FM 3-37.2

ANTITERRORISM

February 2011

HEADQUARTERS, DEPARTMENT OF THE ARMY

This publication is available at
Army Knowledge Online (www.us.army.mil) and
General Dennis J. Reimer Training and Doctrine
Digital Library at (www.train.army.mil).

Field Manual
No. 3-37.2

Headquarters
Department of the Army
Washington, DC, 18 February 2011

Antiterrorism

Contents

Figures

Tables

Preface

Field Manual (FM) 3-37.2 establishes fundamental operations for antiterrorism (AT) operations across the full spectrum of military operations. It is based on lessons learned from terrorist attacks, wartime engagements, and existing and developing AT strategies (military, federal, state, and local), policies, and doctrine.

The primary audience for FM 3-37.2 is commanders, leaders, planners, and AT officers. FM 3-37.2 applies to the Active Army, the Army National Guard (ARNG)/Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR) unless otherwise stated.

FM 3-37.2 follows national strategies, Department of Defense (DOD) policies, and joint doctrine to introduce Army AT doctrine and its purpose of protecting force personnel (combatant and noncombatant), infrastructure, and information against terrorist attacks. FM 3-37.2 links Army AT doctrine to the defense, joint, and Army guidance found in DOD O-2000.12-H, Joint Publication (JP) 3-07.2, and Army regulation (AR) 525-13. FM 3-37.2 is written for global operations and provides operational force commanders and AT officers with the tools and expertise needed for AT operations. It is not intended to be a complete stand-alone reference. Users of FM 3-37.2 should know of sources that will help them apply the information given.

Terms that have joint or Army definitions are identified in the glossary and the text. Terms for which FM 3-37.2 is the proponent publication (the authority) have an asterisk in the glossary. For other definitions in the text, the term is italicized, and the number of the proponent FM follows the definition.

The proponent of this publication is the United States Army Training and Doctrine Command (TRADOC). Send comments and recommendations on Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commandant, U.S. Army Military Police School, ATTN: ATZT-CDC, 320 MANSCEN Loop, Suite 270, Fort Leonard Wood, Missouri 65473-8929. Submit an electronic DA Form 2028 or comments and recommendations in the DA Form 2028 format by e-mail to <leon.cdidcodddmpdoc@conus.army.mil.>

Appendix A is a metric conversion chart that is included according to Army Regulation (AR) 25-30.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Introduction

Modern terrorism has continued to grow and adapt since the end of World War II. During the Cold War, the United States engaged in a protracted struggle with the Soviet Union, fighting to prevent communist expansion and promote democratic ideals and a free market economic system. The possibility of nuclear war limited direct confrontation between U.S. and Soviet forces. This caused both countries to restrain the hostile actions of allies and create well-defined rules for political and military conduct.

Recent terrorist attacks against the United States and other nations represent terrorist organizations that have broken free from state funding and ventured out on their own as criminal and radical enterprises. Regional and intrastate conflict, once suppressed by the influence of the United States and Soviet Union, is occurring more frequently now. Modern terrorists operate for global submission to an ideology that they have warped to support their worldviews. Throughout the world, these groups continue to adapt and modify their tactics. They use new technology and communications to recruit supporters, enhance their operations, and share lessons learned.

AT efforts have undergone significant changes and improvements over the past two decades, and FM 3-37.2 is written to meet the growing and evolving terrorist threat. It links directly to the concepts and guidance laid out in FM 3-0, FM 3-37, JP 3-07.2, and JP 3-26. FM 3-37.2 combines the most important elements of U.S. policy with operational experiences. It integrates the tactical tasks in FM 7-15, the AT tasks in AR 525-13, the operations process, composite risk management process (CRM), and lessons learned from ongoing experiences to create an approach that provides commonality between the generating force and the operational Army. FM 3-37.2 also provides a distinctive focus to mitigate and defeat the violent and nonviolent tactics of terrorists. It prepares commanders for—

- Defending against and defeating violent asymmetric tactics associated with terrorist and similar armed nonstate groups through threat analysis, awareness, risk management, and physical protection measures to preserve combat power.
- Understanding the impact of nonviolent psychological and information deception tactics used by terrorists to defeat the support of the local populace and the global observer.
- Analyzing the threat, criticality, vulnerability, and risk beyond bases and units and extending AT protective measures into the local populace, enhancing local support and mission accomplishment especially during peace operations and irregular warfare (IW).

FM 3-37.2 contains six chapters and five appendixes as follows:

- **Chapter 1.** Chapter 1 provides an overview of terrorism in the operational environment. It discusses the challenges that U.S. forces face in an era of persistent conflict and the effects that terrorism can have across the spectrum of conflict. It concludes with a brief evolution of terrorist tactics throughout history.
- **Chapter 2.** Chapter 2 examines terror tactics. It describes terror tactics and their use by terrorists and other armed nonstate groups. It discusses how terrorist organizations are made up, what motivates their actions, and how they plan and prepare for attacks. It also discusses the commander's awareness of insider threats and self-radicalization. It concludes with a discussion of specific terrorist defensive and offensive tactics.
- **Chapter 3.** Chapter 3 provides doctrine for the execution of AT tasks within the operational Army. It outlines the three tactical tasks and the supporting AT tasks to effectively plan and defend against the terrorist threat. It also introduces the AT principles and how these principles guide the unit to mitigate terrorist actions.
- **Chapter 4.** Chapter 4 is about implementation. It shows how the steps to counter terrorist actions are applied during movement operations and throughout full spectrum operations.

- **Chapter 5.** Chapter 5 discusses how AT is integrated within the operations process through the military decisionmaking process (MDMP), mission command, and the CRM process to assess and mitigate risk associated with terrorist activity.
- **Chapter 6.** Chapter 6 addresses the AT officer's role at various organizational levels. It concludes with an introduction to a variety of working groups to assist units in focusing AT planning efforts.
- **Appendix A.** Appendix A is a metric conversion chart that is included according to AR 25-30.
- **Appendix B.** Appendix B contains personal protection measures.
- **Appendix C.** Appendix C contains information on the integration of AT tactics, techniques, and procedures (TTP) into various exercises.
- **Appendix D.** Appendix D contains information on AT measures in operational contract support requirements packets.
- **Appendix E.** Appendix E contains guidance on completing threat, criticality, and vulnerability assessments (VAs) and the conduct of risk analysis.

As a modular force conducting decentralized operations, continuing to learn from the enemy and remaining vigilant to the potential for terrorist attacks at all phases of movement and operations is essential. FM 3-37.2 establishes a common frame of reference for commanders and staff members to assess, detect, warn of, defend against, and recover from terrorist attacks. As an Army, strategies and ideas of what AT means are adapted and extend thinking beyond bases and entry control points (ECPs). FM 3-37.2 expresses the need to make every Soldier aware of his vulnerabilities to terrorist actions and his ability to trust his instincts and report when something is out of place. Just as the principles of counterinsurgency have institutionalized, the same must be done to defeat terrorism and provide commanders and leaders with a basic foundation. Commanders who continue to consider and defend against the terrorist threat across full spectrum operations come into the situation better prepared and ready to adapt to mission changes and evolving asymmetric threat tactics.

Chapter 1

Terrorism in the Operational Environment

The Army operates in a world that faces complex challenges influenced by enduring trends, rising regional powers, emerging space and cyber threats, and pandemic disasters. At the head of these challenges is the present and growing rise of violent transnational terrorist networks. This chapter addresses the presence of terrorist networks throughout the spectrum of conflict, their impact on full spectrum operations, and the evolution of their tactics throughout history.

STRATEGIC CONTEXT

1-1. A *terrorist* is an individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives (JP 3-07.2). Joint doctrine defines *terrorism* as the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological (JP 1-02). Terrorism ranges from individual acts of damage or destruction, to highly sophisticated operations conducted by organized extremist groups with social, environmental, religious, economic, or political agendas. These terrorist activities can have a significant negative impact on the mission conducted by U.S. military forces.

1-2. Terrorists use violent and nonviolent acts to attract attention to their cause. Through the publicity that these acts generate, they communicate a message to their target audience. Terrorists seek to obtain the advantage, influence, and power that they lack and bring change on a local or international level. Terrorism is increasingly recognized as a threat to national security interests and domestic security. Timing and target selection by terrorists can affect U.S. interests.

1-3. The *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (FM 3-0). The operational environment includes adversary, friendly, and neutral elements across the spectrum of conflict. The operational environment also includes an understanding of the physical environment, governance, technology, local resources, and culture. The conventional military capabilities of the United States cause adversaries to pursue strategic victory through asymmetric and nontraditional strategies, tactics, capabilities, and methods. Adversaries employing asymmetry will seek to circumvent or negate U.S. strengths while exploiting U.S. weaknesses. Due to the superior capability of U.S. forces, terrorists will likely—

- Apply asymmetric methods.
- Deny easy U.S. access to a region.
- Attack symbolic targets.
- Degrade regional social and civil stability.
- Disrupt regional economic confidence.
- Seek catastrophic attack capabilities.
- Distribute misinformation to a global audience.
- Erode U.S. political resolve.
- Promote protracted political conflict.
- Use emerging media technologies.
- Recruit domestically so that they blend in.

1-4. Within today's operational environment, Army forces face a global terrorist network. Emerging global threats predict a period of persistent conflict that will challenge the international security environment. In the past, great powers and alliances and the bipolar world combined to suppress many independent actors and sources of conflict. An increasing number of actors (state, nonstate, and individual), in a less constrained international arena, are more willing to use violence to pursue their ends. This will result in an expanding set of actors and conflicts. The following enduring trends (see figure 1-1) exacerbate these sources of conflict:

- Globalization.
- Technology.
- Demographic changes.
- Urbanization.
- Resource demands.
- Natural disasters.
- Proliferation of weapons of mass destruction effects.
- Failed or failing states.

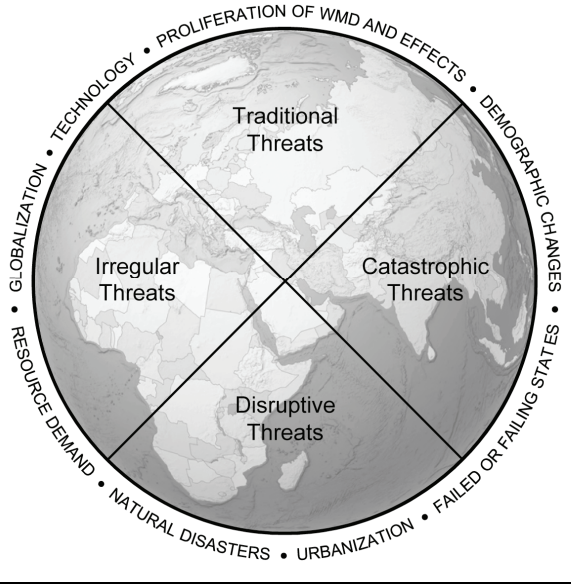


Figure 1-1. Challenges within persistent conflict

1-5. These trends will create a future environment that presents a wide range of compound problems that occur unpredictably and perhaps simultaneously, not limited to natural disasters, terrorism, insurgency, civil war, state-on-state, or coalition conflict. Shattered internal societies, characterized by the absence of rule of law and extensive criminal activity, will complicate crises. Overall, the strategic environment presents a broad set of variables and a complex range of conditions that will set the stage for future land warfare and make analytical, detection, and assessment tools and processes critical factors in discerning threat actors and actions amidst ambiguous populations.

1-6. In the complex conditions of this operational environment, fluid groupings of actors will seek to achieve their ends through hybrid combinations of traditional, irregular, catastrophic, and disruptive challenges. No longer will these challenges present themselves in their traditional form. The most capable opponents may combine disruption with traditional, irregular, or catastrophic forms of warfare. They will pursue their interests asymmetrically, unconstrained by moral and legal restrictions.

Note. Adversaries in Iraq and Afghanistan presented traditional and irregular challenges. Terrorist groups (al-Qaida) are irregular threats, but they also actively seek catastrophic capabilities. North Korea poses traditional, irregular, and catastrophic challenges.

1-7. Terrorist networks may apply hybrid combinations to enhance the achievement of strategic terrorist aims. Army forces will always have some degree of vulnerability to terrorist operations. Al-Qaida specifically identifies military targets as a major priority. Contributing factors that increase danger to Army forces include—

- **Exposure.** Exposure increases as units and individuals are forward deployed and internationally based. Increases in the operations tempo, the number of overseas deployments, and periodic surge requirements into an operational area raise the opportunity for Army forces to operate in areas that are more accessible to terrorist groups.
- **Symbolic.** Value of the symbolic value of successful attacks against military targets has often been a consideration in terrorist planning. Terrorist groups recognize that even relatively small losses of military forces from terrorist attacks receive extensive international media coverage and can aid in reducing public and political support to military operations.
- **Extremist persuasion.** Extremist persuasion fuels turmoil in many regions of the world, aiding in the recruitment of actors, followers, and supporters who have become desensitized to violence, are seeking purpose and meaning in their lives, and want to escape the despair of their environment.

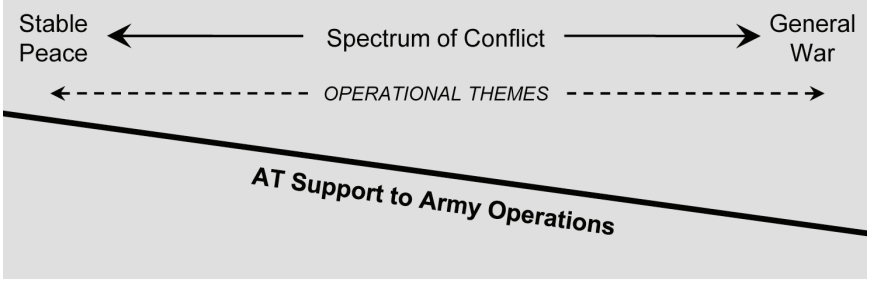
ANTITERRORISM IN ARMY OPERATIONS

1-8. The Army is a critical component of the joint team, employing land power throughout the operational themes, from peacetime military engagement to major combat operations. The effective employment of land power requires securing and maintaining the initiative and combining types of operations. As an element of the protection warfighting function, AT is integrated throughout the operations process and across full spectrum operations.

1-9. Contact with violent organizations, ranging from street gangs to terrorists to insurgents, has changed how warfare and the use of land power to achieve national goals is viewed. Commanders maneuvering, as part of the same task force and in the same country, may find themselves operating simultaneously within different operational themes along the spectrum of conflict.

1-10. AT tasks play a critical role in the defense against terrorist acts and in how the force preserves combat power against actions by nonstate actors. AT plays the greatest role in a commander's actions to protect the force when the likelihood of conventional enemy contact is minimal and combat is not envisioned (see figure 1-2, page 1-4). AT continues to serve as a foundation for a unit's security posture and how it applies actions within the protection warfighting function, even as the unit transitions to offensive operations within the category of general war.

Note. See FM 3-0 for more information on the spectrum of conflict, operational themes, and full spectrum operations.



Legend:
AT antiterrorism

Figure 1-2. AT support across the spectrum of conflict

SPECTRUM OF CONFLICT

1-11. The spectrum of conflict is the backdrop for Army operations. It places levels of violence on an ascending scale that ranges from stable peace to general war. On the left end of the spectrum, stable peace represents an operational environment characterized by the absence of militarily significant violence. Activities of international actors (states, corporations, nongovernmental organizations) are confined to peaceful interaction in politics, economics, and other areas of interest.

1-12. On the right end of the spectrum, general war describes an environment dominated by interstate and intrastate violence. *General war* is armed conflict between major powers in which the total resources of the belligerents are employed, and the national survival of a major belligerent is in jeopardy (JP 1-02). It can result when diplomatic and economic channels have broken down and violence has reached such a level that it will end only by the exhaustion, defeat, or destruction of the military capabilities of one or more antagonists.

1-13. Army forces operate on the spectrum of conflict and will find themselves operating at different levels within the same theater of operations. Across the varying levels of violence, the threat of terrorist actions or the use of terrorist tactics will constantly exist. Commanders who are lulled into a comfortable security posture during missions closer to the left end of the spectrum may inadvertently cause an opening for terrorists to take advantage. Threats to these missions will use the tactics of terror as a means to conduct criminal activity, divert U.S. attention, further exacerbate poor conditions for a particular ethnicity or state, or simply attack symbols of American strength. AT officers use proven measures, within their AT program or mission-essential task list, as a means to focus resources necessary to protect U.S. forces and the local populace against the terrorist threat, even as the level of violence escalates closer to the right side of the spectrum of conflict.

OPERATIONAL THEMES

1-14. A *major operation* is a series of tactical actions (battles, engagements, strikes) conducted by combat forces of a single Service or several Services, coordinated in time and place, to achieve strategic or operational objectives in an operational area (FM 3-0). An operational theme describes the character of the dominant major operation being conducted at any time within a land force commander's area of operation (AO) (see table 1-1). AT is part of the combating terrorism function within IW; however, the threat of terrorism exists within operational themes and military operations. These themes help to convey the nature of the major operation to the force to facilitate common understanding of how the commander broadly intends to operate. Operational themes have implications for task-organization, resource allocation, protection, and tactical task assignment. (See FM 3-0.)

Table 1-1. Operational themes and military operations

Security Cooperation	*Limited Intervention*	*Peace Operations*
• Multinational training events and exercises • Security assistance • Joint combined exchange training • Recovery operations • Arms control • Nation assistance • Counterdrug activities • Civil support	• Noncombat evacuation operations • Strike • Raid • Show of force • Foreign humanitarian assistance • Consequence management • Sanction enforcement • Elimination of weapons of mass destruction	• Peacekeeping • Peace building • Peacemaking • Peace enforcement • Conflict prevention

Irregular Warfare	*Major Combat Operations*
• Foreign internal defense • Support to insurgency • Counterinsurgency • Combating terrorism • Unconventional warfare	• Offense operations • Defense operations • Stability operations

1-15. AT planning and execution should consider a wider range of operational environments and the varying degree of terrorism risk. Each operational theme corresponds broadly to a range along the spectrum of conflict. Operational themes provide a useful means of characterizing phases of a joint operation. The transition between operational themes requires careful planning and continuous assessment. For example, at the conclusion of major combat operations, the character of the operation may evolve into IW or peace operations. While the scope of their defeat may induce an enemy to accept occupation and peace enforcement without a period of IW, commanders plan for a potential insurgency and prepare accordingly, as seen after the Iraq invasion of 2003. Though the attacks that occurred were against a combatant U.S. force, terrorist tactics were prevalent in the engagements between nonstate actors and U.S. forces.

1-16. It is important for commanders and staffs to understand that terrorists can attack in operational environments. Terrorists attack at a time and place of their choosing based on their own planning, execution factors, and objectives. They are not encumbered by U.S. planning and operations methodology or by the categorization of operational themes. The traditional threat spectrum concepts (the level of risk increases from peacetime military engagement upward toward major combat operations) may no longer be true. Therefore, commanders should proactively conduct AT assessment, planning, and preparations across operations to understand the terrorist threat and plan their countermeasures.

1-17. A change in operational theme may require modification to the mission-essential task lists and additional training for deploying units and units in the AO. The benefit of an AT program integrated throughout unit training (at home, camp station, and abroad) extends individual Soldier awareness and the unit's understanding of physical security measures across the spectrum of conflict without requiring new training. As AT training evolves due to changes in the threat, lessons learned from exercises and applications provide Soldiers and commanders with a solid foundation that enhances protection. Further, Soldiers will develop the skills necessary to act as sensors and decisionmakers anywhere within the spectrum of conflict.

IRREGULAR WARFARE

1-18. *Irregular warfare* is a violent struggle among state and nonstate actors for legitimacy and influence over a population (FM 3-0). This broad form of conflict has insurgency, counterinsurgency, terrorism, and

unconventional warfare as its principal activities. IW favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities to erode an adversary's combat power, influence, and will. These adversaries employ terrorism and transnational criminal activities that target Army operational forces supporting a wide range of missions. In the event that special operations and host nation (HN) forces cannot defeat unconventional and irregular threats, conventional Army forces may assume the lead role. IW operations include—

- Foreign internal defense.
- Support to insurgency.
- Counterinsurgency.
- Combating terrorism.
- Counterterrorism.
- Unconventional warfare.

1-19. IW differs from conventional operations dramatically in two aspects. First, it is warfare among and within the people. The conflict is waged, not for military supremacy, but for political power. Military power can contribute to the resolution of this form of warfare, but it is not decisive. The effective application of military forces can create the conditions for other instruments of national power to exert their influence. Second, IW also differs from conventional warfare by its emphasis on the indirect approach and the avoidance of direct military confrontation. Instead, IW combines irregular forces and indirect, unconventional methods (terrorism) to subvert and exhaust the opponent. It is often the only practical means for a weaker opponent to engage a superior military force. IW seeks to defeat the opponent's will through steady attrition and constant low-level pressure. In some instances, it targets the populace and avoids conventional forces altogether. This approach creates instability within the community and directly challenges the civil authority's ability to provide security.

1-20. Increasingly, the threats that U.S. forces face include or desire a hybrid mix of tactics from the threat categories. Adversaries are operating on the battlefield with a mix of conventional weapons, utilizing irregular tactics and funding and hiding their operations through criminal or terrorist behavior to obtain their political objective. These unconventional forces study Western tactics and identify vulnerabilities that are exploited using a mix of high-tech capabilities, cyber-warfare, and low-tech weapons. Modern examples of these tactics include the—

- **Vietnam War (1959 to 1975).** The United States fought to contain and defeat the spread of communism from northern Vietnam into the south. U.S. forces engaged in a conventional war against the North Vietnamese Army while engaging the guerilla forces of the National Liberation Front or Vietcong.
- **Soviet/Afghanistan War (1979 to 1989).** The Soviet military deployed a limited contingent set of forces, upwards of 108,000, into key bases, urban centers, and strategic locations throughout Afghanistan. The Soviets immediately faced a nationalistic guerilla force, the Mujahideen, who fought the Soviet conventional force with varied asymmetric tactics and U.S.-supplied weapons and training until Soviet withdrawal in 1989.
- **Second Lebanon War (2006).** Israeli military invaded southern Lebanon in response to a series of rocket attacks and an ambush of an Israeli patrol that resulted in the kidnapping of two Israeli soldiers. The Israeli military became engaged in a conventional and guerilla fight with an entrenched urban Hezbollah paramilitary force while facing continued rocket attacks on Israeli homesteads.

1-21. The association between or among terrorist groups increases their capabilities through the exchange of knowledge and other resources. Exchanges occur directly and indirectly. Direct exchange occurs when one group provides the other with training or experienced personnel that are not readily available otherwise. Indirect exchange occurs when terrorist organizations post lessons learned or videos to enhance future attacks or drive monetary contributions for their own supporters that other organizations obtain as well. Understanding the organizational structure and operational methods of terrorist groups that are able to influence the AO is critical in knowing the threat capabilities and intentions.

1-22. Terrorism and combating terrorism are activities conducted as part of IW and are frequently tactics associated with insurgency and counterinsurgency. However, terrorism may also stand alone when its purpose is to coerce or intimidate governments or societies without overthrowing them. Insurgency and terrorism are relatively inexpensive to conduct, but the support necessary to sustain the organization is a critical point of emphasis for counterthreat finance. Adversaries employing IW against the United States and partner security forces may not have to defeat them on the battlefield to win. In many cases, adversaries need only to survive or outlast the United States to win.

