerations for specific assets (such as military-working-dog [MWD] and explosive-ordnance-disposal [EOD] teams and their abilities to detect and disassemble a bomb) must be identified. Units must have the ability to improvise in a tactical environment. Their training and resourcefulness will compensate for shortcomings in the field.

2-34. The systems approach to security provides focus and integration of resources. Protective systems are mutually supporting and systematically developed to negate the threat. Commanders conduct an intelligence preparation of the battlefield (IPB) and vulnerability assessments (VAs) to determine risks. Security resources and measures are applied to mitigate risks and to deter, detect, defend, and defeat the threat.

Chapter 3

Design Approach

Developing protective systems to protect assets depends on an effective partnership between engineers and physical-security personnel. Physical-security personnel need to understand the basic approaches the engineers will take in laying out protective systems. Engineers must understand the issues involved with ensuring that anything they lay out is compatible with security operations and the operations of the asset users. The best way to ensure a viable design is through teamwork. This chapter provides a summary of the basic approaches to protecting assets against threats (the design strategies). Understanding these strategies is critical to being an effective team member in developing protective systems.

DESIGN STRATEGIES

3-1. There are separate design strategies for protecting assets from each tactic described in Chapter 2. There are two types of strategies associated with each tactic—the general-design and specific-design strategies. The general-design strategy is the general approach to protecting assets against tactics. The specific-design strategy refines the general-design strategy to focus the performance of the protective system on a particular level of protection. (See TM 5-853-1 for more information.)

PROTECTIVE MEASURES

3-2. Protective measures are developed as a result of the general- and specific-design strategies. These protective measures commonly take the form of site-work, building, detection, and procedural elements.

- Site-work elements include the area surrounding a facility or an asset. Technically, they are associated with everything beyond 5 feet from a building. They can include perimeter barriers, landforms, and standoff distances.
- Building elements are protective measures directly associated with buildings. These elements include walls, doors, windows, and roofs.
- Detection elements detect such things as intruders, weapons, or explosives. They include IDSs, CCTV systems used to assess intrusion alarms, and weapon and explosive detectors. These elements can also include the guards used to support this equipment or to perform similar functions.
- Procedural elements are the protective measures required by regulations, TMs, and standing operating procedures (SOPs). These elements provide the foundation for developing the other three elements.

VEHICLE BOMBS

3-3. Vehicle-bomb tactics include both moving and stationary vehicle bombs. In the case of a moving vehicle bomb, the aggressor drives the vehicle into the target. This is commonly known as a suicide attack. In a stationary vehicle bomb, he parks the vehicle and detonates the bomb remotely or on a timed delay.

GENERAL-DESIGN STRATEGY

3-4. Blast pressures near an exploding vehicle bomb are very high, but they decrease rapidly with distance from the explosion. The design strategy for these tactics is to maintain as much standoff distance as possible between the vehicle bomb and the facility and then, if necessary, to harden the facility for the resulting blast pressures. Barriers on the perimeter of the resulting standoff zone maintain the required standoff distance. The difference between moving and stationary vehicle-bomb tactics is that the aggressor using the moving vehicle bomb will attempt to crash through the vehicle barriers; the aggressor using the stationary vehicle bomb will not. Therefore, vehicle barriers for the moving vehicle bomb must be capable of stopping a moving vehicle at the perimeter of the standoff zone. For a stationary vehicle bomb, vehicle barriers must mark the perimeter of the standoff zone, but they are not required to stop the moving vehicle. They only need to make it obvious if an aggressor attempts to breach the perimeter.

LEVELS OF PROTECTION

3-5. There are three levels of protection for vehicle bombs—low, medium, and high. The primary differences between the levels are the degree of damage allowed to the facility protecting the assets and the resulting degree of damage or injury to the assets.

- **Low.** The facility or the protected space will sustain a high degree of damage but will not collapse. It may not be economically repairable. Although collapse is prevented, injuries may occur and assets may be damaged.
- **Medium.** The facility or the protected space will sustain a significant degree of damage, but the structure will be reusable. Occupants and other assets may sustain minor injuries or damage.
- **High.** The facility or the protected space will sustain only superficial damage. Occupants and other assets will also incur only superficial injury or damage.

SITE-WORK ELEMENTS

3-6. The two primary types of site-work elements for vehicle bombs are the standoff distance and vehicle barriers. The vehicle's speed must also be taken into consideration.

Standoff Distance

3-7. The standoff distance is the maintained distance between where a vehicle bomb is allowed and the target. The initial goal should be to make that distance

as far from the target facility as practical. Figure 3-1 shows the distances required to limit building damage to particular levels (including the levels of protection described above) for a range of bomb weights. All bomb weights are given in terms of equivalent pounds of trinitrotoluene (TNT), which is a standard way of identifying all explosives regardless of their composition. The example in Figure 3-1 is a building of conventional construction (common, unhardened construction). Buildings built without any special construction at these standoff distances will probably withstand the explosive effects. Conventionally constructed buildings at standoff distances of less than those shown in Figure 3-1 will not adequately withstand blast effects. (Refer to TM 5-853-1 for information on hardening buildings to resist a blast.) Do not allow vehicles to park within the established standoff distances. Recognize that this restriction can result in significant operational and land-use problems.

3-8. Exclusive Standoff Zone. When an exclusive standoff zone is established, do not allow vehicles within the perimeter unless they have been searched or cleared for access. The zone's perimeter is established at the distance necessary to protect the facility against the highest threat explosive. All vehicles should be parked outside the exclusive standoff zone; only

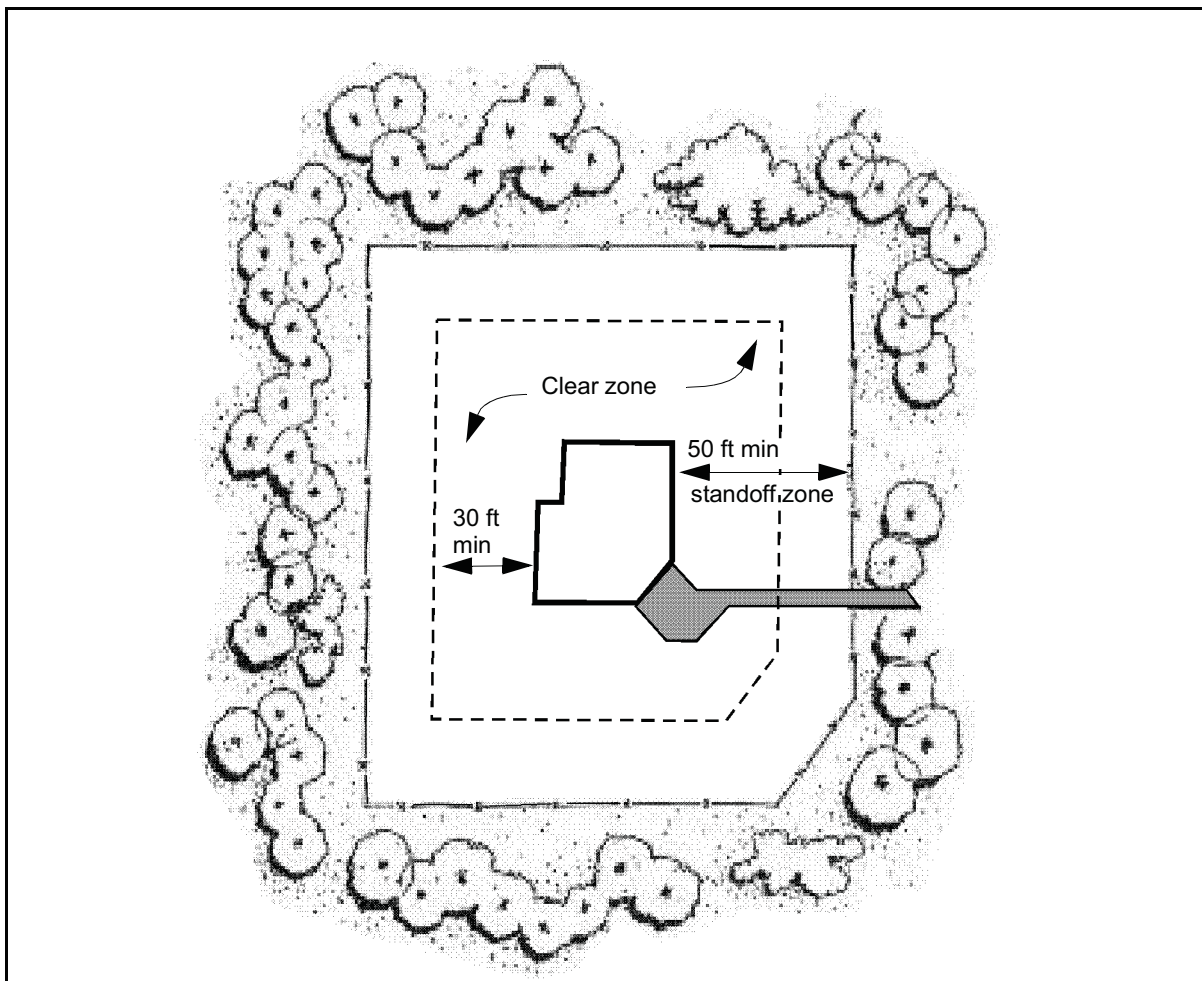


Figure 3-1. Standoff Distance

maintenance, emergency, and delivery vehicles should be allowed within the zone after being searched. Figure 3-2 shows an exclusive standoff zone.

3-9. Nonexclusive Standoff Zone. A nonexclusive standoff zone is established in a location having a mixture of cars and trucks (with relatively few trucks). A nonexclusive standoff zone takes advantage of aggressors being able to conceal a smaller quantity of explosives in a car than they can in a truck. Therefore, a nonexclusive standoff zone includes inner and outer perimeters. The inner perimeter is set at a distance corresponding to the weight of explosives that can be concealed in cars. The outer perimeter is set at a distance associated with the weight that can be placed in trucks (refer to TM 5-853-1). With these two perimeters, cars can enter the outer perimeter without being searched but they cannot enter the inner perimeter. Trucks cannot enter the outer perimeter, since it is established based on what they can carry. Figure 3-3 shows a nonexclusive standoff zone. The nonexclusive standoff zone provides the advantages of allowing better use of the parking areas and limiting the number of vehicles that need to be searched at the outer perimeter.

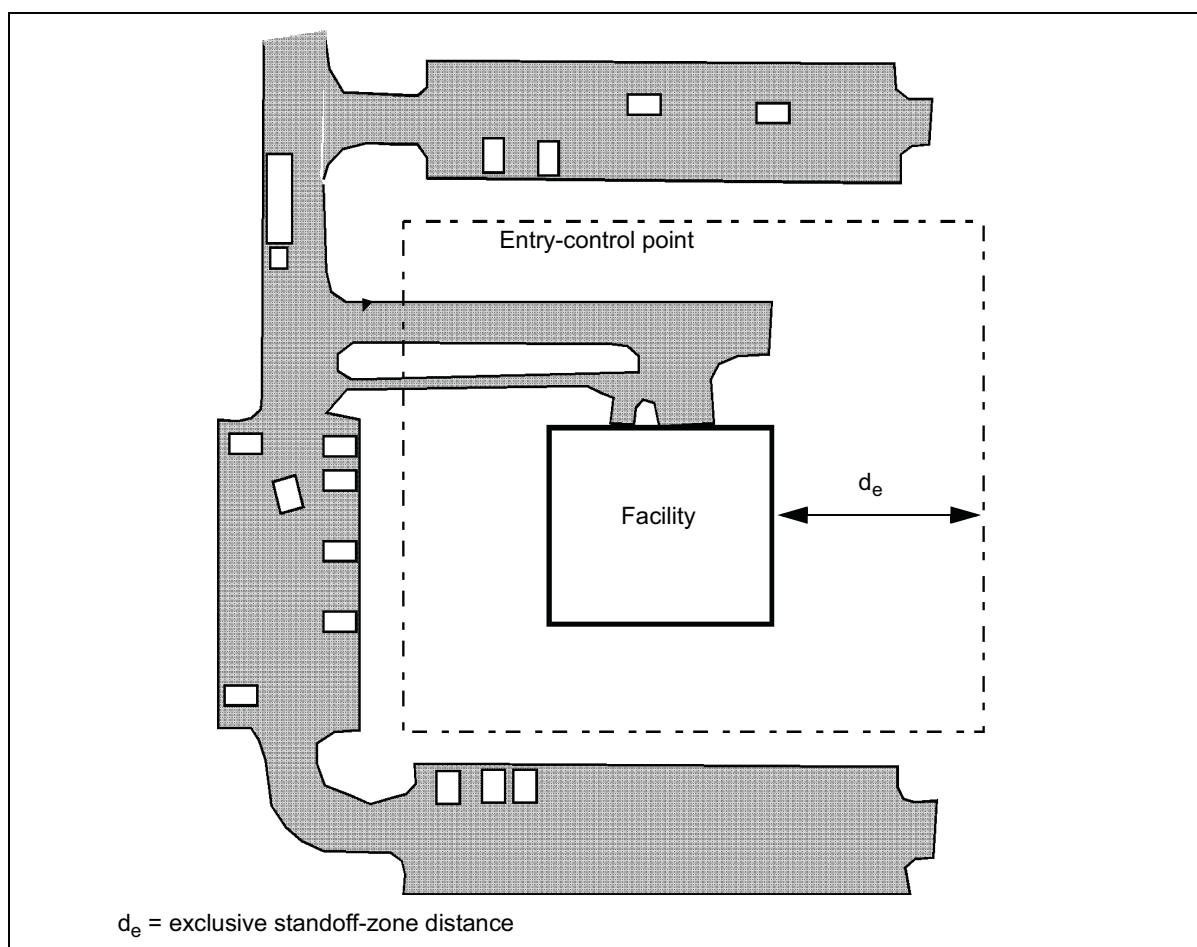


Figure 3-2. Exclusive Standoff Zone

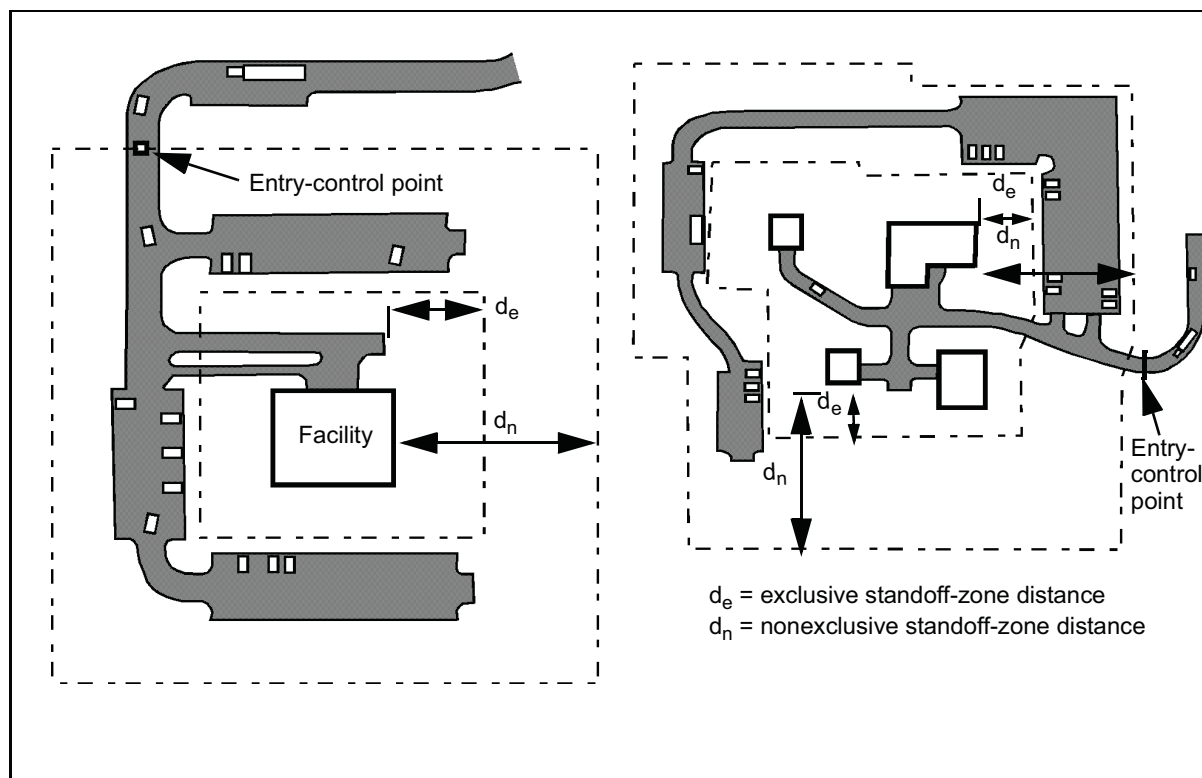


Figure 3-3. Nonexclusive Standoff Zone

Vehicle Barriers

3-10. Two types of vehicle barriers are used for vehicle bombs—perimeter and active barriers. The type of barrier used for a moving vehicle bomb differs from the barrier used for a stationary vehicle bomb. The barrier used for a stationary vehicle bomb does not have to stop a vehicle's motion. The goal for that barrier is to make anybody driving through the barrier noticeable. The assumption is that the aggressor's goal in the stationary vehicle bomb is to park the vehicle and sneak away without being noticed. Crashing through a barrier would be noticeable. Barriers for the moving vehicle bomb need to stop the vehicle's motion; they must be much more substantial.

3-11. **Perimeter Barriers.** Perimeter barriers are fixed barriers placed around the entire perimeter of a standoff zone. Anything that presents a fixed obstacle will work for the stationary vehicle bomb. Common applications include chain-link fences, hedges made of low bushes, and high (over 8 inches) curbs. Aggressors driving through such barriers are likely to be noticed. Barriers capable of stopping moving vehicles include chain-link fences reinforced with cable, reinforced concrete "Jersey barriers", pipe bollards, planters, ditches, and berms. When barriers such as the Jersey barriers and planters are used to stop moving vehicles, they must be anchored into the ground to be effective. The cables in the reinforced fence also have to be anchored into the ground or partially buried. Spaces between barriers should

be no greater than 4 feet. Figure 3-4 shows common perimeter barriers for stationary or moving vehicle bombs. Refer also to TM 5-853-1.

