CHAPTER 18

Planning Terrorism Counteraction

At Army installations worldwide, terrorism counteraction is being planned, practiced, assessed, updated, and carried out. Ideally, the total Army community helps develop and implement installation plans for terrorism counteraction. And MP are involved extensively. MP help develop and they can help implement both the antiterrorism and the counterterrorism components of terrorism counteraction.

CONTENTS

ANTITERRORISM

Antiterrorism measures are developed to reduce vulnerability to terrorist attack. They are used to prevent or to defend against terrorist acts. Antiterrorism measures are used to defend US personnel, equipment, and facilities. They may be used to defend allied personnel and facilities, but such use must be specifically requested and approved. MP antiterrorism measures include collecting intelligence, analyzing vulnerabilities, and taking preventive measures. And MP are active in installation antiterrorism planning. The PM, his representative, or his staff–

- Participates in the development and periodic update of the installation's Threat Assessment.
- Develops the installation's physical security plan and crime prevention plan.
- Conducts appropriate inspections, surveys, and vulnerability assessments.
- Participates in the overall assessment of installation vulnerabilities.
- Coordinates with USACIDC for personal security vulnerability analysis of high-risk personnel.
- Participates in designating mission essential vulnerable areas (MEVA) and the orientation of planned protection for these areas.
- Reviews antiterrorism programs to ensure OPSEC programs and the like developed by other agencies on the installation complement those developed by the PM office.
- Participates in developing memorandums of understanding with federal, state, and local law enforcement agencies.

COLLECTING INTELLIGENCE AND ANALYZING VULNERABILITIES

Obtaining intelligence and analyzing vulnerabilities are prerequisites to planning preventive measures. A well-planned, systematic, all-source intelligence program is essential to knowing the threat. The role of intelligence is to identify and quantify the threat. It also provides a timely evaluation of terrorist capabilities, tactics, and targets. As knowledge is gained, a threat assessment can begin. All available information is examined to develop intelligence indicators of future terrorist activities. Analyzing the threat is an essential step in preventing or reducing vulnerability to terrorist acts.

Intelligence activities in terrorism counteraction are a team effort. Many federal agencies are actively involved in countering terrorism. These agencies provide technical

support and evaluation. And they share information. And controlled liaison with civilian and HN police and intelligence agencies is essential. Exchanging information prevents duplication of effort and reduces the likelihood of compromising ongoing intelligence collection efforts.

US Army Intelligence and Security Command (INSCOM) is the lead Army agency for Army, foreign, and counterintelligence activities against terrorism. INSCOM coordinates with appropriate US and HN agencies when initiating any intelligence activity. It also provides overall direction and coordination for the Army counterintelligence effort. Local INSCOM offices provide area coverage at all levels of command. The Intelligence and Threat Analysis Center (ITAC) is an agency of INSCOM. It disseminates specific threat warnings to applicable commands and activities. Periodic regional threat packets are provided to supported commands and activities. On request, ITAC provides current intelligence data on terrorist groups and individuals.

The MP serve as a major source of information in support of terrorism counteraction. Terrorists violate the law when they commit terrorist acts. MP agencies maintain information on known criminal incidents within their jurisdiction. (See section on criminal intelligence earlier in text.) This information is of vital interest to intelligence efforts. MP activities and USACIDC units collect and evaluate criminal intelligence. Local units and higher headquarters coordinate the development and dissemination of information. USACIDC disseminates terrorist-related information to installation and activity commanders within the affected area and to INSCOM.

Successful efforts to counter terrorism depend on successfully providing commanders timely, user-specific information of the terrorist threat. Integrating information provided by civilian, military, and governmental agencies produces a composite. This permits a commander to see what is happening or is about to happen and to plan accordingly.

Coordination of information among MP units, USACIDC area offices, military intelligence units, and civilian police agencies is active. In the US, MP and USACIDC field offices exchange information and intelligence with installation security and INSCOM elements. Outside the US, liaison is conducted by MP, USACIDC, and INSCOM elements with HN and allied law enforcement and intelligence agencies. Liaison is conducted in accordance with SOFAs. Regardless of locale, any information and intelligence exchange includes briefing the local commander. And wherever located, MP elements, in coordination with military intelligence elements, investigate and report illegal terrorist acts against the US Army. They also conduct liaison with civilian police agencies as required.

