Appendix E

Countering Terrorism

Incidents of terrorism take place almost daily. Therefore, it is essential that security personnel know what to expect from terrorists and something of their beliefs and goals. This appendix addresses the following aspects of terrorism:

- ❑ History of violence
- ❑ The threat

- ❑ Target selection
- ❑ News media
- ❑ Weapons
- ❑ Typical operations
- ❑ Methods
- ❑ Jurisdiction
- ❑ Reporting incidents
- ❑ Installation vulnerability
- ❑ Countermeasures.

E-1 History of Violence

a. Violence dates back thousands of years. Torture was prevalent then and persisted into the 18th and 19th centuries. The 20th century introduced various forms of chemical and psychological torture.

b. Terrorism, historically, is most closely related and referenced to the reign of terror of the French Revolution in 1793. This was the first time an attempt was made to create an organization outside of a governmental body, whose philosophy was to systematically murder and set a rule of lawlessness based upon a political belief.

c. The terrorist threat has encompassed all areas of government, business and community life—international, national, and local. Terrorists have acted to spread fear for the following reasons:

(1) Retaliation-for a variety of political and/or organizational reasons.

(2) Destruction of Property-a message warning, or sign of things to come.

(3) Taking of hostages as bargaining tools for various goals.

d. The use of terror has always been:

(1) A means of coercion.

(2) A well planned campaign. (It still is.)

(3) The threat that further violence is possible/probable.

E-2 Target Selection Criteria

a. For maximum shock effect.

b. An environment that presents a low risk to the assault team, such as isolated situations and sites.

c. High risk environments to demonstrate potential and ability, such as:

(1) Communication/operational nerve centers.

(2) Heavily populated living areas and/or establishments.

d. To gain international attention.

e. Assault a target because of the high dollar placed upon it.

f. For maximum disruption of a facility's operation.

E-3 News Media

The final result of all terrorist acts is that they receive widespread news media exposure. Results of such exposure must be considered in view of the following:

a. In hostage situations, the hostage has been known to identify with his captors. This association increases the difficulty of the situation.

b. Increase of publicity of an incident may increase sympathy for a particular cause.

E-4 Terrorist Weapons

a. The most common weapons of terrorists include:

(1) Handguns

(2) Automatic weapons

(3) Explosive devices

(4) Other sophisticated weapons.

b. Sale and smuggling of guns has forced increased security and enforcement measures by Federal agencies. It is estimated that there are some 40 million handguns in the possession of citizens in the United States. This does not include automatic weapons, explosive devices and rocket firepower.

c. Major concern and priority is to be given to installations with chemical and nuclear material. These sensitive installations must receive maximum security.

d. The handheld automatic weapon is a favorite of terrorist groups because of its availability, size, weight, ease of concealment, high rate of fire and psychological impact on lightly armed security forces or unarmed civilians.

E-5 What to Expect

Members of terrorist organizations usually meet these standards:

- Well disciplined for violence.
- Attacks are well planned.
- Members are well armed and trained.
- Expertly executed.
- Reconnaissance conducted by persons other than strike force.
- Terrorist assault and/or negotiation team has a designated leader.
- Use available rapid transportation.
- Terrorism techniques embrace:
  - Subversion
  - Penetration
  - Indoctrination
  - Direct assault
  - Skyjacking
  - Kidnapping
  - Sabotage.

E-6 Methods of Operation

a. Robbery of needed equipment and supplies is an indication of possible terrorist activity, such as theft of ammunition, weapons, communications equipment, large amounts of paper, or copying machines to produce propaganda.

b. Attack selected persons or property to cause confusion, disorder or to force nations to confront one another.

c. Blackmail is an intelligence or Federal investigation matter. A DOD member maybe blackmailed into providing information about the installation.

d. Kidnapping a family member of a high ranking or influential officer of DOD as a hostage for ransom or other demand (figure E-1, page 304).

e. Arson of government property as a gesture of their ability.

f. Bombing of specific or indiscriminate targets to convey a message and display their serious intent on an issue.

g. Shootouts (ambushes) of guards to

Figure E-1—Family members are susceptible to kidnapping.

gain access to a restricted area. Critical areas of security demand reaction teams.

h. Hijacking of aircraft and trains.

E-7 Jurisdiction

Considerations must include the following on jurisdiction when planning and determining counterterrorism reactions:

a. Whether jurisdiction is concurrent or exclusive.

b. Proximity to installation borders.

c. Operational, investigative responsibility (Department of Justice, FBI).

d. Military abroad (Department of State).

e. Military forces command and operational control.