3-12. Active Barriers. Active barriers are placed at openings in perimeters where vehicles need to enter or exit. These barriers must be able to be raised and lowered or moved aside. For the stationary vehicle bomb, barriers can be as simple as chain-link, pipe, or wooden gates that can be raised and lowered. Aggressors crashing through any of these or similar obstructions will likely draw attention. For the moving vehicle bomb, the barriers are heavy structures and have many construction and operations considerations

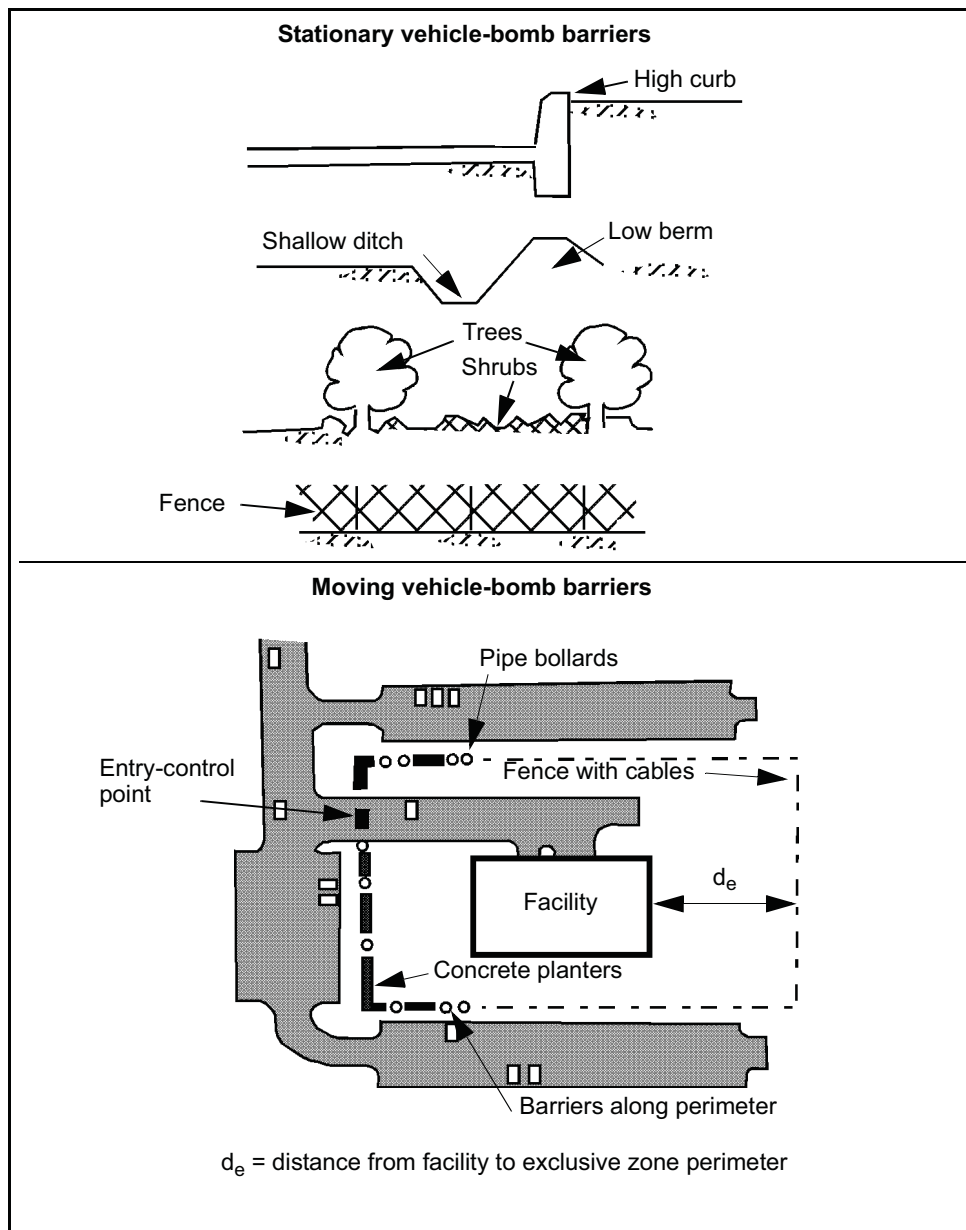


Figure 3-4. Perimeter-Barrier Application

associated with them. These barriers may stop vehicles weighing up to 15,000 pounds and travelling 50 miles per hour. They commonly cost tens of thousands of dollars (refer to TM 5-853-1). Some common active vehicle barriers are shown in Figure 3-5. For temporary or deployed conditions, park a vehicle across an opening and move it aside to grant access.

Speed Control

3-13. It is important to control the speed of a vehicle approaching a barrier used for a moving vehicle bomb. The energy from a vehicle that a barrier must stop increases as its speed increases. The energy also increases with more weight, but the effect of speed is much greater. Therefore, decreasing the vehicle's speed results in smaller and less costly barriers. The best way to limit a vehicle's approach speed to perimeter barriers is to place or retain obstacles in potential approach paths. The vehicles are forced to reduce speed when going around these obstacles. The same principle applies for road approaches. Placing obstacles in a serpentine pattern on the road forces a vehicle to reduce its speed (see Figure 3-6, page 3-8). If the vehicle hits the obstacles instead of going around them, they are still slowed down. Other means to slow vehicles include forcing them to make sharp turns and installing traffic circles.

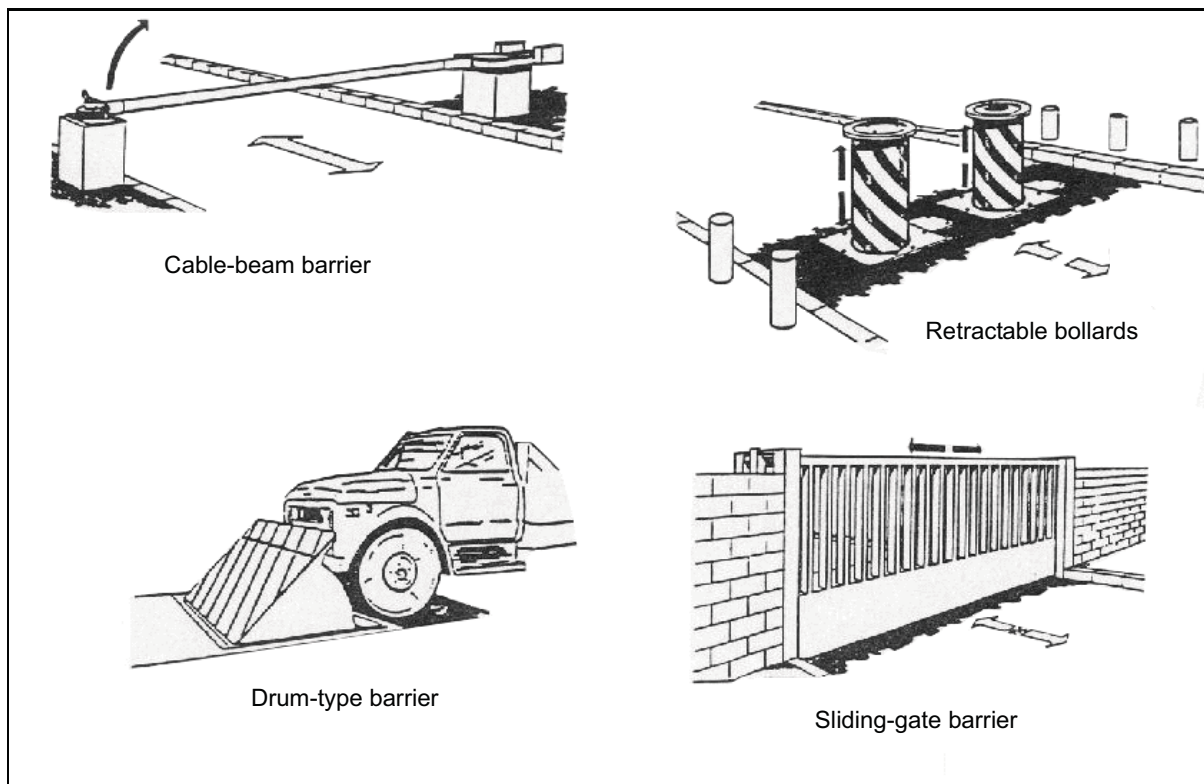


Figure 3-5. Active Vehicle Barriers

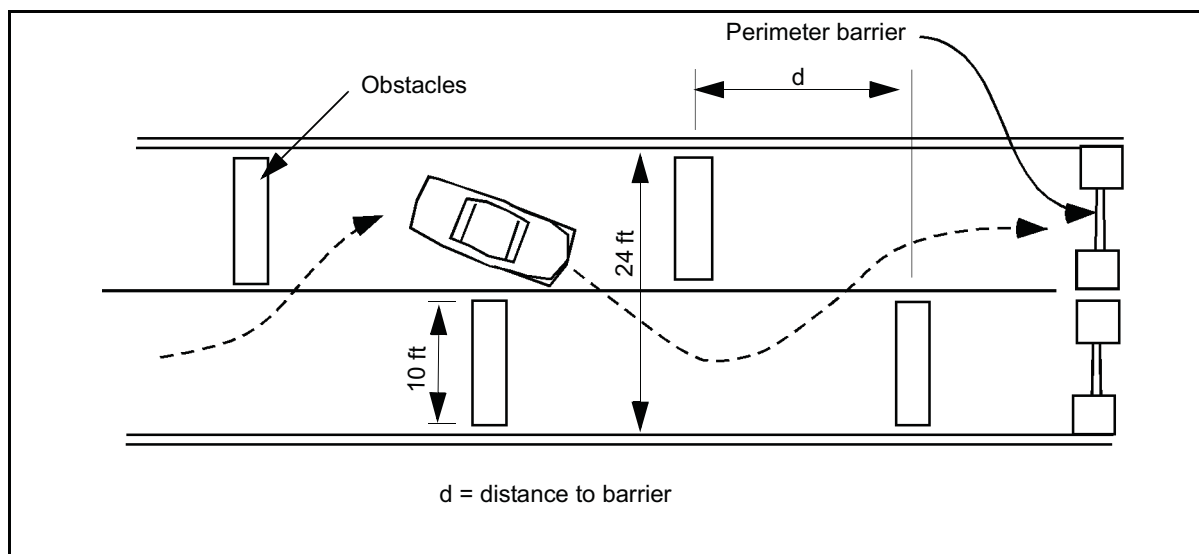


Figure 3-6. Serpentine Pattern

BUILDING ELEMENTS

3-14. Once the standoff distance is established and the site has been laid out, the designers can select the building components necessary to protect the assets against the threat explosives at the standoff distance. The building components include the walls, roofs, doors, and windows. Detailed design issues related to these building elements are covered in TM 5-853-1.

Walls and Roofs

3-15. If the distances shown for the desired damage levels in Figure 3-1, page 3-3, cannot be enforced, the building's walls and roofs will need to be strengthened. This can be achieved in new construction by using reinforced masonry or reinforced concrete in the walls and reinforced concrete in the roof. When the standoff distance is not available for existing construction, a more detailed analysis may be required to determine what the explosion's impact will be on the structure. When the construction is inadequate, more standoff distance should be investigated or the engineers should apply specialized techniques for retrofitting the construction to increase its strength.

Windows

3-16. Historically, glass fragments have caused about 85 percent of injuries and deaths in bomb blasts. There are two basic approaches to mitigating the effects of bomb blasts on glass—retrofitting the windows with film or curtains and using blast-resistant glazing.

3-17. **Retrofitting Windows.** One of the most common means of decreasing the hazards from broken glass is to install fragment-retention film on the glass. The film is a plastic (polyester) sheet that adheres to the window glass with a special adhesive. The film does not strengthen the glass; but when the glass breaks, it keeps the fragments from spreading throughout the room. The

glass fragments stick to the film, and the film either stays in the window frame or falls into the room in one or more large, relatively nonhazardous pieces instead of many small, lethal pieces. Another retrofit approach is to install a blast curtain or a heavy drape behind the window. The curtain or drape catches the glass fragments. The curtains are generally used with fragment-retention film. Another retrofit technique is to use fragment-retention film with a metal bar placed across the window. This “catcher bar” catches the window. The designs for this and other types of retrofit devices are complicated and require specialized engineering-analysis tools. The retrofit techniques are generally thought of as providing a lower level of protection than the glazing replacement techniques. For deployed locations, removing the windows and covering them with plywood minimizes the danger.

3-18. Blast-Resistant Glazing. To achieve higher levels of protection, the window glass must be replaced and the window frame should be reinforced. Because of its expense, this procedure is generally limited to new construction and major renovations. Special blast-resistant glazing and frames are available that use either tempered glass or a plastic glazing (such as polycarbonate). Another promising type of blast-resistant glazing is laminated glass, in which several layers of common glass are adhered together with a special interlayer. The resulting laminated construction is usually stronger than common glass while retaining the same thickness. The interlayer acts similarly to fragment-retention film. For deployed locations, a means of minimizing the danger of windows is to remove them and replace them with plywood.

Doors

3-19. Doors are another building component particularly vulnerable to an explosive blast. Common metal and wood doors provide little resistance to a blast. The two ways to address the problem of doors is to install them in foyers or to replace them. Glass doors or doors containing windows should be avoided.

Foyers

3-20. Door hazards can be reduced by installing doors in foyers during construction or by adding foyers to existing buildings. When a door is located in a foyer and the outer door fails, the outer door flies into a wall instead of the building's interior (see Figure 3-7, page 3-10). The inner door then has a greater chance of remaining intact. This option generally provides a low level of protection.

3-21. Another option is to replace the doors with specially constructed blast-resistant doors and frames. These doors are commercially available and can provide a high level of protection, but they are very expensive and heavy. The doorframe must be made of the same type of material and provide the same level of protection as the door.

DETECTION ELEMENTS

3-22. Detection elements for vehicle bombs are limited to the use of guards to control access into standoff zones. The guards search vehicles seeking entry

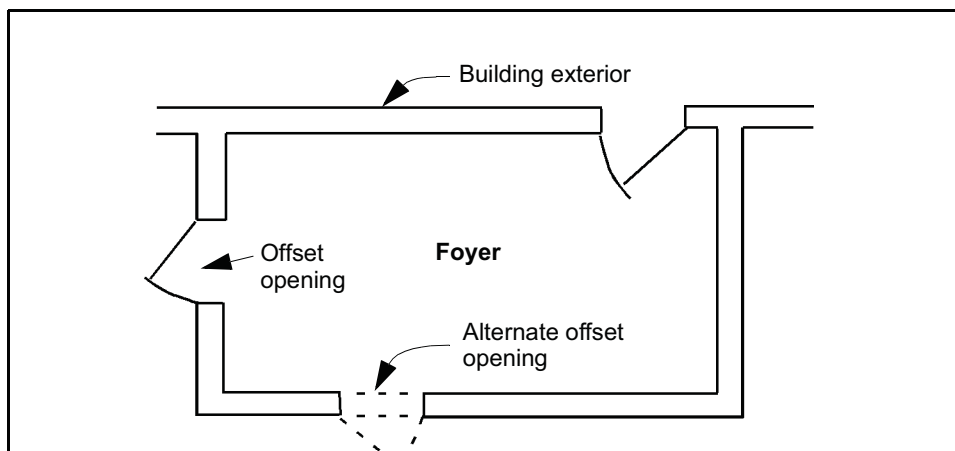


Figure 3-7. Door in Foyer

into the perimeter through an entry-control point. The recommended levels of searches depend on the required level of protection (see TM 5-853-1). Guards can be stationed at entry-control points continuously, or they can be summoned to an entry-control point when access is needed. The latter is commonly the case for the inner perimeter of exclusive standoff zones where only delivery and maintenance vehicles need access.

EXTERIOR ATTACK

3-23. An exterior attack is a physical attack using weapons such as rocks, clubs, improvised incendiary devices (IIDs) such as Molotov cocktails, explosives such as improvised explosive devices (IEDs), and hand grenades. The explosives can be thrown at or placed near a facility's exterior. Examples of IEDs for this tactic range from pipe bombs and hand grenades to briefcase-sized explosives.

GENERAL-DESIGN STRATEGY

3-24. Because the exterior attack is directed at a facility's exterior surfaces, the general-design strategy is to keep aggressors away from the facility (at a standoff distance) and, if necessary, to harden the facility's exterior components to resist the effects of weapons and explosives. A standoff distance from the facility reduces the degree of hardening required to resist weapons effects. When briefcase-sized bombs are a threat, an obstacle-free zone should be established around the facility and the explosives placed within should be detected and disarmed.

LEVELS OF PROTECTION

3-25. The levels of protection for exterior attacks are similar to those for vehicle bombs. Levels of protection vary based on the level of building damage and asset injury or damage allowed. However, due to the limited sizes of explosives involved in this tactic, the damage to the building will be much more localized and injuries or damage to assets will be confined to smaller areas.

SITE-WORK ELEMENTS

3-26. Site-work elements for exterior attacks are relatively limited because the explosive weights are more limited. Large standoff distances are not a consideration. The common approach to site-work elements is to lay out a standoff zone of about 50 feet and to provide a fence or perimeter barrier about 7 feet high. The purpose of the standoff is to make it harder for aggressors to throw pipe bombs and hand grenades at targets inside the perimeter. Trees can be left around the perimeter to make it harder for aggressors to throw explosives over the fence. The remaining component of site-work elements is a clear zone around the facility. A clear zone is applied so that anything placed in that area can be detected visually. This limits the aggressor's ability to place explosives near the target facility.

BUILDING ELEMENTS

3-27. Building elements for exterior attacks are similar to those for vehicle bombs. For small IEDs and IIDs, the building-element requirements do not increase the cost of the building significantly. For larger, briefcase-sized bombs, the measures are more significant than for incendiary devices but less than for vehicle bombs.

Walls and Roofs

3-28. Walls and roofs are not a problem with small explosives. Conventional construction normally provides adequate protection. Walls with 6-inch reinforced concrete or 8-inch, grout-filled, reinforced masonry will withstand the effects of typical pipe bombs or hand grenades. The corresponding roof construction is 6-inch reinforced concrete. In the case of briefcase-sized bombs, considerations similar to those discussed for vehicle bombs need to be employed.

Windows

3-29. A significant goal when constructing windows is to make them difficult to throw an explosive or incendiary device through, especially when considering smaller explosives. This is accomplished by constructing smaller windows or making narrow windows (see Figure 3-8, page 3-12). For existing windows, parts of the windows can be covered to achieve a narrow effect. These windows still may be susceptible to breakage due to explosive effects, even from the smaller explosives. This problem is solved by installing 3/4-inch-thick plastic (polycarbonate) glazing or by raising the windows over 6 feet high to develop a small standoff distance (as shown in Figure 3-9, page 3-12). A 3/4-inch glazing will also stop grenade fragments. Fragment-retention film, a blast curtain, or a heavy drape as described in vehicle-bomb tactics are also good applications for small bombs.