TAKING PREVENTIVE MEASURES

Properly planned preventive measures, when resourced and employed, reduce vulnerability to terrorist attack. Vulnerability assessments identify existing or potential conditions conducive to terrorist or criminal activity. Physical security surveys and inspections, crime prevention surveys, personal security surveys for high-risk personnel, the installation vulnerability determination system, and OPSEC surveys are among the tools available to installation commanders/staff personnel. They are used to determine the vulnerability of installation personnel, equipment, and facilities to terrorist attack or criminal activity.

The Army's programs for OPSEC, personnel protection, and physical security are all excellent means for reducing vulnerability. Each helps to protect operations, activities, installations, and resources from hostile exploitation. But maximum benefit from these measures is gained when all of these programs are

implemented in concert. Each of the programs seeks to reduce installation vulnerability to criminal or hostile acts. Each of the programs focuses on a different level of vulnerability or type of risk. Thus the programs can complement each other. When all of the programs, goals, objectives, and requirements are integrated, a synergistic prevention effect is realized. This is the key to a strong prevention program. The effect of the total interaction is far greater than would be expected of the sum of the parts.

OPSEC denies adversaries information about friendly military operations. This denies terrorists information about potential targets. Terrorists select targets that offer the most opportunity for success. Information passed unknowingly by military personnel and family members is used by terrorists in their planning efforts. OPSEC reduces the availability of this information. OPSEC procedures—

- Protect itineraries, travel plans, and personnel rosters.
- Eliminate established patterns.
- Protect building and facility plans, billeting assignments, and VIP guest lists.
- Ensure discussion of classified or sensitive information only on National Security Agency approved, cryptographically secured telephone or radio circuits; for example, automatic secure voice communications system.
- Protect personal or family information from nonacquaintances.
- Coordinate physical security measures to protect personnel and prevent unauthorized access to equipment, facilities, materiel, and documents.

Personnel protection measures help to protect personnel from criminal and terrorist acts. Personnel protection programs provide protective measures. They also create a threat awareness in people, especially those considered high-risk potential targets. Personnel protection includes protective services provided to high-risk persons by specially trained personnel. (See the chapter on protective services.) And it includes protective measures to be taken by the high-risk persons themselves. These latter measures help persons decrease their vulnerability to terrorist attack. Such measures reduce the likelihood of terrorist success. And they act as deterrents to terrorist activity.

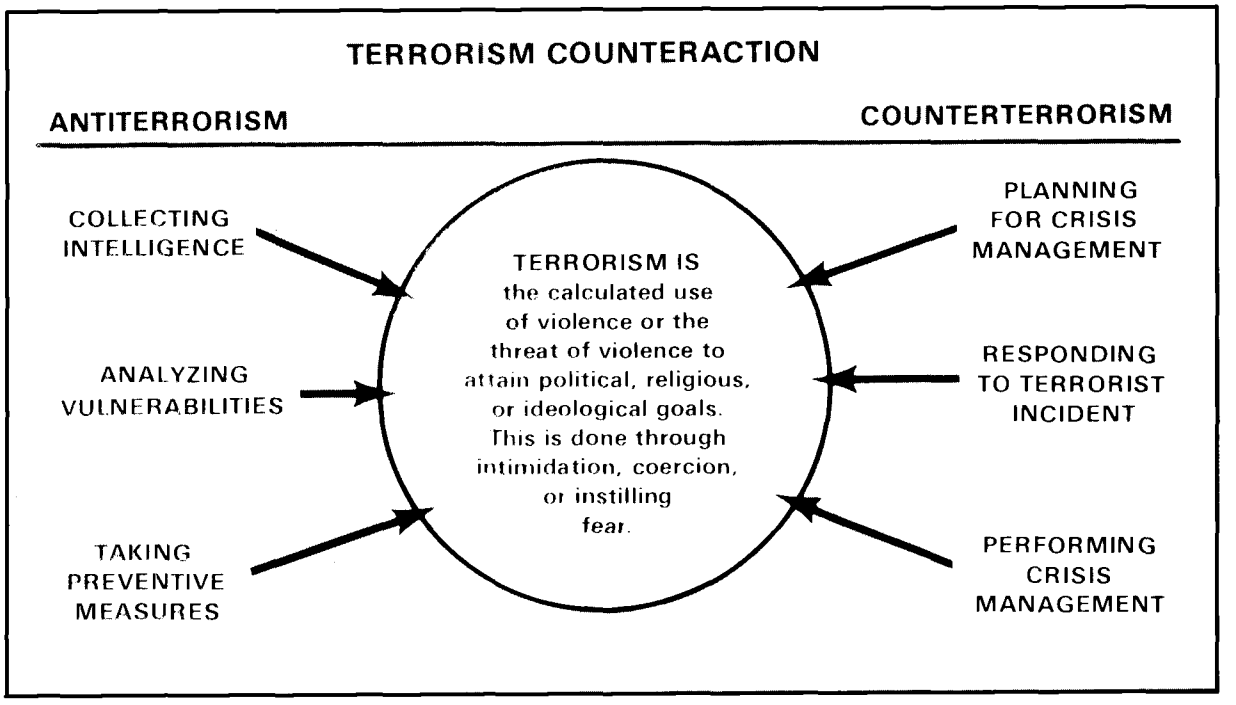
Physical security measures also protect and safeguard personnel from terrorist acts. Physical security programs mesh human resources and mechanical systems to prevent unauthorized access to equipment, facilities, materiel, and documents. Program managers plan and evaluate courses of action that improve physical security of quarters, offices, and installation facilities. Physical security programs help deter or reduce the chances for successful terrorist attacks. They complement other installation programs like crime prevention and OPSEC. (See FM 19-30 for specific measures. See AR 500-50 and FM 19-15 for policy and guidance for the control of terrorist acts in civil disturbances.)