1-23. The Army executes IW operations in support of friendly states, against hostile states, and against nonstate adversaries operating within nonbelligerent states. The following may take place:

- **Shaping operations that begin early.** Before and during shaping operations, commanders should assess the threat of terrorist activities and review AT guidance in anticipation of future operations.
- **Commanders.** Commanders employing integrated force packages that fuse military operations and intelligence activities at the tactical level. When conducting IW, Army forces frequently conduct military operations to generate their own actionable intelligence and targeting data—using human intelligence; signals intelligence; technical intelligence; counterintelligence (CI); and forensic, biometric, and cultural information—to illuminate the adversaries' networks, support activities, and personalities. Intelligence-driven operations require long-term investments to develop the relationships necessary to gain insights regarding the operational environment, personalities, and populace. For example, commanders may establish teams in which military intelligence and law enforcement forces fuse operational intelligence on terrorist groups operating in their AO.
- **Operations.** Operations that focus on enhancing or destabilizing the relationships between a political authority and the relevant populations. Operations in support of enhancing relationships include humanitarian assistance, civic action projects, effective governance promotion, counterinsurgency, counterterrorism, stability operations, and foreign internal defense. Operations in support of destabilizing relationships include using unconventional warfare, training insurgent forces, and providing maneuver and sustainment support to partners. Across these mission areas, which have their own unique threats and security environments, commanders must ensure that units and Soldiers are prepared to defend against terrorist attack.
- **Army forces.** Army forces that reduce their presence after the security situation stabilizes and other government agencies and partners that continue long-term, steady-state activities. The transition toward stability operations and the ultimate handover to HN security forces presents yet another opportunity for terrorists to attack the United States and partner nations as operations become more static and predictable.

FULL SPECTRUM OPERATIONS

1-24. Full spectrum operations are the Army's operational concept; Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action—lethal and nonlethal—proportional to the mission and informed by a thorough understanding of all variables of the operational environment (see figure 1-3, page 1-8). A mission command that conveys intent and an appreciation of the situation guides the adaptive use of Army forces. (See FM 3-0.)

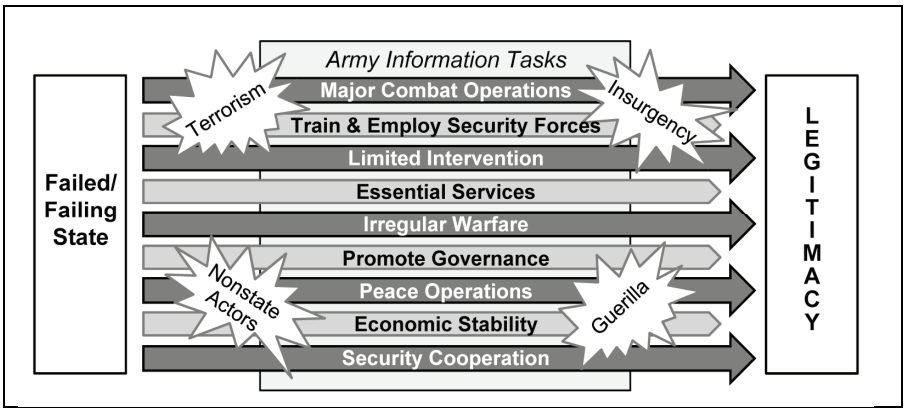


Figure 1-3. Full spectrum operations and adversary influencers

1-25. Full spectrum operations involve dynamic, continuous interaction between friendly forces and diverse groups throughout the AO. In addition to adversaries, units regularly interact with the populace, multinational partners, civil authorities, local businesses, and civilian agencies. Terrorist violence evolved in recent years from an agenda-forcing and attention-getting tool of the politically disenfranchised to a significant asymmetric form of conflict. Terrorist aims do not lie with the interests of the local populace, but terrorist acts demonstrate a profound impact on populations at the local, regional, national, and international levels.

OPERATIONAL VARIABLES

1-26. Terrorism influences, and is influenced by, the operational variables that planners use to describe the operational environment. Terrorist organizations transcend borders and may serve as a shadow element within a state's established governing power. The motives for attacks in one nation may occur as a result of variables in another country. Terrorists employ information activities, threats, intimidation, and acts of violence to coerce people and governments to gain control of their land or resources, while immersing themselves in the population.

1-27. Army planners analyze the operational environment in terms of eight interrelated operational variables: political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT). Broader information on the PMESII-PT can be found in FM 3-0. The information below is more specific to terrorism and terrorist organizations.

POLITICAL

1-28. Commanders focus on the political variable to identify laws and methods of governance that assist in countering the rise of terrorist organizations and terrorist activities. The creation of Israel, liberation from British rule, economic equality in Colombia, and perceptions of U.S. imperialism are some of the historical political influences that have helped to shape terrorist causes and tactics. Analyzing the actions and goals of the formally elected authorities, informal political systems (tribal elders and councils), and covert political organizations aid the commander in identifying causes for potential or existing terrorist activity. Terrorists often set out with the goal of disrupting or changing the political order or ambitions with an ideology and political practice that is closer to their own beliefs. AT officers assess the threat to forces and the local population by understanding election cycles and the corresponding activities necessary for selecting political leaders. They also examine popular grievances, laws, and actions that promote ethnic or religious biases, trade unions, and the will of the people to oppose terrorist influence within their communities.

1-29. AT officers also analyze how multinational and local political decisions within the AO impact, or are influenced by other operational variables (economic, social, infrastructure-related factors). Sometimes, political ideology is shaped by factors (religion) that play an overarching role in the worldview of a group of people. One example is the role of Islamic or Sharia (Islamic law) in shaping social and political

structures in Islamic culture. Political ideology that is inconsistent with Sharia is often seen as a threat to Islamic society. In this sense, the perceived encroachment of Western political ideology and culture in the Middle East is sometimes cited by Islamic terrorist groups as one of the reasons for their fight.

1-30. Failed or failing states hold a number of attractions for terrorist organizations. Failed states retain the outward signs of sovereignty, though they are unable to control their own territory. The presumption against interference in the internal affairs of another state, enshrined in the United Nations charter, remains a major impediment to cross-border action and the ability to eliminate terrorist networks. Failed or failing states can also support terrorism by—

- Providing the opportunity for terrorist organizations to acquire territory on a scale much larger than a collection of safe houses distributed around the globe. This land can be enough to accommodate entire training complexes, arms depots, and communications facilities that are free from international interference.
- Permitting terrorist groups to engage in smuggling and drug-trafficking operations and establish transshipment points to raise funds for operations.
- Creating pools of recruits and supporters for terrorist groups who can use their resources and organizations to step into the vacuum left by the collapse of official state power and civil society.
- Providing legitimate passports and other documents or the templates needed to forge credible copies that enable terrorists to move around the world and disguise themselves.

MILITARY

1-31. The military variable includes state and nonstate armed forces' capabilities within the operational environment. Commanders analyze the force's capabilities to defend against and defeat terrorists operating within their area and to analyze the terrorist's capabilities to attack U.S. and multinational forces, high-risk personnel (HRP), critical infrastructure, and information networks. The AT officer reviews friendly forces' training cycles and schedules for periods of vulnerability, particularly while forces are massed, in recovery, or in-transit. The AT officer assists the commander by identifying known terrorist organizations that are operating in the operational environment and other insurgent, guerilla, paramilitary, gang, or organized crime elements as a means to determine historical weaknesses. The AT officer focuses on terrorist tactics, equipment, support networks, and leadership, including their ability to recruit, train, and share doctrine and lessons learned across a variety of communication capabilities. AT officers assist in developing a plan to defend against these tactics and to mitigate their impact on the mission and strategic goals.

ECONOMIC

1-32. The economic variable encompasses individual and group behavior related to producing, distributing, and consuming resources. AT officers help the commander to understand factors within economic behaviors that could or do influence and support terrorist actions/factors (unemployment, hiring practices, class delineation, the cultivation of alternative illegal enterprises [drugs]). The AT officer analyzes harvest cycles, holidays, trade routes, smuggling routes, currency and commodity movements, and key economic-producing infrastructure to determine its vulnerability to terrorist acts.

1-33. Terrorist organizations require money to operate and fund training, recruitment, equipment, and media capabilities. Terrorist tactics are cheap to finance, making them an appealing means to influence change. The decentralization of terrorist organizations and advanced technologies, coupled with local traditions, have aided in financing and supporting global terrorism. Executive Order 13224, Operation Green Quest, and the Financial Action Task Force are just some of ways that the United States and its partners are working to disrupt and end terrorism financing. Many independent cells have found ways to operate their own front companies to fund operations without relying on network support or state sponsorship. Terrorists will most likely generate their funding from some of the following:

- **Extortion and kidnapping.** Terrorist organizations engage in this type of activity as a means of getting ransom or blackmail money to finance future operations.
- **Smuggling.** Organizations smuggle drugs, weapons, and people as a means of enhancing their current capabilities or for monetary compensation.

- **Counterfeiting.** Reproducing currency or designer goods is an inexpensive way to generate financing and support operations.
- **Drug trafficking.** The Revolutionary Armed Forces of Colombia and the Taliban are examples of organizations that link to the drug trade as a primary means of funding their operations.
- **Front companies.** The operation of legitimate companies generates profits, but can also be used as a cover to ship weapons, equipment, and funds to other organizations or smaller terrorist cells worldwide.
- ***Hawala.*** *Hawala* is a money transferring system that exists in the absence of, or is parallel to, conventional banking systems. Originally developed in India, *hawala* is prominent in several Middle-Eastern, African, and South Asian countries. In Afghanistan, where traditional banks were dissolved under the Taliban rule, *hawala* became the only means of currency exchange and movement of money within the country. Moving money without physically moving it, using an honor system, and leaving no paper trail make *hawala* an attractive way to launder money or move profits from narcotic sales within key terrorist havens.
- **Charities.** One of the pillars of Islam, *Zakat*, is the compulsory giving of a set proportion of one's wealth to charity. Terrorist organizations take advantage of this part of Islamic beliefs to finance terrorism. Many charities begin with the intent of spreading Islam and supporting the citizens of poverty-stricken countries, while some are created with the sole intention of funding terrorism. At times, al-Qaida has received more than $30 million per year in ostensibly charitable donations.

SOCIAL

1-34. Social structure refers to the relations among groups of persons within a system of groups. It includes institutions, organizations, networks, and similar groups. (See FM 3-24 for sociocultural analysis.) To effectively operate among an urban population, it is important to develop a thorough understanding of the society and its culture, including its values, needs, history, religion, customs, and social structure. The AT officer examines social patterns and trends (holidays, school schedules, vacations, other recurring observances) for their potential to be exploited by terrorist actions. Social factors have greater impact in urban operations and in areas where terrorists operate than they do in other environments. Terrorists rely on population support to operate and be successful. They may create friction between various groups, ethnicities, or religions to distract U.S. forces and manipulate their own standing within a certain faction. The density of the local populations and the constant interaction between them and U.S. forces greatly increase the importance of social considerations. By embracing the local population, commanders may gain combat information and actionable intelligence to combat terrorist organizations.

INFORMATION

1-35. Broadcast media sources (print, television, radio, the Internet, and social media networks) can rapidly disseminate views on military operations worldwide. Many organizations (al-Qaida) have advanced their media production and development capabilities to rival U.S. film production companies. Media coverage, in turn, influences U.S. political decisionmaking and public opinion. Given the advanced nature of telecommunication networks (cellular telephones, portable computers), terrorists have unprecedented global access to gather and share a variety of information to support operations against the West. Terrorists also use and shape media events and exposure to exploit their goals and objectives, shaping the story to control how others interpret events. As a result, terrorists rely heavily on televised news and propaganda to segment and influence their target audience.

1-36. AT officers, with the assistance of Army Public Affairs, seek to identify predictable news or media cycles and submission timelines as terrorists may seek to synchronize their operations to coincide with local, national, or international broadcast news schedules. They observe information delivery methods (radio, broadcast and social network media, the Internet, graffiti, flyers) to best develop information operation engagements to maintain the moral high ground. Understanding the various means of communications and influencers is important when integrating protective measures. Responding to terrorist events quickly, by engaging the media on the commander's terms, can mitigate terrorist exploitation effects after an incident.

INFRASTRUCTURE

1-37. The infrastructure consists of the basic resources, support systems, communications, and industries upon which the population depends. The key elements that allow an urban area to function are also significant to operations, especially stability and civil support operations. The force that controls the water, electricity, telecommunications, natural gas, sewage, food production and distribution, and medical facilities will virtually control the urban area. The infrastructure upon which an urban area depends may also provide human services and cultural and political structures that are critical beyond that urban area, perhaps for the entire nation.

1-38. Planners analyze strengths and shortfalls. These may help determine critical assets for future protection or reflect technological influences (cell and Internet capabilities) that could benefit terrorist communication capabilities. Terrorists also understand the importance of infrastructure in solidifying a newly formed government or U.S. mission in the AO. Troop occupation or the defacement of cultural landmarks and structures is used as disinformation to fuel the terrorist cause and aid in recruitment. Sabotage by terrorists of energy supplies, key bridges, water lines, and schools reduces public confidence and influences mission success, especially during peacekeeping and stability operations.

PHYSICAL ENVIRONMENT

1-39. Terrorists understand that simpler, open terrain exposes their capabilities to U.S. military strengths. Recent history has shown terrorist ingenuity in overcoming the technological strengths of satellites, air power, weapon systems, and armored vehicles by taking advantage of the physical environment. Analysis, especially through the intelligence preparation of the battlefield, reveals surface and subsurface features, complex terrain, varying weather patterns, trafficability, visibility, and their impact on the protection of personnel, infrastructure, and information. This analysis could also reveal hiding spots, smuggling routes, safe houses, and underground excavation as a means of supporting terrorist activities.

1-40. In the close confines of urban areas, small arms and light weapons (rocket-propelled grenades) can be more effectively employed by a terrorist force. Dense buildings can degrade friendly command and control (C2) and intelligence, surveillance, and reconnaissance efforts. While streets provide the means for rapid advance or withdrawal, military vehicles moving along streets are often channeled by buildings and have little space for maneuvering.

TIME

1-41. Terrorist groups consider patience an operational necessity and will attempt to achieve strategic goals through small battles fought over long periods. Terrorists seek to overstretch and erode U.S. forces by applying asymmetry and aggressive information activities. These actions are designed to exploit their successes and produce a psychological impact on populace support and political processes within the United States and the host country. The longer the U.S. military is engaged against an elusive enemy, the greater the burden on the economic, political (diplomatic), and military elements of national power.

1-42. The time variable influences decision cycles, operational tempos, planning cycles, and the other seven operational variables that planners analyze to discover predictable patterns, trends, and associations. Terrorists predicate planning cycles on a favorable time and place to attack. Through the careful analysis and surveillance detection, AT officers seek to disrupt and defeat a terrorist's time advantage.

INFLUENCE ON MISSION VARIABLES

1-43. An analysis of the operational variables provides the commander with relevant information in identifying potential weaknesses and opportunities when dealing with the terrorist threat. This analysis also provides additional situational awareness when terrorism is not the main threat in a particular area. Table 1-2, page 1-12, shows how these variables influence terrorism considerations at the tactical level through mission variables of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). Upon receipt of a warning order or mission, leaders narrow their focus to the mission variables that directly affect a mission.

Table 1-2. Operational effects on mission variables

		METT-TC					
		Mission	***Enemy***	***Terrain and Weather***	***Troops and Support Available***	***Time Available***	***Civil Consideration***
PMESII-PT	***Political***						X
	Military		X		X		
	Economic						X
	Social						X
	Information				X		X
	Infrastructure						X
	Physical Environment			X			
	Time					X	

Legend:
METT-TC mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
PMESII-PT political, military, economic, social, information, infrastructure, physical environment, and time

EVOLUTION OF TERRORISM

1-44. History points to acts of terrorism taking place roughly 2,000 years ago. These early acts operated under religious convictions and struck at disrupting the rulers in their region. Jewish zealots known as the *Sicarii* (or *dagger men*) used murder and kidnappings to attack Roman occupiers. Another group, the *Hashshashin* (or *the assassins*) was a breakaway faction of Shia Islam; their limited number of followers restricted their ability to engage in open combat. They engaged in the tactic of sending lone assassins to kill enemy leaders through the sacrifice of their own lives, weakening their enemy leadership and inflicting psychological damage on those who became familiar with the organization. During the French Revolution in 1795, use of the word *terrorism* became more prevalent. Loyalists and other opponents of the Revolution employed terrorist tactics in resistance to the revolutionary agents.

1-45. The 20th century did not slow terrorist momentum as a means to engage unpopular regimes. Before World War I, Serbia was conducting state-sponsored terrorist training and organization. Its involvement in the 1914 assassination of Archduke Franz Ferdinand in Sarajevo served as a trigger for World War I. Increased terrorist violence in the 1930s led to proposals at the League of Nations to prevent and punish terrorism and establish an international criminal court. The outbreak of World War II and the tactics to defeat the military and political machines gave many of the existing terrorist organizations and emerging resistance groups legitimacy in using a total war concept of fighting. New weapons and strategies that targeted the civilian population of the enemy and a means to destroy its economic capacity have exposed virtually every civilian to the hazards of combat. Latin American influence gave birth to national revolutions and ideological terrorism, forming lessons learned through history to shape the tactics of guerilla warfare and urban terrorism. Carlos Marighella, a famous influencer and author on guerilla and terrorist tactics, believed that only through psychological effects and violence could his followers be assured victory.

1-46. In the late 20th and early 21st centuries, international terrorist actions and groups continued to grow, along with affiliate groups and persons who mimic terrorist tactics to unleash their own ideals. The Cold War was filled with limited action and proxy engagements between national powers and state-sponsored terrorist organizations. It was here that hybrid tactics began to take shape. Rather than face a global or regional superpower in open combat, states used terrorism or a combination of conventional tactics and

asymmetric tactics to identify weaknesses in technology and skill and exploit them. Some notable modern international terrorist actions that have led to the evolution and rise of AT thinking include—

- **Provisional Irish Republican Army (IRA) (1969 to 1997).** The IRA engaged in an increasingly violent campaign against the British in Northern Ireland and England to influence public opinion in England and force British withdrawal from Northern Ireland.
- **Munich Olympics massacre (1972).** The Palestinian militant group known as *Black September* conducted a commando style raid on Israeli athletes and coaches who were asleep in the Olympic Village in Munich, Germany. The group eventually killed 11 Israelis and 1 German police officer before being killed or captured during a failed rescue attempt.
- **Beirut barracks bombing (1983).** A suicide bomber with the Islamic Jihad drove through a fence and in between two sentry posts before detonating the vehicle-borne explosives (equivalent to 12,000 pounds of trinitrotoluene [TNT]) within the U.S. Marine barracks in Beirut, Lebanon, killing 241 American Service members.
- **Khobar Towers bombing (1996).** Several members of the Hezbollah Al-Hijaz parked a sewage truck, containing explosives equivalent to more than 30,000 pounds of TNT, next to a fence, approximately 72 feet from a building housing U.S. Air Force personnel. The blast killed 19 Service members and heavily damaged apartment complexes in the area.
- **East Africa bombings (1998).** Nearly simultaneous suicide truck bombings occurred at U.S. embassies in the cities of Dar es Salaam, Tanzania, and Nairobi, Kenya, by the Egyptian Islamic Jihad, a supported element of the al-Qaida network. The explosions killed approximately 223 people.
- **11 September attacks (2001).** Coordinated attacks occurred in New York; near Washington, D.C.; and in Pennsylvania on the morning of 11 September 2001 when 19 al-Qaida terrorists hijacked four commercial airliners and flew them into both towers of the World Trade Center, the Pentagon, and a field in Shanksville, Pennsylvania. These attacks killed 3,497 people and the 19 hijackers.
- **Moscow theater hostage crisis (2002).** About 45 armed Chechen Islamist militant separatists took 850 hostages during a sold-out performance in the House of Culture building in Moscow. Russian forces raided the theater, resulting in the death of 39 Chechen militants and 129 hostages.
- **Beslan school hostage crisis (2004).** Chechen rebels raided and took hostage approximately 1,000 men, women, and children of Beslan School Number One. The eventual Russian military assault on the school resulted in the death of about 330 hostages.
- **Madrid train bombing (2004).** Thirteen improvised explosive devices (IEDs) were placed aboard four commuter trains. The coordinated detonation of the explosives resulted in the death of 191 people.
- **London subway bombings (2005).** Four suicide bombers detonated explosive packs on three underground London subway trains and one double-decker bus, killing 56 people. The attacks were in response to England's involvement in the Iraq War.
- **Camp Chapman suicide attack (2009).** Seven people employed by, or affiliated with, the Central Intelligence Agency (CIA) (including the chief of the base and a Jordanian intelligence officer) were killed and six others were seriously wounded in an attack on 30 December 2009. Humam Khalil Abu-Mulal al-Balawi, a Jordanian doctor who was later identified as a double agent loyal to Islamist extremists, entered Camp Chapman with the intent to kill CIA operatives. Because of the number of his previous visits to the base, al-Balawi was considered trusted enough by base security not to be searched on arrival at the gate. Al-Balawi walked up to where more than a dozen CIA operatives had gathered for a meeting and detonated the explosives attached to his body when several of the agents moved to search him.
- **Moscow subway bombing (2010).** Two Chechen rebel female suicide bombers detonated explosives in Moscow subway stations during rush hour as trains pulled into the station, killing 38 people.

1-47. The operational environment includes threats that blur the definitions of *criminal*, *terrorist*, and *insurgent*. Al-Qaida is the best-known example of such organizations. Its movement seeks to transform the Islamic world and reorder its relationships with other regions and cultures. Al-Qaida continues to participate in, take credit for, and support upstart organizations that execute violent and nonviolent actions that are compatible with al-Qaida's goals. Al-Qaida's global enterprise (criminal, terrorist, and insurgent) maintains connections and draws recruits from more than 60 countries, carrying out attacks in almost 20 countries. Al-Qaida's media arm, As-Sahab, has shown significant advances in developing literature, Web sites, photographs, and movies that are created to segment and adapt al-Qaida's message to particular groups and use the media as a weapon for countering U.S. goals.

1-48. The United States also faces a resurgence of terror organizations (Hezbollah, a Shi'a Islamist political organization based in Lebanon; Hamas, a Palestinian political and paramilitary organization; the Taliban, a Sunni Islamist radical religious and political movement that is fighting for control of Afghanistan and Pakistan). The ability of these organizations to feed on local and regional grievances and influence Western ways of thinking, combined with their members' willingness to execute suicide attacks to achieve their goals, makes them especially dangerous to U.S. operations around the globe.

1-49. Many terrorist organizations do not follow the same philosophies or support one another's actions physically, but they are more globally connected than ever before. As a whole, these organizations have learned from one another's successes and failures and have become more innovative. Consequently, organizations have produced instruction manuals, developed new tactics, made use of new technology, and debated future targets. Evolving terrorists are also more violent than in the past. In the 1970s and 1980s, terrorists wanted media headlines to further their cause, but showed restraint in the number of casualties. State-supported terrorists of the Cold War feared public outrage, alienation, and crackdowns by foreign governments or their own sponsor nations.

1-50. The evolution of terrorism in the 21st century allows terrorists to operate without state sponsorship, moving within failing states to remain hidden from global backlash. Terrorists no longer strike only targets on a regional level, but attack on a global scale, constantly trying to increase casualties and send stronger messages to their enemies. The attacks of 11 September 2001 illustrated the possibility of unpredictable attacks, where anything and everything can become a weapon in the global terrorist campaign. Increasing the level of complexity is the terrorist organizations' ability to influence citizens living within U.S. borders to execute attacks on behalf of the cause. Though the campaign goals of these organizations have yet to be achieved, the organizations are accomplishing tactical and strategic results by influencing national elections, troop support, nongovernmental agency participation, and United Nations support to operations in various conflict theaters and nations.