Conventionally Constructed Doors

3-30. Doors are not a significant problem with small bombs and incendiary devices. Generally, metal doors are adequate for incendiary devices, and doors placed in foyers (as shown in Figure 3-7) are adequate for pipe bombs and hand grenades. A similar application for briefcase-sized bombs would provide

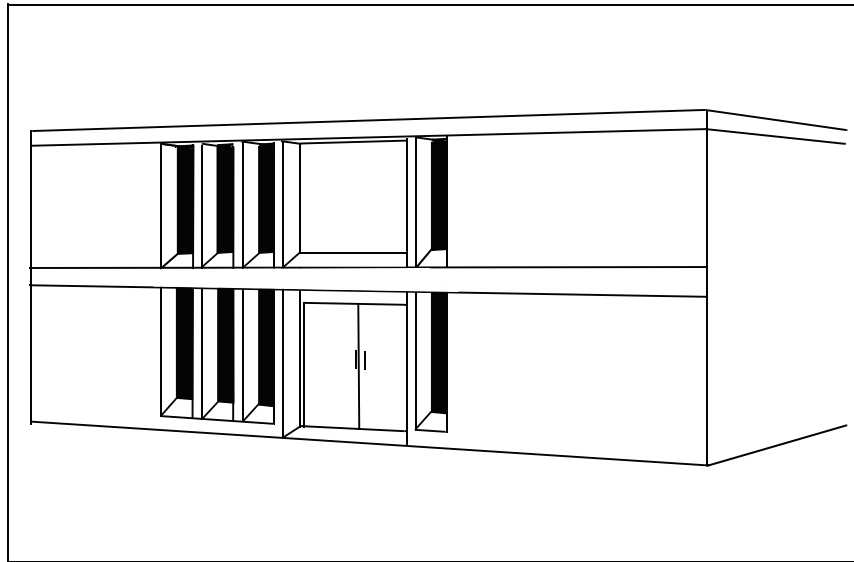


Figure 3-8. Narrow Recessed Windows

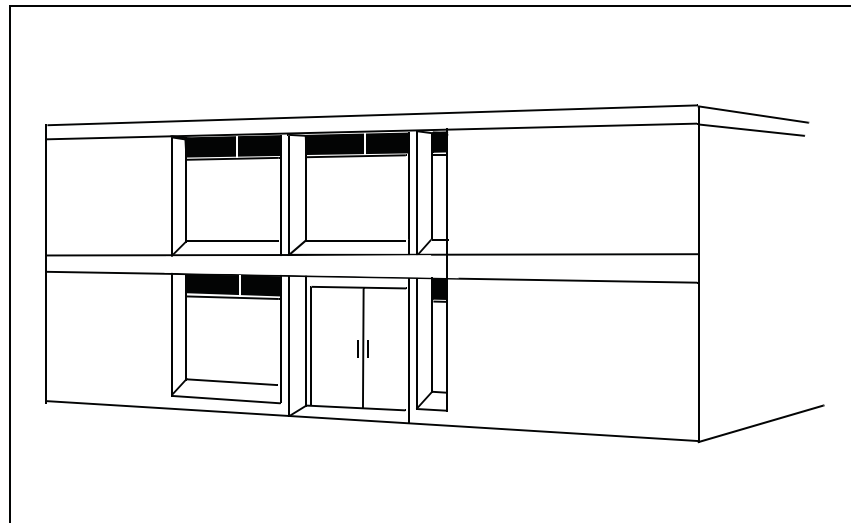


Figure 3-9. Narrow Raised Windows

only a low level of protection. To achieve higher levels of protection for briefcase-sized bombs, blast-resistant doors must be installed.

3-31. The requirements to meet the levels of protection for larger explosives are similar to those described for vehicle bombs, but they will not stop grenade fragments. Fragment-retention film and drapes or curtains can provide a low

level of protection, but blast-resistant glazing is required to achieve a higher level of protection.

DETECTION ELEMENTS

3-32. Other than awareness of aggressor activity on or outside the site, detection is only a specific design goal where briefcase-sized bombs are anticipated. When that is the case, the clear zone around the building must be visually monitored so that any objects placed in it are detected. At higher levels of protection, visual surveillance is augmented by IDSs.

STANDOFF WEAPONS

3-33. The standoff-weapons tactic includes the use of AT weapons and mortars. In both of these tactics, the aggressor fires weapons at assets located in the protected facility from a distance. An AT-weapon attack requires a clear LOS to the target, while mortars can fire over obstacles and only need a clear line of flight.

GENERAL-DESIGN STRATEGY

3-34. Standoff-weapons attacks cannot be detected reliably before they occur. Protective design to resist these tactics relies on blocking LOSs to protected areas of a facility or hardening the facility to resist the particular weapon's effects. The approaches to protection against mortars and AT weapons differ from each other and will be discussed separately. Detection measures are not applicable for these tactics.

LEVELS OF PROTECTION

3-35. There are two levels of protection against both mortars and AT weapons. For AT weapons, the low level of protection depends on detonating the AT round before it hits the target facility. The high level of protection avoids the risk associated with that and hardens the building to resist the direct impact of the AT round.

3-36. For mortars, the low level of protection involves allowing some areas of the facility to be sacrificed. Those spaces provide a buffer to the assets to be protected. The assets within the sacrificial areas and the areas themselves may be destroyed. At the high level of protection, the building's exterior fully resists the mortar rounds and there are no sacrificial areas.

SITE-WORK ELEMENTS

3-37. The primary site-work element for standoff weapons is to obstruct LOSs from vantage points outside of the site. With AT weapons, the aggressor cannot hit what he cannot see. This is not true with mortars, but blocking LOSs from mortar firing points helps to make targeting more difficult. The LOSs are blocked by using trees, other buildings, vehicle parking areas, or fences. Another site-work element, a predetonation screen, applies only to an AT weapon. When using a predetonation screen, the AT round is detonated on the screen and its effects are dissipated in the distance between the screen and the target (see Figure 3-10, page 3-14). Any screen material (such as a

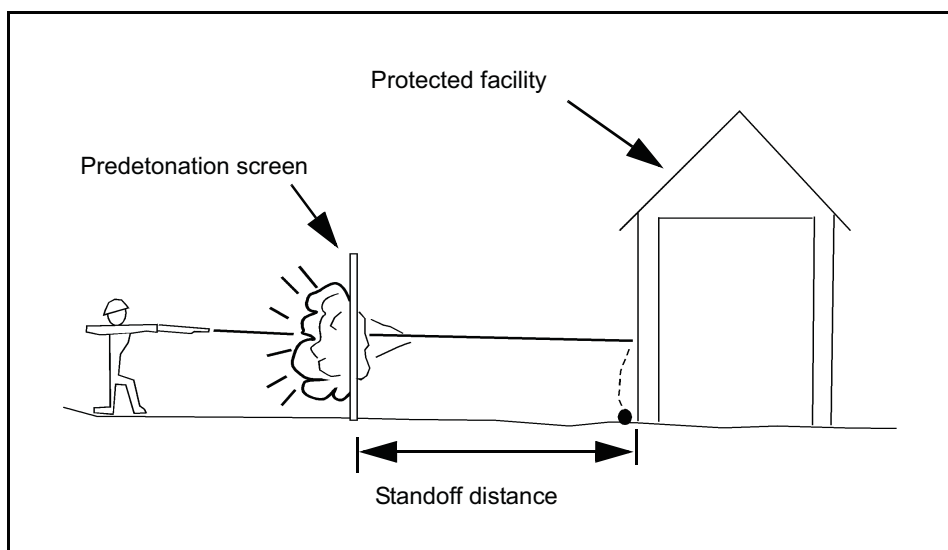


Figure 3-10. Predetonation Screen

wooden fence) will detonate the round unless it has spaces in it. The screen distances vary from less than 10 feet to almost 40 feet, depending on the building construction (see TM 5-853-1). This measure only applies to the low level of protection.

BUILDING ELEMENTS

3-38. Building elements for AT weapons and mortars involve the building's layout. This includes the materials used in the construction.

Layout

3-39. A building's interior layout is only an issue for the low level of protection against a mortar round. The layout issue involves designating sacrificial areas in which unimportant assets are located. The assets to be protected are located in a hardened interior layer. Figure 3-11 includes a plan view (from above). The sacrificial area has to be both around and above the protected area in case a mortar round comes from above. If such a layout is not feasible, other options include going to a higher level of protection and either hardening the entire building or building the facility underground (which are both very expensive).

Walls and Roofs

3-40. Walls and roofs must offer protection against both AT weapons and mortar rounds. The design of walls that protect against AT weapons varies with the level of protection. For the low level of protection where the round is predetonated, the walls can be of conventional construction, varying with the standoff distance from the predetonation screen to the wall. For higher levels of protection, the walls must resist the full effect of the round, requiring the walls to be 24-inch-thick reinforced concrete. Roofs are not an issue in

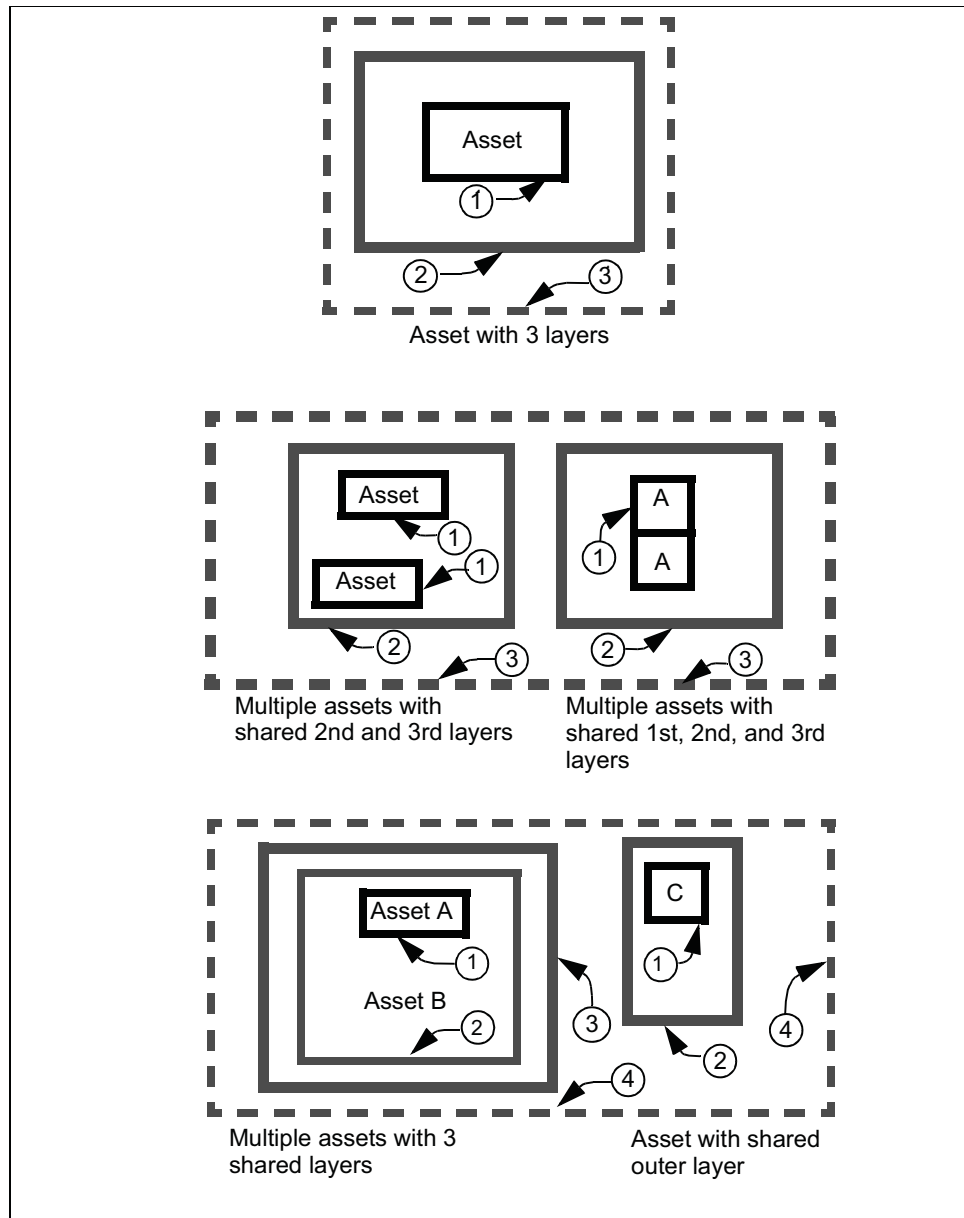


Figure 3-11. Assets Protected by Hardened Interior Layer

protecting against AT weapons because it is difficult to get direct LOSs to roofs. If such LOSs are possible, the roof should be designed like the walls.

3-41. To provide protection against mortar rounds, walls and roofs should be designed to resist the explosive effects in the rounds at the standoff distance that the sacrificial space provides. In the case of sacrificial areas, the walls can be of common construction. The interior protected-area walls are then designed of reinforced concrete or reinforced masonry for the standoff distance those sacrificial walls provide. When the walls must resist the full effect of the rounds (as in the higher level of protection), they are likely to be very thick (up

to 30 inches of reinforced concrete for some improvised mortars). Similar considerations should be made for roofs. Roofs are designed to take the direct effects of the round or to take the round at the standoff distance provided by the sacrificial area.

Doors and Windows

3-42. It is impractical to provide doors and windows that are resistant to mortar rounds and AT weapons. Windows should only be used in sacrificial areas where there is a mortar threat. When there is an AT weapon threat, windows can only be used where the round is predetonated. The windows should be narrowed or raised to present a smaller target (see Figures 3-8 and 3-9, page 3-12). Doors should be placed in foyers (see Figure 3-7, page 3-10) for protection against AT rounds and to achieve a low level of protection against mortars. Blast-resistant doors are necessary to achieve a high level of protection against mortar rounds.

BALLISTICS

3-43. In a ballistics tactic, aggressors fire small arms at assets from vantage points outside of the target facility's control. Ballistic attacks cannot be detected reliably before they occur.

GENERAL-DESIGN STRATEGY

3-44. Protective measures to resist these tactics rely on blocking LOSs to protected areas of a facility or by hardening the facility to resist the ballistic effects. This strategy focuses on assets within buildings. Protecting people or property in the open is difficult and can only be addressed through operational measures. Detection measures are not applicable for this tactic.

LEVELS OF PROTECTION

3-45. There are only two levels of protection for this tactic. The low level of protection depends on blocking LOSs to assets. This strategy assumes that the aggressor cannot hit what he cannot see. The risk of an aggressor firing into a building randomly and hitting something is what makes this the low level of protection. The high level of protection involves hardening building components to resist the ballistic effects. These strategies can be thought of as either hardening or hiding.

SITE-WORK ELEMENTS

3-46. Site-work elements are of limited use for the ballistics tactic. When they are applied, they are used to obstruct LOSs from vantage points outside of the site, which is consistent with the low level of protection. The LOSs can be blocked using trees, other buildings, motor pools, or fences.

BUILDING ELEMENTS

3-47. Building elements are the principal means of protecting assets against a ballistics attack. They can be applied to achieve either the low or high level of protection.

Walls and Roofs

3-48. Walls and roofs are inherently opaque, so it is easy to achieve the low level of protection (hiding) with them. Achieving the high level of protection (hardening) for walls and roofs can be done within conventional construction using reinforced concrete, concrete-masonry units (CMUs), or clay brick. The material's required thickness is shown in Table 3-1. The thicknesses of CMUs and clay brick are nominal, meaning they do not represent the actual thickness of the material; they represent the thicknesses at which those materials are commercially available. Steel plates (mild steel and armor steel) and bullet-resistant fiberglass can be used to retrofit existing building components that would not provide the needed bullet resistance.

Table 3-1. Required Thicknesses, in Inches

Ballistics Type	Reinforced Concrete	Grouted CMU*	Clay Brick*	Steel Plate		Bullet-Resistant Fiberglass
				Mild	Armor	
.38 special	2	4	4	1/4	3/16	5/16
9 mm	2 1/2	4	4	5/16	1/4	7/16
7.62 and 5.56 mm	4	6	6	9/16	7/16	1 1/8
7.62-mm AP	6 1/2	8	8	13/16	11/16	N/A
*Nominal thicknesses						

Windows

3-49. Windows can include openings in walls and skylights, although skylights are only an issue where there are LOSs to them. When skylights require protection, treat them like windows. Achieving the low level of protection (hiding) for windows requires making it difficult to see through them, such as installing reflective film on the glass. An aggressor cannot see through the windows during daylight while it is lighter outside than inside, but he may see through them at night when the opposite might be true. Drapes or blinds that can be closed at night address that vulnerability. To achieve the high level of protection requires bullet-resistant window assemblies. These are commercially available for a wide range of ballistics types. They are purchased as manufactured-and-tested assemblies (including glazing and frames, both of which are equally bullet-resistant). The glazing materials and thicknesses and the framing details are proprietary to their manufacturers. The manufacturers make them according to industry test standards to ensure an effective product.

Doors

3-50. Doors without glass easily meet the requirements for the low level of protection. Meeting the high level of protection requires the installation of bullet-resistant door assemblies. Doors can be installed in foyers so that there is no direct LOS into assets within the building (see Figure 3-7, page 3-10).

FORCED ENTRY

3-51. In the forced-entry tactic, an aggressor tries to forcibly gain access to assets. He may use tools or explosives to breach building components or other barriers.

GENERAL-DESIGN STRATEGY

3-52. The general-design strategy for forced entry is to detect the aggressor early in the forced-entry attempt and delay him long enough for a response force to intercept him. The combination of detection and defensive measures must provide sufficient time for a response force to intercept the aggressor before he reaches the asset or before he escapes with it, depending on the protective goals for the asset. The first goal would apply where the asset is likely to be destroyed or where access to it is not acceptable. The second goal would be applied when the idea is to prevent it from being stolen.

LEVELS OF PROTECTION

3-53. Several levels of protection apply to forced entry. These levels vary in terms of system design, delay time, and response-force arrival time.

SITE-WORK ELEMENTS

3-54. Site-work elements do not normally play a major role in protecting against a forced entry. However, the site should be laid out and maintained so that an aggressor does not have a hiding place nearby that will conceal his attempts to break into the building. Another site-work element is the application of perimeter barriers, most commonly fences. Fences are effective at delineating a boundary and at keeping honest people honest, but they are ineffective for preventing a forced entry. The design strategy for forced entry is based on delaying the aggressor, and any serious aggressor could climb a fence in less than 4 seconds or can cut through a fence in less than 10 seconds. Therefore, fences are not used as delay elements, but they are used to establish boundaries and as platforms on which to hang sensors. The final site-work consideration is securing utility-access ports such as manholes. If there are utility tunnels through which aggressors can enter a building, those accesses should be locked using padlocks or locking bolts.

BUILDING ELEMENTS

3-55. Building elements are the principal construction elements of a system for protecting against a forced entry. The building elements are used to provide delay. The process for designing to resist forced entry involves laying out concentric "rings" of delay (called defensive layers). These defensive layers can include the facility's exterior, interior rooms within that layer, and containers within the interior rooms. The individual building components for each of the layers (walls, doors, windows, floors, ceilings, and roofs) provide the delay time (see TM 5-853-1).

DETECTION ELEMENTS

3-56. For a protective system to be effective against a forced entry, the aggressors must be detected at a point of adequate delay. Detection at that point can be achieved by using an IDS. Once a sensor detects an aggressor, the alarm annunciator communicates that event to security personnel, who then dispatch a response force. The alarm can be assessed through a guard response or via CCTV. Chapter 6 and TM 5-853-4 provide detailed discussion of IDSs, CCTV systems, and other elements of ESSs.

COVERT ENTRY AND INSIDER COMPROMISE

3-57. In the covert-entry tactic, an aggressor who is not authorized to be in the facility attempts to enter using false credentials. In the insider-compromise tactic, personnel with legitimate access to a facility try to compromise an asset. The insider may or may not have legitimate access to the asset itself. The purpose of the entry in either case can be to steal or otherwise compromise the asset or to destroy it. In the latter case, the aggressor may bring IEDs or IIDs.