Some antiterrorist measures are active defense measures. Aggressive countersurveillance is fundamental to countering terrorism. Persons, and certainly high-risk persons, and installation security forces must be trained to be aware that surveillance is possible. They must understand the need to counter it. They must become able to detect and report it. And countersurveillance measures and equipment must be available to them. When gate personnel are equipped with cameras they become a more effective countermeasure. They can photograph persons or vehicles suspected of surveilling an installation.

High-visibility deterrent measures can convince terrorists they will be unable to accomplish their "attack sequence" of surveil, plan, execute, escape. Highly visible security forces and aggressive measures can convince terrorists that the security of an

installation is too effective for them to succeed. If terrorists believe they cannot succeed, they are not as likely to attack. But sometimes a deterrent does not reduce the likelihood of attack. Instead, it may only cause the terrorists to change their methods or their target. And terrorists deterred from their well-defended primary target may decide to attack a more lightly defended target. Use of high-visibility measures requires a frequent reassessment of total target vulnerability.

Providing a high level of security at all times is costly. Using a random application of measures and procedures reduces costs. At the same time, it reduces the attractiveness of the target. Terrorists generally want to avoid the unexpected. Unpredictable coverage patterns can be used for guard and security patrols. On a larger scale, varying an installation's operating schedule may be useful. Even just varying the time, day, and locale of staff meetings can be useful.



COUNTERTERRORISM

Counterterrorism measures are undertaken to resolve terrorist incidents. Army policy stresses deterrence of terrorist incidents through preventive measures. However, when a terrorist incident occurs, military resources respond to gain control of the incident quickly. MP or security patrols on duty at the time of a terrorist incident are the initial response force. And the PM, his designated representative, or his staff should, as a minimum—

- Provide input to the development of the installation's crisis management plan.
- Develop the special threat plan. The plan should include contingency plans to control installation access, response to hostage barricade situations, response to bombings, response to arson, and the like.
- Establish and train an SRT.
- Train selected personnel in protective services operations as required.
- Serve as a member of the installation's crisis management team (CMT).
- Serve as commander of the installation's threat management force (TMF).

LEAD-AGENCY CONCEPT

The US government terrorism counteraction policies are characterized by the lead-agency concept. Terrorist acts that occur within the US are managed by the Department of Justice (DOJ). So are acts within the District of Columbia, the Commonwealth of Puerto Rico, and US possessions and territories. The lead agency for the operational response to a domestic terrorist incident is the FBI. The Federal Aviation Administration is the lead agency for actions affecting the safety of persons aboard aircraft in flight. ("In flight" is defined as that period of time beginning the moment all outside aircraft doors are closed after embarkation. It lasts until the moment when one such door is opened for disembarkation.)