Chapter 2

Terrorist Tactics

Expeditionary forces are tailored to joint mission requirements and have a sustainable operational capability to conduct continuous full spectrum operations. However, since the end of the Cold War, a shift from conventional warfare to IW has occurred as evidenced by fighting in Somalia in 1993 and, most recently, in Afghanistan and Iraq. The terrorist threat to U.S. forces will continue for the near future. In AT, the principle of assess (see more on AT principles in chapter 3) involves a continuous process to compile and analyze available information concerning potential terrorist activities that could target Army assets. A comprehensive threat assessment (TA) will review the factors of operational capability, intentions, activity, operational environment, and threat vulnerabilities. This chapter describes the general categories of terrorist groups and their motivations and tactics as an integral step in identifying the probability of terrorist attack. This chapter addresses security challenges associated with people, motivations, and actions under the general topic of terrorism and the tactics that terrorists employ in contemporary incidents.

ARMED NONSTATE GROUPS

2-1. Since the end of the Cold War, new or nontraditional security challenges have been a source of growing concern, and in some cases, have become dominant security challenges in the initial decades of the 21st century. Challenges include rogue states, failed or failing states, regional conflicts, racial and ethnic tensions, social and economic strife, and ideologies that ferment extremism and oppression. Armed nonstate groups exist in these operational environments. The security challenges and armed nonstate groups are not new to armed conflict, but can be used in adaptive ways by terrorists to present conditions that favor their agenda. Groups labeled *terrorists* can also be categorized as insurgents, terrorist cells, militias, or criminal organizations, depending on how adversaries shape and describe a period of conflict.

2-2. Many armed nonstate groups are almost invisible. This makes it harder to track their capabilities or detect their intentions about when and where they plan to stage an assault. Understanding armed groups requires increased and detailed knowledge of their operational characteristics. Questions that commanders, the assistant chief of staff, intelligence (G-2), and the intelligence officer (S-2) should consider when developing an understanding of the operational characteristics of the threat are—

- Who are the leaders of the group? What are their roles, styles, personalities, abilities, beliefs, rivalries, and insecurities?
- Who makes up the group? Are they cohesive or riddled with factional divisions?
- How are members recruited, trained, and retained?
- What is the group's organizational infrastructure (funding sources, communications, and logistics control)?
- What are the group's propaganda and media resources and capabilities?
- What are the group's security and intelligence resources and capabilities?
- What beliefs; cleavages; and ideological, political, and cultural codes affect or impact the group?
- What are the group's operational doctrine, strategies, and TTP?

- Are there linkages with the police, military, other criminal organizations, political parties or groups, major businesses, or other organizations?
- What are the group's goals?

INSURGENTS

2-3. *Insurgency* is an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict (JP 3-24). The term *insurgent* broadly refers to types of unconventional forces and operations and includes guerrilla, partisan, insurgent, subversive, resistance, terrorist, revolutionary, and similar personnel, organizations, and methods. Insurgent activities include acts of a military, psychological, and socioeconomic nature conducted predominantly by inhabitants of a nation for the purpose of eliminating or weakening the authority of the local government or an occupying power. Actions can include political groupings and measures.

2-4. Growth and continuation of an insurgent force depend on support furnished by the population, even if the insurgent force also receives support from an external power. When an insurgent force is in its formative stage, it may be eliminated by employing civil law enforcement measures and removing factors that motivate grievances. When these measures are ineffective, a stronger force (a military unit) may be able to neutralize or destroy an insurgent force. Resistance movements can be resilient and reorganize or reconstitute as an insurgent force unless the original causative factors are also removed or alleviated. (See FM 3-24.)

GUERRILLAS

2-5. A *guerrilla* is a combat participant in guerrilla warfare (JP 1-02). *Guerrilla warfare* is military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces (JP 3-05.1). A prime characteristic of guerrilla operations is to attack points of enemy weakness in conditions developed by the guerrilla force or as selected by the guerrilla force. Deception and mobility are critical to achieving surprise and avoiding engagements unless the tactical opportunity weighs heavily in favor of the guerrilla. At the tactical level, attacks are planned and conducted as sudden, violent, decentralized actions. Principles of rapid dispersion and rapid concentration facilitate these types of operation.

PARAMILITARY FORCES

2-6. *Paramilitary forces* are forces or groups distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission (JP 3-24). Thus, there are various types of nonstate paramilitary forces (insurgents, guerrillas, terrorist groups, mercenaries). However, there are also nation-state paramilitary forces (internal security forces, border guards, police) who are, specifically, not a part of the regular armed forces of the country.

2-7. A militia can be an irregular armed force operating within the territory of a weak or failing state. The members of militias often come from disenfranchised elements of the population and tend to be composed of young, unemployed males with a desire for money, resources, power, or security. In some instances, people are coerced to join, while others may actively volunteer from a sense of honor or duty.

2-8. Militias can represent specific ethnic, religious, tribal, clan, or other communal groups. They may operate under the auspices of a factional leader, clan, or ethnic group or on their own after the breakup of the state's forces. They may also be in the service of the state, directly or indirectly. Generally, members of militias receive little or no formal military training. Nevertheless, in some cases, they can be highly skilled, unconventional fighters who commit acts of terrorism.

CRIMINAL ORGANIZATIONS

2-9. Criminal organizations are normally independent of nation-state control. However, large-scale criminal organizations often extend beyond national boundaries to operate regionally or worldwide and include a political influence component. Individual criminals or small gangs cannot normally affect

legitimate political, military, and judicial organizations. However, large-scale criminal organizations can challenge governmental authority with capabilities and characteristics similar to an irregular or paramilitary force.

2-10. By mutual agreement or when their interests coincide, criminal organizations may become affiliated with other actors (insurgents, individuals providing capabilities similar to a private army for hire). Insurgents or guerrillas controlling or operating in the same area as a criminal organization can provide security and protection to the criminal organization's activities in exchange for financial assistance, intelligence, arms and materiel, or general logistical support. Guerrilla or insurgent organizations can create diversionary actions or conduct reconnaissance and early warning, money laundering, smuggling, transportation, and civic actions on behalf of the criminal organization. Their mutual interests can include preventing U.S. or government forces from interfering in their activities.

2-11. Some criminals may form loosely affiliated organizations that have no true formal structure. Nevertheless, even low-capability criminals sometimes impact events through opportunistic actions. Criminal violence degrades a social and political environment. As small criminal organizations expand their activities to compete with or support long-established criminal organizations, criminals may seek to neutralize or control political authority to improve their ability to operate successfully and discourage rival criminal enterprises.

2-12. At times, criminal organizations might also be affiliated with nation-state military or paramilitary actors. In time of armed conflict or support to a regional insurgency, a state can encourage and materially support criminal organizations to commit actions that contribute to the breakdown of civil control in a neighboring country.

2-13. Gangs operate as a criminal enterprise (a group of individuals associated in fact, who are engaged in a pattern of criminal activity together), having an organizational structure, and acting as a continuing criminal conspiracy that employs violence and other criminal activity to sustain the enterprise. Internationally, urban youth gangs often operate in association with adult organized-crime organizations, serving as a violent arm to criminal operations.

2-14. Gangs recruit from a pool of disenfranchised youth or persons who lack opportunities to support themselves or family members due to a deficiency in education or work skills or to security problems related to military intervention or active insurgency. Gangs work in conjunction with terrorist organizations to accomplish mutual financial goals. Prisons and internment facilities serve as breeding grounds for the formation or induction of new members into gangs. Gangs in Iraq and Afghanistan typically split or form along tribal or religious affiliation versus criminal opportunities. While some gangs may be influenced to support active insurgencies in weak states, in failed states (such as Somalia) actions have expanded to include piracy.

2-15. Contemporary terrorism relies upon networks of interrelated terrorist groups, social movements, and criminal organizations to conduct operations, secure funds, and influence audiences. Historically, terrorists and criminal organizations were subnational or, occasionally, transnational threats. Rarely did terrorists challenge the nature of the nation-state or the modern state's authority and governance. Today's global threats (international terrorist groups) blur the distinctions between crime and war and challenge the structures of the nation-state. Terrorist organizations and criminal networks and activities often overlap.

TERRORIST NETWORKS

2-16. The rise of global nonstate terrorist networks is a significant characteristic of the past decade. The enemy may not be conventional military forces, but may be distributed multinational and multiethnic networks of terrorists. These networks seek to break the will of nations by attacking their populations. Some terrorist networks use intimidation, propaganda and information activities and indiscriminate violence in an attempt to promote a totalitarian ideology with a radical theocratic tyranny. These networks also aim to exhaust the will of the United States and its multinational partners who oppose them.

2-17. Terrorist networks often oppose globalization and the expansion of freedom it often brings. Though similar to a multinational corporation, they use the instruments of globalization (the existing global

economy, transportation, and communication system) as their preferred means of preparing and conducting attacks (see figure 2-1). Some of the ways terrorist networks make use of modern technology include—

- Exploiting the Internet as a sanctuary that enables the transfer of funds and the training of geographically isolated cells.
- Using cellular telephones, e-mails, chat rooms, and text messages to coordinate and order attacks. Technologies found in cellular telephones have also been used to detonate car and roadside bombs.
- Sending prerecorded video messages to sympathetic media outlets to distribute free information and spread hatred.
- Encouraging copycat and affiliate groups to conduct global attacks. They depend on 24/7 news cycles for publicity and the ability to attract recruits.
- Planning attack targets from safe houses located half a world away by using mapping software.
- Using offshore banking centers to further facilitate the interconnection of terrorist groups by depositing funds that are available to their operatives.

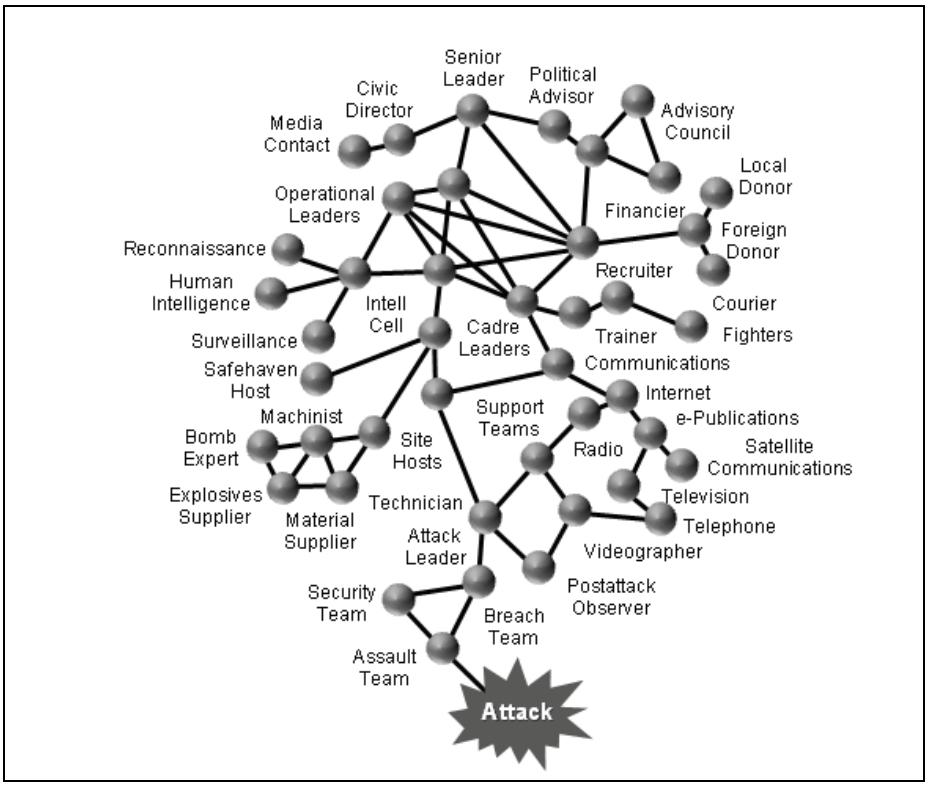


Figure 2-1. Terrorist network

2-18. Terrorist groups have been known to gain control over a territory in a failed or failing state through arrangements with government authorities by offering their services during times of conflict. Al-Qaida and its associated movements operate in more than 80 countries. They have conducted attacks around the world, including the 9-11 attacks in the homeland. State sponsors of terrorism (Iran, Syria) provide safe havens and support to varying degrees. In many states in the developing world, terrorist networks pose a greater threat than external threats. In Western societies, secondary bases take advantage of lax immigration procedures and the low level of scrutiny given to religious and charitable organizations. These operatives and sleepers create a network of safe houses, vehicles, equipment, and local information.

2-19. Terrorist organizations prefer to attack targets that they perceive as weak or vulnerable. Bombings, shootings, and kidnappings are the common terrorist methods, but terrorists have also used arson, hostage taking, hijacking and skyjacking, assassination, and information tampering to further their cause. The

nature and types of threats to the Army vary widely with geographic location, criticality of assets, vulnerability of the target, and level of hostile intent. Terrorists have resorted to asymmetric attacks to further their objectives—an attack that places an adversary's strengths against U.S. weaknesses. The most devastating form of these attacks will be conducted with the use of chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) components.

OPERATIONAL CAPABILITY

2-20. Terrorist groups or operations align along national, transnational, and international areas of influence. National groups operate within the boundaries of a single state or nation. Transnational groups operate across international borders. International groups operate in two or more nations and usually receive support from a foreign government.

2-21. Categorizing terrorist groups by their affiliation with governments provides indications of their operational capability, relative to the availability of the governments supporting intelligence, operations, weapons, and technology. The affiliations are—

- **Nonstate-supported.** These terrorist groups operate autonomously, receiving no significant support from the government.
- **State-supported.** These groups generally operate independently, but receive support from one or more governments.
- **State-directed.** These groups operate as an agent of a government and receive substantial intelligence, logistic, and operational support from the sponsoring government.

OPERATIONAL INTENT AND MOTIVATION OF TERRORISM

2-22. Terrorist acts have profound psychological impact on populations through their use or threat of violence. Terrorist strategies are intent on causing symbolic public damage and inspiring fear. The timing, location, and method of attack are geared to optimize mass media dissemination methods and leverage headline news cycles. Terrorist objectives (long-term and short-erm) generally demonstrate the group's intent as—

- Demonstrating anti-U.S. sentiment.
- Demonstrating anti-HN sentiment.
- Attracting publicity to the group's cause.
- Demonstrating the group's power.
- Demonstrating government weakness.
- Exacting revenge.
- Obtaining logistic support.
- Causing a government to overreact.

2-23. Terrorists tend to align themselves with particular ideologies or political philosophies as a justification for their actions to HN supporters or global observers. It is a common misperception to believe that ideological considerations will prevent terrorists from accepting assistance or coordinating activities with terrorists or states on the opposite side of the religious or political spectrum. Categories overlap, even when there would appear to be ideological conflicts. Some common categories of terrorist identities are—

- **Separatist.** These groups desire separation from existing entities through independence, political autonomy, or religious freedom or domination. The ideologies that these separatists subscribe to include social justice or equity, anti-imperialism, and resistance to conquest or occupation by a foreign power.
- **Ethnocentric.** Groups of this persuasion view race as the defining characteristic of a society, and a select group is often perceived superior because of its inherent racial characteristics. Ethnicity, therefore, becomes a basis of cohesion.

- **Nationalistic.** The loyalty and devotion to a nation and the national consciousness derived from placing one nation's culture and interests above those of other nations or groups are the motivating factor behind these groups. This can find expression in the creation of a new nation or in splitting away part of an existing state to join with another that shares the perceived national identity.
- **Revolutionary.** These groups are dedicated to the overthrow of an established order and replacing it with a new political or social structure. Although often associated with communist political ideologies, this is not always the case; and other political movements can advocate revolutionary methods to achieve their goals.

Ideological Categories

2-24. Ideological categories describe the political, religious, or social orientation of the group. While some groups will be seriously committed to their avowed ideologies, for others, ideology is poorly understood, primarily a rationale to justify their actions to outsiders or sympathizers.

- **Political.** Political ideologies are concerned with the structure and organization of the forms of government and communities. While observers outside terrorist organizations may stress differences in political ideology, the activities of groups that are diametrically opposed on the political spectrum are similar to each other in practice. Political examples are—
  - ***Right wing.*** These groups are associated with the reactionary or conservative side of the political spectrum and are often associated with fascism or neo-Nazism. Despite this, right-wing extremists can be every bit as revolutionary in intent as other groups. However, their intent is to replace existing forms of government with a particular brand of authoritarian rule.
  - ***Left wing.*** These groups are usually associated with revolutionary socialism or variants of communism (Maoist, Marxist-Leninist). With the demise of many communist regimes and the gradual liberalization of the remainder toward capitalism, left-wing rhetoric can often move toward and merge with anarchistic thought.
  - ***Anarchist.*** Anarchist groups are antiauthority or antigovernment and strongly support individual liberty and voluntary association of cooperative groups. Often blending anticapitalism and populist or communist-like messages, modern anarchists tend to neglect the issue of what will replace the current form of government. They generally promote small communities as the highest form of political organization necessary or desirable. Currently, anarchism is the ideology of choice for many individuals and small groups that have no particular dedication to an ideology, and are looking for a convenient philosophy to justify their actions.
- **Religious.** Religiously inspired terrorism is on the rise. Religiously motivated terrorists see their ultimate objectives as divinely sanctioned and therefore infallible and nonnegotiable. Religious motivations can also be tied to ethnic and nationalist identities (Kashmiri separatists combining their desire to break away from India with the religious conflict between Islam and Hinduism). The conflict in Northern Ireland also provides an example of the mingling of religious identity with nationalist motivations. There are frequent instances where groups with the same general goal (Kashmiri independence) will engage in conflict over the nature of that goal (religious or secular government). Numerous religious denominations have seen activists commit terrorism in their name or spawned cults professing adherence to the larger religion while following unique interpretations of that particular religion's dogma. Cults that adopt terrorism are often apocalyptic in their worldview and are extremely dangerous, unpredictable, and difficult to penetrate and deter.
- **Social.** Particular social policies or issues will often be so contentious that they will incite extremist behavior and terrorism. This is frequently referred to as *single-issue* or *special-interest* terrorism.

Insider Threats

2-25. Commanders must also be aware of Soldiers within their ranks who sympathize with extremist groups and terrorist organizations and their ideals. Attacks on fellow Soldiers (Sergeant Hasan Akbar's attack before the Iraq ground campaign in 2003) have raised the need for effective leadership and AT measures to protect the force, even from one another. Exposure to actions in the AO, in conjunction with challenged personal situations or crises that shake belief systems, can test a Soldier's loyalty to his unit, his fellow Service members, and his nation and make him vulnerable to extremist influence. Commanders must make unit members aware of potential violence indicators, possible hostile activity report methods, and proper reporting channels. (See AR 381-12.) Some indicators of insider threats, identified through incident after-action reviews (AARs), are individuals who—

- Ask questions about operations that appear outside his area of responsibility (AOR).
- Attempt to enter restricted areas without proper credentials.
- Make unexplained or excessive copies of files.
- Improperly use information technology systems or repeatedly attempt to access restricted files.
- Request irregular work schedules or attempt to be left alone in a facility.
- Repeatedly make inaccurate statements or excuses for irregular behavior.
- Perform surveillance activities (take photographs, sketch access control points).
- Conduct questionable financial activities (unexplained, unlikely explanations for increased or decreased income or material possessions).
- Build a private weapons collection or steal weapons or key weapon components.
- Purchase bomb-making materials, obtain information about the construction of explosives, or request unusual amounts of munitions before or after a mission.
- Obsessively follow news reports of terrorist actions.

SELF-RADICALIZATION

2-26. The changing face of U.S. homegrown extremism is disturbing as a growing number of unlikely militants in small-town America become radicalized using the Internet and then plot attacks at home and abroad. The ease with which people can be influenced by extremists through online social media sites makes it hard to profile possible militants within the United States and the Army. Interactive online sites that support anonymity and include dynamic and charismatic preachers of hatred and terror have helped al-Qaida and other terrorist groups spread their ideology into the United States and to other citizens of Western society. The distinct phases to radicalization are—

- **Preradicalization.**
  - Absence of psychological profile.
  - Identity crisis.
  - Similar trajectories for joining the jihad.
  - Influenced in meetings at religious institutions, on the Internet, at school, at home, at work, in prison, or through sports activities.
- **Self-identification.**

Note. The stimulus is often a cognitive event or crisis. Ultimately, the individual is alienated from his current life and affiliated with like-minded individuals who strengthen his dedication to extremism via small-group dynamics.

  - Economical (lost a job, had a promotion blocked, received UCMJ discipline from the military).
  - Social (alienation, discrimination, racism [real or perceived]).
  - Political (international conflicts involving a certain demographic, political wing, or religion).

  - Death in the family or death of a unit member.
  - Glorification of jihad.
- **Indoctrination.**
  - Withdrawal from normal functions, church or moderate mosques, and other social activities.
  - Politicization of new beliefs (preaches or argues with other unit members).
  - Increased training—may travel overseas.
  - Role assignments.
  - Group bonding or local training camps.
  - Meetings with like-minded individuals in areas hard to detect (private homes, the countryside).
- **Jihadization.**
  - Jihad acceptance or a decision to commit to jihad.
  - Training and preparation (actions on contact, rehearsals).
  - Mental reinforcement activities.
  - Attack planning (research, surveillance, intelligence gathering, resource acquiring).

2-27. Many behaviors exhibited by an individual in the midst of converting to an extremist mind-set are subtle and do not immediately send warning indicators. This is one of the primary reasons that Soldiers must be aware of one another and their unit and be able and willing to recognize the warning signs that a member of their organization is in trouble. It is imperative for unit members to not dismiss an individual's behaviors or actions simply because they know and have trusted that individual. In fact, experts commonly agree that although there is no useful profile of a Western radical extremist, most individuals who follow that path are considered unremarkable. The close confine in which the individual lives and operates is the best gauge for detecting unusual, out-of-character, or questionable behaviors.

2-28. Radicalization in the West is not often triggered by oppression, suffering, revenge, or desperation. It is a phenomenon that occurs because individuals are looking for an identity and a cause, and individuals often find themselves in extremist Islam. The consensus view among analysts is that converts to Islam—regardless of other demographic factors—bear an elevated risk of radicalization for two key reasons: their desire to prove their conviction and the fact that those converted into radical sects have never been taught the intended peaceful message of the Koran. Although many potential indicators are innocuous alone, when combined, they may paint a more sinister picture, such as—

- Advocating violence, the threat of violence, or use of force to achieve goals that are political, religious, or ideological.
- Advocating support for international terrorist organizations or objectives.
- Providing financial or other material support to a terrorist organization or to a suspected terrorist.
- Having familial ties to known or suspected terrorists or terrorist supporters.
- Associating with or having connections to a known or suspected terrorist.
- Repeating expression of hatred and intolerance of American society, culture, government, military, or the principles of the U.S. Constitution.
- Browsing or visiting Web sites that promote or advocate violence directed against the United States or U.S. forces or that promote international terrorism or terrorist themes.
- Expressing an obligation to engage in violence in support of international terrorism or inciting others to do the same.
- Demonstrating shifts in personal relationships.

2-29. Commanders and leaders should also be aware of, or attempt to discover a Soldier's reliance on some sort of transnational intermediary (an extremist cleric or a terrorist recruiter), to facilitate and catalyze the Soldier's radicalization. These communications often occur online, via e-mail, social networks, or a variety of extremist chat rooms. This phenomenon is hardly new; numerous reports have detailed the growth and potency of Internet radicalization in recent years. Commanders should implement a holistic and

integrated approach to the insider threat, incorporating CI, personnel security, law enforcement, and information assurance capabilities to assess, detect, and mitigate insider threats within their units.