GENERAL-DESIGN STRATEGY

3-58. The general-design strategy for both the insider-compromise and covert-entry tactics is to keep people from entering areas they are not authorized to enter. For covert entry, aggressors are denied access to controlled areas. For insider compromise, aggressors are denied access to assets within controlled areas based on their need to have access to them. The general-design strategy also includes detecting aggressors removing assets from protected areas and detecting aggressors carrying tools, weapons, and explosives into protected areas.

LEVELS OF PROTECTION

3-59. The levels of protection for these tactics address different issues, depending on whether the aggressor's goal is to steal or otherwise compromise an asset or to destroy it. When the goal is to steal or compromise an asset, the levels of protection vary with the number and sophistication of the access controls required to verify personnel access into a controlled area. When the goal is to destroy the assets, the levels of protection vary with the amount of damage the building (and the assets inside) are allowed to sustain and the sophistication of detecting weapons or explosives at entry points.

BUILDING ELEMENTS

3-60. Building elements vary with an aggressor's goal. To protect against theft or compromise of assets, building elements are used to establish and maintain controlled areas into which only authorized personnel can enter. For insider compromise, there may be an additional requirement that access be further limited among personnel otherwise authorized access to the controlled area. That access is based on the need to have access to a specific asset. The result is that the controlled area may be compartmentalized, and each compartmentalized area may have separate access requirements. There are no special construction requirements for these tactics if the goal is theft or compromise. The only requirement is that the building elements of controlled areas should provide enough resistance to require aggressors to force their way through them to gain entry and to provide evidence of the forced entry if it is attempted. Forcing entry would be contrary to the aggressor's assumed goal to be covert. In addition, a common design goal would be to limit the number of entrances into controlled areas because there will need to be access control at each entry.

3-61. To protect against the destruction of assets, building elements are used to shield assets from the effects of explosives going off at access-control points.

The basic approach is to lay out areas at access points in which guards can search for carried-in weapons, explosives, or incendiary devices. The construction of that area is designed to limit damage to the rest of the building if an explosive is detonated in that area. Those levels of damage are similar to those discussed in relation to vehicle bombs. The walls and doors between the access point and the protected area will be hardened, and the walls and doors to the outside will be of lightweight construction so that they may fail and vent the blast pressure away from the building. At the higher level of protection, the access-control area is located in a separate facility and the target building is hardened to resist an explosion in that separate facility.

DETECTION ELEMENTS

3-62. Detection elements for these tactics also vary based on the aggressor's goal. For theft, the detection elements are mainly related to access control. For destruction, the detection elements are used to detect weapons, explosives, or incendiary devices.

3-63. The main detection elements for theft or compromise are access-control devices. These can include procedural systems (such as guards checking ID), mechanical systems (such as keyed or combination locks), or electronic entry-control elements (such as electronic card readers, keypads, and biometric devices). Chapter 6 provides detailed discussion of electronic devices. The sophistication of these elements and the number used varies with the level of protection. For example, achieving the higher levels of protection requires the application of multiple forms of access-control elements such as a card reader and an electronic keypad for electronic-entry control or a badge check and badge exchange for a procedural system.

3-64. When destruction of the assets is the goal, detection is oriented toward detecting weapons, explosives, or incendiary devices. At the lower levels of protection, it is sufficient for guards to search for carried-in items. Achieving higher levels of protection requires the application of such equipment as metal detectors, X-ray machines, and explosive detectors.

SURVEILLANCE AND EAVESDROPPING

3-65. Surveillance and eavesdropping tactics include visual surveillance, acoustic eavesdropping, and electronic-emanations eavesdropping. In these tactics, aggressors remain outside of controlled areas and try to gather information from within those areas. The tools used for these tactics include ocular devices for the visual-surveillance tactic and listening devices and electronic-emanations-eavesdropping equipment for the eavesdropping tactic.

GENERAL-DESIGN STRATEGY

3-66. The general-design strategy for these tactics is to deny aggressors access to information assets. The kind of information (objects, operations, or files; secure conversations; or electronically processed data) and how it can be compromised differs for each tactic as do the specific protective strategies. Therefore, each tactic is addressed separately.

LEVELS OF PROTECTION

3-67. Each of these tactics has only one level of protection. Either one protects or fails to protect against these tactics.

SITE-WORK ELEMENTS

3-68. Site-work elements play a minor role in protecting assets from all surveillance or eavesdropping tactics. The main issue is to eliminate or control vantage points from which aggressors can surveil or eavesdrop on assets or operations. In addition, for the visual-surveillance tactic, a design goal can be to block LOSs from vantage points. Items used to block LOSs include trees, bushes, fences, and other buildings (see Figure 3-12).

BUILDING ELEMENTS

3-69. Building elements are the principal components of the protective strategies for surveillance and eavesdropping tactics. For visual surveillance,

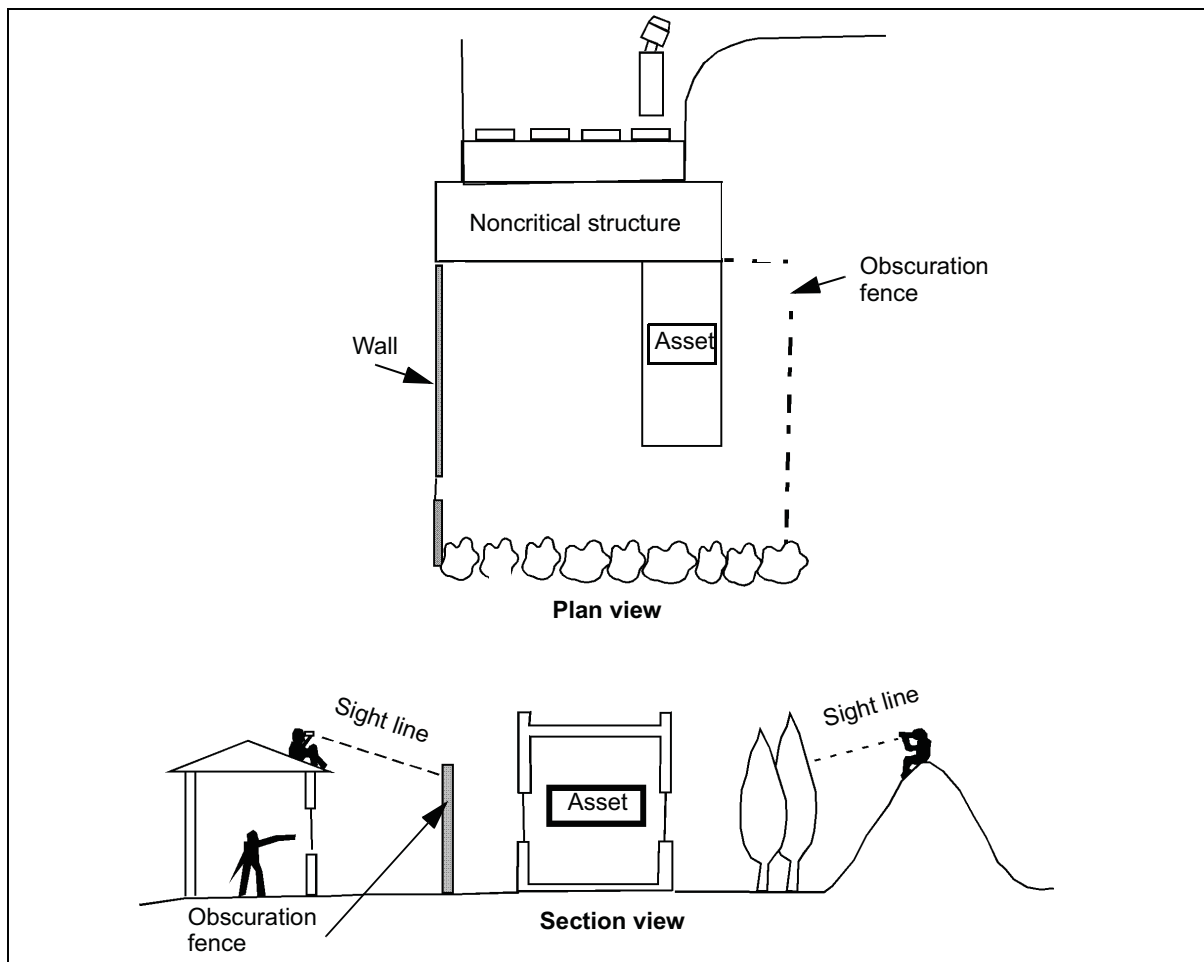


Figure 3-12. LOS Blocked From Potential Vantage Points

the building elements must block LOSs from outside the building. Walls and roofs perform this function effectively. Doors are only a problem when they have windows in them or are made of transparent materials. When this is the case, they can be treated like windows or they can be placed in foyers so that there are no direct LOSs through them. Windows can be treated with reflective film and drapes or blinds as described in the ballistics tactics. When there are LOSs through skylights, they should be treated like windows.

3-70. Building elements for acoustic eavesdropping relate to the construction of areas (preferably separated from the building exterior) that minimize the sound that can be transmitted through them. This requires specialized construction that has a sound-transmission-coefficient (STC) rating. Walls, floors, and ceilings can be constructed to achieve specific STC ratings using conventional construction materials as described in TM 5-853-1. Doors and windows that are STC rated are commonly manufactured and tested as assemblies. This type of design and construction can be expensive.

3-71. Protection against electronic-emanations eavesdropping involves the application of Terminal Electromagnetic-Pulse Emanation Standard (TEMPEST) guidance, most of which is classified. The protection is based on a TEMPEST assessment done for the Army by the US Army Intelligence and Security Command (INSCOM) and on guidance in AR 380-19. The results of a TEMPEST assessment will commonly lead to countermeasures from one or more of the following categories:

- Follow information security policies and procedures recommended during the assessments.
- Provide controlled space both inside and outside the facility.
- Provide TEMPEST-shielded equipment.
- Provide separation between electronic circuits that handle classified information and those that do not. This is commonly called red/black separation.
- Provide TEMPEST-shielded enclosures. This is specialized, metal-shielded construction that is very expensive.

MAIL AND SUPPLY BOMBS

3-72. In mail- and supply-bomb tactics, aggressors place bombs in materials delivered to a facility. Explosives used in supply bombs are significantly larger (briefcase size) than those in mail bombs (pipe bombs or smaller). Mail bombs are usually directed at individuals, while supply bombs may be used to target larger numbers of people. These tactics assume that the facility containing the asset has a mail-handling area or a supplies-handling and -receiving area. These tactics do not apply if mail or supplies are handled and screened in a different facility.

GENERAL-DESIGN STRATEGY

3-73. A bomb exploding within a building has more severe effects than the same size bomb exploding outside of the facility because the blast pressures cannot dissipate inside. Also, there is no standoff distance between the explosive and the facility to mitigate blast effects. The general-design strategy

for mail and supply bombs is to detect delivered bombs before they explode and to harden the area where the explosion takes place. This minimizes the damage to the remainder of the facility. Occupants and contents within the mail room or supplies-handling area are likely to be killed or destroyed if an undetected bomb explodes.

LEVELS OF PROTECTION

3-74. The levels of protection for mail and supply bombs are based on the amount of damage allowed to the building and, therefore, the occupants of the building. They also vary based on the sophistication of the detection measures used.

BUILDING ELEMENTS

3-75. The purpose of building elements in relation to these bomb tactics is to shield assets from the effects of explosives going off at supply areas, receiving points, or mail rooms. The basic approach is to lay out either a mail room or a supplies-receiving area in which people can search suspicious packages for explosives or incendiary devices. Constructing this type of area will limit the damage to the rest of the building if an explosive is detonated there. Those levels of damage are similar to those discussed in relation to vehicle bombs.

Mail Rooms

3-76. Mail rooms should be located on the facility's exterior, away from any critical assets. The walls and ceiling between the mail room and the remainder of the building are hardened to keep the blast effects out of the facility. The exterior walls and doors should be of lightweight construction so that they may fail and vent the blast pressure away from the building. There may be an explosives container in the mail room where suspicious packages can be placed. If the package explodes, the container will keep its effects from causing damage or injury. The hardened construction will protect assets outside of the mail room if the explosion occurs outside of the container. Check with EOD personnel to determine the local policy for using explosive containers. At higher levels of protection, the mail room is constructed to completely contain the effects of an explosion either through hardened construction or by using a specialized construction called vented suppressive shielding. Mail rooms should not have windows into protected areas. Doors between the mail room and the rest of the building should be avoided, placed in foyers, or replaced with blast-resistant doors, depending on the desired level of protection.

Supplies-Handling Areas

3-77. Supplies-handling areas should also be on the building's exterior, away from critical areas of the facility. Walls and doors between the handling area and the protected area should be hardened, and the exterior walls and doors should be of lightweight construction so that they may fail and vent the blast pressure away from the building. There should be no windows between the handling area and the protected area. At the higher level of protection, the handling area is located in a separate facility and the target building is hardened to resist an explosion in that separate facility.

DETECTION ELEMENTS

3-78. Detection for these assets varies with the level of protection. At the lower levels of protection, bombs are detected by inspection. As the level of protection goes up, the sophistication of the detection increases. At the higher levels of protection, equipment such as X-ray examining devices, metal detectors, and explosives detectors can be used. Explosive-detection dogs are an alternative to explosive detectors.

CHEMICAL AND BIOLOGICAL CONTAMINATION

3-79. When using chemical- and biological-contamination tactics, aggressors introduce contaminants into the air or water supply to a facility or a group of facilities. Both airborne and waterborne contaminants include chemical, biological, and radiological agents. Aggressors may also forcibly enter a facility to contaminate water or air using the forced-entry tactic.

GENERAL-DESIGN STRATEGY

3-80. Both chemical and biological agents are difficult to detect in water and air supplies. Radiological agents are relatively easy to detect in water, but they are not commonly included in water-quality examinations. It is unlikely that all agents will be detected, so the general-design strategy for these tactics is to filter out suspected airborne contaminants or to shut off suspected waterborne contaminants. Also, because contaminants can easily be entered into the environment from inside a facility, the strategy includes limiting access to the facility (especially mechanical rooms, water intakes, and so forth).

LEVELS OF PROTECTION

3-81. The levels of protection for each of these tactics differ only in the frequency with which some protective measures are exercised. For the low level of protection, they are exercised only in response to a known threat. In the high level of protection, they are exercised continuously.

SITE-WORK ELEMENTS

3-82. Site-work elements are only significant for waterborne contamination. They include protecting water-treatment plants and water-storage structures. This protection may include constructing perimeter barriers (such as chain-link fences) and controlling access to the plant site. These measures are used because most contaminants require quantities on the order of truckloads to contaminate a water supply, so the focus of security is to keep such large vehicles under control. The perimeter barriers do not need to stop the vehicles because the assumption is that the aggressor wants to be covert. An overt act would alert people to avoid the water supply.

BUILDING ELEMENTS

3-83. Building elements for both tactics include controlling access so that aggressors cannot sneak in and plant devices in the building. Protection against airborne contamination at a facility involves making elements of the

air-handling system (including air intakes) inaccessible and laying out toxin-free areas for people to be protected. A toxin-free area is an area in which the internal air pressure is higher than the external air pressure. Therefore, if a chemical, biological, or radiological device is set off outside, its contaminant will not be able to penetrate the protected area. Achieving that “net positive pressure” requires a significant air-handling system with air filters to filter contaminants out of the air. It also requires an air-lock entrance into the area so contaminants cannot enter through the door. At the low level of protection, the filters and the air-handling system are only used in response to a credible threat. At the high level of protection, that risk is not acceptable and the filters are run continuously.

3-84. The building-element issues for waterborne contamination are limited to providing protection against forced and covert entries into water-treatment plants and water-storage areas. These methods have been previously described. The only additional issue is the provision for alternative water sources. If it is suspected or detected that the water is contaminated, a backup water source should be in place (such as bottled water). For the high level of protection, bottled water should always be used for drinking.

Chapter 4

Protective Barriers

Protective barriers are used to define the physical limits of an installation, activity, or area. Barriers restrict, channel, or impede access and are fully integrated to form a continuous obstacle around the installation. They are designed to deter the worst-case threat. The barriers should be focused on providing assets with an acceptable level of protection against a threat.

OVERVIEW

4-1. Protective barriers form the perimeter of controlled, limited, and exclusion areas. Utility areas (such as water sources, transformer banks, commercial power and fuel connections, heating and power plants, or air-conditioning units) may require these barriers for safety standards. Protective barriers consist of two major categories—natural and structural.

- Natural protective barriers are mountains and deserts, cliffs and ditches, water obstacles, or other terrain features that are difficult to traverse.
- Structural protective barriers are man-made devices (such as fences, walls, floors, roofs, grills, bars, roadblocks, signs, or other construction) used to restrict, channel, or impede access.

4-2. Barriers offer important benefits to a physical-security posture. They create a psychological deterrent for anyone thinking of unauthorized entry. They may delay or even prevent passage through them. This is especially true of barriers against forced entry and vehicles. Barriers have a direct impact on the number of security posts needed and on the frequency of use for each post.

4-3. Barriers cannot be designed for all situations. Considerations for protective structural barriers include the following:

- Weighing the cost of completely enclosing large tracts of land with significant structural barriers against the threat and the cost of alternate security precautions (such as patrols, MWD teams, ground sensors, electronic surveillance, and airborne sensors).
- Sizing a restricted area based on the degree of compartmentalization required and the area's complexity. As a rule, size should be kept to a minimum consistent with operational efficiency. A restricted area's size may be driven by the likelihood of an aggressor's use of certain tactics. For example, protecting assets from a vehicle bomb often calls for a substantial explosives standoff distance. In these cases, mitigating the vehicle bomb would often be more important than minimizing the restricted area to the extent necessary for operational efficiency. Protective barriers should be established for—
 - Controlling vehicular and pedestrian traffic flow.

- Providing entry-control points where ID can be checked.
- Defining a buffer zone for more highly classified areas.
- Precluding visual compromise by unauthorized individuals.
- Delaying forced entry.
- Protecting individual assets.

4-4. If a secured area requires a limited or exclusion area on a temporary or infrequent basis, it may not be possible to use physical structural barriers. A temporary limited or exclusion area may be established where the lack of proper physical barriers is compensated for by additional security posts, patrols, and other security measures during the period of restriction. Temporary barriers (including temporary fences, coiled concertina wire, and vehicles) may be used. Barriers are not the only restrictive element, and they may not always be necessary. They may not be ideal when working with limited or exclusion areas or when integrated with other controls.

4-5. Because barriers can be compromised through breaching (cutting a hole through a fence) or by nature (berms eroded by the wind and rain), they should be inspected and maintained at least weekly. Guard-force personnel should look for deliberate breaches, holes in and under barriers, sand dunes building up against barriers, and the proper functioning of locks.

FENCING

4-6. Three types of fencing are authorized for use in protecting restricted areas—chain link, barbed wire, and barbed tape or concertina. The type used for construction depends primarily on the threat and the degree of permanence. It may also depend on the availability of materials and the time available for construction. Fencing may be erected for other uses besides impeding personnel access. It can impede observation, can serve as a means to defeat standoff-weapon systems (such as rocket-propelled grenades [RPGs]), and can serve as a barrier to hand-thrown weapons (such as grenades and firebombs).