The lead agency for terrorism against US personnel and facilities not within the US or its possessions and territories and for the foreign relations aspects of domestic terrorism is the Department of State. HNs have responsibilities in accordance with international law and applicable SOFAs. Coordination between the US and HN governments is accomplished by the Department of State.

Military personnel support the lead agencies in accord with federal laws or memorandums of agreement. Command and control of military forces for counterterrorist operations resides with the DOD. Army regulations require that procedures, guidance, and policies for the protection of US resources be established for all Army installations or activities. Such contingency plans must contain specifics for terrorism counteraction.

The installation commander is responsible for command and control of installation resources during a terrorist incident. Command and control actions, however, are typically planned, coordinated, and directed by the emergency operations center (EOC). This center is activated immediately when terrorist/special threat incidents occur. The EOC controls or assists in directing the military response and coordinates with higher, lower, and adjacent military headquarters and organizations. The CMT is composed of selected representatives from the installation staff. It is formed to assist the commander in controlling the incident. The CMT provides advice to the commander and the TMF through the EOC. The TMF is the tactical element of the EOC. The TMF commander has operational control of all installation military forces at the incident site. (See the chapter on special reaction teams for further discussion.)

RESPONSE OPERATIONS

Counterterrorist response operations on military installations within the US and its territories and possessions are characterized by three phases. The occurrence itself institutes the first phase.

MP respond to isolate, contain, and evaluate the incident. MP—

- Provide the initial patrol response.
- Determine the scope of the incident.
- Determine the motives of perpetrators.

MP provide the initial report to the PM. If the incident requires it, MP direct inner/outer perimeter forces and implement the special threat plan. If the incident is declared to be a possible terrorist act, the installation terrorist threat response contingency plan is implemented. In such a case the FBI, the Army Operations Center, and higher headquarters are notified immediately.

Phase II begins with the commitment of FBI or military forces from outside the installation. (Requests by an installation commander for additional military forces are coordinated through DA channels if the FBI has not assumed jurisdiction.) The FBI has primary jurisdiction for domestic terrorism. It assumes jurisdiction if the incident is of significant federal interest.

Installation personnel continue under the direct control of the military even when the FBI assumes jurisdiction. The military provides support to the FBI based on provisions of the DOD and DOJ Memorandum of Understanding. When the FBI assumes jurisdiction of the incident, military personnel continue to support the FBI as needed. Command and control of military personnel remains with the military.

The commitment of additional military forces by the National Command Authority to resolve the terrorist incident initiates phase III. If the FBI has jurisdiction of the incident, requests for these additional resources are accomplished through DOJ channels in accordance with the Memorandum of Understanding between the DOD and DOJ. If military forces are committed, the secretary of defense directs military operations according to law enforcement policies determined by the attorney general. If the installation commander retains jurisdiction (no FBI involvement), requests for additional military forces are accomplished through DA channels.

Upon termination of the incident, certain key military personnel, if requested by the FBI, remain at the site to protect the integrity of the investigative process. USACIDC special agents, in conjunction with the FBI, collect and process evidence for possible criminal prosecution. Investigation results are coordinated with local military intelligence elements who, in turn, forward them to ITAC.

RESPONSE OPERATIONS WITHIN HOST NATIONS

In response operations outside the US and its territories and possessions the basic responsibility lies with the HN. SOFAs, however, may grant the right (not the responsibility) to US forces to do whatever is necessary to maintain order and security on the installation. US procedures for responding to terrorist incidents on the installation are established according to US and HN law and SOFAs and in coordination with HN governmental agencies.

The military response on installations outside the US might consist of an initial response by installation law enforcement, other military resources, and HN law enforcement agencies. The installation commander is responsible for the initial response to a terrorist incident. Notification of the incident is made in accordance with applicable SOFAs and Army regulations. As a minimum, higher headquarters, the HN, and the Department of State (country team) are notified. Phase II starts when US military forces from elsewhere in the country are brought in or HN forces are committed. Phase III starts when the HN commits specially trained counterterrorist forces. Augmentation by US forces from outside the country requires HN consent. Coordination between the US and HN governments is provided by the Department of State.