2-30. In regard to lone actors, community or personal outreach is an important step to preventing an attack because it is often a close friend or family member who may see the signs of trouble. The families of terrorists and extremists—in particular, close friends, fellow Soldiers, wives, and parents—can have an important role in trying to persuade their relatives to leave and stay out of these organizations. Commanders should consider them an integral element in a counterradicalization program.

GEOGRAPHIC CATEGORIES

2-31. Geographic designations are sometimes used to categorize terrorist groups (see figure 2-2). In some instances, geography overlaps with ethnic, national, religious, or ideological aspirations. Geographical association with the area of the group's primary concern will be made, though these designations are only relevant to the government or state that uses them.

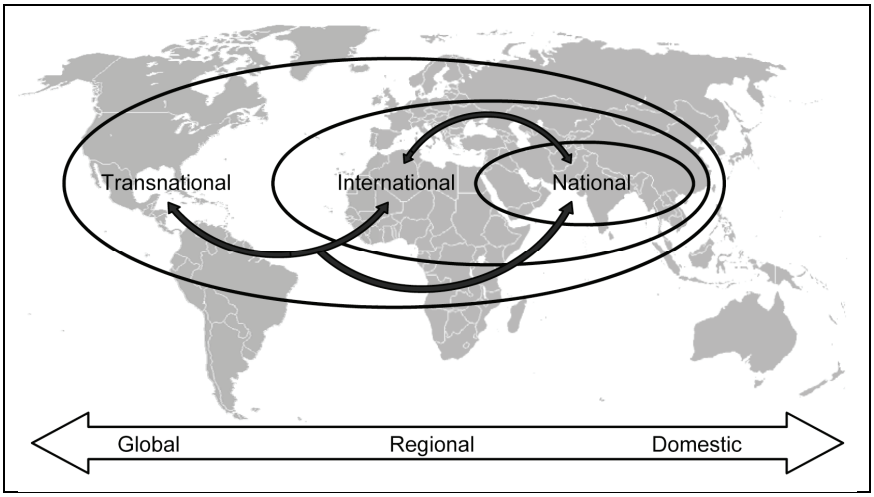


Figure 2-2. Operational reach of terrorists

2-32. Examples of geographically categorized terrorists are—

- **Domestic or national.** These terrorists are homegrown and operate within and against their home country. They are frequently tied to extreme political, religious, or social factions within a particular society and focus their efforts specifically on their nation's sociopolitical arena.
- **International.** Often describing the support and operational reach of a group, the terms *transnational* and *international* are often loosely defined and can be applied to widely different capabilities. International groups typically operate in multiple countries, but retain a geographic focus for their activities. For example, Hezbollah has cells worldwide and has conducted operations in multiple countries, but is primarily concerned with events in Lebanon and Israel. An insurgency-linked terrorist group that routinely crosses an international border to conduct attacks and then flees to a safe haven in a neighboring country is international in the strict sense of the word, but it does not compare to groups that habitually operate across regions and continents.
- **Transnational.** Transnational groups operate internationally, but are not tied to a particular country or even one region. Al-Qaida is a transnational group. It consists of many nationalities, has been based out of multiple countries (simultaneously), and conducts operations throughout the world. Its objectives affect dozens of countries with differing political systems, religions, ethnic compositions, and national interests.

TERRORIST ACTIVITY

2-33. Terrorist activity includes actions during the planning process and the specific attack forms or tactics employed. The activities of the group may include—

- Identifying target accessibility.
- Moving operatives.
- Collecting intelligence activities (pretarget selection, preattack, and postattack).
- Planning and rehearsing.
- Establishing weapons caches or access to weapons.
- Observing suspicious activity in and around the target area.
- Disrupting security forces.
- Fundraising to support the activity.
- Establishing and operating from a safe haven.

2-34. Whether terrorism comes from an individual with a single agenda or a terrorist organization with global reach, a variety of motivations and goals are considered in target selection. The specific reason to target U.S. military forces or individuals is equally varied. A principal consideration in terrorist targeting is the psychological impact of an attack on a selected audience. Attacking U.S. forces can serve that goal of the terrorist. The most common rationales for targeting U.S. military forces are to—

- Exploit the obvious symbolic value of the target.
- Demonstrate organizational capability.
- Delay or prevent military movements.
- Reduce operational capability.
- Degrade the social environment.
- Disrupt the economic environment.
- Influence U.S. government policy.

ORGANIZATIONAL STRUCTURE

2-35. Terrorist groups develop various organizational structures that are functional for their operational purpose and environment. Presenting a generalized organizational structure can be problematic. In addition, terrorist groups can be at various stages of development in terms of capabilities and sophistication. The design may simply be driven by limited resources and the need for survival (see figure 2-3).

2-36. The level of knowledge and commitment within a specific organization varies as widely as its goals and membership. The following are generally associated with threat groups:

- **Leaders.** Leaders provide direction, approve goals and objectives, and give guidance for achieving the organization's mission. Leaders are broken into two levels of command structure:
  - ***Senior leaders.*** Senior leaders are fully committed and charismatic representatives of their cause. They attempt to justify their acts through politics and use theology as inspiration. They do not participate in tactical operations, but strategize over potential targets and timeframes for attack.
  - ***Operational leaders.*** Operational leaders are select individuals who control geographic areas and command and control active terrorist networks. They provide direction and guidance, approve goals and objectives, and provide overarching strategies for operations in line with senior leaders' themes but may act out those themes in their own vision. Usually, leaders rise from within the ranks of an organization or splinter and create their own organization, as did Abu Musab al-Zarqawi.
- **Cadre.** The cadre is the active members of the terrorist organization. This echelon plans and conducts operations, and also manages intelligence, finances, logistics, propaganda, and communications. Midlevel cadres tend to be trainers and technicians (bomb makers, financiers,

surveillance experts). Low-level cadre, inspired actors, and recruits are the actual bombers and direct-action terrorists.

- **Active supporters.** Active supporters are active in the political, fundraising, and information activities of the group. They may also conduct intelligence, surveillance, and reconnaissance missions and activities and provide safe havens, financial contributions, medical assistance, and transportation for other members. Active supporters are fully aware of their relationship to the group, but do not normally commit overt violent acts.
- **Passive supporters.** Passive supporters are typically individuals or groups that are sympathetic to the goals and intentions of a specific group, but are not committed enough to take an active role. They may not be aware of their precise relationship to the terrorist group, but instead interface with a front that hides the overt connections. Sometimes, fear of reprisal from terrorists (for overt noncompliance) is a compelling factor for passive supporters.

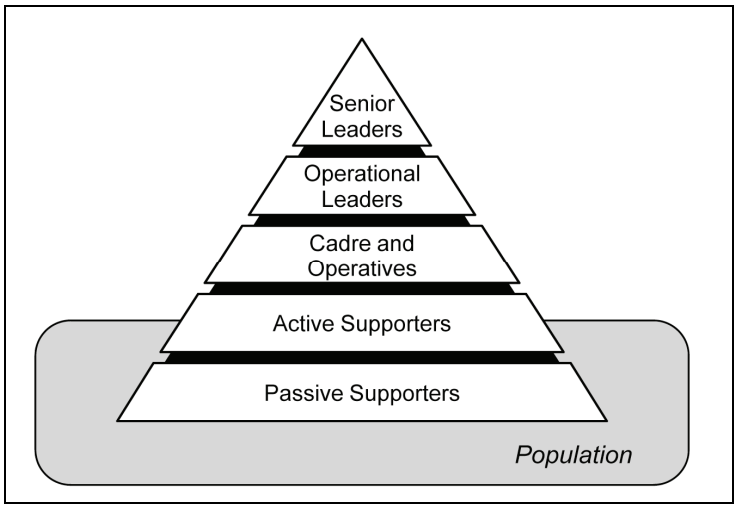


Figure 2-3. Terrorist organizational support pyramid

2-37. The cell is the smallest element at the tactical level of a terrorist organization. Individuals (usually three to ten people) make up a cell and act as the basic tactical element. One primary reason for a cellular configuration is security; each component is relatively isolated from the others and is limited to performing a specific function (financing, recruitment, intelligence, logistics, transportation, forging documents). Some groups have multifunction cells that combine multiple skills into a single entity. Others create cells of specialists that come together for a specific operation.

2-38. Evolving patterns display an increasing use of loosely affiliated networks that plan and act on generalized guidance to wage terror. For instance, individuals with minimal or no direct connection to al-Qaida may take their inspiration for terrorism from ideological statements of senior al-Qaida leaders, yet their direct actions are unilateral.

2-39. A terrorist organization's structure, membership, resources, and security determine its capabilities and reach (see figure 2-1, page 2-4). The knowledge of current and emergent models of terrorist organization improves an understanding of terrorism. Terrorist groups normally organize around functional elements to plan and execute attacks, which include—

- **Operations.** The operations function will determine the operational objectives of the attack, the participants, the specific target, the timing, and the attack method.
- **Intelligence.** The intelligence function may combine intelligence and security. It will usually include collection, analysis, and dissemination of target-specific information. The collection of intelligence involves sources (including open-source materials). Some aspects of intelligence gathering may be outsourced to supporting groups or individuals with specific skills or current and relevant knowledge of the target area. The security subfunction may also include operations security (OPSEC) to prevent compromise of the group and its mission.

- **Support.** The support function normally fulfills requirements (recruitment and personnel support, media, financing, education, camp management, logistics, supplies, weapons, munitions, transportation, communications).
- **Cadre or cells.** The cadre, or combat element, is the heart of the organization and is manned by those who are trained to execute the attack or emplace the bombs.

2-40. Terrorist groups recruit from populations that are sympathetic to their goals. Legitimate organizations can serve as recruiting grounds for terrorists. Sympathizers can be useful for political activities, fund-raising, and unwitting or coerced assistance in intelligence gathering and other nonviolent activities. Recruitment can gain operatives from many diverse social backgrounds. Some terrorist organizations have sought members with U.S. citizenship.

2-41. Some groups will use coercion and leverage to gain cooperation from useful individuals. This cooperation can range from gaining information to conducting a suicide bombing operation. Blackmail and intimidation are common forms of coercion. Threats against family or community members or a targeted individual may be employed to gain cooperation.

2-42. In addition to structure and the type of members, threat group capabilities include training, weapons, equipment, and threat tactics. Training seeks to achieve a level of proficiency with tactics, techniques, technology, and weapons that are useful for terrorist operations. The proliferation of technical expertise and advanced technology enables terrorist groups to obtain targeted skill sets. In addition to the number of terrorists and groups that are willing to exchange training, there are also experts in the technical, scientific, operational, and intelligence fields willing to provide training or augment operational capabilities on a contract basis.

2-43. The threat of domestic terrorism (groups or individuals whose activities are directed at the U.S. government) includes extremist groups, militia groups, and individual actors. Domestic terrorism within the United States in the 1990s revealed a wide variety of homegrown terrorist groups made up of U.S. citizens who are affiliated with special-interest groups, anarchists, race-based hate groups, and militias, to name a few. Many of these domestic terrorists may be native born or naturalized citizens. They operate within their own country and against their own government and citizens. They may or may not have direct association with foreign terrorist groups. Other forms of domestic terrorism called *single-interest* or *special-issue groups* base their reasons for attacks on animal rights; abortion; ecology; the environment; an antigovernment stand; or ethnic, race, or minority rights.

Domestic Terrorist Attacks

In the United States, acts of domestic terrorism are generally considered uncommon. However, according to the Federal Bureau of Investigation, from 1980 through 2000, 250 of the 335 incidents confirmed as, or suspected to be, terrorist acts in the United States were carried out by American citizens or individuals residing in the United States. Some notable acts of domestic terrorism include—

- Los Angeles Times building bombing (1910).
- Wall Street bombing (1920).
- Bath school bombings (1927).
- Unabomber attacks (1978-1995).
- Murrah Federal Building, Oklahoma City, bombing (1995).
- Centennial Olympic Park bombing (1996).
- Anthrax attack through U.S. Postal Service (2001).
- Fort Dix attack plot (2007).
- Times Square bombing attempt (2010).

TERRORIST PLANNING CYCLE

2-44. There is no universal model to reflect the terrorist planning process. Figure 2-4 depicts a general cycle that terrorists would modify based on specific objectives, resources, and time available. Although terrorist activities may appear as random acts, they are typically purposeful and directed activities that are carried out by sophisticated groups who generally follow a deliberate planning cycle.

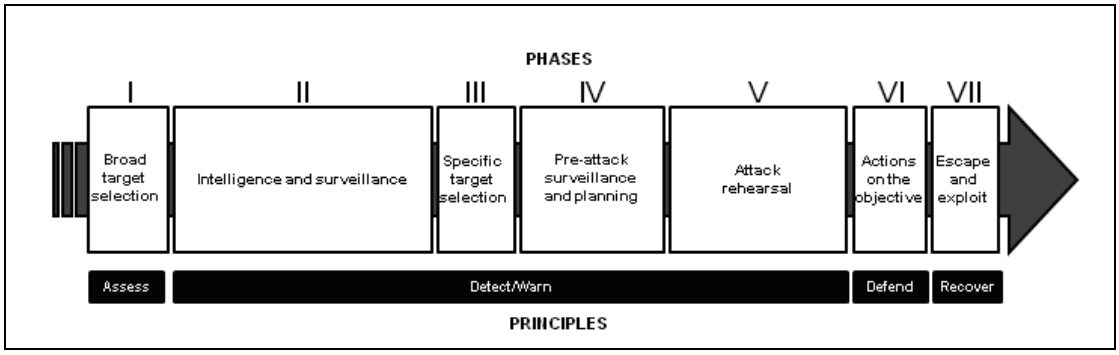


Figure 2-4. Terrorist planning cycle

2-45. Throughout a continuous planning cycle, the terrorist gathers information on potential targets, determines the likelihood of a successful attack, makes decisions on tactics, commits resources, establishes execution timelines, and trains and rehearses for the operation. At any time throughout the cycle, attack planning can be halted or accelerated based on information gathered, friendly force actions, or changes in the group's intentions. U.S. forces can influence the terrorist planning cycle throughout all phases. However, the greatest likelihood of identifying terrorist activities and influencing activities is during the intelligence and surveillance phases (Phases II and IV) when threat force actions are likely observable.

PHASE I: BROAD TARGET SELECTION

2-46. This phase involves collecting information on potential targets using available sources. Collectors may be core members of the terrorist cell, sympathizers, or people providing information without knowledge of the intended purpose. This phase also includes open-source and general information collection. Some features of this type of collection are—

- Stories from newspapers and other media that provide background information.

- Internet research that provides data (texts, pictures, blueprints, video information).
- Potential targets that are screened based on the intended objective and assessed areas (symbolic value, critical infrastructure points of failure, expected casualties, potential to generate high-profile media attention).

2-47. The number of targets that can be screened is limited only by the capabilities and patience of the group targeting them. Targets that are considered vulnerable and could further terrorist goals are selected for the next phase of intelligence collection.

PHASE II: INTELLIGENCE GATHERING AND SURVEILLANCE

2-48. This phase can be very short or span many years. Some elements of information typically gathered include—

- **Practices, procedures, and routines.** This includes regularly scheduled deliveries, work schedules, identification procedures, and observable routines.
- **Residences and workplaces.** The physical layout and individual activities at the two places the target typically spends the most time.
- **Transportation and travel routes.** The mode of transport, common travel routes (house, work, gym, school), ingress and egress points, vehicles allowed on the grounds, and public transportation.
- **Security measures.** This includes security around the target, presence, reaction time of security forces, hardened structures and barriers, security technology screening procedures (people, packages, vehicles), and emergency response drill procedures. Adversaries plan to bypass or avoid security measures; therefore, this is one of the most important areas to consider.

2-49. The entire Army (Soldiers, DA civilians, and contractors) plays an important role in contributing to the security of people, units, and bases. Intelligence, law enforcement, and security force personnel, in particular, need to be alert for activities that may be precursors to terrorist acts. These personnel are especially well trained and well disposed to be vigilant.

2-50. The following are examples of activities or conditions that may be indicators of terrorist threats:

- Suspicious activities near or on bases and critical infrastructure facilities.
- Badge, credential, identification card, or military equipment or apparel thefts.
- Discovery of individuals with false identification.
- Sensitive material and property thefts.
- Individuals taking photos or sketches or conducting surveillance of bases and ECPs.
- Individuals who trespass near key facilities.
- Uncommon or abandoned vehicles, packages, or containers.
- Individuals who search trash containers.
- Individuals who purchases or attempt to purchase, steal, or possess large numbers of weapons, explosives, or supplies that are necessary to manufacture explosive devices.
- Increase in cyber attacks or e-mail probes for information about operations.
- Increase in threats to facilities that require evacuation.
- Unknown workers who try to gain access to facilities.
- Unusual patterns of seemingly unimportant activity: patterns of travel (vehicle, foot, boat, air) or routes of travel that seem to serve no purpose may be used as a means to observe targeted individuals, activities, installations, or ports.

2-51. The list above was compiled by the DOD Inspector General in September 2002. The activities and conditions listed are by no means all-inclusive. Further, some activities may reflect innocent behavior or relate to other types of criminal behavior. However, U.S. forces must be aware that even outwardly innocent activities may be part of a larger scheme, with the ultimate goal of harming U.S. citizens and resources and disrupting the vital U.S. mission of protecting citizens and their way of life. If observed, these activities should be reported to the appropriate law enforcement or intelligence agencies.

PHASE III: SPECIFIC TARGET SELECTION

2-52. The decision to proceed requires continued intelligence collection against the chosen target. Targets not receiving immediate consideration may still be collected against for future opportunities. The selection of a target for detailed operational planning considers some of the following factors:

- Will the target attract high-profile media attention?
- Does the target provide an advantage to the group by demonstrating its capabilities?
- What are the chances of success?
- Does the target have exploitable weaknesses according to the current security status?
- Is the security status going to change between decision and execution?
- Does success make the desired statement to the correct target audiences?
- What are the costs versus the benefits of conducting the operation?
- Is the effect consistent with group objectives?
- Does success affect a larger audience than the immediate victims?

PHASE IV: PREATTACK SURVEILLANCE AND PLANNING

2-53. Members of the operational cells begin to appear during the preattack surveillance phase. Trained intelligence and surveillance personnel may conduct this phase. In some cases, the operators themselves will conduct the preattack surveillance. This phase gathers information on the target's current patterns over an extended period. The attack team confirms information gathered from previous surveillance and reconnaissance activities and adds new observations and data. The areas of concern are essentially the same as in Phase II but with greater focus based on target vulnerabilities. The information gained is used to—

- Conduct security studies.
- Conduct detailed preparatory operations.
- Recruit specialized operatives (as needed).
- Procure a base of operations in the target area (safe house, cache).
- Design and test escape routes.
- Select transportation means.
- Determine a weapon type or attack method.

PHASE V: ATTACK REHEARSAL

2-54. Rehearsals are conducted to improve the odds of success, confirm planning assumptions, and develop contingency plans. Terrorists also rehearse to test security reactions to particular attack methods. Some typical rehearsals include—

- Equipment checks and weapons training.
- Staging for final preparatory checks.
- Deployment into the target area.
- Actions on the objective.
- Escape routes.

2-55. Rehearsals for upcoming attacks have taken place at unpopulated weapons ranges, at paintball facilities, and on the grounds near terrorists residences. Low-scale, successful terrorist attacks provide organizations with lessons learned that can support future planning and the execution of operations. Limited tests within the target area may also be conducted to confirm the—

- Target information.
- Target activities patterns.
- Physical layout of the target or operations area.
- Security force reactions (state of alert, timing response, equipment, routes).

PHASE VI: ACTIONS ON THE OBJECTIVE

2-56. When terrorists reach this stage of their operation, the odds favor a successful attack. The attacker has the advantage of initiative, which provides them with—

- Surprise.
- Choice of time, place, and conditions of attack.
- Employment of diversions and secondary or follow-up attacks.
- Employment of security and support positions to neutralize reaction forces and security measures.

PHASE VII: ESCAPE

2-57. Escape plans are usually well rehearsed and well executed. The exception is a suicide operation. However, even in suicide attacks, there are usually support personnel and handlers who must escape or evade response force personnel.

2-58. Postattack exploitation is a primary objective of a terrorist operation. The operation must be properly publicized to achieve the intended effect. Media-control measures and prepared statements are examples of threat group preparations to effectively exploit a successful operation. High-profile attacks often include spotters and support personnel who are recording the event for use in future media products. These activities will be timed to take advantage of media cycles for selected target audiences.

THREAT VULNERABILITIES

2-59. Vulnerabilities exist in terrorist plans, operations, and support functions. The U.S. targets eight specific threat vulnerabilities with the intent to maintain the initiative and set the tempo, timing, and direction of military operations. The eight targets are—

- Ideological support.
- Leadership.
- Foot soldiers.
- Safe havens.
- Weapons.
- Funds and financing.
- Communications and movements.
- Access to targets.

2-60. Denying resources to terrorists and terrorist networks is critical to countering the ideological support of terrorism. These efforts minimize or eliminate state and private support for terrorism and make it politically unsustainable for a country to support or condone terrorism. Techniques in coordinating such actions may include a methodology of identifying or mapping key organizational components that affect resources (technology key figures, locations). Identifying the major connections among these components can spotlight weak, assailable links of networks where targeting and action plans may be most effective. Measuring results and adapting operations enable a process for improved leader education, training, and operations.

2-61. Establishing alliances and coalitions is a U.S. goal for most operations, but U.S. unilateral action is always a consideration. Efforts to exploit terrorist group vulnerabilities include military options and the other elements of national power: diplomacy, economy, and information.

2-62. During the MDMP, the understanding and application of threat characteristic analysis increases the multinational forces' ability to know the threat and exploit threat vulnerabilities. Threat characteristics provide a construct from which to view the threat. Including personality targeting rounds out the factors used for conventional warfare analysis. This includes—

- Composition.
- Disposition.

- Strength.
- Tactics and operations.
- Training.
- Logistics.
- Combat effectiveness.
- Electronic technical data.

2-63. The threat model allows the analyst to graphically depict the threat. This allows the analyst to form a picture of the threat and track threat patterns over time. The threat model allows the analyst to better identify threat activity levels by comparing the realistic model to current activities, patterns, and trends.

TERRORIST TACTICS

2-64. Terrorist tactics display common principles of armed conflict and propaganda with the intent to cause psychological anxiety and tactical surprise and to weaken resolve in the targeted population. Nonetheless, each situation in an operational environment can present tactical variations and techniques used to conduct a mission. In applying a definition of tactics as the ordered arrangement and their maneuver of forces in relation to an adversary or openly hostile force to achieve a mission objective, the terrorist has a wide range of technique options in conventional, unconventional, or irregular conflict. Techniques that link to a tactic describe methods used to conduct a mission and accomplish required functions or tasks. Techniques evolve thorough the analysis of mission successes and failures. Procedures are standardized steps, performed deliberately and consistently, that prescribe how to perform specific tactical functions and tasks. The how-to of terrorist tactics is a composite of TTP.

2-65. Incidents of terrorism can be the rogue action of a lone individual or the sanctioned activities of a large organization acting under state policy. The following description focuses on individual and small unit actions categorized as a sudden, violent engagement among friendly and hostile forces. These engagements may be offensive in terrorist purpose, but may also require terrorists to transition temporarily to defensive forms of conflict.