E-8 Reporting Incidents

a. Any terrorist incident must be reported immediately to security supervisors, operational alert centers, jurisdictional agencies, police response forces, and adjacent installations.

b. Security supervisory personnel should be familiar with command relationships during counterterrorism operations. Memorandums of understanding should be prepared and mutually signed concerning when and how FBI/military authorities interact during incidents. Also, how Status of Forces Agreements (SOFAS) apply in host countries when incidents occur on military installations. As a minimum, memorandums of understanding should include:

- Command-relationships and jurisdiction
- Sharing of information
- Control of military operations
- Organization-composition of joint forces
- Negotiating tactics
- Use of equipment
- Use of force measures
- Liaison with media and public officials.

E-9 Counterterrorism Actions

a. Each terrorist incident is categorized in three phases—initial response, negotiation, and assault.

(1) Initial response phase is the period during which military and security personnel become aware of a terrorist committed act and prepare to counter the act through peaceful persuasion or military force.

(a) Terrorists seize buildings and take hostages. The nearest military police or security patrol arrives on the scene to estimate the situation. Military police/security patrol report incident to the military police/guard operations desk.

(b) In CONUS, the following agencies are alerted:

- ❑ MP duty officer
- ❑ Provost marshal
- ❑ Installation headquarters
- ❑ Installation operations center
- ❑ CID
- ❑ MI

(c) The installation duty officer at the operations center notifies installation commander who informs:

- **FBI**
- Next Army operations center, DA, who alerts the next higher command (see figure E-2, next page).

(d) OCOPOS, installation headquarters operation centers contact the major command (USAREUR, Eighth Army, etc.). Alert notifications are cited in AR 190-40 (see figure E-3, page 307).

(e) Step-by-step:

- Initial on-scene commander with military and/or security police personnel sustains contact with terrorists and in accordance with doctrine and preestablished procedures, and attempts to ascertain a precise estimate of the situation.
- Provost marshal, or designated representative, arrives on scene at nearby location to establish forward command post, assuming forward operational control as commander. The initial, now former, commander remains at the command post to provide information and assistance.
- Security and reconnaissance personnel of the predesignated reaction force arrive on scene and establish physical security cordon of the area. They determine best access to and egress from the terrorist target (building with terrorists/hostages).
- Tactical elements or predesignated reaction force moves to assembly area beyond sight and hearing of terrorists and prepares for possible assault operations.
- Forward command post establishes communications with installation emergency operations center (IEOC).
- Installation commander arrives at IEOC to command counterterror operations, first obtaining an estimate of the situation from the provost marshal.