4-7. Generally, chain-link fencing will be used for protecting permanent limited and exclusion areas. All three types of fencing may be used to augment or increase the security of existing fences that protect restricted areas. Examples would be to create an additional barrier line, to increase existing fence height, or to provide other methods that effectively add to physical security. It is important to recognize that fencing provides very little delay when it comes to motivated aggressors, but it can act as a psychological deterrent.

CHAIN LINK

4-8. Chain-link fence (including gates) must be constructed of 6-foot material, excluding the top guard. Fence heights for conventional arms and ammunition security must be 6 feet for standard chain-link, wire-mesh fencing. Chain-link fences must be constructed with 9-gauge or heavier wire. They must be galvanized with mesh openings not larger than 2 inches per side and have twisted and barbed selvages at the top and the bottom. The wire must be taut and securely fastened to rigid metal or reinforced-concrete posts set in

concrete. It must reach within 2 inches of hard ground or pavement. On soft ground, it must reach below the surface deep enough to compensate for shifting soil or sand. Materials and construction must meet with the US Army Corps of Engineers (USACE) guide specifications shown in the USACE Standard (STD) 872-90 series. Weaknesses in the chain-link fence occur as a result of weather (rusting) or failure to keep it fastened to the post that affects the desired tightness. Damage to the fence and fence fabric may be the result of allowing vegetation and trees to grow on or near the fence. The interaction between the fence and the overgrowth often leads to fence damage and reduces the integrity and continuity of the fence as a perimeter boundary and barrier. The perimeter fence is the most obvious protective measure. A well-maintained fence indicates that the asset owner is dedicated to physical security.

BARBED WIRE

4-9. Standard barbed wire is twisted, double-strand, 13.5-gauge wire, with four-point barbs spaced an equal distance apart. Barbed-wire fencing (including gates) intended to prevent human trespassing should not be less than 6 feet high and must be affixed firmly to posts not more than 6 feet apart. The distance between strands should not exceed 6 inches, and at least one wire should be interlaced vertically and midway between posts. The ends must be staggered or fastened together, and the base wire must be picketed to the ground.

BARBED TAPE OR CONCERTINA

4-10. A barbed-taped obstacle (BTO) is fabricated from 0.025-inch stainless steel and is available in 24-, 30-, 40-, and 60-inch-diameter coils. The barbs shall have a minimum length of 1.2 inches, and the barb cluster's width shall be 1.21 inches. A BTO deploys tangle-free for fast installation. It may be recovered and used again. Fifty feet (plus or minus 2 inches) can be covered by 101 coil loops. Handling barbed tape requires the use of heavy barbed-tape gauntlets instead of standard barbed-wire gauntlets.

Barbed-Tape Concertina

4-11. Barbed-tape concertina (standard concertina barbed tape) is a commercially manufactured wire coil of high-strength-steel barbed wire that is clipped together at intervals to form a cylinder. When opened, it is 50 feet long and 3 feet in diameter. When used as the perimeter barrier for a restricted area, the concertina must be laid between poles with one roll on top of another or in a pyramid arrangement (with a minimum of three rolls).

4-12. Reinforced barbed-tape concertina consists of a single strand of spring-steel wire and a single strand of barbed tape. The sections between barbs of the barbed tape are securely clinched around the wire. Each coil is about 37 1/2 inches in diameter and consists of 55 spiral turns connected by steel clips to form a cylindrical diamond pattern when extended to a coil length of 50 feet. One end turn is fitted with four bundling wires for securing the coil when closed and each end turn is fitted with two steel carrying loops. The concertina extends to 50 feet without permanent distortion. When released, it can be retracted into a closed coil.

4-13. When possible, a top guard should be constructed on all perimeter fences and may be added on interior enclosures for additional protection. A top guard is an overhang of barbed wire or tape along the top of a fence, facing outward and upward at about a 45-degree angle. Placing barbed wire or tape above it can further enhance the top guard. Top-guard supporting arms will be permanently affixed to the top of fence posts to increase the overall height of the fence by at least 1 foot. (Due to liability issues in some locations, the top guards will not be allowed to face outward where the fence is adjacent to public areas.) Three strands of barbed wire spaced 6 inches apart must be installed on the supporting arms. The number of strands of wire or tape may be increased when required. The top guard of fencing adjoining gates may range from a vertical height of 18 inches to the normal 45-degree outward protection but only for sufficient distance along the fence to open the gates adequately. Bottom and top tension wires should be used in lieu of fence rails. A concrete sill may be cast at the bottom of the fence to protect against soil erosion. A bottom rail is used on high-security fences to prevent intruders from lifting the fence.

Gates and Entrances

4-14. The number of gates and perimeter entrances must be the minimum required for safe and efficient operation of the facility. Active perimeter entrances must be designed so that the guard force maintains full control. Semiactive entrances, such as infrequently used vehicular gates, must be locked on the inside when not in use. When closed, gates and entrances must provide a barrier structurally comparable to their associated barriers. Care must be afforded against the ability to crawl under gates. Top guards, which may be vertical, are required for all gates.

Triple-Standard Concertina (TSC) Wire

4-15. This type of fence uses three rolls of stacked concertina. One roll will be stacked on top of two rolls that run parallel to each other while resting on the ground, forming a pyramid. In many situations, this fence has been used effectively in place of a chain-link fence. (If perimeter fencing consists of TSC, a top guard is not feasible.)

Tangle-Foot Wire

4-16. Barbed wire or tape may be used in appropriate situations to construct a tangle-foot obstruction either outside a single perimeter fence or in the area between double fences to provide an additional deterrent to intruders. The wire or tape should be supported on short metal or wooden pickets spaced at irregular intervals of 3 to 10 feet and at heights between 6 and 12 inches. The wire or tape should be crisscrossed to provide a more effective obstacle. The space and materials available govern the depth of the field.

AIRCRAFT CABLE

4-17. Although not used very often, aircraft cable can be used as a temporary barrier. Refer to FM 5-34 for information required for determining the barrier's strength. The barrier is created using wire rope. Clips are spaced six times the diameter of the wire rope. Aircraft cable (deployed as described

above or attached to a chain-link fence) can also be made to act as a barrier to moving vehicles. To do so, the cable must be anchored into the ground at both ends at about 200-foot intervals (see TM 5-853-1).

UTILITY OPENINGS

4-18. Sewers, air and water intakes and exhausts, and other utility openings of 10 inches or more in diameter that pass through perimeter barriers must have security measures equivalent to that of the perimeter (see TM 5-820-4). Specific requirements of various openings are discussed below:

- Manhole covers 10 inches or more in diameter must be secured to prevent unauthorized opening. They may be secured with locks and hasps, by welding them shut, or by bolting them to their frame. Ensure that hasps, locks, and bolts are made of materials that resist corrosion. Keyed bolts (which make removal by unauthorized personnel more difficult) are also available.
- Drainage ditches, culverts, vents, ducts, and other openings that pass through a perimeter and that have a cross-sectional area greater than 96 square inches and whose smallest dimension is greater than 6 inches will be protected by securely fastened welded bar grilles (refer to TM 5-853-3, Figure 8-1). As an alternative, drainage structures may be constructed of multiple pipes, with each pipe having a diameter of 10 inches or less. Multiple pipes of this diameter may also be placed and secured in the inflow end of a drainage culvert to prevent intrusion into the area. Ensure that any addition of grilles or pipes to culverts or other drainage structures is coordinated with the engineers so that they can compensate for the diminished flow capacity and additional maintenance that will result from the installation.

OTHER PERIMETER BARRIERS

4-19. Buildings less than two stories high that form part of a perimeter must have a top guard along the outside edge to deny access to the roof. When using masonry walls as part of a perimeter barrier, they must be at least 7 feet high and have a barbed-wire top guard. The top guard should be sloped outward at a 45-degree angle and carry at least three strands of barbed wire. This will increase the vertical height of the barrier by at least 1 foot.

4-20. Protect windows, active doors, and other designated openings by securely fastening bars, grilles, or chain-link screens. Fasten window barriers from the inside. If hinged, the hinges and locks must be on the inside. Building elements that provide delay against forced entry have stringent requirements. These elements should be designed according to TM 5-853-1.

SECURITY TOWERS

4-21. It is not acceptable to observe a perimeter from towers only. However, all towers should be located to provide maximum observation and should be constructed for protection from small-arms fire.

4-22. Mobile towers are useful in some temporary situations such as a large, open storage area where receiving and storing activities take place. All facilities using towers must have a support force available for emergencies. Tower personnel should be rotated at frequent intervals.

4-23. The height of a tower increases the range of observation during daylight hours and at night with artificial illumination. However, during inclement weather and during a blackout, towers lose this advantage and must be supplemented by on-ground observation.

4-24. The following considerations should be made when planning for the use of towers:

- Hardening the tower against small-arms effects by using sandbags, salvaged armor, or commercially fabricated bullet-resistant construction. This may require strengthening the tower supports, which should be performed only under the supervision of an engineer. The level of protection required must equate to the threat level identified during the IPB or the military decision-making process (MDMP). The best approach is to design for the worst identified threat rather than to try and modify the tower at a later date on short notice.
- Installing communications and alarm systems, both audible and visual (primary and alternate).
- Using appropriate surveillance, target-acquisition, and night-observation (STANO) equipment with the tower and perimeter barriers being surveilled. Infrared (IR) items may be especially valuable. Considerations for the selection and use of STANO equipment must be made while evaluating the effects of perimeter protective lighting.
- Providing security lighting for route protection to the tower. Security lighting also allows for support of the guard force entering or exiting the perimeter.
- Ensuring that the tower's height is determined according to the area of observation.
- Ensuring that towers have overlapping, mutually supporting fields of observation and fire.
- Providing towers with a backup fortified defensive fighting position, as appropriate.

INSTALLATION ENTRANCES

4-25. The number of installation or activity gates and perimeter entrances in active use should be limited to the minimum number required for safe and efficient operations. When necessary, install vehicle barriers in front of vehicle gates. Security lighting should be considered at entry points (see Chapter 5). Refer to TM 5-853-1 for the application and selection of these barriers.

4-26. Plans to use guards for controlling entry to an installation or activity must be predetermined based on the threat conditions (THREATCON). The construction of the guard post must be included in the security plan.

PERIMETER ENTRANCES

4-27. Active perimeter entrances should be designated so that security forces maintain full control without an unnecessary delay in traffic. This is accomplished by having sufficient entrances to accommodate the peak flow of pedestrian and vehicular traffic and having adequate lighting for rapid and efficient inspection. When gates are not operational during nonduty hours, they should be securely locked, illuminated during hours of darkness, and inspected periodically by a roving patrol. Additionally, warning signs should be used to warn drivers when gates are closed. Doors and windows on buildings that form a part of the perimeter should be locked, lighted, and inspected.

ENTRY-CONTROL STATIONS

4-28. Entry-control stations should be provided at main perimeter entrances where security personnel are present. Considerations for construction and use should be based on the information outlined in USACE STD 872-50-01.

4-29. Entry-control stations should be located as close as practical to the perimeter entrance to permit personnel inside the station to maintain constant surveillance over the entrance and its approaches. Additional considerations at entry-control stations include—

- Establishing a holding area for unauthorized vehicles or those to be inspected further. A turnaround area should be provided to keep from impeding other traffic.
- Establishing control measures such as displaying a decal on the window or having a specially marked vehicle.

4-30. Entry-control stations that are manned 24 hours each day should have interior and exterior lighting, interior heating (where appropriate), and a sufficient glassed area to afford adequate observation for personnel inside. Where appropriate, entry-control stations should be designed for optimum personnel ID and movement control. Each station should also include a telephone, a radio, and badge racks (if required).

4-31. Signs should be erected to assist in controlling authorized entry, to deter unauthorized entry, and to preclude accidental entry. Signs should be plainly displayed and be legible from any approach to the perimeter from a reasonable distance. The size and coloring of a sign, its letters, and the interval of posting must be appropriate to each situation.

4-32. Entry-control stations should be hardened against attacks according to the type of threat. The methods of hardening may include—

- Reinforced concrete or masonry.
- Steel plating.
- Bullet-resistant glass.
- Sandbags, two layers in depth.
- Commercially fabricated, bullet-resistant building components or assemblies.

WARNING SIGNS

4-33. A significant amount of warning signs should be erected to ensure that possible intruders are aware of entry into restricted areas. Warning signs augment control signs. They warn intruders that the area is restricted and that trespassing may result in the use of deadly force.

4-34. Warning signs should be installed along the limited area's physical barriers and at each entry point where they can be seen readily and understood by anyone approaching the perimeter. In areas where English is one of two or more languages commonly spoken, warning signs must contain the local language in addition to English. The wording on the signs will denote warning of a restricted area. The signs should be posted at intervals of no more than 100 feet. They must not be mounted on fences equipped with intrusion-detection equipment. Additionally, the warning signs prescribed in AR 190-13 should be posted at all entrances to limited, controlled, and exclusion areas. See Chapter 7 for more details.

OTHER SIGNS

4-35. Signs setting forth the conditions of entry to an installation or area should be plainly posted at all principal entrances. The signs should be legible under normal conditions at a distance not less than 50 feet from the point of entry. Such signs should inform the entrant of the provisions (search of the person, the vehicle, packages, and so forth) or prohibitions (such as against cameras, matches, and lighters and entry for reasons other than official business) that may be prescribed by the installation commander.

4-36. Signs or notices legibly setting forth the designation of restricted areas and provisions of entry should be plainly posted at all entrances and at other points along the perimeter line as necessary. The wording of these signs or notices is prescribed in AR 190-13.

INSTALLATION PERIMETER ROADS AND CLEAR ZONES

4-37. When the perimeter barrier encloses a large area, an interior all-weather perimeter road should be provided for security-patrol vehicles. Clear zones should be maintained on both sides of the perimeter barrier to provide an unobstructed view of the barrier and the ground adjacent to it. Roads within the clear zone should be as close to the perimeter barrier as possible without interfering with it. The roads should be constructed to allow effective road barriers to deter motor movement of unauthorized personnel during mobilization periods.

4-38. Clear zones should be kept clear of weeds, rubbish, or other material capable of offering concealment or assistance to an intruder attempting to breach the barrier. A clear zone of 20 feet or more should exist between the perimeter barrier and exterior structures, parking areas, and natural or man-made features. When possible, a clear zone of 50 feet or more should exist between the perimeter barrier and structures within the protected area, except when a building's wall constitutes part of the perimeter barrier. Ammunition supply points (ASPs) will have clear zones 12 feet outside of the ASP and 30 feet inside, and the vegetation will not exceed 8 inches (4 inches

for high-threat and highly controlled areas). Refer to AR 190-11 and DOD 0-2000.12-H, Appendix EE, for further information.

4-39. When it is impossible to have adequate clear zones because of property lines or natural or man-made features, it may be necessary to increase the height of the perimeter barrier, increase security-patrol coverage, add more security lighting, or install an intrusion-detection device along that portion of the perimeter.

4-40. When considering the construction of a new site or perimeter, ensure that the plans include a fence located well inside the property line, thus permitting control of enough space outside the fence to maintain at least a minimal clear zone. The following considerations apply:

- On a large installation (such as a proving ground), it is unreasonable to construct an expensive perimeter fence and keep it under constant observation. Such an installation is usually established in a sparsely inhabited area. Its comparative isolation and the depth of the installation give reasonable perimeter protection. Under these circumstances, it is usually sufficient to post warning signs or notices, reduce access roads to a minimum, and periodically patrol the area between the outer perimeter and the conventionally protected vital area of the installation.
- An alternative to erecting new or replacing old chain-link fence involving an entire installation perimeter is to relocate or isolate the sensitive area or item by—
 - Relocating the item within a safe perimeter.
 - Consolidating the item with other items.
 - Erecting a chain-link fence (regulations permitting) around individual assets rather than the installation's perimeter.

ARMS-FACILITY STRUCTURAL STANDARDS

4-41. It is next to impossible to build a protective barrier that cannot be penetrated by a human or heavy armor. Therefore, as opposed to protecting a facility using only one barrier, enhance security by using a combination of barriers to increase delay. Multiple barriers also cause aggressors to expend more energy trying to breach all of the barriers. They also provide the appearance of additional security and may further deter some aggressors.

4-42. The interest of security must be kept in mind when constructing walls, ceilings, floors, and roofs. Facilities that house arms and ammunition are constructed as security barriers in the interest of deterring and delaying penetration. Construction guidelines for arms facilities are outlined in AR 190-11. AR 190-11 requires coordination with the engineer office, the safety office, the provost marshal office (PMO), or the security-force office when definitive drawings and specifications for new construction or upgrades or modifications of AA&E storage structures are proposed. This coordinated effort ensures that safety and physical-security requirements are met. AR 190-11 also addresses waivers and exceptions for AA&E storage structures, as well as the requirements for a tactical (training or operational) or shipboard environment. Waivers and exceptions are not discussed in this manual. The

following guidelines are provided for securing AA&E in tactical and shipboard environments:

- The criteria and standards for protecting AA&E will be developed by the major Army command (MACOM) according to AR 190-11.
- The deploying commander will establish and enforce procedures for securing deployed AA&E based on the assessment of the threat, the objectives, the location, and the duration of the deployment.
- The AA&E in the tactical environment will be secured at all times.
- The AA&E will be under continuous positive control.
- Persons charged with the custody of AA&E will have the capability to sound the alarm if a forceful theft is attempted.
- A response force will be available to protect the AA&E.
- A system of supervisory checks will be established to ensure that all personnel comply with security measures. Supervisory checks of the AA&E holding area will be made to ensure that the AA&E being guarded have not been tampered with.
- All officers, noncommissioned officers (NCOs), or civilian equivalents will closely monitor the control of ammunition and explosives during field training or range firing.
- Selection of personnel to perform guard duties at AA&E holding areas will be closely monitored by commanders to ensure that only responsible individuals are assigned duties.

Chapter 5

Physical-Security Lighting

Security lighting allows security personnel to maintain visual-assessment capability during darkness. When security-lighting provisions are impractical, additional security posts, patrols, MWD patrols, NVDs, or other security means are necessary.

OVERVIEW

5-1. Security lighting should not be used as a psychological deterrent only. It should also be used along perimeter fences when the situation dictates that the fence be under continuous or periodic observation.

5-2. Lighting is relatively inexpensive to maintain and, when properly used, may reduce the need for security forces. It may also enhance personal protection for forces by reducing the advantages of concealment and surprise for a determined intruder.

5-3. Security lighting is desirable for those sensitive areas or structures within the perimeter that are under observation. Such areas or structures include pier and dock areas, vital buildings, storage areas, motor pools, and vulnerable control points in communication and power- and water-distribution systems. In interior areas where night operations are conducted, adequate lighting facilitates the detection of unauthorized persons approaching or attempting malicious acts within the area. Security lighting has considerable value as a deterrent to thieves and vandals and may make the job of the saboteur more difficult. It is an essential element of an integrated physical-security program.

5-4. A secure auxiliary power source and power-distribution system for the facility should be installed to provide redundancy to critical security lighting and other security equipment. During deployed operations, primary power may not exist or may be subject to constraints or interruptions due to poor infrastructure or hostile activity. Auxiliary power sources must be available for critical electrical loads and must be secured against direct and indirect fires as well as sabotage. If automatic-transfer switches are not installed, security procedures must designate the responsibility for the manual start of the source.