2-66. A terrorist uses a flexible array of means and materiel to accomplish assigned missions. The terrorist makes decisions under conditions of uncertainty, but will seek to identify vulnerabilities that can be attacked. Deception and surprise compound the effects of massing an attack against a point of weakness to achieve kinetic effects and create nonkinetic effects of anxiety or fear. Understanding and applying this debilitating coercion on people is central to the intended physical and psychological effects of terrorism on Soldiers, leaders, and the civilian population in an AO.

2-67. The terrorist is adaptive and learns from tactical success and failure. Learning from practical experience, a terrorist will adjust techniques to particular conditions to achieve an objective. Examples of offensive and defensive tactics describe and illustrate terrorist tactics experienced in the operational environments of the U.S. homeland and other U.S. combatant commands. TTP examples underscore the fact that the science of tactics is only as effective as the leadership, training, and experience in a terrorist cell. Elements (demonstrated capabilities, weapon systems, location, restrictions and constraints, logistic support, time-distance factors) are important in planning and conducting a terrorist act, but the essential aspect of executing a terrorist act is the motivation and commitment of each terrorist in the individual or collective execution of tasks to achieve a mission objective.

DEFENSE

2-68. Terrorist tactics include defensive actions conducted to defeat an enemy attack, gain time, economize terrorist capabilities, and/or develop conditions favorable for subsequent operations. Other objectives for conducting defensive actions include retaining decisive terrain or denying access to an area, causing extensive commitment of enemy forces and materiel, or fixing hostile forces for a specific time.

2-69. Terrorist operations might use variations of an area defense and forms of retrograde action. In an area defense, the terrorist may attempt to deny access to designated terrain or a resource for a specific time, limit the freedom of maneuver to an opposing hostile force, or channel hostile force elements into killing

zones to attack them. Within terrorist cell capabilities, mutually supporting defensive positions will attempt to defeat or destroy a hostile force as it attacks. A reserve element could be available to sustain the temporary ability to defend through reinforcement or counterattack or to help terrorist elements disengage and hide from an AO. The retrograde is a transitional operation to regain the initiative and renew offensive actions. Terrorists achieve defensive requirements through asymmetric tactics that take advantage of resources on the battlefield, reduce U.S. capabilities, and restrict rules of engagement. Some defensive tactics are—

- Dispersing and hiding.
- Using human shields.
- Exploiting sensitive infrastructure.
- Conducting information operations.

Dispersion and Hiding

2-70. Dispersion and hiding in complex terrain and urban environments degrade situational awareness and complicate U.S. intelligence and targeting efforts. Urban areas offer excellent cover and concealment from U.S. ground forces and airpower because building interiors and subterranean areas are hidden from airborne observation, and vertical obstructions hinder the line of sight to ground targets. The C2 of terrorist organizations is often decentralized. Terrorist operations are nonlinear and dispersed.

2-71. Within an AO, terrorists make use of safe houses that support terrorist operations due to a true belief in the cause or out of fear. Safe houses (guest houses) facilitate an individual's ability to discreetly transit from one location to another by providing a place to spend the night, acquire resources, obtain false documentation, or secure transportation. Organized-crime syndicates, terrorist networks, and traffickers rely on safe houses to move people from place to place.

2-72. Safe houses may be houses, apartments, mosques, stores, refugee camps, barracks, or another infrastructures that house individuals involved in criminal or terrorist activities. Al-Qaida, the Taliban, and their associates have leveraged the safe house network to great ends, particularly in Afghanistan and Pakistan. The exploitation of infrastructure (residential buildings, shrines, and ruins) can be sensitive for political, religious, cultural, or historic reasons. Enemy forces deliberately occupy sensitive buildings under the assumption that U.S. forces will refrain from entering or returning fire.

Human Shields

2-73. Terrorists deliberately use noncombatants as human shields that limit forces to more stringent rules of engagement and limit their heavy firepower capability. In some areas, enemy forces have prevented civilians from evacuating likely engagement areas to ensure that a source of human shields remained available. Subversives have closed down schools and orchestrated work strikes to produce crowds of civilians in potential operational areas. Attackers have also used peaceful demonstrations as cover and a means of escape after executing an attack. Terrorists use crowds of noncombatants to cover and conceal their movements and to negate multinational force movements. In some cases, children were used as human roadblocks.

Information Operations

2-74. Enemy forces have used information operations to disrupt popular support for multinational forces and to garner regional and international sympathy and support for insurgent forces, mainly from Europe and the Islamic world. Terrorists spread rumors or misinformation in marketplaces and cafes as a means to offset the official information from the HN or U.S. commanders. To gain sympathy for their cause or mask the destructive results of violence on innocent civilians, terrorists create videos that contain footage of attacks on multinational forces, wounded women and children, and damaged local infrastructure. These videos have appeared in regional marketplaces immediately after attacks. This footage is often manipulated to implicate U.S. forces for the resulting damage and deaths to local civilians.

2-75. Terrorist groups use the Internet to disseminate their message as quickly as events occur. An immediate press release from a Web site is not only cheap, but also offers direct control over the content of

the message. Sites are managed to manipulate images in support of the resistance and to create special effects or deception. Video footage of terrorist successes is used for recruitment and to sustain morale. Multimedia sites display manufactured evidence of U.S. and multinational atrocities and war crimes to turn domestic and international opinion against the U.S. government. Enemy forces use sympathetic media to reinforce their information operation plan. Some media companies repeatedly display images of casualties and massive collateral damage and accuse multinational forces of using excessive force.

OFFENSE

2-76. Attack is the primary type of offensive operation that U.S. forces will experience from a terrorist. TTP display numerous ways to conduct a terrorist attack. Creating the ability to focus overwhelming combat power (a single bullet or a massive IED) against a specified objective requires a terrorist to have keen situational awareness and an understanding of the AO. Reconnaissance and surveillance aid in information and intelligence collection to provide this awareness and understanding, therefore improving the terrorist's ability to combine effects at a time and place for the optimum expectation of mission success.

2-77. Terrorists employ a broad range of technology to support their TTP, from low-tech to high-tech. Their ability to exploit advanced, low-cost technology (microchips) and integrate with low-level tactics (roadside bombs) increases their range of available attack methods. As multinational forces develop countermeasures for terrorist tactics, terrorists adapt their TTP in an attempt to remain elusive. As multinational forces counter the terrorists' use of advanced technologies, terrorists may revert to previous low-tech tactics. Multinational forces in Iraq and Afghanistan have seen terrorists and insurgent groups continuously and, at times, rapidly shift between low- and high-tech TTP. Their cycles are not easily predicted, and the manner in which they adaptively operate attempts to counter or preempt U.S. or multinational operations.

2-78. Effective offensive operations develop and use intelligence regarding a hostile force, terrain and weather, and local conditions. Terrorists may shape conditions by deliberately making contact with a hostile force or civilian population to develop a situation, mislead leader decisionmaking, or identify hostile force capabilities and the timeliness of response. Exploitation or pursuit may be conducted if initial offensive actions are successful, but most terrorist actions are planned and executed as a sudden violent attack, followed by a rapid withdrawal from the attack site. The terrorist planning cycle described in this manual provides a model for a generalized sequence of actions for offensive and defensive terrorist operations.

TERRORIST-TARGETING METHODS

2-79. Terrorist targeting of U.S. military forces spans the worldwide U.S. presence in contemporary operational environments (the operational Army, in-transit forces, and the generating force). Whether U.S. military forces are deployed, in-transit, or located on installations and facilities, these forces can be vulnerable to terrorist attack.

2-80. Terrorist TTP continue to evolve, mixing violent asymmetric tactics and conventional operations in an effort to create instability, locally and internationally. The more common types of violent and nonviolent attacks are—

- Assassination.
- Arson.
- Bombing.
- Kidnapping and hostage taking.
- Raid and ambush.
- Hijacking.
- Seizure.
- Sabotage.
- Threat or hoax.
- Environmental destruction.

- Man-portable, air defense system use.
- Chemical, biological, radiological, and nuclear (CBRN) weapons use.

2-81. These tactics can apply various terrorist techniques. Some terms are clearly defined in Army and joint doctrine, some terms are stated in the U.S. code, and others acquire an evolving general definition from contemporary events. Timely intelligence preparation of the battlefield and continuous operational assessments use descriptive categories to accurately and effectively integrate observations and lessons learned from terrorism incidents into AT awareness for individual and collective training, professional military education, and operational missions.

Assassination

2-82. An assassination is a deliberate action to kill a specific, usually prominent, individual (a political leader, notable citizen, collaborator, particularly effective government official). A terrorist group will assassinate individuals who it cannot intimidate, individuals who have left the group, individuals who support the enemy, or individuals who have some symbolic significance to the enemy or the world. Terrorist groups may refer to these killings as punishment or justice as an attempt to legitimize the acts.

Arson

2-83. Arson is a malicious act that uses fire or an incendiary agent to damage, sabotage, or destroy property. Arson is one of the hardest acts or crimes for which to prove guilt, due to a lack of trace evidence left at the scene that could be linked back to the perpetrator. The goal of arson is to conduct physical and psychological damage and overstretch unit resources by reducing their commitment to other missions.

Bombing

2-84. Bombing involves using an explosive device that is fused to detonate in a specific condition against a target. Bombs have been employed by terrorists using military munitions or IEDs. IEDs can be inexpensive to produce and, because of the various detonation techniques available, may pose low risk to the perpetrator. The most notable types of bombs that terrorists use are vehicle-borne and person-borne improvised explosive devices. Bomb techniques have also included aerial delivery, maritime delivery, ground surface implant, subsurface implant, and marine surface and subsurface mining.

2-85. Advantages to these tactics include notoriety and the ability to sometimes control casualties through detonation time and device placement. Announcing responsibility for the bombing or denying responsibility for the incident, should the action produce undesirable results, generates media interest and may lead to increased coverage of a terrorist group's agenda.

Vehicle-Borne Improved Explosive Device

2-86. Vehicle-borne improvised explosive devices have ranged from a simple passenger car, to a large delivery or sewage truck. Units have also dealt with situations where explosives were placed within generators, donkey-drawn carts, and ambulances to disguise their intent from U.S. forces. Bombs are used against U.S. forces who operate in the area during combat patrols, or terrorists position bombs near a facility with the intent to kill forces, as in the Khobar Towers bombing (see figure 2-5). The bomb is then detonated by suicide initiation, time delay, or remote control.

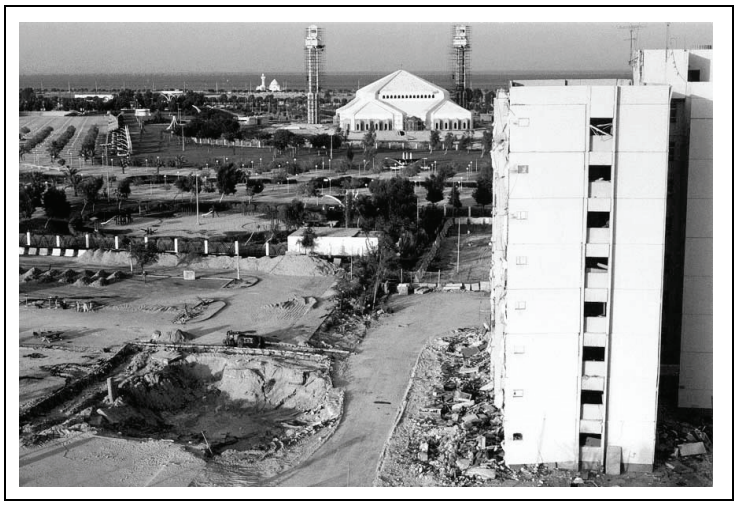


Figure 2-5. Khobar Towers 1996 bombing incident

Person-Borne Improved Explosive Device

2-87. In this tactic, attackers attempt to enter or get close to a target or place or throw an explosive or incendiary device. It also includes a person-borne suicide bomb, which usually employs high explosives and a switch or button that the person activates by hand. Explosives can also be detonated remotely by a handler. It can be a fragmentation bomb and can be contained in a vest, belt, or clothing that is specifically modified to conceal the bomb.

Delivered Device

2-88. A mail, parcel, or letter bomb is an explosive device sent through the mail or delivered to a mail-handling location with the intent to injure or kill a specific person or someone within a specific organization. Theodore Kaczynski (the "Unabomber") killed 3 people and injured 23 others from May 1978 to April 1995 by sending bombs through the postal system to his targets. Kaczynski's bombs were made of wooden parts, and some contained nails and other fragments and performed like a claymore mine when opened. He believed that the bombings were necessary to attract attention to the erosion of human freedom by modern technology.

Suicide Bombers

2-89. This tactic has increased in use over the past 20 years. A suicide bomber is a terrorist version of precision munitions. These bombers have the ability to think, move, react, and determine the actual place of detonation to increase the impact. In some cases, bombers may change their minds, and the bombs can still be triggered remotely. Suicide bombings are popular because—

- Bombings are physically and psychologically impacting to society, tugging at humanity's respect for innocence and life and undermining public confidence in their safety.
- Bombings are inexpensive, costing as little as $150 for a simple attack to approximately $400,000 for the attacks on 11 September 2001.
- Bombers are difficult to stop and can take advantage of societies where the freedom of passage, hesitancy to conduct thorough body searches, or lack of technologically advanced screening devices increases the bomber's chance of success.
- Bombings can be highly lethal and difficult to trace back to the responsible person or organization, limiting operational security risks. The carnage resulting from the attack instantly gains media notoriety.

2-90. Suicide bombings are comprised of the—

- Recruiter.
- Trainer.
- Bomber.

2-91. History has shown that the supply of potential suicide bombers is great. However, the supply of recruiters and bomb makers with the understanding of the terrorist organization strategies, the ability to obtain parts and explosive material, and the skills to fabricate IEDs in a variety of formats is in limited supply.

2-92. A profile for suicide bombers has become increasingly diverse. Males, females, children, married couples, pregnant women, and families have engaged in suicide attacks. Those who volunteer to be suicide bombers may be motivated from within the conflict area (Sri Lanka, Palestine, Chechnya) or outside it (foreign fighters in Iraq). Potential suicide bombers and terrorists can be indoctrinated at an early age to avenge family grievances. They may be traumatized by violence or participate for nationalistic or self-defense reasons. Bombers draw motivation from recruiters and the media exploitation on the Internet.

2-93. The AT officer assists the unit in defending against suicide bombers. The AT officer analyzes information gathered from police, intelligence, and Soldiers on patrol or manning checkpoints that may assist AT forces in preventing and defending against the efforts of suicide bombers. Through AARs, the AT officer can continue to update battle drills for Soldiers who man ECPs and Soldiers on patrol to deal with this threat.

2-94. The briefcase, backpack, or carried form of IED is restricted by the size of the case and can be easily identified and separated from the attacker. The grenade or handheld bomb is used in crowded areas, especially near buses and other forms of mass transit. The vest or belt form of IED is the preferred method of suicide terrorists. Worn under loose-fitting clothing, the device can be undetected unless the suspect is physically searched, and it cannot easily be separated from the bomber. Women have placed bombs around their chest or belly, disguising the bombs within their anatomy or appearing to be pregnant. Examples of suicide bombings include—

- The 1983 suicide vehicle bombing of temporary military billets in Beirut, Lebanon.
- The 2004 suicide vest bombing of a dining facility in Mosul, Iraq.
- The 2010 suicide vest bombing in Khost, Afghanistan.

2-95. To react to a suspected person-borne improvised explosive device perform the following steps (this list is not all inclusive):

- **Step 1:** Alert unit members to the suspect, and evacuate the area if possible.
- **Step 2:** Issue a command in a loud, firm voice to the suspect to stop. A weapon should be trained on the suspect.
- **Step 3:** Direct the suspect to show his hands palms up. The suspect must show his palms and spread his fingers, so that it can be determined if the suspect is palming a detonator. There may be a remote detonator.
- **Step 4:** Tell the suspect to place carried items on the ground and to step two paces away from them.
- **Step 5:** Direct the suspect to remove outer clothing and to place garments on the ground.
- **Step 6:** Direct the suspect to raise or remove his undershirt and to hold it up while turning in a complete circle.
- **Step 7:** Direct the suspect to lie face down, with arms outstretched palms up and face turned away from you. Do not approach, even if the suspect is injured. Maintain cover and wait for the arrival of explosive ordnance disposal personnel.
- **Step 8:** Report the suicide bomber to higher headquarters using the 10-line explosive hazard spot report.
- **Step 9:** Determine if the suspect is noncompliant (deadly force will be used according to the theater rules of engagement).

- **Step 10:** Evacuate the area around the suspect.
- **Step 11:** Establish security, and scan for secondary person-borne IEDs.
- **Step 12:** Maintain security in case of possible ambush.
- **Step 13:** Follow the directions of the vehicle or squad leader.

2-96. Actions to preempt, dissuade, or deter suicide attackers require a comprehensive military and law enforcement program of intelligence support and operational vigilance to identify and defeat or destroy terrorists, cells, and support networks early in a terrorist planning cycle. At individual and organizational levels, applying the AT principles (assess, detect, warn, defend, and recover) with an integrated and layered terrorism awareness posture is a practical way of assessing risk and enhancing the protection of resources, information, and people. There is always a high probability that the suicide bomber will attempt to detonate the explosive device even after receiving specific direction by Army forces. Soldiers must be prepared to use deadly force according to the theater rules of engagement.

DANGER

Physically restraining a suspected suicide bomber from detonating the device requires coordination with other Soldiers and is very dangerous.

Maritime Delivery Tactic

2-97. Terrorists can use small, fast maritime vessels and loaded with explosives and a team of suicide bombers to attack or cripple commercial or naval vessels. In 2000, two al-Qaida members conducted a suicide attack on the United State Ship (USS) Cole, killing 17 Service members. The terrorists made adjustments based on the failed attack against the USS The Sullivans earlier in the year and obtained intelligence on refueling operations and stationary time in port to plan the engagement, pulling up alongside the USS Cole with approximately 270 kilograms of composition C4 and detonating it (see figure 2-6).

Figure 2-6. Attack on the USS Cole

Kidnapping and Hostage Taking

2-98. Kidnapping is the unlawful seizure and captivity of one or more individuals. Kidnappings usually result in the individual being held hostage to extract specific demands, but kidnapping may be for intelligence gathering or execution. A successful kidnapping usually requires elaborate planning and logistics. Similarly, hostage taking is the seizure of one or more individuals, usually overtly, with the intent of gaining advantage (publicity, ransom, political concessions, or release of prisoners). Targets of terrorist-related kidnappings and hostage taking are usually prominent individuals (high-ranking foreign diplomats, officers of symbolic value [government, military, law enforcement personnel; foreign businessmen; tourists]). Because the perpetrator may not be known for a long time, the risk to the perpetrator is less than in the overt hostage situation. Hostages can also serve as human shields, increasing terrorists' chances of

success in carrying out a mission or to use in exchange for other government detainees or prisoners. While dramatic, hostage and hostage barricade situations are risky for the perpetrator. The killing of hostages may occur once the terrorist group believes that it has fully exploited the media coverage from the situation.

Raid and Ambush

2-99. A terrorist raid is similar in concept to a conventional military operation, but is usually conducted with smaller forces against targets marked for or destruction, hijacking, or hostage or barricade operations. In some cases, the raid is designed to allow control of the target for the execution of another operation. An ambush is a surprise attack characterized by violent execution and speed of action that intends to destroy a target. Swarming tactics may be used with multiple small teams to attack simultaneous targets to confuse and tax response forces.

2008 Mumbai Mass Murder and Hostage Crisis

On 26 November 2008, a heavily armed, ten-person terrorist cell attacked several prominent sites in Mumbai, India, in nearly simultaneous assaults that caused more than 170 deaths and wounded over 300 people in site seizures and hostage crises lasting more than 60 hours. The cell was linked to the Pakistan-based, Lashkar-e-Taiba terrorist group. The choice of targets was business and commercial hubs, famous entertainment sites, and cultural landmarks, combined with indiscriminate killing and murders based on nationality or religion. The Lashkar-e-Taiba intent appeared to be exceptional psychological trauma on a major urban population and nation, undermining the confidence in India's ability to protect its people and foreigners, and expanding a Lashkar-e-Taiba regional agenda to global attention and international ideological extremism.

The terrorist cell was thoroughly trained and indoctrinated. More than one year in preparation, surveillance and reconnaissance refined intelligence. Methodical infiltration of the objective area was followed by ruthless actions at each objective and the corresponding exploitation of mass media during and after the crisis. The terrorists used global positioning system and an array of communications to transit more than 500 kilometers by sea to a rendezvous point off the shoreline of Mumbai. Having seized a small fishing trawler at sea, the terrorists murdered the crew and transferred their weapons and explosives to an inflatable boat to reach the shore. Four, two-person teams went ashore and used taxis while one team walked to their target. A fifth, two-person team continued in an inflatable boat along the shore to their target. With teams at their urban objectives, attacks were initiated within minutes of one another at five dispersed locations. Mass murder occurred as terrorists used semiautomatic rifle fire and hand grenades against people in a rail station, hospital, urban streets, café, hotels, and Jewish cultural center. Earlier, IEDs had been hidden in two taxis and were timed to explode well after the main attacks were underway. These explosions caused additional confusion and mayhem in the first hours of the incident. After attacking the café, one team quickly joined the team assault on the hotel, killing people, starting fires in the hotel, and seizing hostages. Hostages were seized at a Jewish cultural center and eventually murdered. Another team entered a second hotel and immediately started killing people and seizing hostages. One team shot people randomly in a train station and a hospital and departed to probably link up with other team members. Several other IEDs were emplaced at some of the sites but were discovered before they could cause casualties.

The terrorist team members were well armed with AK-56 assault rifles and 8 to 10 ammunition magazines, pistols with 2 extra magazines, 8 to 10 hand grenades, explosives for IEDs, and basic food and water. They communicated with one another and operational handlers remotely from Mumbai using cellular telephones and subscriber identity module cards, Voice Over Internet Protocol, satellite telephone, and personal digital assistant devices; and they referenced high-resolution, satellite imagery. Handlers provided ideological encouragement, direction, and tactical advice based on the observation of live media coverage at the attack sites. Local law enforcement was initially overwhelmed by terrorist firepower. Once federal military forces arrived on site, police and military forces killed nine terrorists and captured one.

2008 Mumbai Mass Murder and Hostage Crisis (continued)

Hijacking is the forceful commandeering of a conveyance (plane, ship, motor vehicle, train). This unlawful seizure of transportation means is normally associated with holding people on the conveyance as hostages. The 1970 Dawson Field hijackings, where four airliners were hijacked and taken to Jordan and Cairo by the Popular Front for the Liberation of Palestine and the events on 11 September 2001 represent well-planned, well-organized hijacking terrorist events.

Seizure

2-100. Seizure is an act normally associated with the forceful occupation of a symbolic location or key facility (energy plant, cyber node, civil education center). This unlawful seizure can be associated with holding people in a location or facility as hostages, as in the 2004 Beslan school siege by Chechen militants in North Ossetia (Russia).

Sabotage

2-101. Sabotage is a deliberate action aimed at weakening another entity through subversion, obstruction, disruption, or destruction. The objective in most sabotage incidents is to demonstrate how vulnerable society and its critical infrastructure are to terrorist actions and the inability of the government to stop terrorism. Utilities, communications, and transportation systems are interdependent, and a serious disruption of one affects all and attracts immediate public and media attention. Military facilities and installations, information systems, commercial industry, human resources, and energy and communication infrastructures are examples of attractive targets of terrorist sabotage (an oil refinery, a cyber attack on a sensitive communications capability).