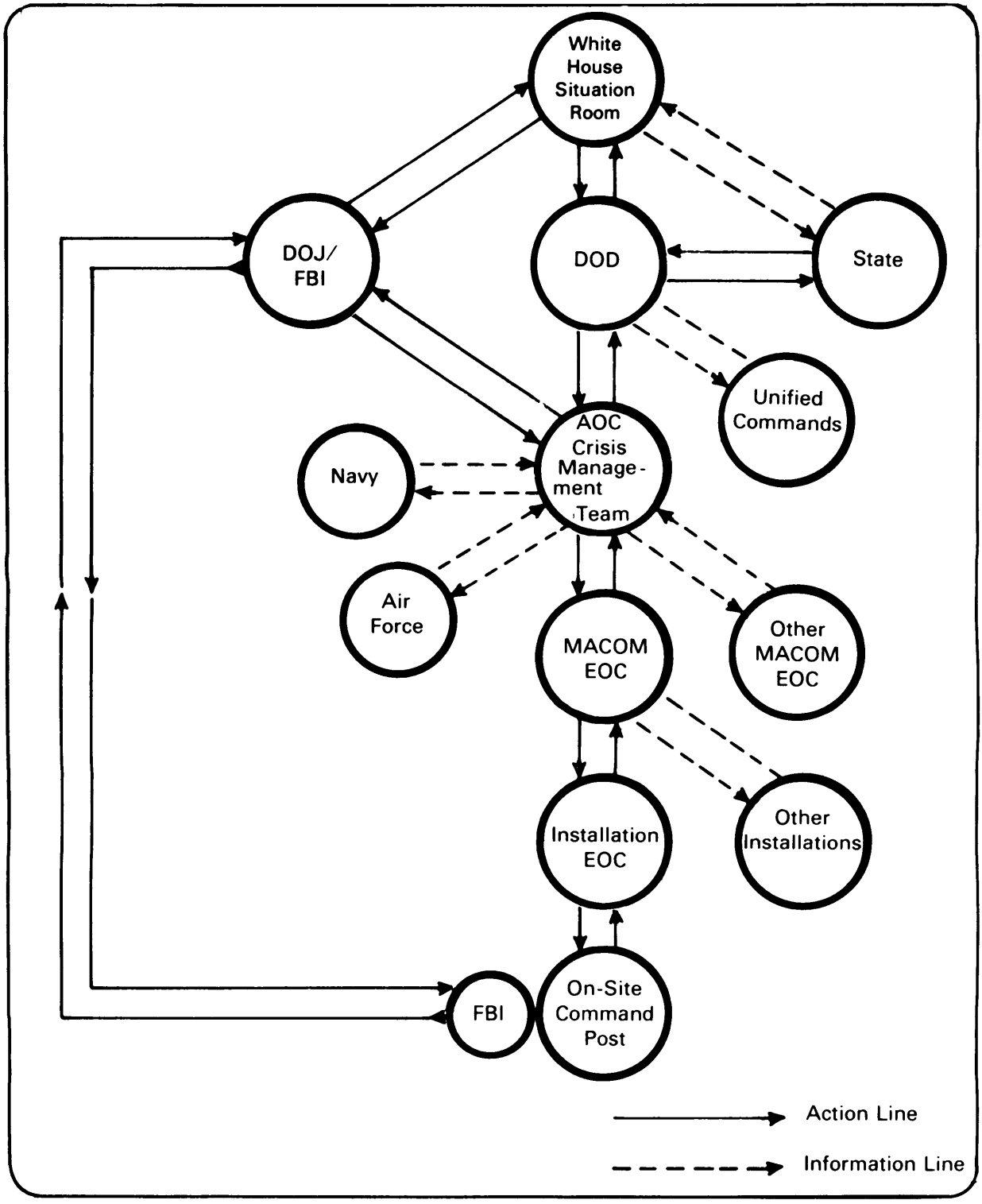

Figure E-2—CONUS Terrorist Alert Notification Process. This flowchart outlines notification channels and depicts interface with all areas of the government.