COMMANDER'S RESPONSIBILITY

5-5. Commanders determine perimeter lighting needs based on the threat, site conditions along the perimeter, surveillance capabilities, and available guard forces. Commanders ensure that security lighting is designed and used to discourage unauthorized entry and to facilitate the detection of intruders approaching or attempting to gain entry into protected areas.

PLANNING CONSIDERATIONS

5-6. Security lighting usually requires less intensity than working lights, except for ID and inspection at entry-control points. Each area of a facility presents its own unique set of considerations based on physical layout, terrain, atmospheric and climatic conditions, and security requirements. Information is available from the manufacturers of lighting equipment and from the installation's director of public works, who will assist in designing a lighting system. This information includes—

- Descriptions, characteristics, and specifications of various lighting fixtures, arc, and gaseous-discharge lamps.
- Lighting patterns of various fixtures.
- Typical layouts showing the most efficient height and spacing of equipment.
- Minimum levels of illumination and lighting uniformity required for various applications.

5-7. In planning a security-lighting system, the physical-security manager considers the—

- Cost of replacing lamps and cleaning fixtures, as well as the cost of providing the required equipment (such as ladders and mechanical buckets) to perform this maintenance.
- Provision of manual-override capability during a blackout, including photoelectric controls. These controls may be desirable in a peacetime situation but undesirable when a blackout is a possibility.
- Effects of local weather conditions on lighting systems.
- Fluctuating or erratic voltages in the primary power source.
- Grounding requirements.
- Provisions for rapid lamp replacement.
- Use of lighting to support a CCTV system.
- Limited and exclusion areas. Specific lighting requirements are referenced in AR 190-59 and TM 5-853-2. TM 5-853-4 provides guidance for facility applications that include CCTV cameras.
 - Lighting in these areas must be under the control of the guard force.
 - For critical areas (such as weapons storage areas), instantaneous lighting with a backup source is required. Any period without lighting in a critical area is unacceptable. Therefore, these areas generally have a requirement for backup power (such as diesel-engine generators, uninterrupted power supplies, and batteries) in case of power loss.
 - Security-lighting systems are operated continuously during hours of darkness.
 - Protective lights should be used so that the failure of one or more lights will not affect the operation of the remaining lights.
- Lighting requirements for adjoining properties and activities.
- Restrike time (the time required before the light will function properly after a brief power interruption).

- Color accuracy.
- Other facilities requiring lighting, such as parking areas.

PRINCIPLES OF SECURITY LIGHTING

5-8. Security lighting enables guard-force personnel to observe activities around or inside an installation while minimizing their presence. An adequate level of illumination for all approaches to an installation will not discourage unauthorized entry; however, adequate lighting improves the ability of security personnel to assess visually and intervene on attempts at unauthorized entry. Lighting is used with other security measures (such as fixed security posts or patrols, fences, and ESSs) and should never be used alone. Other principles of security lighting include the following:

- Optimum security lighting is achieved by adequate, even light on bordering areas; glaring lights in the eyes of an intruder; and little light on security-patrol routes. In addition to seeing long distances, security forces must be able to see low contrasts (such as indistinct outlines of silhouettes) and must be able to detect an intruder who may be exposed to view for only a few seconds. Higher levels of illumination improve these abilities.
- High brightness contrast between an intruder and the background should be the first consideration when planning for security lighting. With predominantly dark, dirty surfaces or camouflage-type painted surfaces, more light is needed to produce the same brightness around installations and buildings than when clean concrete, light brick, and grass predominate. When the same amount of light falls on an object and its background, the observer must depend on contrasts in the amount of light reflected. His ability to distinguish poor contrasts is significantly improved by increasing the illumination level.
- The observer primarily sees an outline or a silhouette when the intruder is darker than his background. Using light finishes on the lower parts of buildings and structures may expose an intruder who depends on dark clothing and darkened face and hands. Stripes on walls have also been used effectively, as they provide recognizable breaks in outlines or silhouettes. Providing broad-lighted areas around and within the installation against which intruders can be seen can also create good observation conditions.

5-9. To be effective, two basic systems or a combination of both may be used to provide practical and effective security lighting. The first method is to light the boundaries and approaches; the second is to light the area and structures within the property's general boundaries. Protective lighting should—

- Discourage or deter attempts at entry by intruders. Proper illumination may lead a potential intruder to believe detection is inevitable.
- Make detection likely if entry is attempted.
- Prevent glare that may temporarily blind the guards.

TYPES OF LIGHTING

5-10. The type of lighting system used depends on the installation's overall security requirements. Four types of lighting units are used for security-lighting systems—continuous, standby, movable (portable), and emergency.

5-11. Continuous lighting is the most common security-lighting system. It consists of a series of fixed lights arranged to flood a given area continuously during darkness with overlapping cones of light. Two primary methods of using continuous lighting are glare projection and controlled lighting.

- The glare security-lighting method is used when the glare of lights directed across the surrounding territory will not be annoying nor interfere with adjacent operations. It is a strong deterrent to a potential intruder because it makes it difficult to see inside of the area. Guards are protected by being kept in comparative darkness and being able to observe intruders at a considerable distance beyond the perimeter.
- Controlled lighting is best when it limits the width of the lighted strip outside the perimeter, such as along highways. In controlled lighting, the width of the lighted strip is controlled and adjusted to fit the particular need. This method of lighting may illuminate or silhouette security personnel.

5-12. Standby lighting has a layout similar to continuous lighting. However, the luminaries are not continuously lit but are either automatically or manually turned on when suspicious activity is detected or suspected by the security force or alarm systems.

5-13. Movable lighting consists of manually operated, movable searchlights that may be lit during hours of darkness or only as needed. The system normally is used to supplement continuous or standby lighting.

5-14. Emergency lighting is a system of lighting that may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on an alternative power source such as installed or portable generators or batteries.

FENCED PERIMETERS

5-15. Fenced perimeters require the lighting specifications indicated in TM 5-853-2. Specific lighting requirements are based on whether the perimeter is isolated, semi-isolated, or nonisolated.

- Isolated fenced perimeters are fence lines around areas where the fence is 100 feet or more from buildings or operating areas. The approach area is clear of obstruction for 100 or more feet outside of the fence. Other personnel do not use the area. Use glare projection for these perimeters and keep patrol routes unlit.
- Semi-isolated fenced perimeters are fence lines where approach areas are clear of obstruction for 60 to 100 feet outside of the fence. The general public or installation personnel seldom have reason to be in the area. Use controlled lighting for these perimeters and keep patrol routes in relative darkness.

- Nonisolated fenced perimeters are fence lines immediately adjacent to operating areas. These areas may be within an installation or public thoroughfares. Outsiders or installation personnel may move about freely in this approach area. The width of the lighted strip depends on the clear zones inside and outside the fence. Use controlled lighting for these perimeters. It may not be practical to keep the patrol area dark.

ENTRANCES

5-16. Entrances for pedestrians will have two or more lighting units providing adequate illumination for recognition of persons and examination of credentials. Vehicle entrances will have two lighting units located to facilitate the complete inspection of passenger cars, trucks, and freight cars as well as their contents and passengers. Semiactive and inactive entrances will have the same degree of continuous lighting as the remainder of the perimeter, with standby lighting to be used when the entrance becomes active. Gatehouses at entrances should have a low level of interior illumination, enabling guards to see approaching pedestrians and vehicles.

OTHER

5-17. Areas and structures within the installation's property line consist of yards; storage spaces; large, open working areas; piers; docks; and other sensitive areas and structures.

- Open yards (unoccupied land only) and outdoor storage spaces (material storage areas, railroad sidings, motor pools, and parking areas) should be illuminated. An open yard adjacent to a perimeter (between guards and fences) will be illuminated according to the perimeter's illumination requirements. Where lighting is necessary in other open yards, illumination will not be less than 0.2 foot-candle at any point.
- Lighting units are placed in outdoor storage spaces to provide an adequate distribution of light in aisles, passageways, and recesses to eliminate shadowed areas where unauthorized persons may hide.
- Illuminating both water approaches and the pier area safeguards piers and docks located on an installation. Decks on open piers will be illuminated to at least 1 foot-candle and the water approaches (extending to a distance of 100 feet from the pier) to at least 0.5 foot-candle. The area beneath the pier floor will be lit with small wattage floodlights arranged on the piling. Movable lighting is recommended as a part of the protective lighting system for piers and docks. The lighting must not in any way violate marine rules and regulations (it must not be glaring to pilots). Consult the US Coast Guard (USCG) for approval of protective lighting adjacent to navigable waters.

WIRING SYSTEMS

5-18. The wiring circuit should be arranged so that failure of any one lamp will not leave a large portion of the perimeter line or a major segment of a critical or vulnerable position in darkness. Feeder lines will be placed underground (or sufficiently inside the perimeter in the case of overhead

wiring) to minimize the possibility of sabotage or vandalism from outside the perimeter. Another advantage to underground wiring is reduced effects from adverse weather conditions.

MAINTENANCE

5-19. Periodic inspections will be made of all electrical circuits to replace or repair worn parts, tighten connections, and check insulation. Keep fixtures clean and properly aimed.

POWER SOURCES

5-20. Primary and alternate power sources must be identified. The following is a partial list of considerations:

- The primary source is usually a local public utility.
- An alternate source (standby batteries or diesel-fuel-driven generators may be used) is provided where required and should—
 - Start automatically upon failure of primary power.
 - Be adequate to power the entire lighting system.
 - Be equipped with adequate fuel storage and supply.
 - Be tested under load to ensure efficiency and effectiveness.
 - Be located within a controlled area for additional security.

CCTV-CAMERA LIGHTING REQUIREMENTS

5-21. TM 5-853-4 provides a detailed discussion of CCTV-camera lighting requirements and guidelines for minimum lighting levels and lighting uniformity. The following considerations apply when lighting systems are intended to support CCTV assessment or surveillance:

- The camera's field of view.
- Lighting intensity levels.
- Maximum light-to-dark ratio.
- Scene reflectance.
- Daylight-to-darkness transitions.
- Camera mounting systems relative to lighting.
- The camera's spectral response.
- The cold-start time.
- The restrike time.

Chapter 7

Access Control

Perimeter barriers, intrusion-detection devices, and protective lighting provide physical-security safeguards; however, they alone are not enough. An access-control system must be established and maintained to preclude unauthorized entry. Effective access-control procedures prevent the introduction of harmful devices, materiel, and components. They minimize the misappropriation, pilferage, or compromise of materiel or recorded information by controlling packages, materiel, and property movement. Access-control rosters, personal recognition, ID cards, badge-exchange procedures, and personnel escorts all contribute to an effective access-control system.

DESIGNATED RESTRICTED AREAS

7-1. The installation commander is responsible for designating and establishing restricted areas. A restricted area is any area that is subject to special restrictions or controls for security reasons. This does not include areas over which aircraft flight is restricted. Restricted areas may be established for the following:

- The enforcement of security measures and the exclusion of unauthorized personnel.
- Intensified controls in areas requiring special protection.
- The protection of classified information or critical equipment or materials.

DEGREE OF SECURITY

7-2. The degree of security and control required depends on the nature, sensitivity, or importance of the security interest. Restricted areas are classified as controlled, limited, or exclusion areas.

- A controlled area is that portion of a restricted area usually near or surrounding a limited or exclusion area. Entry to the controlled area is restricted to personnel with a need for access. Movement of authorized personnel within this area is not necessarily controlled since mere entry to the area does not provide access to the security interest. The controlled area is provided for administrative control, for safety, or as a buffer zone for in-depth security for the limited or exclusion area. The commander establishes the control of movement.
- A limited area is a restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the item. Escorts and other internal restrictions may prevent access within limited areas.

- An exclusion area is a restricted area containing a security interest. Uncontrolled movement permits direct access to the item.

7-3. The security protection afforded by a restricted area pertains particularly to subversive-activity control; that is, protection against espionage, sabotage, or any such action adversely affecting national defense. Within this context, the designation "restricted area" is not applicable to an area solely for protection against common pilferage or misappropriation of property or material that is not classified or not essential to national defense. For example, an area devoted to the storage or use of classified documents, equipment, or materials should be designated as a restricted area to safeguard against espionage. An installation communications center should also be so designated to safeguard against sabotage. On the other hand, a cashier's cage or an ordinary mechanic's tool room should not be so designated, although the commander may impose controls to access. This may be a simple matter of posting an "off limits to unauthorized personnel" sign. The PM or the physical-security manager acts as an advisor to the commander. In his recommendations, he must consider evaluating the purpose of designating a restricted area and coordinating with the intelligence officer and the staff judge advocate (SJA).

7-4. A restricted area must be designated in writing by the commander and must be posted with warning signs according to AR 190-13. In areas where English is one of two or more languages commonly spoken, warning signs will be posted in English and in the local language (see Figure 7-1).

7-5. An installation may have varying degrees of security. It may be designated in its entirety as a restricted area, with no further restrictions; or it may be subdivided into controlled, limited, or exclusion areas with restrictions of movement and specific clear zones. Figure 7-2 depicts a simplified restricted area and the degrees of security.

CONSIDERATIONS

7-6. There are other important considerations concerning restricted areas and their lines of division. These considerations include the following:

- A survey and analysis of the installation, its missions, and its security interests. This can determine immediate and anticipated needs that require protection. Anticipated needs are determined from plans for the future.
- The size and nature of the security interest being protected. Safes may provide adequate protection for classified documents and small items; however, large items may have to be placed within guarded enclosures.
- Some security interests are more sensitive to compromise than others. Brief observation or a simple act by an untrained person may constitute a compromise in some cases. In others, detailed study and planned action by an expert may be required.
- All security interests should be evaluated according to their importance. This may be indicated by a security classification such as confidential, secret, or top secret.

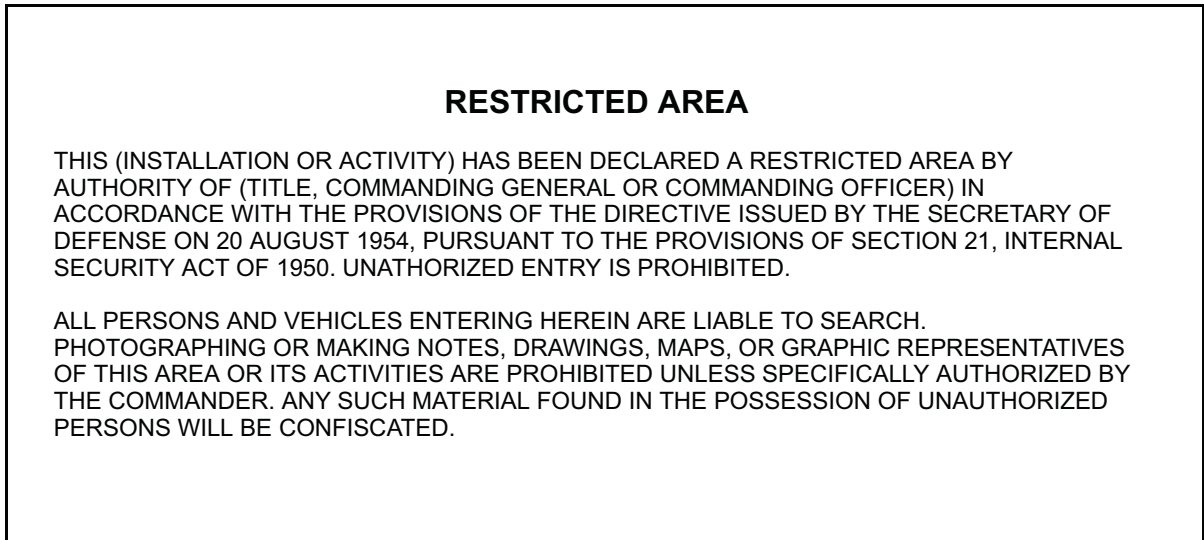


Figure 7-1. Sample Restricted-Area Warning

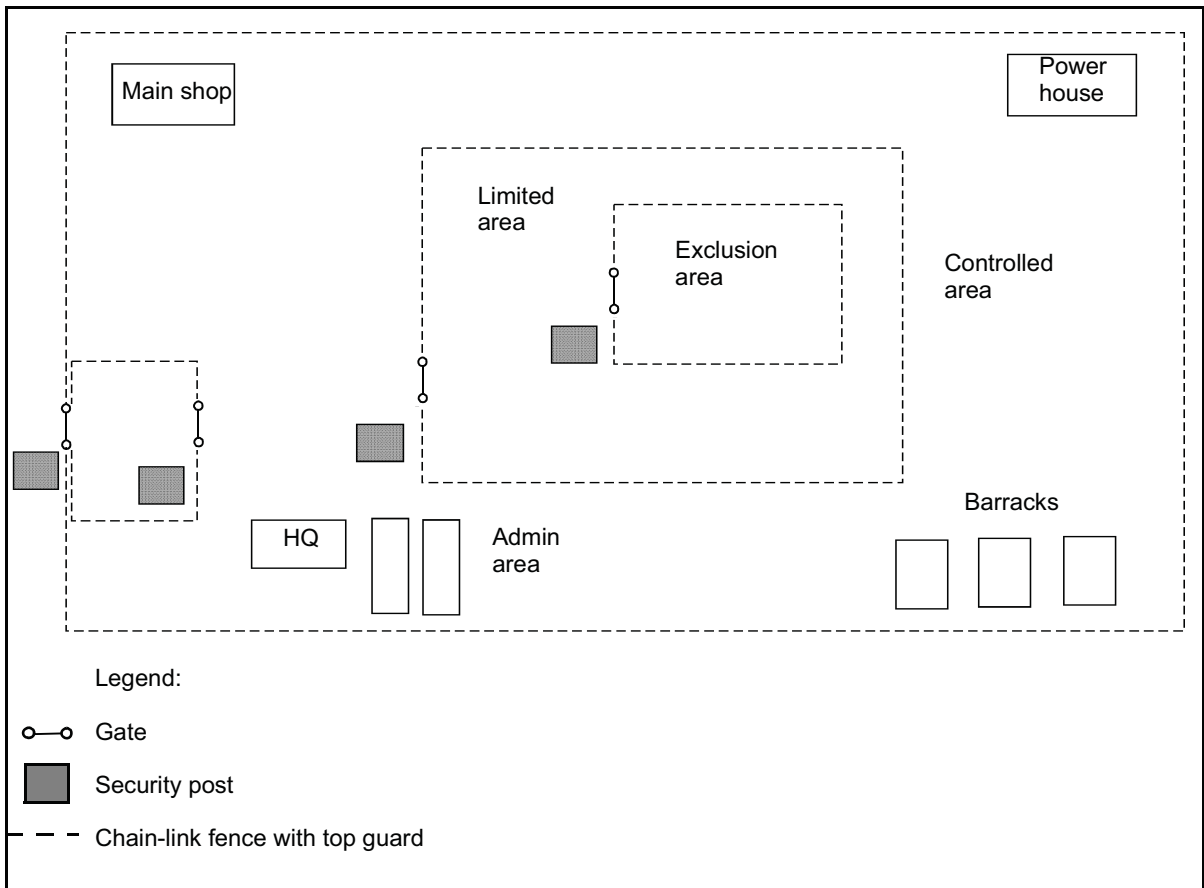


Figure 7-2. Schematic Diagram of a Simplified Restricted Area and the Degrees of Security

- Parking areas for privately owned vehicles (POVs) are established outside of restricted areas. Vehicle entrances must be kept at a minimum for safe and efficient control.
- Physical protective measures (such as fences, gates, and window bars) must be installed.