Threat or Hoax

2-102. A terrorist group with established credibility can employ a hoax with considerable success. A hoax is an announcement or action intended to deceive a receiving target audience. Threats announced by a terrorist may be a ruse to build anxiety in a target audience, consume resources and time of an opposing force, or enable observation of the response capabilities of an opposing force. Repetitive threats and false alarms could reduce vigilance and reaction time if a real event should occur.

Environmental Destruction

2-103. Terrorists have used environmental destruction in limited cases to distribute their message. The destruction of oil tankers, poisoning of public water systems, poisoning of local food supplies, and burning or destruction of oil fields can have a major impact on local economies and U.S. operations to stabilize peace and governments in conflicted regions.

Man-Portable, Air Defense System

2-104. Man-portable, air-defense systems have been used in a variety of major conflicts as a means to provide ground forces with the capability to reduce the threat of enemy aircraft. Their availability to terrorist organizations is a significant capability for attacking military and commercial aircraft. Examples of man-portable, air-defense system use are—

- The 1994 assassination of Rwandan president Juvenal Habyarimana and Burundian president Cypien Ntaryamira while their plane attempted to land in Kigali, Rwanda.
- The 2002 downing of a Russian Mi-26 military heavy transport helicopter in Grozny, Chechnya.

Chemical, Biological, Radiological, and Nuclear Weapons Use

2-105. The means of CBRN attack can range from a highly sophisticated weapon system (a nuclear bomb, rudimentary improvised radiological device). The threat of chemical contamination or biological infection adds to the array of possible terrorist weapons. As the United States confronts terrorism, foreign and domestic, the most significant U.S. concerns are terrorist organizations with demonstrated global reach and the intention to acquire and use weapons of mass destruction.

2-106. Terrorists have employed, and some terrorist cells will continue to seek, CBRN material and will use these weapons when they can be obtained. Chemical, biological, and radiological materials could be used as weapons with or without conventional explosives in many situations. Although an explosive nuclear device and the capability to weaponize chemical or biological material are beyond the reach of most terrorist groups, the use of chemical or biological materials as a weapon or the use of a radiological dispersal device is more feasible.

2-107. Attackers could introduce CBRN material into the air or into a facility in this tactic. These agents can be delivered by external or internal release. External release can be from directed plumes spread from a standoff distance, from a point or line source, from general aerial release, or by directly inserting the agent into outside air intakes of facilities. Internal release can be through the mail, by supply delivery, direct release within a building or area, or insertion into a ventilation system. Many chemical and biological weapon ingredients are commercially available, and instructions on building a device have been found on the Internet.

1995 Tokyo Subway Sarin Attack

On 20 March 1995, five, two-person teams, who were members of Aum Shinrikyo (a Japanese doomsday cult), executed near-simultaneous sarin attacks on the Tokyo Metro during the height of the morning rush hour. The liquid nerve agent was contained in plastic bags wrapped in newspaper. The attackers each carried approximately 900 milliliters of sarin (a single pinhead-size drop can be lethal). At subway stations, the sarin packets were left and punctured with the sharpened tips of umbrellas, allowing the liquid chemical agent to ooze out, slowly vaporizing within the train cars and stations. The attacks were coordinated to occur where and when the subway train routes converged on Kasumigaseki Station, the center of the capital's government district. The attackers fled in prestaged escape vehicles. The attacks killed 12 people and injured or contaminated more than 5,500 people. The sarin attacks marked a turning point and new level of sophistication and lethality for the terrorist use of CBRN in an attempt to generate a lethal airborne agent, and the psychological and operational effect and use of CBRN weapons a lucrative tactic for terrorists. First responders, hospital staffs, and hospital facilities became contaminated, increasing casualties and degrading emergency response and recovery operations. A postattack analysis and criminal case studies of Aum Shinrikyo revealed a history of escalating violence and showed that, the Japanese police suspected Aum's experimentation with and intent to use chemical weapons before the attack.

Chapter 3
Foundations of Antiterrorism

This chapter explains AT as a tactical task and places AT into context with combating terrorism and the protection warfighting function. It introduces the five principles of AT: assess, detect, defend, warn, and recover. By understanding the principles of AT and the relationship of AT to combating terrorism and the protection warfighting function, AT planners will be better prepared to integrate AT into Army operations. *Antiterrorism* is composed of the defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces. (JP 3-07.2) AT is a consideration for forces during military operations as the Army's defensive program to protect against terrorism. Army AT, at a minimum, focuses on risk management, planning (including the AT appendix), training, exercises, resource generation, measures of effectiveness, and random AT measures. AT planning coordinates specific AT security requirements with the efforts of other security enhancement programs (intelligence support to AT, law enforcement, physical security, OPSEC, information security). Effective AT programs synchronize intelligence, CRM, and existing security programs to provide a holistic approach to defend against terrorist threats. The eight AT tasks that guide the commander in the development of a unit AT program are—

- AT Task 1. Establish an AT program.
- AT Task 2. Collect, analyze, and disseminate threat information.
- AT Task 3. Assess and reduce critical vulnerabilities.
- AT Task 4. Increase AT awareness (see appendix B).
- AT Task 5. Maintain defenses.
- AT Task 6. Establish civil-military partnerships.
- AT Task 7. Conduct terrorist threat/incident response planning.
- AT Task 8. Conduct exercises and evaluate/assess the plan (see appendix C).

Terrorists can target Army elements at any time and location. By effectively preventing and responding to terrorist attacks, commanders protect activities and people so that Army missions can proceed unimpeded. AT is not a discrete task or the sole responsibility of a single branch—all branches bear responsibility. AT must be integrated into Army operations and considered at all times. Installations in the continental United States or outside the continental U.S., Corps of Engineers projects, bases, and combat units should consider AT principles in every assigned mission.

COMBATING TERRORISM

3-1. *Combating terrorism* consists of actions, including AT (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum (JP 3-07.2). As a strategy, a program, and an Army tactical task, there is recognition that the fight against terrorism is a different kind of fight. The Army promotes freedom and human dignity as alternatives to the terrorists' perverse vision of oppression and totalitarian rule. The U.S. paradigm for combating terrorism involves

applying elements of national power and influence. The United States will employ military power; use diplomatic, financial, intelligence, and law enforcement activities to protect the homeland; extend defenses; disrupt terrorist operations; and deprive enemies of what they need to operate and survive.

3-2. *Counterterrorism* consists in operations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism (JP 3-07.2). Counterterrorism actions include strikes and raids against terrorist organizations and facilities outside the United States and its territories. Although counterterrorism is a specified mission for selected special operations forces, conventional Army forces may also contribute. Commanders who employ conventional forces against terrorists are conducting offensive operations, not counterterrorism operations.

3-3. The defensive element of combating terrorism (AT) overlaps with the commander's protection efforts. Combating terrorism also includes two critical supporting functions: incident management (preparation for and response to a terrorist incident or event) and intelligence support (collection and dissemination of terrorism-related information) taken to oppose terrorism throughout the entire threat spectrum.

PROTECTION WARFIGHTING FUNCTION

3-4. *Protection* is the preservation of the effectiveness of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area (FM 3-37). FM 3-37, the Army's keystone manual for protection, establishes doctrine for the protection warfighting function. A *warfighting function* is a group of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions and training objectives (FM 3-0). The six Army warfighting functions are—

- Movement and maneuver.
- Intelligence.
- Fires.
- Mission command.
- Sustainment.
- Protection.

3-5. Preserving the force includes protecting personnel (combatant and noncombatant), and physical assets of the U.S. and U.S. multinational military and civilian partner information. FM 3-37 discusses the tasks and systems of the protection warfighting function. It uses many of the other tactical tasks within the protection warfighting function for the sole purpose of preventing and recovering from terrorist acts. The other tasks are—

- Air and missile defense.
- Personnel recovery.
- Information protection.
- Fratricide avoidance.
- Operational area security.
- Survivability.
- Force health protection.
- CBRN.
- Operations.
- Safety.
- OPSEC.
- Explosive ordnance disposal.

While AT integrates a variety of assessments and defensive actions into a comprehensive program to protect against terrorist attacks, it does not include all aspects of protection.

3-6. AT is a key task within the protection warfighting function and a major component of the combating terrorism program. Within each of these constructs, the commander serves as the central figure in the success of the unit's AT program. Commanders apply combat power through the key warfighting functions (mission command, protection, intelligence, and maneuver), balancing the ability to mass lethal and nonlethal effects to mitigate the risk associated with terrorism actions. Commanders tailor forces to balance mission requirements associated with full spectrum operations and their inherent responsibility to protect the force (see figure 3-1).

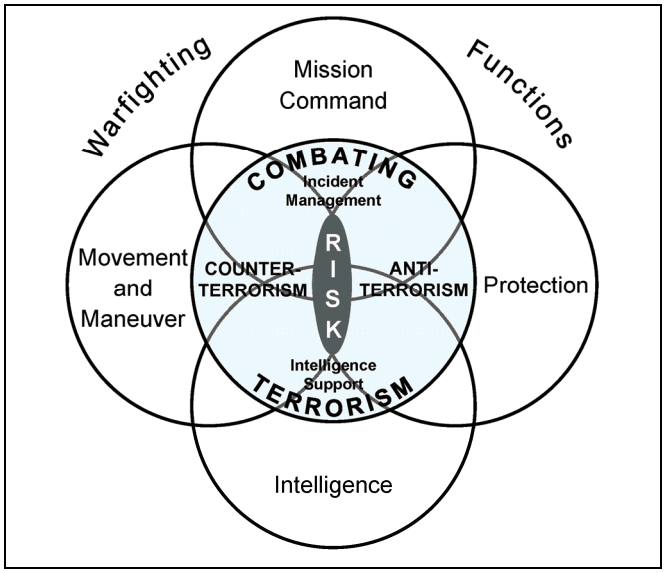


Figure 3-1. AT supported functions

3-7. Military activities have some inherent or organic protection capability. Through combined arms and unified action, commanders ensure that they have the right mix of resources and capabilities and take into consideration the protection and utilization of multinational and HN partners. AT measures, within combating terrorism, are complementary or reinforcing to combat power generation:

- **Complementary.** Complementary capabilities protect the weakness of one system or organization with the capabilities of a different warfighting function.
- **Reinforcing.** Reinforcing capabilities combine similar systems or capabilities within the same warfighting function to increase the function's overall capabilities.

3-8. Through mission command, commanders and staffs introduce AT principles into the operations process, CRM, and mission orders to accomplish full spectrum operations. Through authority, direction, intent, and information, commanders empower subordinate leaders and Soldiers to adapt to a tough and often elusive enemy and perform effectively in a complex and chaotic environment. The key elements of AT tasks are—

- Assessment.
- Force protection conditions (FPCONs).
- Random AT measures (RAMs).
- Physical security.

The commander must be provided with the tools to support the overall protection warfighting function and represent a visible and physical manifestation of resources to deter terrorist acts.

3-9. Protection determines the degree to which potential terrorist threats can disrupt operations and counters or mitigates the risk associated with terrorist threats. The emphasis on protection increases during predeployment and mission preparation and continues throughout mission execution. Protection is a continuing activity that integrates protection capabilities to safeguard bases, protect the local populace, and protect forces.

3-10. The intelligence warfighting function provides timely and actionable terrorist threat information in support of the combating terrorism operations. This information is used by commanders to make better risk decisions when protecting the force during force projection and deployment and provides the necessary targeting information to conduct counterterrorism (offensive) operations.

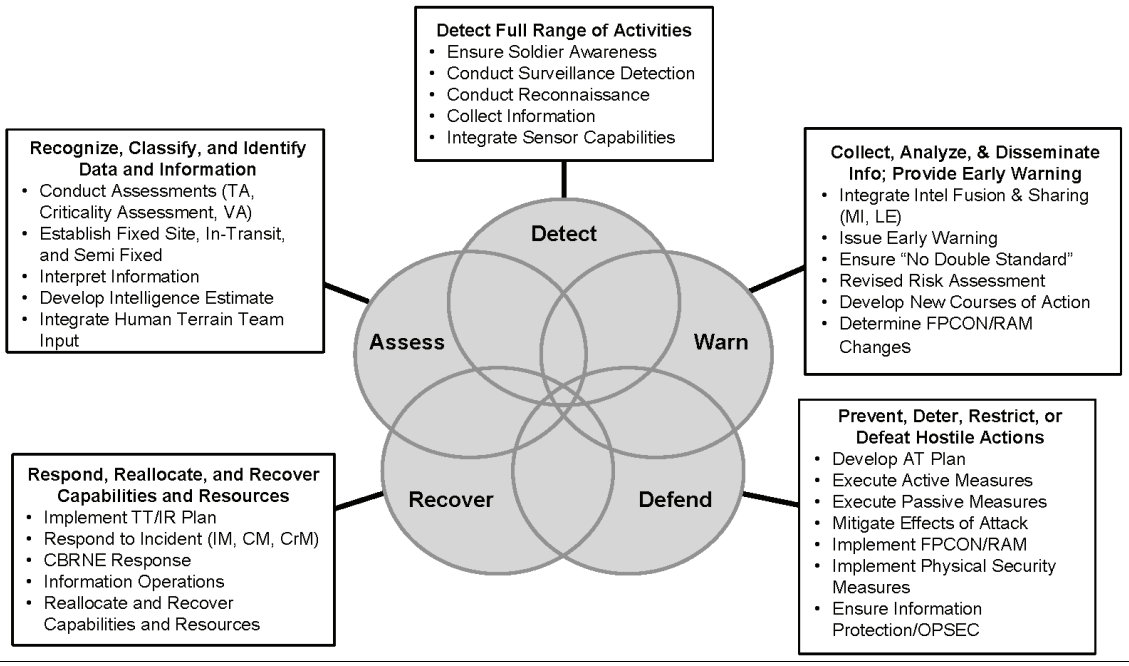
3-11. Army CI is a key contributor in preventing and deterring terrorist activities and is responsible for identifying terrorist indications and warning. Army CI supports the AT tasks through the execution of the CI functions (investigations, collection, analysis and production, and technical services and support). Army CI generally focuses on the foreign intelligence and security services and international terrorist organizations' intelligence collection and targeting activities directed at Army equities to provide indications and warnings of exploitation or potential attacks. Unless assigned to a counterterrorism unit, Army CI is continually engaged in an AT role to help detect, identify, and assess foreign intelligence and security services and international terrorist organizations' collection threats and terrorism indications and warnings. To support AT, CI—

- Conducts foreign intelligence collection and CI activities to collect and disseminate information on foreign threats against the Army.
- Sustains an intelligence capability to monitor and report on the activities, intentions, and capabilities of foreign intelligence and security services, international terrorist organizations, and other foreign threat groups according to applicable regulations and directives.
- Maintains a capability to report and disseminate time-sensitive information concerning the foreign threat against Army personnel, facilities, and other assets.
- Provides supported Army commanders with information concerning the foreign threat against their personnel, facilities, and operations, consistent with the provisions and limitations of AR 381-10 and other applicable regulations and directives.
- Includes foreign threat information in briefings on CI according to AR 381-12.
- Serves as the Army intelligence liaison representative to federal, state, and local agencies and HN federal, state, and local agencies to exchange foreign threat information.

3-12. The maneuver warfighting function supports combating terrorism operations and unit AT tasks by serving as the principal counterterrorism arm. Units within the maneuver warfighting function use intelligence information to support special operations forces in killing or capturing terrorists to immediately mitigate their influence and overall strategic effect in an AO.

ANTITERRORISM PRINCIPLES

3-13. The five AT principles (assess, detect, warn, defend, and recover) represent the characteristics of successful AT integration and synchronization within the Army and the joint functional concept of protection. These principles allow the force to protect itself from terrorist attacks and threats through the persistent detection of threats in an integrated, shared understanding of the operational environment and on-time dissemination of accurate decisions, warnings, and taskings. AT within combating terrorism operations and the protection warfighting function is proactive, focused, and conducted by integrating military and cross-government capabilities against enemies. These principles guide the commander and AT officer to protect personnel (combatant and noncombatant), information, and physical assets by applying active and passive measures against the full threat spectrum. These principles (see figure 3-2) are not a process and may be applied as the situation dictates.



Legend:

AT	antiterrorism
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CM	consequence management
CrM	crisis management
FPCON	force protection condition
IM	incident management
intel	intelligence
IR	incident response
LE	law enforcement
MI	military intelligence
OPSEC	operations security
RAM	random antiterrorism measures
TA	threat assessment
TT	terrorist threat
VA	vulnerability assessment

Figure 3-2. AT principles

ASSESS

3-14. Assessment is the method of monitoring and evaluating the current situation and the progress of an operation. Assessing includes the analysis of the security environment, adversary threat information, and the effectiveness of planning and execution measures to mitigate vulnerabilities. Examples are maintaining a common operational picture; completing detailed threat, vulnerability, criticality, and risk assessments; maximizing available analytical devices and sensors; and conducting training and exercises to evaluate the effectiveness of AT measures and force capabilities.

DETECT

3-15. Detection identifies an act of aggression and analyzes its validity. It also supports the principles of defend and warn by providing appropriate information to units, response forces, and C2 elements. A detection system must provide all three of these capabilities to be effective. Detection may identify an adversary's movement via direct observation; intelligence, surveillance, and reconnaissance; or electronic

security systems capabilities. Other examples of detection are perimeter patrols or security technology, unmanned aircraft systems, and reconnaissance and surveillance patrols.

DEFEND

3-16. Defense protects an asset from aggression by delaying or preventing an adversary's movement toward the asset or by shielding the asset from threat tactics, tools, weapons, and explosives. Defensive measures may be active or passive:

- Active measures are a manual or automated response (reaction force, activation of entry control barriers) to acts of aggression.
- Passive measures do not rely on detection or response activities (blast-resistant building components, perimeter fencing, Jersey barriers).

WARN

3-17. Warning includes the knowledge and communication of a broad range of dangers, from general to specific and imminent threats, due to the wide spectrum of potential adversary activities. Examples of warning tasks are training, education, and awareness of the terrorist threat; use of local area networks, electronics, and communication devices to disseminate threat warnings and indications; and imminent threat warning systems (command information networks).

RECOVER

3-18. Recovery deals with the need to recover operations as the response to a terrorist incident occurs. In an almost seamless evolution, the emphasis upon response gives way to recovery operations. Within recovery, actions are taken to help military personnel, installations, facilities, and operating units return to preincident operating status. Short-term (hours to weeks) recovery includes immediate measures that support crisis response activities. Examples of crisis response and recovery are providing essential health and safety services, restoring interrupted utility and other essential services, reestablishing transportation routes, operating decontamination sites, and providing food and shelter for displaced persons. Long-term consequence management and recovery may also involve some of the same actions, but can continue for months or years, depending on the severity and extent of the damage sustained. Long-term recovery may include the complete redevelopment of damaged areas.

DEPLOYED ANTITERRORISM PROGRAM

3-19. Commanders communicate the spirit and intent of AT doctrine throughout the chain of command or line of authority by establishing AT tasks and measures to develop and disseminate terrorist-related information necessary to protect the force. The tasks provide standards, policies, and procedures to reduce vulnerabilities from terrorist attacks.

3-20. Commanders, with the assistance of the AT officer, develop and maintain an AT appendix to operations order or implementation guidance found in an annex to inform their units how to defend against terrorist threats. The AT appendix usually pertains to battalion-size or great units and to operational deployments (50 or more personnel) through training, deployment, and redeployment. This appendix or standing operating procedure (SOP) should outline specific threat mitigation measures to establish a local baseline defensive posture and indications for the decision to elevate security postures, including the application of RAM. AT planning includes physical security measures, AT measures for HRP, operational contract support actions (see appendix D), measures for in-transit movements, construction and building consideration, critical asset security, and FPCON implementation and measures for incident response and incident management.

3-21. Units integrate AT thinking and planning into their battle rhythm through normal staff actions and functional cells, which coordinate and synchronize forces and activities by warfighting function. Staff sections manage information related to their individual fields of interest. They routinely analyze factors that include operations and collect, process, store, display, and disseminate information that flows

continuously into the headquarters. Staffs seek to identify problems affecting their fields of interest or the entire command.

3-22. Whereas functional cells are organized by warfighting functions, integrating cells coordinate and synchronize forces and warfighting functions within a specified planning horizon (long-, mid-, and short-term) and include the plans, future operations, and current operations integration cells. Units below the division level may not be resourced for three integration cells and may combine responsibilities into one integration cell or even create working groups to assist in focusing efforts pertaining to a particular mission or threat.

3-23. One way to focus AT efforts and planning is through the creation or inclusion of an AT working group (ATWG). Commanders and AT officers use the ATWG to oversee the implementation of the AT plan and tasks, develop and refine AT guidance, and address emergent or emergency AT issues. Within the unit ATWG, key personnel throughout the command staff and subordinate commanders use the working group format to assist in developing and refining terrorism TAs and to coordinate and disseminate threat warnings, reports, and summaries throughout the command. The ATWG and threat dissemination protocols are particularly effective for commanders whose responsibility extends to include forward operating bases (FOBs) or base clusters as a means to convene units from across multiple disciplines.

3-24. AT supports the protection warfighting function and the protection of combat power through the execution of three primary tactical tasks found in the Army universal task list—identify potential terrorist threats and other threat activities, reduce vulnerabilities to terrorist acts and attacks, and react to a terrorist incident (see FM 7-15). These primary tasks are supported by five AT tasks that commanders and AT officers should use to achieve objectives that deter terrorist incidents, employ countermeasures, mitigate effects, and conduct incident recovery (see figure 3-3).

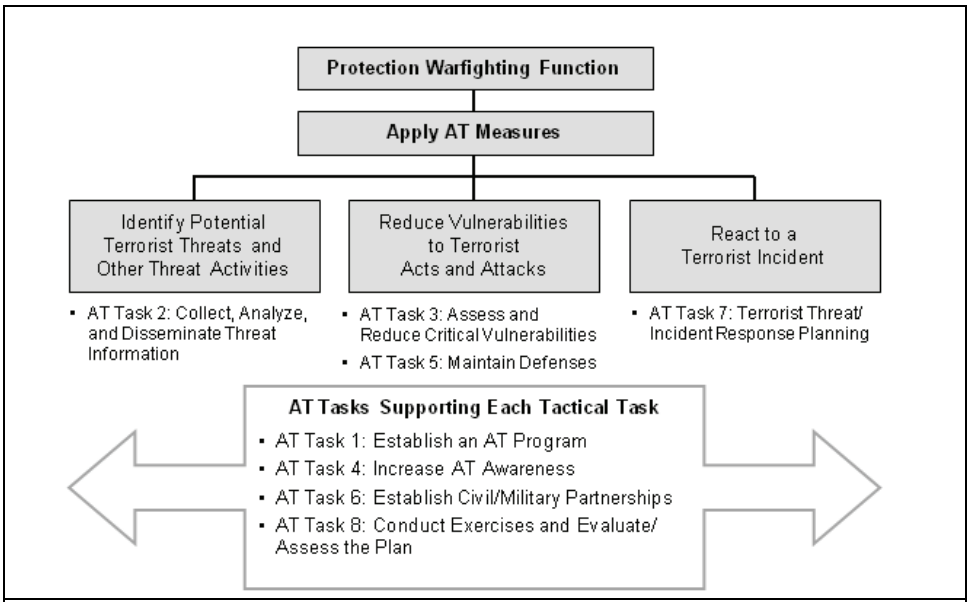


Figure 3-3. Army tactical tasks and supporting AT tasks

IDENTIFY POTENTIAL TERRORIST THREATS AND OTHER THREAT ACTIVITIES

3-25. Units enhance freedom of action by identifying and reducing friendly vulnerability to terrorist threats, acts, influence, or surprise. This includes measures to protect from surprise, observation, detection, interference, espionage, terrorism, and sabotage. Commanders and AT officers empower their own staffs and coordinate with multiple entities to identify terrorist risk to units operating within the United States, during in-transit movement to deployed locations, while conducting peace operations, and during multinational exercises in an HN.