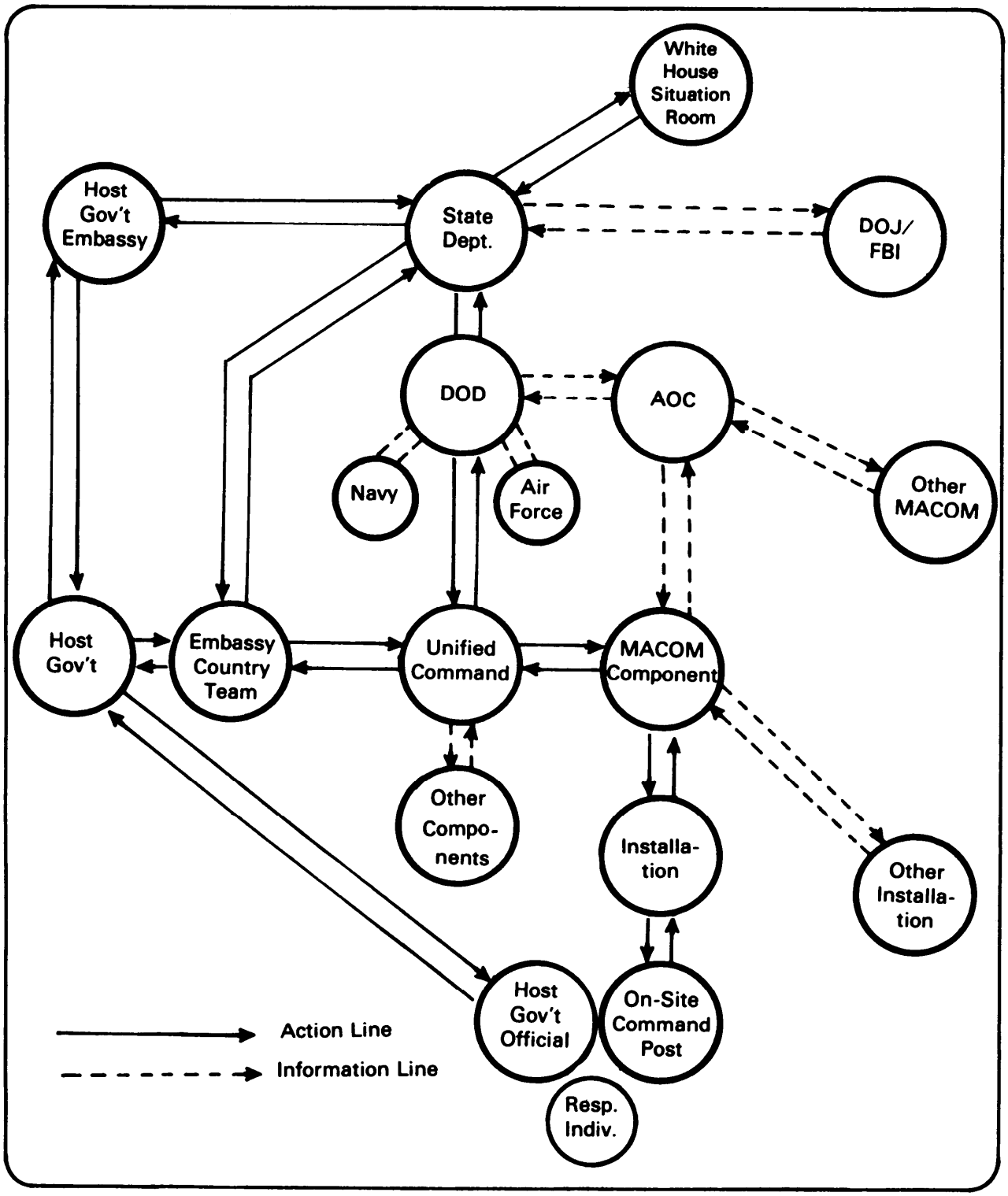

Figure E-3—OCONUS Terrorist Alert Notification Process.

● The provost marshal sustains contact with terrorists and determines:

❑ The number of hostages, who they are, and their condition.

❑ Precise interpretation of terrorist demands.

❑ Number of terrorists, type of terrorist group(s), position of terrorists in the building, and movement patterns of both terrorists and hostages.

❑ Name(s) of terrorists, especially the leaders.

❑ Terrorist behavior characteristics (such as nervousness, tense, easily excitable, or unemotional).

❑ Terrorist weapons, explosives, equipment.

❑ Best access and egress to and from building (from reports by elements of the reaction force).

❑ Tactical military options for use by tactical elements.

❑ If available resources will support planned tactical military operations.

❑ Begins formal negotiations with terrorists (NOTE: Terrorists may reject the assigned negotiator and request to negotiate only with installation commander or other official party.) Report results of all above to IEOC.

● Senior FBI official arrives at IEOC and receives briefing on situation from installation commander or provost marshal and assumes responsibility along with the installation commander as director of operations.

(2) Negotiation phase.

(a) Negotiating team, or negotiator, contacts the terrorists and buys as much time as possible from terrorists for the consideration of their demands.

(b) IEOC forwards clarification of demands to AOC/DA and awaits guidance on how the US Government will react. OCONUS reports to OPNS center, major command.

(c) Forward command post forwards to IEOC recommended tactical military options with estimated risk factors.

(d) IEOC analyzes tactical military options and determines best security option, then alerts forward command post of the option selected.

(e) Forward command post alerts support elements (such as medical, transportation, etc.) to embark on support mission.

(f) Forward command post alerts the leader of the tactical element and provides this individual with the military option plan although **permission to conduct such a plan is yet to be granted.**

(g) The option may be to conduct assaults to free hostages and take prisoners.

(h) Leader of tactical element returns to rear assembly area and briefs element to conduct the plan. Element obtains additional equipment, if needed, and undergoes full preparation, rehearsing actions repeatedly.

(i) FBI official and/or installation commander (US, i.e., on command prerogative) may move to forward command post. However, it should be noted that the appearance of additional authority may be viewed by terrorists as an indication of impending final action.

(j) AOC/DA forwards to IEOC a decision on use or nonuse of tactical military option. IEOC reports decision to forward command post (FCP) commander of the tactical element. If a decision is made to conduct tactical military operation(s), the third phase is initiated.

(3) Assault phase.

(a) Tactical element completes rehearsals, regroups at assembly area, establishes mobile command post, and informs forward command post when ready to embark on military operation.

(b) On order, tactical element moves as covertly as possible from assembly area to its objective.

b. Control is the essential element during

Evaluation of Situational Control/Counterterror

(Hostage Incident)

Phase	Exercising Direct Tactical Control	Exercising Indirect Tactical Control	Exercising Overall Strategic Decision-Making Control	Exercising Overall Policy Effects Control
Initial Response Phase	First authority on scene (MP)	Installation duty officer	Installation duty officer	
	Comdr, fwd CP (Provost marshal)	Comdr, IEOC (instal Comdr, or early-on a designated senior representative	Comdr, IEOC (as left of this column)	
Negotiation Phase	Comdr, fwd CP (Provost marshal) negotiator	Comdr, IEOC (Instal Comdr)	FBI official (and installation Comdr)	HQDA (AOC); or, as OCONUS situations, major command or US Dept State (embassy)
Assault Phase	Comdr, fwd CP Comdr, tactical element	IEOC (Instal Comdr)	FBI official	Same as above.