EMPLOYEE SCREENING

7-7. Screening job applicants to eliminate potential acts of espionage and sabotage and other security risks is important in peacetime and is critical during a national emergency. Personnel screenings must be incorporated into standard personnel policies.

7-8. An applicant should be required to complete a personnel security questionnaire, which is then screened for completeness and used to eliminate undesirable applicants. A careful investigation should be conducted to ensure that the applicant's character, associations, and suitability for employment are satisfactory. The following sources may be helpful in securing employment investigative data:

- State and local police (including national and local police in overseas areas).
- Former employers.
- Public records.
- Credit agencies.
- Schools (all levels).
- References. (These references should include those names not furnished by the applicant. These are known as throw offs, and they are obtained during interviews of references furnished by applicants.)
- Others as appropriate. (These may include the FBI, the US Army Criminal Records Repository, and the Defense Investigative Agency).

7-9. Medical screening considerations should be made (based on an applicant's position [such as a guard]) to evaluate physical and mental stamina. Once an applicant has been identified for employment, he is placed on an access-control roster.

IDENTIFICATION SYSTEM

7-10. An ID system is established at each installation or facility to provide a method of identifying personnel. The system provides for personal recognition and the use of security ID cards or badges to aid in the control and movement of personnel activities.

7-11. Standard ID cards are generally acceptable for access into areas that are unrestricted and have no security interest. Personnel requiring access to restricted areas should be issued a security ID card or badge as prescribed in AR 600-8-14. The card's/badge's design must be simple and provide for adequate control of personnel.

7-12. A security ID card/badge system must be established for restricted areas with 30 or more employees per shift. Commanders may (at their

discretion) authorize a card/badge system in restricted areas for less than 30 people.

ID METHODS

7-13. Four of the most commonly used access-control ID methods are the personal-recognition system, the single-card or -badge system, the card- or badge-exchange system, and the multiple-card or -badge system.

Personal-Recognition System

7-14. The personal-recognition system is the simplest of all systems. A member of the security force providing access control visually checks the person requesting entry. Entry is granted based on—

- The individual being recognized.
- The need to enter has been established.
- The person is on an access-control roster.

Single-Card or -Badge System

7-15. This system reflects permission to enter specific areas by the badge depicting specific letters, numbers, or particular colors. This system lends to comparatively loose control and is not recommended for high-security areas. Permission to enter specific areas does not always go with the need to know. Because the ID cards/badges frequently remain in the bearer's possession while off duty, it affords the opportunity for alteration or duplication.

Card- or Badge-Exchange System

7-16. In this system, two cards/badges contain identical photographs. Each card/badge has a different background color, or one card/badge has an overprint. One card/badge is presented at the entrance to a specific area and exchanged for the second card/badge, which is worn or carried while in that area. Individual possession of the second card/badge occurs only while the bearer is in the area for which it was issued. When leaving the area, the second card/badge is returned and maintained in the security area. This method provides a greater degree of security and decreases the possibility of forgery, alteration, or duplication of the card/badge. The levels of protection described in TM 5-853-1 require multiple access-control elements as the levels of protection increase. In the case of the badge exchange, this system counts as two access-control elements.

Multiple-Card or -Badge System

7-17. This system provides the greatest degree of security. Instead of having specific markings on the cards/badges denoting permission to enter various restricted areas, the multiple card/badge system makes an exchange at the entrance to each security area. The card/badge information is identical and allows for comparisons. Exchange cards/badges are maintained at each area only for individuals who have access to the specific area.

MECHANIZED/AUTOMATED SYSTEMS

7-18. An alternative to using guards or military police (MP) to visually check cards/badges and access rosters is to use building card-access systems or biometric-access readers. These systems can control the flow of personnel entering and exiting a complex. Included in these systems are—

- Coded devices such as mechanical or electronic keypads or combination locks.
- Credential devices such as magnetic-strip or proximity card readers.
- Biometric devices such as fingerprint readers or retina scanners.

7-19. Access-control and ID systems base their judgment factor on a remote capability through a routine discriminating device for positive ID. These systems do not require guards at entry points; they identify an individual in the following manner:

- The system receives physical ID data from an individual.
- The data is encoded and compared to stored information.
- The system determines whether access is authorized.
- The information is translated into readable results.

7-20. Specialized mechanical systems are ideal for highly sensitive situations because they use a controlled process in a controlled environment to establish the required database and accuracy. One innovative technique applied to ID and admittance procedures involves dimension comparisons. The dimension of a person's full hand is compared to previously stored data to determine entry authorization. Other specialized machine readers can scan a single fingerprint or an eye retina and provide positive ID of anyone attempting entry.

7-21. An all-inclusive automated ID and access-control system reinforces the security in-depth ring through its easy and rapid change capability. The computer is able to do this through its memory. Changes can be made quickly by the system's administrator.

7-22. The commercial security market has a wide range of mechanized and automated hardware and software systems. Automated equipment is chosen only after considering the security needs and the environment in which it operates. These considerations include whether the equipment is outdoors or indoors, the temperature range, and weather conditions. Assessment of security needs and the use of planning, programming, and budgeting procedures greatly assist a security manager in improving the security posture.

CARD/BADGE SPECIFICATIONS

7-23. Security cards/badges should be designed and constructed to meet the requirements of AR 600-8-14. Upon issuing a card/badge, security personnel must explain to the bearer the wear required and the authorizations allowed with the card/badge. This includes—

- Designation of the areas where an ID card/badge is required.

-
- A description of the type of card/badge in use and the authorizations and limitations placed on the bearer.
 - The required presentation of the card/badge when entering or leaving each area during all hours of the day.
 - Details of when, where, and how the card/badge should be worn, displayed, or carried.
 - Procedures to follow in case of loss or damage of the card.
 - The disposition of the card/badge upon termination of employment, investigations, or personnel actions.
 - Prerequisites for reissuing the card/badge.

VISITOR IDENTIFICATION AND CONTROL

7-24. Procedures must be implemented to properly identify and control personnel. This includes visitors presenting their cards/badges to guards at entrances of restricted areas. Visitors are required to stay with their assigned escort. Guards must ensure that visitors stay in areas relating to their visit; an uncontrolled visitor, although conspicuously identified, could acquire information for which he is not authorized. Foreign-national visitors should be escorted at all times.

7-25. Approval for visitors should be obtained at least 24 hours in advance (if possible). Where appropriate, the installation should prepare an agenda for the visitor and designate an escort officer. Measures must be in place to recover visitor cards/badges on the visit's expiration or when they are no longer required.

7-26. Physical-security precautions against pilferage, espionage, and sabotage require the screening, ID, and control of visitors. Further information about visiting requirements and procedures are found in ARs 12-15 and 381-20. Visitors are generally classed in the following categories:

- Persons with whom every installation or facility has business (such as suppliers, customers, insurance inspectors, and government inspectors).
- Individuals or groups who desire to visit an installation or facility for personal or educational reasons. Such visits may be desired by educational, technical, or scientific organizations.
- Individuals or groups specifically sponsored by the government (such as foreign nationals visiting under technical cooperation programs and similar visits by US nationals). Requests for visits by foreign nationals must be processed according to AR 380-10.
- Guided tours to selected portions of the installation in the interest of public relations.

7-27. The ID and control mechanisms for visitors must be in place. They may include the following:

- Methods of establishing the authority for admitting visitors and any limitations relative to access.

- Positive ID of visitors by personal recognition, visitor permit, or other identifying credentials. Contact the employer, supervisor, or officer in charge to validate the visit.
- The use of visitor registration forms. These forms provide a record of the visitor and the time, location, and duration of his visit.
- The use of visitor ID cards/badges. The cards/badges bear serial numbers, the area or areas to which access is authorized, the bearer's name, and escort requirements.

7-28. Individual groups entering a restricted area must meet specific prerequisites before being granted access. The following guidance is for group access into a restricted area:

Visitors

7-29. Before allowing visitors into a restricted area, contact the person or activity being visited. After verifying the visitor's identity, issue a badge, complete the registration forms, and assign an escort (if required). Visitors may include public-utility and commercial-service representatives.

Very Important Persons

7-30. The procedures for admitting very important persons (VIPs) and foreign nationals into restricted areas are contained in AR 12-15. Special considerations and coordination with the protocol office are necessary. A 24-hour advance notice is desirable for these requests, along with an agenda for the visit and the designation of an escort, if appropriate.

Civilians Working on Jobs Under Government Contract

7-31. To allow these personnel to conduct business in restricted areas, the security manager must coordinate with the procurement office. The security manager must also identify movement-control procedures for these employees.

Cleaning Teams

7-32. Supervisors using cleaning teams must seek technical advice from the physical-security office on internal controls for each specific building. This may include providing escorts.

DOD Employees in Work Areas After Normal Operating Hours

7-33. Supervisors establish internal controls based on coordination with the security manager. They also notify security personnel of the workers' presence, type, and duration of work.

ENFORCEMENT MEASURES

7-34. The most vulnerable link in any ID system is its enforcement. Security forces must be proactive in performing their duties. A routine performance of duty will adversely effect even the most elaborate system. Positive enforcement measures must be prescribed to enhance security. Some of these measures may include—

- Designating alert and tactful security personnel at entry control points.
- Ensuring that personnel possess quick perception and good judgment.
- Requiring entry-control personnel to conduct frequent irregular checks of their assigned areas.
- Formalizing standard procedures for conducting guard mounts and posting and relieving security personnel. These measures will prevent posting of unqualified personnel and a routine performance of duty.
- Prescribing a uniform method of handling or wearing security ID cards/badges. If carried on the person, the card must be removed from the wallet (or other holder) and handed to security personnel. When worn, the badge will be worn in a conspicuous position to expedite inspection and recognition from a distance.
- Designing entry and exit control points of restricted areas to force personnel to pass in a single file in front of security personnel. In some instances, the use of turnstiles may be advisable to assist in maintaining positive control.
- Providing lighting at control points. The lighting must illuminate the area to enable security personnel to compare the bearer with the ID card/badge.
- Enforcing access-control measures by educating security forces and employees. Enforcement of access-control systems rests primarily with the security forces; however, it is essential that they have the full cooperation of the employees. Employees must be instructed to consider each unidentified or improperly identified individual as a trespasser. In restricted areas where access is limited to a particular zone, employees must report unauthorized individuals to the security force.
- Positioning ID card/badge racks or containers at entry control points so that they are accessible only to guard-force personnel.
- Appointing a responsible custodian to accomplish control procedures of cards/badges according to AR 600-8-14. The custodian is responsible for the issue, turn in, recovery, and renewal of security ID cards/badges.

7-35. The degree of compromise tolerable in the ID system is in direct proportion to the degree of security required. The following control procedures are recommended for preserving the integrity of a card/badge system:

- Maintenance of an accurate written record or log listing (by serial number) all cards and badges and showing those on hand, to whom they are issued, and their disposition (lost, mutilated, or destroyed).
- Authentication of records and logs by the custodian.
- A periodic inventory of records by a commissioned officer.
- The prompt invalidation of lost cards/badges.
- The conspicuous posting at security control points of current lists of lost or invalidated cards/badges.
- The establishment of controls within restricted areas to enable security personnel to determine the number of persons within the area.
- The establishment of the two-person rule (when required).

- The establishment of procedures to control the movement of visitors. A visitor-control record will be maintained and located at entry control points.

SIGN/COUNTERSIGN AND CODE WORD

7-36. This method of verifying identity is primarily used in a tactical environment. According to the local SOP, the sign/countersign or code-word procedures must be changed immediately if compromised.

DURESS CODE

7-37. The duress code is a simple word or phrase used during normal conversation to alert other security personnel that an authorized person is under duress. A duress code requires planning and rehearsal to ensure an appropriate response. This code is changed frequently to minimize compromise.

ACCESS-CONTROL ROSTERS

7-38. Admission of personnel to a restricted area is granted to those identified and listed on an access-control roster. Pen-and-ink changes may be made to the roster. Changes are published in the same manner as the original roster.

7-39. Rosters are maintained at access control points. They are kept current, verified, and accounted for by an individual designated by the commander. Commanders or their designated representatives authenticate the rosters. Admission of persons other than those on the rosters is subject to specific approval by the security manager. These personnel may require an escort according to the local SOP.

METHODS OF CONTROL

7-40. There are a number of methods available to assist in the movement and control of personnel in limited, controlled, and restricted areas. The following paragraphs discuss the use of escorts and the two-person rule:

ESCORTS

7-41. Escorts are chosen because of their ability to accomplish tasks effectively and properly. They possess knowledge of the area being visited. Escorts may be guard-force personnel, but they are normally personnel from the area being visited. Local regulations and SOPs determine if a visitor requires an escort while in the restricted area. Personnel on the access list may be admitted to restricted areas without an escort.

TWO-PERSON RULE

7-42. The two-person rule is designed to prohibit access to sensitive areas or equipment by a lone individual. Two authorized persons are considered present when they are in a physical position from which they can positively detect incorrect or unauthorized procedures with respect to the task or operation being performed. The team is familiar with applicable safety and

security requirements, and they are present during any operation that affords access to sensitive areas or equipment that requires the two-person rule. When application of the two-person rule is required, it is enforced constantly by the personnel who constitute the team.

7-43. The two-person rule is applied in many other aspects of physical-security operations, such as the following:

- When uncontrolled access to vital machinery, equipment, or materiel might provide opportunity for intentional or unintentional damage that could affect the installation's mission or operation.
- When uncontrolled access to funds could provide opportunity for diversion by falsification of accounts.
- When uncontrolled delivery or receipt for materials could provide opportunity for pilferage through "short" deliveries and false receipts.
- When access to an arms or ammunition storage room could provide an opportunity for theft. Keys should be issued so that at least two people must be present to unlock the locks required under the provisions of AR 190-11.

7-44. The two-person rule is limited to the creativity of the PM and the physical-security manager. They should explore every aspect of physical-security operations in which the two-person rule would provide additional security and assurance and include all appropriate recommendations and provisions of the physical-security plan. An electronic-entry control system may be used to enforce the two-person rule. The system can be programmed to deny access until two authorized people have successfully entered codes or swiped cards.

SECURITY CONTROLS OF PACKAGES, PERSONAL PROPERTY, AND VEHICLES

7-45. A good package-control system helps prevent or minimize pilferage, sabotage, and espionage. The local SOP may allow the entry of packages with proper authorization into restricted areas without inspection. A package-checking system is used at the entrance gate. When practical, inspect all outgoing packages except those properly authorized for removal. When a 100 percent inspection is impractical, conduct frequent unannounced spot checks. A good package-control system assists in the movement of authorized packages, material, and property.

7-46. Property controls are not limited to packages carried openly, but they include the control of anything that could be used to conceal property or material. Personnel should not be routinely searched except in unusual situations. Searches must be performed according to the local SOP.

7-47. All POVs on the installation should be registered with the PM or the installation's physical-security office. Security personnel should assign a temporary decal or other temporary ID tag to visitors' vehicles to permit ready recognition. The decal or the tag should be distinctly different from that of permanent-party personnel.

7-48. When authorized vehicles enter or exit a restricted area, they undergo a systematic search, including (but not limited to) the—

- Vehicle's interior.
- Engine compartment.
- External air breathers.
- Top of the vehicle.
- Battery compartment.
- Cargo compartment.
- Undercarriage.

7-49. The movement of trucks and railroad cars into and out of restricted areas should be supervised and inspected. Truck and railroad entrances are controlled by locked gates when not in use and are manned by security personnel when unlocked. The ID cards/badges are issued to operators to ensure proper ID and registration for access to specific loading and unloading areas.

7-50. All conveyances entering or leaving a protected area are required to pass through a service gate manned by security forces. Drivers, helpers, passengers, and vehicle contents must be carefully examined. The examination may include—

- Appropriate entries in the security log (including the date, operator's name, load description, and time entered and departed).
- A check of the operator's license.
- Verification of the seal number with the shipping document and examination of the seal for tampering.

7-51. Incoming trucks and railroad cars must be assigned escorts before they are permitted to enter designated limited or exclusion areas. Commanders should establish published procedures to control the movement of trucks and railroad cars that enter designated restricted areas to discharge or pick up cargo (escorts will be provided when necessary).

7-52. The best control is provided when all of these elements are incorporated into access-control procedures. Simple, understandable, and workable access-control procedures are used to achieve security objectives without impeding operations. When properly organized and administered, access-control procedures provide a method of positively identifying personnel who have the need to enter or leave an area.

TACTICAL-ENVIRONMENT CONSIDERATIONS

7-53. Access-control procedures during tactical operations may establish additional challenges for the commander. In some instances, the commander cannot provide a perimeter barrier (such as a fence) based on METT-TC. Commanders are still required to provide security measures for restricted areas, although they may not always have the necessary assets. Early-warning systems and the use of guards become crucial. A restricted area may become a requirement without prior notice during an operation. Figure 7-3 and Figure 7-4, page 7-14, are examples of temporary tactical restricted and exclusion areas.

7-54. Commanders must plan for these considerations when developing their budget. Funding must be requested and set aside to support physical-security requirements during tactical operations. Resources will not always be available; therefore, commanders must implement procedures that support access-control measures. Improvising will become common practice to overcome shortfalls concerning access-control equipment in the field.