Antiterrorism Task 2. Collect, Analyze, and Disseminate Threat Information

3-26. The TA is used to identify the terrorist threats posed to Army assets and/or the threats that could be encountered in executing a mission and is inherent within the intelligence preparation of the battlefield or intelligence estimate process. The TA is a product developed from the threat analysis, which identifies and evaluates potential threats based on such factors as a threat's intent, capabilities, intentions, past activities, and specific targeting information. This assessment represents a systematic approach to identifying potential threats before they materialize. However, this assessment might not adequately capture emerging threats, even in cases where the assessment is frequently updated.

3-27. Terrorist threat information can be obtained at all levels of the U.S. government and its allies. Through partnerships, commanders and staffs obtain terrorist-related and local threat information from local and state law enforcement intelligence and counterterrorist units. The intelligence collection and the all-source intelligence process serve as key contributors to the TA. The exploitation of terrorist-related information and intelligence can lead to and support the evaluation and analysis of terrorism activities, capabilities, and specific terrorist groups and cells. Units without an organic G-2/S-2 section could develop an internal threat working group to assist in analyzing threat-related information for the commander. The result of carefully assessed and fused intelligence data provides commanders and leaders with actionable intelligence to conduct offensive operations while leading the direction of AT and defensive operations to ensure mission success.

3-28. Threats include hazards with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation from hostile actions. Threats from hostile actions include a capability that terrorists or criminal elements have to inflict damage upon personnel, physical assets, or information. These threats may include IEDs, suicide bombings, information network attacks, mortars, asset theft, air attacks, and the employment of CBRN weapons.

3-29. Assessing the threat considers the risk or likelihood of an incident adversely impacting mission, capabilities, people, equipment, or property. What is the likelihood (probability) of a specific type of attack occurring, and what is the effect (severity) of the incident if it does occur? Threats and associated risks are assessed during mission analysis; course of action (COA) development, analysis, and rehearsal; and MDMP execution steps and must consider mission- and non-mission-related aspects that may have an impact. The result is an initial estimate of risk for each identified hazard, expressed in terms of low, moderate, high, or extremely high. These factors are indicated as—

- **Probability.** Probability is the likelihood of an event, an estimate, based on information that is known and that others provide. The probability levels estimated for each hazard are based on the mission, COA, or frequency of a similar event. For the purpose of CRM, there are five levels of probability:
  - ***Frequent.*** Occurs very often, known to happen regularly. Examples are surveillance, criminal activities, cyber attacks, and small arms fire.
  - ***Likely.*** Occurs several times, a common occurrence. Examples are IEDs, hostages, ambushes, and bombings.
  - ***Occasional.*** Occurs sporadically, but is not uncommon. Examples are injury or death from attacks against aircraft, hijacking, or skyjacking.
  - ***Seldom.*** Remotely possible, could occur at some time. Examples are the releases of chemical or biological weapons.
  - ***Unlikely.*** Presumably, the action will not occur, but it is not impossible. Examples are the detonation of containerized ammunition during transport or the use of a dirty bomb.
- **Severity.** Severity is expressed in terms of the degree to which an incident will impact combat power, mission capability, or readiness. The degree of severity estimated for each hazard is based on knowledge of the results of similar past events and is addressed in the following levels:
  - ***Catastrophic.*** Complete mission failure or the loss of ability to accomplish a mission, death, or permanent total disability, loss of major or mission-critical systems or equipment, major property or facility damage, mission-critical security failure, or unacceptable collateral damage.

- ***Critical.*** Severely degraded mission capability or unit readiness, permanent partial disability or temporary total disability exceeding three months, extensive major damage to equipment or systems, significant damage to property or the environment, security failure, or significant collateral damage.
- ***Marginal.*** Degraded mission capability or unit readiness; minor damage to equipment or systems, property, or the environment; lost days due to injury or illness not exceeding three months; or minor damage to property or the environment.
- ***Negligible.*** Little or no adverse impact on mission capability, first aid or minor medical treatment, slight equipment or systems slight damage (remain fully functional or serviceable) or little or no property or environmental damage.

3-30. Threat analysis provides the staff with information upon which to base warnings. The intelligence officer works in conjunction with the operations officer, AT officer, and staff to provide the commander with a clear operating picture of the terrorism threat to their activity or operation. Commanders review the information and direct the following actions—

- Ensure that AT and threat information is distributed up and down the chain of command and laterally, as appropriate.
- Implement effective processes to integrate and fuse the sources of available threat information.
- Prepare specific terrorism TAs to support operational planning and risk decisions for unique mission requirements or special events, including in-transit forces, training and exercises, operational deployments, and large public gatherings (conferences, foreign police academy graduations, Independence Day celebrations).
- Integrate terrorism TAs into the CRM process and be a major source of analysis and justification for recommendations to raise or lower FPCON levels; implement RAM AT enhancements, including physical security program changes and program and budget requests; and conduct terrorism VAs.
- Ensure that terrorism TAs are a part of the intelligence preparation of the battlefield, MDMP, and the leader's reconnaissance in conjunction with deployments. Follow-on terrorism TAs are conducted for deployments as determined by the commander or directed by higher headquarters.

3-31. Threat analysis is the process of compiling and examining information to develop intelligence indicators of possible terrorist activities. DOD has identified factors in the collection and analysis of information from sources concerning terrorist threats. To assist in focusing the threat analysis, intelligence and CI officers develop essential elements of information to help identify likely targets by using the following considerations—

- Organization, size, and composition of groups operating in the AOR.
- Motivation (religious, political, ecological).
- Long- and short-range goals.
- Religious, political, and ethnic affiliations.
- International and national support (moral, physical, financial).
- Recruiting methods, locations, and targets (students).
- Identity of group leaders, opportunists, and idealists.
- Group intelligence capabilities and connections with other terrorist groups.
- Sources of supply and support.
- Important dates (religious holidays).
- Planning ability.
- Internal discipline.
- Preferred tactics and operations.
- Willingness to kill.
- Willingness for self-sacrifice.

- Group skills (demonstrated or perceived) (sniping, demolition, masquerade, industrial sabotage, airplane or boat operations, tunneling, underwater, or electronic surveillance, poisons or contaminants).
- Equipment and weapons (on hand and required).
- Transportation (on hand and required).
- Medical support availability.
- Means and methods of C2.
- Means and methods of communicating to the public.

Intelligence Support to Antiterrorism

3-32. Intelligence plays a crucial role in supporting AT efforts by assisting commanders and staffs in distinguishing preincident indicators to prevent attacks against U.S. and multinational forces. Intelligence facilitates a greater understanding of the operational environment, with emphasis on the populace, criminal activity, HN, and active terrorist organizations. Actionable intelligence provides a foundation that an AT program can build upon to assess and clearly identify the threat and develop measures to defend against and mitigate its risk to Army assets. Intelligence synchronization and fusion assist the commander, staff, and AT officer to better assess the terrorist threat, determine the appropriate protection conditions, mitigate the risk of terrorist actions, prepare combat patrols, and determine RAM. (See FM 2-0, FM 2-19.4, FM 2-22.2, FM 2-91.4, and FM 2-91.6.)

3-33. Future intelligence collection and analysis must provide improved indications and warnings of attack and increased specificity at the tactical level. Because the terrorist has the ability to choose where, when, and how he will attack, his actions will always be difficult to predict. He has the advantage of time—time to select his target and the choice of the exact time of attack. Terrorists will be prepared to sacrifice their lives to achieve their goals. Human intelligence and CI assume greater importance to the effort than technical sensors, although they will remain complementary disciplines and may not succeed in isolation from each other. The precise warning of terrorist attacks depends on intelligence to identify specific targets and the time and nature of the attack.

3-34. Terrorists also rely on an effective intelligence capability to carry out their attacks and have shown great patience in obtaining information before attacks. Continuous fixed, mobile, or progressive surveillance techniques of a specific target can go on for months so that the target's daily routine and those areas that affect his daily life are completely understood. During these surveillance and planning phases, terrorists are most vulnerable to being caught or deterred from executing an attack.

3-35. Commanders (through their AT officers, staffs, and working groups) develop a system to monitor, report, collect, analyze, and disseminate terrorist threat information. Intelligence supports the commander across full-spectrum operations and is one of the warfighting functions. The intelligence warfighting function not only includes assets within the military intelligence branch, but also includes the assets of branches that can collect information as a part of the intelligence, surveillance, and reconnaissance effort. Every Soldier, civilian, or contractor (as a part of a small unit, organization, or FOB) is a potential information collector and an essential component to help reach situational understanding (every Soldier is a sensor).

3-36. Each person develops a special level of awareness simply due to exposure to events occurring in the commander's AOR and has the opportunity to collect information by observation and interaction with the population. This is especially true in AT efforts, in which the enemy is not as clearly defined and displayed as in previous operational assessments. This assessment and awareness result in a bottom-up flow of information, often straining the capabilities of smaller units and activities, therefore relying on solid analysis, synchronization, and fusion by their higher headquarters to provide direction in implementing FPCON measures and RAM responses. CI should be thoroughly integrated into the commander's operational planning and preparation. The CI mission makes it an ever-present AT enabler through the routine execution of its functions. However, CI can tailor its functions to provide support to AT and protection-specific operations, including—

- Screening locally employed persons working on outside the continental United States (OCONUS) military bases.
- Tailoring security education and awareness briefings and programs.
- Conducting travel and foreign contact briefings and debriefing programs.
- Supporting TAs and VAs.
- Providing foreign intelligence and security service and international terrorist organizations threat analysis and products.
- Conducting CI investigations and collection that impact AT and protection.

3-37. Intelligence support to AT provides protection to the operational Army fighting capability so that it can be applied at the appropriate time and place. This includes the measures that the force takes to remain viable and functional by protecting itself from the effects of or recover from terrorist activities. To do this, intelligence disciplines monitor and report the activities, intentions, and capabilities of adversarial groups and determine their possible COAs. Detecting the adversary's methods in today's operational environments requires a higher level of situational understanding, informed by current and precise intelligence. The asymmetrical threat from terrorist activities drives the need for predictive intelligence based on the analysis of focused information from intelligence, law enforcement, and security activities that are fused to provide commanders and leaders with the knowledge to make the right decisions in protecting the force.

REDUCE VULNERABILITIES TO TERRORIST ACTS AND ATTACKS

3-38. Reduce personnel vulnerability to terrorism by understanding the nature of terrorism, knowing current threats, identifying vulnerabilities to terrorist acts, and implementing protective measures against terrorist acts and attacks.

Antiterrorism Task 3. Assess and Reduce Critical Vulnerabilities

3-39. Commanders continuously assess AT capabilities. These assessments review the overall program; individual, physical, and procedural security measures; and unit predeployment preparation. Commanders and the AT officer analyze the TA and implement physical protection measures according to the terrorists' known or potential capabilities.

Criticality Assessment

3-40. The criticality assessment evaluates and prioritizes assets and functions to identify which assets and missions are relatively more important and to protect them from attack. A *critical asset* is a facility, equipment, service, or resource considered essential to DOD operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation; protection from disruption, degradation, or destruction; and timely restoration. For AT purposes, the criticality assessment should also include high-population facilities (recreational activities, theaters, or sports venues), which may not necessarily be mission-essential. Units conducting tactical operations should focus not only on assets that are most critical to the operation, but also on identifying the most critical aspect of the mission.

3-41. Mission planning and the commander's priorities and intent determine critical assets. Critical assets can be people, property, equipment, activities, operations, information, facilities, or materials. For example, important communications facilities, utilities, and criticality assessments provide information to prioritize resources while reducing the potential application of resources on lower-priority assets. Major weapons systems might be identified as critical to the execution of U.S. military war plans and, therefore, receive additional protection.

3-42. The criticality assessment identifies assets supporting Army missions, units, or activities deemed critical by military commanders or civilian agency managers. Leaders will conduct a criticality assessment to identify, classify, and prioritize mission-essential assets, facilities, resources, and personnel. Additionally, commanders will conduct a criticality assessment to identify, classify, and prioritize assets (high-population facilities, mass-gathering activities [recreational activities, theaters, sports venues] and other facilities, equipment, services, or resources deemed sufficiently important by the commander to warrant protective measures) to ensure continued efficient operation; protection from disruption, degradation, or destruction; and timely restoration. It addresses the impact of temporary or permanent loss of assets and examines costs of recovery and reconstitution, including time, expenditure, capability, and infrastructure support.

3-43. The staff at each command echelon determines and prioritizes critical assets. The staff gauges how quickly a lost capability can be replaced before giving an accurate status to the commander. The commander who is responsible for AT approves the prioritized list. The goals of a criticality assessment are to—

- Identify the operating base or unit key assets and capabilities.
- Determine whether critical functions or combat power can be duplicated with other elements of the command or an external resource under various attack scenarios.
- Determine the time required to reconstitute key assets, infrastructure, and capabilities in the event of temporary or permanent loss.
- Determine the priority response to personnel, key assets, functions, infrastructure, and information in the event of fire, multiple bombings, or other terrorist acts.

3-44. It may also be useful to link identified threat attack means to a specific time or location. For example, a terrorist group operating in proximity to an installation may typically target certain or specific areas (headquarters facilities, unit staging areas that contain a large number of people at certain times). Criticality will be assessed using the following criteria:

- Importance.
- Effect.
- Recoverability.
- Mission functionality.
- Substitutability.
- Repair.

3-45. Initial protection planning requires various assessments to support protection prioritization—TA, VA, and criticality assessment. These assessments are used in planning to determine and differentiate those assets to protect, given no constraints (critical assets), from assets that U.S. forces can protect with available resources (defended assets). Commanders make decisions on acceptable risk and provide guidance to the staff to employ protection capabilities based on the critical-asset list and the defended-asset list. Forms of protection are used and employed during preparation and continue through execution to reduce friendly vulnerability.

3-46. Criticality decision support tools (mission, symbolism, history, accessibility, recognizability, population, and proximity [MSHARPP] and criticality, accessibility, recuperability, vulnerability, effect, and recognizability [CARVER]) may support protection planning by assisting the commander in implementing AT measures while conducting full spectrum operations. Staffs, ATWG, or selected individuals may find MSHARPP and CARVER assessment tools helpful. MSHARPP assesses potential

targets from the inside out, and CARVER assesses targets from the outside in. Appendix B discusses MSHARPP and CARVER in detail.

Vulnerability Assessment

3-47. A VA is a command or unit level evaluation to determine the potential weaknesses for personnel, an installation, a unit, an exercise, a residence, a facility, a network, an infrastructure, information, or another friendly capability to a particular terrorist threat. It identifies areas of improvement to prevent, defend against, mitigate, or deter threats. The analysis addresses the questions of who or what is vulnerable and how. This assessment determines the susceptibility of the commander's assets to various attack scenarios identified during the TA. Multidisciplinary experts in such areas as terrorist tactics, structural engineering, physical security, and installation preparedness conduct these assessments.

3-48. The VA identifies physical characteristics or procedures that render critical assets, areas, or special events vulnerable to known or potential threats. Assessment teams should use their imagination to determine the number of possible ways that the target is vulnerable and not become fixed on one scenario or a specific set of assessment tools. The assessment provides a basis for developing controls to eliminate or mitigate vulnerabilities. Vulnerability is the component of risk over which the commander has the most control and greatest influence. Examples of VA are—

- Predeployment site survey.
- In-transit movement VA.
- Special event VA.
- Off-base asset VA.
- War-gaming results during MDMP.
- Personal-security VA performed by the criminal investigation division.

3-49. The AT officer and the protection cell or ATWG members serve as the assessment team in a collaborative effort. Teams should include representation from various specialties (operations, security, intelligence, CI, law enforcement, communications, safety, fire, engineers, medical services, CBRN planning and response).

3-50. A proper VA enables the commander to plan appropriate countermeasures to reduce the vulnerability and associated risk. The commander can change the mission profile or apply additional assets to reduce vulnerability. Tactical commanders seek to reduce their susceptibility to tactical surprise when looking at their unit's vulnerability. Tactics of terrorist organizations seek to use the element of surprise to obtain a greater advantage over forces more powerful than they are. A commander's ability to thwart potential terrorist actions will be greatly enhanced through COA development, red teaming, and identifying a force's susceptibility to surprise. When assessing vulnerability to terrorism during full-spectrum operations, staffs assist the commander by providing answers to the following questions:

- Who or what is vulnerable?
- How or why is the unit vulnerable? To what is it vulnerable?
- What is the threat or hazard? What specific capability of the threat or hazard causes the greatest risk?
- When or where is the unit vulnerable? Is the unit vulnerable based on equipment, terrain, or events?
- What is known about the mission?
- Can the enemy predict the mission, specific route, or time of day for execution? Can the enemy expose gaps in the current security posture?
- How much information could have been collected? Are movement routes anticipated?

3-51. Commanders and staffs assess the vulnerability of an asset based on its accessibility and recognizability. Staffs assess whether an asset is accessible and when a potential terrorist can reach the target with sufficient personnel and equipment to accomplish his mission. This analysis entails identifying and studying critical paths that the terrorist must take to achieve an objective and the unit's means to impede terrorist tactics. A target's recognizability is the degree to which it can be recognized by an

operational element and/or intelligence collection and reconnaissance asset under varying conditions. Weather can influence a target's recognizability, as can its size, complexity, and camouflaging. Through detailed surveillance, threats can distinguish a unit's or person's level of importance and choose to strike at those perceived to be most critical to their goals and objectives.

3-52. The end state of the VA is the identification of physical characteristics or procedures that render critical assets, areas, or special events vulnerable to a range of known or feasible terrorist capabilities. Determination of vulnerability is partly a function of the commander's desired level of protection for the asset, area, or special event. Although performing an effective VA requires detailed analysis, the results quantifying and rating the effectiveness of protective measures are invaluable and provide a major tool for developing AT protective measures. The VA methodology should follow this sequence:

- List assets and capabilities.
- List the threats against those assets.
- Determine common criteria for assessing vulnerabilities.
- Train the assessment team in assessment methodology and intent.
- Conducts assessment (assessment team).
- Consolidate and evaluate the assets and capabilities and their vulnerability.

Antiterrorism Task 5. Maintain Defenses

3-53. Commanders use AT-specific security procedural and physical measures to protect personnel, information, and materiel from terrorist threats. Within the AT appendix, commanders outline specific threat mitigation measures as part of developing controls during the CRM process (see chapter 5) to establish a baseline defensive posture through the use of physical security and FPCON measures, including the application and planning of RAM. Individual Soldier awareness and training are key elements in successfully detecting and thwarting terrorist acts.

Force Protection Conditions

3-54. The DOD FPCON system is a progressive level of protective security measures implemented in response to terrorist threats. This system is the principal means for a commander to apply an operational decision on how to protect against terrorism, and it facilitates inter-Service coordination and support for AT activities. The unit AT appendix should contain detailed instructions on implementing security measures across FPCON levels. Each set of FPCON measures is the minimum that must be implemented when a particular baseline FPCON level is designated.

Note. The geographic combatant commands have tactical control (for force protection) authority and responsibility for DOD elements and personnel within their respective AOR. The geographic combatant command is responsible for establishing the baseline FPCON for the AOR and procedures to ensure that FPCON measures are uniformly disseminated and implemented.

3-55. Although not completely applicable in a combat zone, these measures can be used as a template in developing protection guidance. Well-designed AT measures facilitate the AT principles of assess, detect, defend, and warn. FPCON measures include provisions for reinforcing physical security; increasing security personnel and inspections of vehicles, hand-carried items, and packages; RAM; and other emergency measures. FPCON measures are designed to be scalable and proportional to changes in the local threat. The FPCON levels are normal, alpha, bravo, charlie, and delta. Further explanations of the FPCON levels can be found in AR 525-13 and FM 3-37.

Note. An AT appendix, with a complete listing of site-specific AT security measures linked to a FPCON, will be classified *CONFIDENTIAL* at a minimum. When separated from the AT appendix (and other classified sections), site-specific AT security measures and FPCONs can be handled as *FOR OFFICIAL USE ONLY* to allow widest possible dissemination.

Random Antiterrorism Measures

3-56. A key component of an active AT appendix is RAM, which provides the commander with a flexible means to increase security and minimize or prevent the establishment of predictable patterns of security. While specified measures must be tailored for each location and each FPCON, each commander has the flexibility to introduce physical security measures from higher FPCON levels and self-generated measures to enhance unit security. By implementing additional physical security measures or measures from higher FPCON, RAM conveys an image of increased vigilance and awareness to observers who are external to the military site. RAM, if properly implemented, presents to terrorist groups an ambiguous and confusing assessment of the military site security posture.

3-57. The unit AT appendix should contain detailed instructions on the implementation of RAM, which should be visible (to confuse surveillance attempts), be based on an irregular schedule, and involve tenant units and commands on a base, not just the security forces. RAM should also be conducted at all levels and include measures developed by the command or locally established to shape security to the location and situation. The impact of RAM on terrorists is difficult to measure, but such programs introduce uncertainty and unpredictability to planners and organizers of terrorist attacks. Examples of RAM are:

- Moving Jersey barriers, vehicular barriers, Class IV objects, and materials to route traffic near and within the ECP.
- Changing ECP security force shifts at random.
- Changing the access time for ECPs.
- Changing access procedures at random.
- Changing vehicle and personnel inspection procedures randomly.
- Observing surrounding areas with remote sensors at random times.
- Changing the patterns and schedules of patrols in and around bases and protected locations.

High-Risk Personnel

3-58. As part of an expeditionary Army, maneuver commanders serve as extended symbols of U.S. military power, making them attractive and accessible terrorist targets while operating abroad. Under DOD and Army guidelines, some personnel are assessed to be at a greater risk than the general population by virtue of their rank, assignment, symbolic value, vulnerabilities, or location or be a specific threat that requires additional security to reduce or eliminate risks. These personnel may be formally designated HRP or high-risk billet.

3-59. The commander of a geographical area is responsible for the safety and security of dignitaries and HRP traveling through his area. Corps and division commanders conducting full spectrum operations, through combatant command authorization, may be designated HRP or high-risk billet, based on a threat in the area. Brigade and battalion commanders normally do not require the same level of protection as an HRP or high-risk bullet but may warrant a security detail taken from within the command or, at a minimum, a squad to enhance movement within the AO.

3-60. Principles of risk management should be employed in designating and HRPs and high-risk billets, approving protective support, and determining the number and type of assigned protective services detail personnel, whose support is maintained at the minimal level required and employed only as necessary and appropriate based on the threat. Status-of-forces agreements and memoranda of understanding between the U.S. government and a foreign government may limit the use of supplemental security measures. These constraints should be carefully considered when conducting security surveys, developing plans, and implementing additional security measures to protect executives. Commanders can find specific information on protective services detail structure and utilization by reading AR 525-13, Department of Defense Instruction [DODI] O-2000.22, FM 3-19.12, and U.S. Army Forces Command [FORSCOM] Regulation 190-58). Technical assistance is also available from the supporting criminal investigation division unit.

Physical Security

3-61. *Physical security* is concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft (JP 6-0). In support of AT, physical security measures identify physical vulnerabilities to terrorist attacks on bases, personnel, and materiel and take actions to reduce or eliminate those vulnerabilities. Survivability operations and general engineering support may be required to emplace compensatory measures for identified vulnerabilities. The physical security system builds on the premise that baseline security and the preparedness posture are based on the local threat, site-specific vulnerabilities, identified critical assets, and available resources. The Army's Physical Security Program supports AT through the coordinated efforts of policies, plans, and procedures specifically designed to achieve a strong physical security posture.