Figure E-4—Outline of control for hostage incident.

any of the three phases. The outcome of a terrorist event depends on counterterrorist situational control; therefore, command and control links must contain limitations imposed upon them by policy direction.

(1) Military and security police duties and responsibilities must be clearly established.
(2) Installation and unit contingency plans/SOP must be developed.
(3) Security personnel must be schooled and/or trained to react to a terrorist situation.

E-10 Vulnerability

a. To determine the vulnerability of any given installation, ten major factors are considered:

(1) Installation characteristics and sensitivity— personnel/mission. There are four subfactors.

(a) Consider personnel as hostage candidates. General officers and foreign personnel assigned to the installation.
(b) Sensitivity of the installation mission. Maximum consideration to nuclear or chemical storage sites.
(c) Consider open post versus closed post.
(d) The installation considered a symbol of national significance.

(2) Law enforcement resources-available personnel. Three categories to consider:

(a) Military
(b) Federal
(c) Local.

The law enforcement resource is responsible for law and order, and should be a priority when analyzing for safety and control. The military is immediately available and under direct control of the installation commander. FBI and local authorities are considered supplements to the military resources because of response time. Another important aspect is the number of MPs on duty or available within the required response time.

(3) Distance from population centers— miles/time. Experts on terrorism say that heavily populated urban areas usually provide these advantages to terrorists:

(a) Concealment of supplies and equipment.
(b) Safe houses are more readily available.
(c) More of a tendency for popular support.
(d) More freedom of movement.

On the other hand, low density population areas have the following characteristics:

(e) Strangers are noticed.

(f) Local law enforcement personnel tend to be close to day-to-day activities.

(4) Size of installation— area population.

(a) The larger the installation population the larger number of potential targets created due to increased requirements for arms, ammunition, banks, schools, clubs, etc.
(b) With increased population, the popularity for infiltration and support within is increased.

(5) Routes for access and egress— method of transportation. There are generally three major means of approaching and leaving a military installation-aircraft, vehicle, and boat. Because of the capabilities of a helicopter, all military installations are considered equally vulnerable. The number of roads and their quality should be considered. Only major waterways or large bodies of water should be viewed as transportation routes.

(6) Area social environment— social. Some geographical areas of the United States either have a history of, or a tendency for, unrest and dissident elements.

(7) Proximity to borders— jurisdiction. This factor of vulnerability takes into consideration the desirability of preparing for a terrorist attack in a foreign country and for escape after the act.

(8) Distance from other US military installation— support. Major governing factor is response time. If a local agreement for military support exists with a non-US military installation, the supporting force must be periodically exercised for an efficient cooperative response.

(9) Terrain. The terrain adjacent to the installation is another condition to be considered in overall installation vulnerability. Some types of terrain are built-up areas which present advantages to planning and executing a successful terrorist act or incident. (See TC 7-1, chapter 3, Cover, Concealment, Camouflage, and Target Acquisition.)

(10) Communications with next higher echelon.

(a) A significant influence is if terrorists have knowledge of the effectiveness of the installation communication system.
(b) Consider communications and the influence it may have on the outcome of a terrorist act.
(c) The more prolonged the act (such as hostage), the more influence communications can have in providing advice and assistance in coping with the situation. On the other hand, a bombing is a sudden event and the communications then serve primarily as a means of reporting.
(d) Both land and line telephone and radio must be evaluated. Land line telephone is more secure and reliable than radio because the radio is more subject to interruption either by terrorist act, by accident, or jamming.
(e) Interpersonal communication, your ability to perform your command of required security measures which will aid the safety of the installation, is a key factor.

b. Included with these ten factors are two aspects which are the results of actions taken by the installation commander. These two factors are **area social environment and law enforcement resources.**

c. The area social environment can be reduced to zero if the installation command and/or provost marshal is an active participant, on a regular basis, in meetings or councils with other area law enforcement agencies.

d. With the restriction imposed on Federal authorities in collection of domestic intelligence, close contact with state and local authorities provides the most effective means for staying current on the social environment surrounding the installation.

e. The assessed vulnerability value of the law enforcement factor can be reduced if military law enforcement assets have certain capabilities. These can be unique equipment or training:

(1) Equipment, armored car, aircraft, special firearms and suppression devices.

(2) Unique training (such as sniper, special reaction team, negotiating team) gives additional capabilities to law enforcement personnel.

f. AR 190-13, The Army Physical Security Program, provides guidance as well as a formal system for surveys and inspections to test vulnerability of an installation.