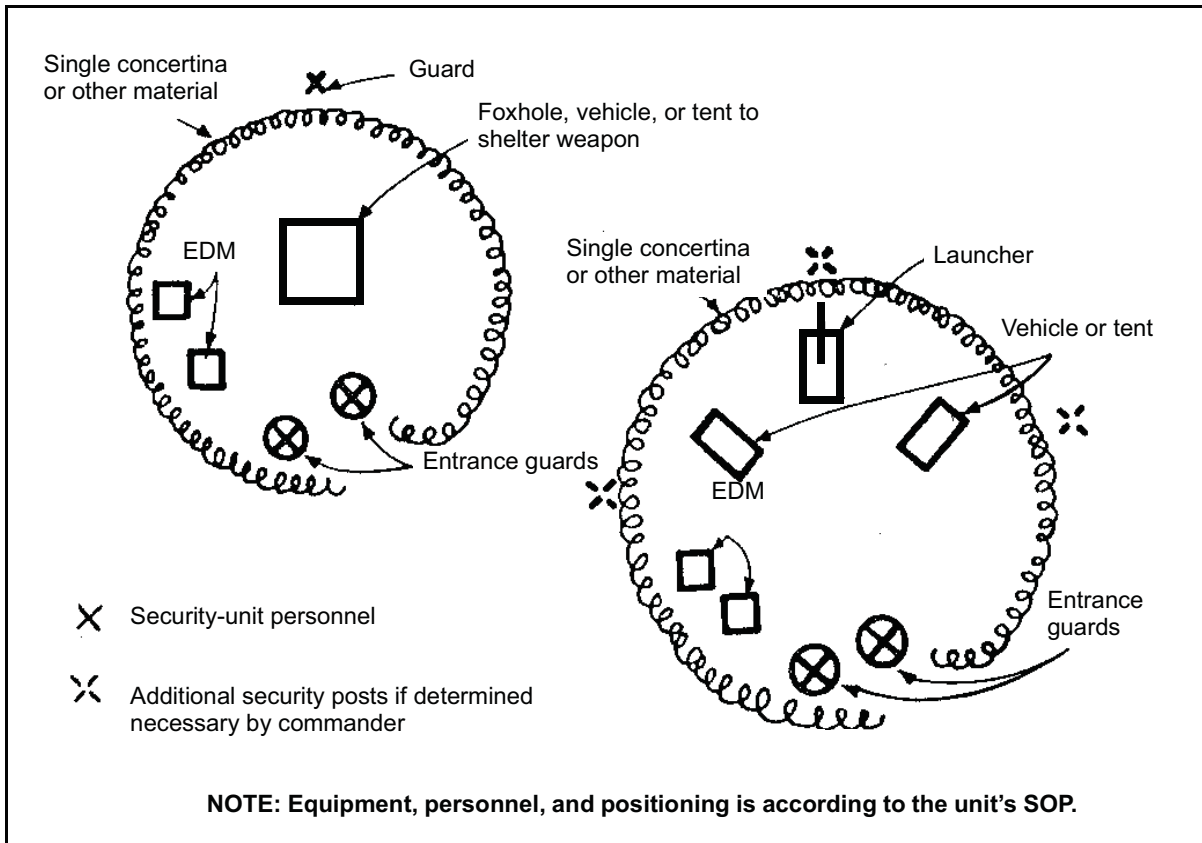


Figure 7-3. Sample Layout of Temporary Tactical Restricted Areas

Appendix H

Bombs

Terrorists have frequently used homemade devices or IEDs to carry out their attacks against DOD personnel, facilities, and assets. The IEDs are ideal terrorist weapons. They are relatively inexpensive to make, and the components of many IEDs are common items that can be obtained from many sources and are difficult to trace. The IEDs can be large or small and be designed so that they are transported to the attack site in components for last-minute assembly. Such design concepts make detection more difficult and provide an additional increment of personal safety to the terrorists.

GENERAL

H-1. The use of IEDs can enhance the violence that gives terrorist groups their ability to intimidate or coerce a target population. The detonation itself creates a highly visual, newsworthy scene, even hours after the detonation occurs. Bombs can detonate anywhere, without apparent reason and without warning. The use of bombs in a terror campaign emphasizes the authorities' inability to safeguard the public and maintain law and order. Bombs are ideal weapons because they can be designed to give terrorists opportunities to escape from the scene of their crimes.

CONCEALING BOMBS

H-2. Given the question, "Where have terrorists placed bombs in the past, and where should we look for them?" results in no easy answer. Table H-1, page H-2, lists a few obvious locations that should be examined. Terrorists who use bombs as their weapons of choice can be very creative in designing and placing their weapons.

H-3. Bombs can be found anywhere people can place them. Without becoming paranoid and seeing a bomb under every rock and behind every tree, the practical answer to the above questions is: "Where they can be easily placed without the bomber being caught."

DAMAGE AND CASUALTY MECHANISMS

H-4. The IEDs and other explosive devices inflict casualties in a variety of ways, including the following:

- Blast over pressure (a crushing action on vital components of the body; eardrums are the most vulnerable).
- Falling structural material.
- Flying debris (especially glass).
- Asphyxiation (lack of oxygen).

Table H-1. Potential IED Hiding Places

Outside Areas	
• Trash cans	• Street drainage systems
• Dumpsters	• Storage areas
• Mailboxes	• Parked cars
• Bushes	
Inside Buildings	
• Mail parcels or letters	• Restrooms
• Inside desks/storage containers	• Trash receptacles
• Ceilings with removable panels	• Utility closets
• Areas hidden by drapes or curtains	• Boiler rooms
• Recent repaired/patched segments of walls, floors, or ceilings	• Under stairwells
In Plain Sight	

- Sudden body translation against rigid barriers or objects (being picked up and thrown by a pressure wave).
- Bomb fragments.
- Burns from incendiary devices or fires resulting from blast damage.
- Inhalation of toxic fumes resulting from fires.

H-5. It is impossible to calculate a single minimum safe distance from an IED or other explosive device. The safe distance varies with each device and its placement. As a rule, the farther away from a bomb, the safer the intended or collateral targets are. Blast effects, fragmentation injuries, and injuries resulting from flying debris diminish greatly as the distance between a bomb and possible targets increase. The amount of material in the device, the type of explosive material, the manner in which the device is constructed, and the location or the container in which it is placed all have a bearing on the specific destructive potential for each IED.

H-6. The following are four general rules to follow to avoid injury from an IED:

- Move as far from a suspicious object as possible without being in further danger from other hazards such as traffic or secondary sources of explosion (such as POL storage).
- Stay out of the object's LOS, thereby reducing the hazard of injury because of direct fragmentation.
- Keep away from glass windows or other materials that could become flying debris.
- Remain alert for additional or secondary explosive devices in the immediate area, especially if the existence of a bomb-threat evacuation assembly area has been highly publicized.

H-7. Some terrorists have used two especially devious tactics in the past to intensify the magnitude of casualties inflicted by bombing attacks. In some instances, they have detonated a small device to lure media attention and curiosity seekers to the site; a larger, more deadly device has detonated some time after the first device, thereby inflicting a large number of casualties.

H-8. Other terrorists have used a real or simulated device to force the evacuation of a facility only to detonate a much more substantial device in identified bomb-threat evacuation assembly areas. These attacks are especially harmful because the evacuation assembly areas often concentrate government or commercial office workers more densely than they are when dispersed throughout their usual workplaces.

TELEPHONIC THREATS

H-9. When receiving a telephonic threat, treat the call seriously. Often, an anonymous telephone call is made regarding a bomb or an IED. See Figure H-1, page H-4, for information to record/obtain when receiving these calls

H-10. When an anonymous warning or threat is received, initiate the bomb-threat data card and notify the PMO, security police, security forces, or other law-enforcement/security offices immediately. Local SOPs will determine subsequent actions. Immediate action may include a search without evacuation, the movement of personnel within the establishment, a partial evacuation, or a total evacuation. The following criteria helps determine what immediate action to take:

- Factors favoring a search before the movement of personnel:—
 - There is a high incidence of hoax telephone threats.
 - Effective security arrangements have been established.
 - Information in the warning is imprecise or incorrect.
 - The caller sounded intoxicated, amused, or very young.
 - The prevailing threat of terrorist activity is low.
- Factors favoring movement of personnel before searching:
 - The area (post or base) is comparatively open.
 - Information in the warning is precise as to the matters of location, a description of the device, the timing, and the motive for the attack.
 - A prevailing threat of terrorist activity is high.

EVACUATION DRILLS

H-11. Evacuation and search drills should be performed periodically under the supervision of the installation's or unit's senior officer. The drills should be held in cooperation with local police if possible. Personnel in adjacent buildings should be informed of drills to avoid causing unnecessary alarm.

H-12. Evacuation procedures depend on the circumstances. Prepare, publicize, and rehearse evacuation plans in advance. Address alarm systems, assembly areas, routes to assembly areas, personnel-evacuation responses, building and area clearances, and evacuation drills.

PERSONNEL-EVACUATION RESPONSE

H-13. The bomb-threat alarm system should be easily distinguished from the fire alarm. When the alarm sounds, personnel should—

- Lock up or secure all classified materials.
- Conduct a quick visual search of their immediate working area.

Instructions: Be calm. Be courteous. Listen, do not interrupt the caller. Notify supervisor/security officer by prearranged signal while caller is on line.

Name of Operator _____ Time _____ Date _____

Caller's Identity

Sex: Male Female Adult Juvenile Approximate age: Years _____

Origin of Call

Local Booth Internal (From within bldg)
 Long Distance If internal, leave line open for tracing the call.

Voice Characteristics	Speech	Language
<input type="checkbox"/> Loud <input type="checkbox"/> Soft <input type="checkbox"/> Fast	<input type="checkbox"/> Slow	<input type="checkbox"/> Excellent <input type="checkbox"/> Good
<input type="checkbox"/> High Pitch <input type="checkbox"/> Deep <input type="checkbox"/> Distinct	<input type="checkbox"/> Distorted	<input type="checkbox"/> Fair <input type="checkbox"/> Poor
<input type="checkbox"/> Raspy <input type="checkbox"/> Pleasant <input type="checkbox"/> Stutter	<input type="checkbox"/> Nasal	<input type="checkbox"/> Foul <input type="checkbox"/> Other _____
<input type="checkbox"/> Intoxicated <input type="checkbox"/> Other _____ <input type="checkbox"/> Slurred	<input type="checkbox"/> Lisp	
	<input type="checkbox"/> Other _____	

Accent	Manner	Background Noises
<input type="checkbox"/> Local	<input type="checkbox"/> Calm	<input type="checkbox"/> Factory Machines <input type="checkbox"/> Trains
<input type="checkbox"/> Not Local	<input type="checkbox"/> Rational	<input type="checkbox"/> Bedlam <input type="checkbox"/> Animals
Region _____	<input type="checkbox"/> Coherent	<input type="checkbox"/> Music <input type="checkbox"/> Quiet
<input type="checkbox"/> Foreign	<input type="checkbox"/> Deliberate	<input type="checkbox"/> Office Machines <input type="checkbox"/> Voices
Race _____	<input type="checkbox"/> Righteous	<input type="checkbox"/> Airplanes
	<input type="checkbox"/> Angry	<input type="checkbox"/> Street Traffic <input type="checkbox"/> Party Atmosphere
	<input type="checkbox"/> Irrational	
	<input type="checkbox"/> Incoherent	
	<input type="checkbox"/> Emotional	
	<input type="checkbox"/> Laughing	
	<input type="checkbox"/> Mixed	
	<input type="checkbox"/> Slurred	

Bomb Facts

Pretend difficulty with your hearing. Keep caller talking.

If caller seems agreeable to further conversation, ask questions like —
 When will it go off? Certain Hour - Time Remaining - What kind of bomb? - Where are you now?
 How do you know so much about the bomb? - What is your name and address?

If building is occupied, inform caller that detonation could cause injury or death.
 Did caller appear familiar with plant or building by his description of the bomb location?

Write out the message in its entirety and any other comments on a separate sheet of paper and attach to this checklist.

Action To Take Immediately After Call

Notify your supervisor/security officer as instructed. Talk to no one other than as instructed by your supervisor/security officer.

Figure H-1. Sample Bomb-Threat Data Card

- Open windows (wherever possible).
- Leave the building, taking only valuable personal belongings.
- Leave doors open and immediately proceed to the assembly area.

H-14. Opening the building will reduce internal damage due to blast effects. It will also somewhat mitigate the extent of debris flying out of or falling from the building should a detonation occur.

ASSEMBLY AREAS

H-15. Choose the routes to the assembly area so that personnel do not approach the IED at any time. Preselect the routes to the assembly area, but devise a system to inform personnel of the location of the suspected IED and alternate routes. Routes prevent confusion and bunching and avoid potential hazards (such as plate glass, windows, and likely locations of additional IEDs).

H-16. Assembly areas should be preselected and well known to personnel. Establish a clearly defined procedure for controlling, marshaling, and checking personnel within the assembly area. If buildings or establishments are in a public area, coordinate the assembly areas with local police. Assembly areas are selected using the following criteria:

- Locate assembly areas at least 100 meters from the likely target or building (if possible).
- Locate assembly areas in areas where there is little chance of an IED being hidden. Open spaces are best. Avoid parking areas because IEDs can be easily hidden in vehicles.
- Select alternate assembly areas to reduce the likelihood of ambush with a second device or small-arms fire. If possible, search the assembly area before personnel occupy the space.
- Avoid locating assembly areas near expanses of plate glass or windows. Blast effects can cause windows to be sucked outward rather than blown inward.
- Select multiple assembly areas (if possible) to reduce the concentration of key personnel. Drill and exercise personnel to go to different assembly areas to avoid developing an evacuation and emergency pattern that can be used by terrorists to attack identifiable key personnel.

BUILDING AND AREA CLEARANCE

H-17. Establish procedures to ensure that threatened buildings and areas are cleared. Prevent personnel from reentering the building. Establish a cordon to prevent personnel from entering the danger area. Establish an initial control point (ICP) as the focal point for the PMO and for MP control.

H-18. Cordon suspicious objects to a distance of at least 100 meters, and cordon suspicious vehicles to a distance of at least 200 meters. Ensure that nobody enters the cordoned area. Establish an ICP on the cordon to control access; relinquish ICP responsibility to the PMO or local police upon their arrival. Maintain the cordon until the PMO, security police, security forces, or local police have completed their examination or stated that the cordon may stand down.

SEARCHING FOR A SUSPECTED IED

H-19. Searches are conducted in response to a telephonic threat or a report of an unidentified object on or near premises occupied by DOD personnel. The following types of searches may be used when searching for a suspected bomb or IED:

- An occupant search is used when the threat's credibility is low. Occupants search their own areas. The search is completed quickly because occupants know their area and are most likely to notice anything unusual.
- A team search is used when the threat's credibility is high. The search is very thorough and places the minimum number of personnel at risk. Evacuate the area completely, and ensure that it remains evacuated until the search is complete. Search teams will make a slow, thorough, systematic search of the area.

H-20. The following procedures should be followed if a search for explosive devices must be conducted before qualified EOD teams arrive:

- Make an audio check, listening for unusual sounds.
- Sweep the area visually up to the waist, then sweep up to the ceiling. Do not forget the tops of cabinets and cupboards.
- Perform a thorough and systematic search in and around containers and fixtures.
- Pass search results as quickly as possible to the leader responsible for controlling the search area. Do not use a radio; it may detonate the explosive.

H-21. Circumstances might arise in the case of a very short warning period. In other instances, a threat of a bomb against some facilities (if true) might necessitate the evacuation of a very large area. In these circumstances, searching for the presence of an explosive device to identify its location, appearance, and possible operating characteristics may be warranted.

H-22. Personnel who have not been trained in IED search and ID techniques should not search for explosive devices. Two types of errors are very common—the false ID of objects as IEDs and the incorrect ID of IEDs as benign objects. Depending on the devices used to arm and trigger an IED, the search process could actually result in an explosion.

SEARCH ORGANIZATION

H-23. The person controlling the search should have a method of tracking and recording the search results (such as a diagram of the area). Delegate areas of responsibility to the search-team leader, who should report to the person controlling the search when each area has been cleared. Pay particular attention to entrances, toilets, corridors, stairs, unlocked closets, storage spaces, rooms and areas not checked by usual occupants, external building areas, window ledges, ventilators, courtyards, and spaces shielded from normal view.

DISCOVERY OF A SUSPECTED IED

H-24. When a suspicious object has been found, report its location and general description immediately to the nearest law-enforcement or supervisory person. Do not touch or move a suspicious object. Instead, perform the following steps:

- If an object appears in an area associated with a specific individual or a clearly identified area—
 - Ask the individual/occupant to describe objects they have brought to work in the past few days.
 - Ask for an accounting of objects.
 - Ask for a verbal description/ID of objects.
- If an object's presence remains inexplicable—
 - Evacuate buildings and surrounding areas, including the search team.
 - Ensure that evacuated areas are at least 100 meters from the suspicious object.
 - Establish a cordon and an ICP.
 - Inform personnel at the ICP that an object has been found.
 - Keep the person who located the object at the ICP until questioned.
 - Avoid reentering the facility to identify an object that may or may not be an IED.

REACTING TO AN EXPLODED IED

H-25. The following procedures should be taken when an explosive/IED detonates at a DOD facility:

- For explosions without casualties—
 - Maintain the cordon. Allow only authorized personnel into the explosion area.
 - Fight any fires threatening undamaged buildings without risking personnel.
 - Report the explosion to the PMO, security police, security forces, or local police if they are not on the scene.
 - Report the explosion to the installation operations center even if an EOD team is on its way. Provide as much detail as possible, such as the time of the explosion, the number of explosions, the color of smoke, and the speed and spread of fire.
 - Ensure that a clear passage for emergency vehicles (fire trucks, ambulances, and so forth) and corresponding personnel is maintained.
 - Refer media inquiries to the PAO.
 - Establish a separate information center to handle inquiries from concerned friends and relatives.
- For explosions with casualties—
 - Select a small number of personnel to help search for casualties.
 - Assign additional personnel the responsibility for maintaining the cordon to keep additional volunteers searching for casualties.

Maintain the cordon until the EOD team verifies no further presence of bombs/IEDs at the site and the fire marshal determines that risk of additional injury to searchers from falling debris is acceptable.

- Prepare a casualty list for notification of next of kin; delay publication of the list until its accuracy is determined.
- Arrange for unaffected personnel to contact their next of kin immediately.

H-26. Civilian management officials and subordinate military commanders continue to have important personal roles to fulfill during a bomb/IED attack on DOD personnel, facilities, and assets. Perform the following procedures when reporting an attack:

- Pass available information to the operations center.
- Avoid delaying reports due to lack of information; report what is known. Do not take risks to obtain information.
- Include the following information in the report:
 - Any warning received and if so, how it was received.
 - The identity of the person who discovered the device.
 - How the device was discovered (casual discovery or organized search).
 - The location of the device (give as much detail as possible).
 - The time of discovery.
 - The estimated length of time the device has been in its location.
 - A description of the device (give as much detail as possible).
 - Safety measures taken.
 - Suggested routes to the scene.
 - Any other pertinent information.

H-27. Perform the following procedures when providing emergency assistance to authorities:

- Ensure that the PMO, security police, security forces, and other emergency-response units from local police, fire and rescue, and EOD teams are not impeded from reaching the ICP. Help maintain crowd control and emergency services' access to the site.
- Evacuate through the doors and windows of buildings.
- Assist the on-scene commander by obtaining a building diagram showing detailed plans of the public-service conduits (gas, electricity, central heating, and so forth), if possible. If unavailable, a sketch can be drawn by someone with detailed knowledge of the building.
- Locate, identify, and make witnesses available to investigative agency representatives when they arrive on the scene. Witnesses include the person who discovered the device, witnessed the explosion, or possesses detailed knowledge of the building or area.

H-28. Performing the above steps will provide substantial assistance to the crisis-management team and give other personnel constructive, supportive actions to take in resolving the crisis. Care must be exercised, however, that additional explosive devices are not concealed for detonation during the midst of

rescue operations. These attacks add to the physical damage and emotional devastation of bomb/IED attacks.

H-29. The use of bombs and IEDs during terrorist attacks against DOD personnel, facilities, and assets is a common occurrence. The procedures outlined in this appendix are intended to help a DOD facility respond to an attack before an explosive device detonates. The procedures are also intended to help mitigate the consequences of an attack in case efforts to find an explosive device and render it inoperable are not successful. Incurring the costs to DOD facilities and installations of detecting an explosive device and terminating a terrorist incident before the device can detonate are almost always preferable rather than exercising plans and options to respond to a detonation. Several of the security measures discussed will help reduce the likelihood of a successful bomb/IED attack against DOD assets.