3-62. Less permanent bases (intermediate staging bases, lodgments, FOBs) benefit from physical security efforts through the application of active and passive security measures. The protection of these locations is enhanced by integrating existing security capabilities with physical barriers, facility hardening, and active delay and denial systems. As the base expands and improves to establish a more permanent presence, commanders can increase and adjust the physical security measures to meet the scale and complexity of the base. Commanders reduce the effects of threats by implementing physical security programs that form the basis of integrated defense plans, which build physical security into contingency, mobilization, AT, and wartime plans. The program goal is to safeguard personnel and protect property by preventing, detecting, and confronting unauthorized acts. (See ATTP 3-39.32.)

3-63. The physical security officer provides assistance to the AT officer and commander in the defensive planning, implementation, and control of AT operations. This officer provides expert advice and assistance in developing crime prevention and physical security plans and programs. These programs help identify, reduce, eliminate, or mitigate conditions favorable to criminal, terrorist, and insurgent activities. Commanders rely on the physical security officer to comprehensively evaluate units, facilities, and installations and to determine preparedness to deter, defend against, and recover from the full range of adversarial capabilities based on the TA, compliance with protection standards, and risk management. Physical security systems installed in and around installations, facilities, and units form the physical backbone of AT efforts. The facilities, equipment, and personnel that form the installation security force are critical resources that help defend against terrorist attacks.

Entry Control

3-64. Entry control ensures the proper level of access for Army personnel, visitors, contract personnel, and vehicle traffic. The objective of an ECP is to secure the base from unauthorized access and to intercept contraband (weapons, explosives, drugs, classified material) while maximizing vehicular traffic flow. The full containment and control of vehicles is required for ECP. The design of an ECP should ensure that vehicles are contained through an arrangement of passive and active vehicle barrier systems. The primary objective of the design is to prevent an unauthorized vehicle or pedestrian from entering the base (see ATTP 3-39.32). Entry control also serves as a means of shutting down the ability of personnel to exit as a means to contain and capture criminal or terrorist perpetrators.

3-65. ECPs have historically been primary attack points for vehicle bombs. These attacks have also been coupled with deliberate assaults to gain access for the assault force into the deployed operating base (DOB). Attacks may also include suicide bombers wearing IED vests. Entry control procedures are designed to identify and screen personnel, vehicles, and materials to ensure that only authorized personnel gain entry to the DOB. These procedures can also help detect contraband and mitigate the potential for sabotage, theft, trespass, terrorism, espionage, or other criminal activity. Entry control procedures are intended to accomplish the following objectives as part of the defense in depth for a DOB:

- Permit personnel, vehicles, and delivered materials to move through the DOB without unduly interfering with day-to-day operations. Some interference will be necessary, depending on the security requirements.
- Help maintain adequate security throughout the DOB, and protect critical assets.

- Contain and resolve actual and potential attacks, and apprehend perpetrators.
- Delay attackers in reaching critical assets, and inhibit egress from the DOB so that security personnel can sound alarms and take immediate protective actions.

Information Protection

3-66. *Information protection* is active or passive measures that protect and defend friendly information and information systems to ensure timely, accurate, and relevant friendly information. It denies enemies, adversaries, and others the opportunity to exploit friendly information and information systems for their own purposes (FM 3-0). External and internal information perimeter protection prevents unknown or unauthorized users or data from entering a network. External efforts include communications security, router filtering, access control lists, and security guards (see FM 3-37).

3-67. Critical information is information that is vital to a mission: if an adversary obtains, correctly analyzes, and acts upon critical information, the compromise could prevent or seriously degrade mission success. Critical information can be classified or unclassified. Classified critical information requires OPSEC measures for additional protection because it can be revealed by unclassified indicators. The use of essential elements of friendly information protects critical information because it does not reveal sensitive or classified details. Instead of stating the details of critical information, the essential elements of friendly information are critical information converted into a question. The use of essential elements of friendly information is an effective way to ensure the widest dissemination of a units or organization's critical information while protecting classified and sensitive information.

3-68. CI support to OPSEC entails identifying adversary intelligence, TTP, collection methods, analysis, and exploitation capabilities that target essential elements of friendly information, and developing countermeasures. CI investigations, CI source operations, debriefing of Army personnel, and screenings of local nationals and contract linguists can determine what essential elements of friendly information are being targeted by foreign intelligence and what adversary collection methods and capabilities are being used to collect essential elements of friendly information. Additionally, cyber CI elements can perform Internet open-source collection and DOD network and systems analysis to determine OPSEC vulnerabilities and provide support to the Army network TAs and VAs. The commander, Intelligence and Security Command, provides data on the foreign intelligence threat, terrorist threat, and CI support to OPSEC programs for Army units, Army Service component commands (ASCCs), direct reporting units, and above.

3-69. Units use the critical information list to create a consolidated list of the unit or organization's critical information. The list will be classified if one of the items of critical information is classified. At a minimum, the critical information list will be sensitive information and must be protected. A method to ensure the widest dissemination of a unit is or organization's critical information, while protecting it, is to convert it to essential elements of friendly information.

3-70. OPSEC applies to operations across the spectrum of conflict. Units conduct OPSEC to preserve essential secrecy. OPSEC is the process of identifying essential elements of friendly information and subsequently analyzing friendly actions attendant to military operations and other activities to—

- Identify those actions that can be observed by adversary intelligence systems.
- Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
- Select and execute measures that eliminate or reduce, to an acceptable level, the vulnerabilities of friendly actions to adversary exploitation (see FM 3-13).

3-71. OPSEC denies terrorists information about potential targets. Terrorists select targets that offer the most opportunity for success. Information passed unknowingly by military personnel 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 base plans, billeting assignments, and very important person guest lists.

- Ensure that classified or sensitive information is discussed only on cryptographically secured telephone or radio circuits approved by the National Security Agency; for example, automatic secure voice communications systems.
- Protect personal or family information from strangers.
- Coordinate physical security measures to protect personnel and prevent unauthorized access to facilities, materiel, and documents.

3-72. The technology also serves as a potential information source for the enemy and terrorists. Soldiers deployed on military operations have included information about living situations, weaknesses in protection, and ongoing and future operations in e-mails, blogs, and photographs and on social sites for those with Internet access. Attacks from terrorists are not limited to - weapons and bombs, but can also be linked to Internet hacking. Commanders should ensure that Soldiers and units understand the potential harm that comes from releasing too much specific information about current operations across unsecure means. The patience that terrorists exhibit during their planning cycle displays their seriousness in gathering weeks, if not months, of unsecured Internet chatter that can be used later to attack friendly forces operating outside and inside the wire.

Israeli Forces Cancel Offensive Operations

In March 2010, information pertaining to an upcoming raid was posted by an Israeli Defense Force member on a social networking site just a day before the offensive operations into Palestinian territory. Soldiers assigned to the unit saw the information and reported it to their superiors. Details posted about the operation included unit information, the exact time of the operation, and the location. Commanders felt that the information could jeopardize mission success and place Israeli Defense Force personnel in danger.

REACT TO TERRORIST INCIDENT

3-73. Implement measures to treat casualties, minimize property damage, restore operations, and expedite the criminal investigation and collection of lessons learned from a terrorist incident. (See FM 19-10.) Commanders ultimately negate the ability of terrorist actions to have a strategic effect on current operations by how well they respond to a terrorist act, preserve combat power and HN infrastructure, and continue to progress toward mission success without drastic impacts on unit capabilities.

Antiterrorism Task 7. Conduct Terrorist Threat/Incident Response Planning

3-74. Commanders develop terrorist threat/incident response plans that prescribe appropriate actions for reporting terrorist threat information, responding to threats or actual attacks, and reporting terrorist incidents. Units that are charged with the security and defense of a FOB use the AT officer and ATWG to develop procedures for an attack warning system that becomes integrated into base procedures. Commanders outline base responsibilities and enhance defensive measures by exercising the attack warning system and conducting drills on emergency evacuations, movements to safe havens, and shelters in place. Finally commanders and their AT officers coordinate with friendly units, the HN, the supporting contracting organization, and selected contract service company managers (first responders, the company providing firefighter services to the base) to plan for terrorism consequence management, CBRN and public health emergency preparedness, and emergency response measures to respond to a terrorist attack. These measures focus on mitigating vulnerabilities of personnel (including DOD civilians), facilities, and material to terrorist use of CBRN weapons.

3-75. *Incident management* is a comprehensive approach to preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies. Incident management includes measures and activities performed at the local, state, and national levels and includes crisis and consequence management activities (JP 3-28). Incident management also acts as a deterrent to terrorist

attacks by mitigating potential effects of an attack. Plans for incident management preparedness and incident response measures and plans for continuing essential military operations are important to an effective AT program.

Incident Management

3-76. Incident response measures to a terrorist attack include procedures to provide C2, communication, and intelligence to the first responders charged with the task of determining the full nature and scope of the incident, containing damage, and countering the terrorists who may still be present. The term *first responders* refers to military, HN, or contracted personnel, including police, fire, and emergency personnel. The objective of terrorist incident response measures is to limit the effects and the number of casualties resulting from a terrorist attack. Incident management includes crisis and consequence management activities. The definitions of crisis and consequence management are—

- **Consequence management.** *Consequence management* is actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters or catastrophes, including natural, man-made, or terrorist incidents (JP 3-28).
- **Crisis management.** *Crisis management* is measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or an act of terrorism. This is predominantly a law enforcement response, normally executed under federal law (JP 3-28).

Note. Consequence management, particularly in response to a CBRN attack, is laid out in great detail in FM 3-11.21.

3-77. The Army continues to support efforts to provide consequence management capabilities worldwide through domestic consequence management, DOD-led consequence management and, in support of allies, foreign consequence management. The primary objective of AT incident response management is to mitigate the number and severity of casualties resulting from a terrorist attack. Well-developed response measures can save lives, preserve health and safety, protect property, and secure and eliminate the hazard. A slow or uncoordinated response may result in further damage to the base or critical facility, resulting in the terrorist identification of unit vulnerability.

Note. The National Incident Management System is a comprehensive and consistent national approach to incident management that applies at jurisdictional levels and across functional disciplines that enable government, private-sector, and nongovernment organizations to work together during domestic incidents. Commanders adopt this method to assist in potential civil support operations in defense of the homeland and meet the requirements outlined in Homeland Security Presidential Directive 5.

Incident Management Plan

3-78. A commander's responsibility and authority to enforce security measures and to protect persons and property are important during conflict. The focus of incident management is on the organic assets of a unit or base and the ability to cope with the situation using organic assets until outside assistance arrives. The terrorist incident response measures should include procedures for determining the nature and scope of incident response; procedures for coordinating security, fire, and medical first responders; and steps to reconstitute the base's ability to perform mission-essential functions. To be effective, incident response measures must be fully coordinated, exercised, and evaluated. Attacks employing CBRNE weapons may produce mass casualties or widespread destruction, which can quickly overwhelm organic resources. Command considerations for incident management include—

- Knowing the response route.
- Approaching uphill and upwind if possible.
- Avoiding choke points.
- Designating rally points.

- Identifying safe staging locations for incoming units.
- Ensuring the use of personal protective equipment and personnel accountability.
- Continually assessing security.
- Evaluating the need for specialized units (explosive ordnance disposal).
- Treating every incident as a crime scene by creating a buffer zone around the site, recording movements in and out of the site, and treating everything at the site as evidence.
- Knowing the mass-casualty and first-responder requirements.

3-79. The AT appendix should prepare for the most probable or likely threats as identified through the TA and maximize the use of existing plans and SOPs that can be referenced in the AT appendix. Establishing a mechanism to respond to a terrorist incident is an essential element of AT. Within the boards, bureaus, centers, cells, and working groups Army construct, the ATWG—comprising the AT officer, key unit staff (S-2, operations and training officer [S-3], civil affairs officer [S-5]), selected contracted first responders, supporting contracting office personnel, and personnel who make up the base defense operations center (BDOC)—acts as the principal planning agency. One effective method for determining which areas should plan and execute the response is to use the weapon of mass destruction response functions as a foundation for terrorist attack planning.

3-80. Response members should be predesignated, train together, and be prepared to perform individual and collective crisis management missions under the control of the incident commander or the designated representative. Tenant commanders may also serve or have staff representation in this organization. The most common participants in the crisis management organization are as follows:

- **Medical team.** This team is capable of triage, patient decontamination, and backup responder decontamination as necessary.
- **Firefighters.** The senior firefighter normally becomes the on-scene commander upon arriving at the incident. This team establishes staging areas and can call backup forces for hazmat conditions or assistance in controlling a fire.
- **Law enforcement.** This team is responsible for securing the crime scene, providing responder security, and controlling ingress and egress at the incident site.
- **Search and rescue teams.** These teams usually work in pairs and are responsible for casualty extraction. If available, a structural engineer on the team can conduct safety and damage assessment.
- **Explosive ordnance disposal.** The explosive ordnance disposal team is responsible for detecting, identifying, and rendering-safe suspected munitions and looking for secondary devices.

Tenant Unit Responsibility

3-81. Tenant unit commanders must actively participate in the preparation of base security and defense plans even if they do not fall under the direct command of the base commander. Tenant units provide security for their own forces and high-value assets, provide individuals to perform perimeter and gate security, and are often assigned battle positions according to base security plans. These forces, when provided, will be under the tactical control of the base commander for the purpose of base defense. Key concerns of tenant involvement, because of lessons learned from operations in Iraq and Afghanistan) are training, rehearsals, coordination, and competing requirements between the security mission and other operational tasks.

Initial Response

3-82. Response is a short-lived, confused, creative, fast-paced flow of events after an attack or a life-threatening, damage-causing event. It is paramount that immediate action be taken to save lives, prevent suffering, and protect friendly forces, facilities, equipment, and supplies from further harm. This response requires that critical actions take place immediately after an incident to minimize the impact on friendly force operations and expedite the recovery of the operating base to full operational capability. A typical base response team should be task-organized to respond to incidents, regardless of threat, tactic, or event.

This requires establishing an on-scene commander who coordinates activities at an incident site through an incident command system (a systemic procedure whereby operating base staffs are organized to respond to an incident). The operating base should have the capability to perform the following standard actions:

- Establish C2 at the incident site, and secure the area.
- Perform a tactical appraisal of the situation.
- Prepare a damage and casualty assessment.
- Take immediate actions to save lives, prevent suffering, and reduce or mitigate great property damage.
- Determine a priority of response effort and subsequent order for follow-on response forces, equipment, and supplies.
- Establish staging locations where forces and equipment can be located to support an incident.
- Establish mass-casualty care and evacuation centers.

3-83. A terrorist incident begins with the detection of an unlawful act of violence or the threat of violence. Detection may result from routine surveillance performed by unit patrols, base defense guard or security force, or through a facility intrusion detection system. Once a terrorist act is detected, first responding security forces must perform an initial assessment. The initial response force is identified in the unit or base AT appendix with on-scene command relationships and a clearly established chain of command. When responding to requests for support from the HN, the initial response force acts in a supporting role. However, the commander does not relinquish command responsibility and authority.

3-84. First and follow-on responders must use caution when entering the attack site. Terrorist and criminal tactics have revealed the planning and detonation of secondary devices or direct fire engagements primarily focused on killing first and follow-on responders. One of the first tasks should be to establish security of the incident location to protect the initial responders and to control access and preserve evidence. Responders should use the same skills that they would use to target the location of primary IEDs, devices, or snipers. Be aware of commonly used concealment items and the number of abandoned vehicles, carts, or trailers in the area of the attack. Response forces may be under constant observation so responders must maintain a heightened level of security when exposed.

3-85. Once the initial response force has responded to the incident and determined the circumstances, the base commander should activate required forces and begin notification procedures for military, contractor, and HN authorities. The initial response force should immediately identify and report the nature of the situation, isolate the incident, and contain the situation until relieved by the reaction force commander. Initial response force actions are critical, and units must have trained personnel who are aware of the threat and are capable of reacting promptly, 24 hours a day.

3-86. Responses will vary according to the incident. For example, if terrorists escape before additional forces arrive, the initial response force should provide medical aid, seal off the crime scene, and secure other potential targets in case the initial attack was a diversionary tactic. If the event is a hostage or barricade situation, the initial response force should seal off and isolate the incident scene to ensure that no one enters or leaves the area. The initial response force must also be prepared to locate witnesses, direct them to a safe location for debriefing, and interface with local law enforcement or emergency service personnel, HN police, and military forces responding to the incident according to the existing status of forces agreement.

Note. CBRNE incidents or threats of terrorist CBRNE attacks may overwhelm a unit or operating base's minimum capability to adequately detect, assess, and mitigate the effects. Commanders and AT officers must adequately coordinate and prepare for such an incident. (See FM 3-11.21.)

Base Defense Operations Center

3-87. A BDOC is a C2 facility that is established by the base commander as the focal point for protection, security, and defense within the base boundary. Through the BDOC, the base commander plans, directs,

integrates, coordinates, and controls base security efforts and coordinates and integrates area security operations with the base cluster operations center (if established) or other designated higher-level staff. If units occupying the FOB are organic to the commanding headquarters, then a BDOC may not be necessary and base defense requirements would be managed through the unit's operations section. BDOCs become important when a headquarters is given command of a FOB but the units that occupy or are assigned to the base defense are not organic. BDOCs serve as a permanent part of base defense for as long as the FOB remains in the area or the requirement for an additional mission command element is proven from recent experiences.

3-88. The nature of a BDOC depends on the combination of forces involved and may include other U.S. Service or agencies multinational, a HN agencies' personnel, depending on the combination of forces located at each particular base. Such entities should be part of the BDOC when elements of their armed forces, police, or paramilitary forces are directly involved in the overall base defense effort or when they are a major tenant organization on the base. The center normally consists of the following primary sections:

- Command.
- Intelligence.
- Operations.
- Logistics.

Communications

3-89. Tenant units, program managers for contractors deploying with the force, or security forces will often be operating with incompatible communications equipment. The base commander and subordinate commanders who are responsible for planning and executing base defense operations must ensure that specific base, base cluster, and line-of-communication security measures are planned for and tested to ensure compatibility. An uninterrupted communications network with backups is essential for the BDOC to maintain situational awareness and take the appropriate actions. Everyone must be able to talk to the BDOC without causing chaos. A standard reporting procedure and infrastructure allow for timely and accurate reporting.

Forward Operating Base Marez Suicide Attack, Mosul, Iraq

A terrorist incident on 21 December 2004 in Iraq shows a FOB's initial response. A suicide bomber, wearing an explosive vest and the uniform of the Iraqi security force, entered a dining tent at FOB Marez and killed 14 Soldiers, 4 American contractors, and 4 Iraqis and wounded 72 others. Soldiers inside the tent turned their lunch tables upside down, placed the wounded on them and then carried them outside. The BDOC took immediate action; medics were onscene instantly and removed the rest of the wounded. Triage occurred, and those seriously wounded were medically evacuated to Ramstein Air Base in Germany for treatment at Landstuhl Regional Medical Center. The mass casualty response, planned by the FOB's medical officer and rehearsed before the incident, was well executed and, most likely, prevented more deaths from injuries.

The attack was attributed to a member of Ansar al-Sunna, a 24-year-old man from Mosul, who worked at the base for two months and had provided information about the base to the group. Security at U.S. bases is ordinarily extremely tight. Local Iraqi workers are typically searched before entering the base and are monitored on the base. The only Iraqi nationals usually allowed in dining mess halls are Iraqi soldiers. This suggests that base facilities have been infiltrated by adversaries who are collecting and providing information on base vulnerabilities. Further, this attack was carried out in daylight against the largest facility on the base, exactly when the largest number of Soldiers would be present. This combination of evidence indicates a good probability that the attack was well planned and professionally executed.

Additional Response Considerations

3-90. Although the primary goal is to end a terrorist incident without injury, another goal is to prosecute terrorists. Witness testimony, photographic evidence, and other evidence are important in achieving a successful prosecution. Maintaining the continuous chain-of-custody of evidence obtained during an incident requires documenting the location, control, and possession of the evidence from the time custody is established until the time evidence is presented in court. Failure to maintain the chain of custody or contamination of the scene can result in exclusion of the evidence. Consult law enforcement or staff judge advocates on proper procedures unless doing so would harm military operations. The types of evidence for which the chain of custody must be established include—

- Photographs taken during the incident.
- Physical evidence, including items used by the terrorists. The AT appendix must include planning for contaminated-evidence preservation and collection, storage, and chain of custody procedures.
- Tape recordings of conversations between terrorists and hostage negotiators.
- Demand notes or other messages recorded by written, audio, or video means prepared by the terrorists.
- Sample collection, including samples collected at the scene during initial and follow-on response.

3-91. Apprehended military personnel are handled according to the Uniform Code of Military Justice, DOD and Service regulations, and applicable installation SOPs. In foreign incidents, civilian detainees may be processed according to the status of forces agreement, diplomatic note, or other agreements with that particular country. Unless exigent circumstances dictate otherwise, the staff judge advocate should be consulted before releasing an individual to HN authorities. The United States does not normally render its own nationals to the custody of a third party, including an HN. When this does occur, it is only in very limited circumstances and under the direction of the executive office. In coordination with the staff judge advocate, an AAR should be prepared within seven working days after termination of the event.

3-92. Each Service and command has a reporting procedure that requires a timely report of the incident to higher military authorities. The crisis management plan should dictate required reports and timelines for notification. This should include staff journals and other documentation, including detailed information concerning the disposition of evidence and captured individuals. The staff judge advocate and law enforcement personnel should ensure that reports are submitted to higher headquarters in sufficient detail to meet prosecution requirements.

3-93. Information from the command concerning positive, negative, and neutral factors that contributed to the incident and its resolution should be analyzed to determine elements of base or unit plans that should be changed. Contracted or HN officials involved in the activity should also be engaged to determine their perspective. Once compiled, AARs or lessons learned should be shared with other units and defense components.

Activities in Incident Management

3-94. Employing IW tactics, the terrorist's greatest weapon is his ability to influence operations and public opinion through aggressive domination of the media information cycle. The rapid release of information as press releases, audio/video, or printed products tied to an event (spectacular IEDs, suicide bombing, civilian casualties, attacks on U.S. forces) seizes the information initiative. Information is always secondary to the timing. The burden to disprove the "facts" of a terrorist's information product rests with the target of the attack. In the deployed joint operations area, units face an adaptive and technologically savvy enemy who recognizes that the global information network is his most effective tool for attacking what he perceives to be the center of gravity—public opinion, domestic and international. These types of information warfare have aided in increasing the flow of money and aid from around the globe, influenced civilian opinion of U.S. forces in occupied areas, and had an effect on public opinion within the United States.

3-95. The release of timely information following a terrorist attack is critical to getting ahead of the media information cycle and terrorist attempts to influence public opinion. In a deployed environment, planning for such events requires a coordinated influence line of effort among planners, psychological operations elements, and public affairs officers. Public affairs offices can provide quick statements from a commander concerning a terrorist incident to seize the media initiative. Psychological operations can provide products, (flyers, radio and television spots, coordinated HN civilian key leader engagements) that highlight factual details surrounding a controversial incident or event to prevent distortion by the terrorists. Timing of post-event public affairs releases and psychological operations products is critical, as they are far less effective if not placed on the street within minutes or a few hours after an event.

3-96. Terrorist groups often disseminate crude (but effective) flyers very quickly after a terrorist attack, sometimes within minutes or hours if the products are prepared ahead of time. They flood the streets with these flyers to stir emotions among the populace. Following an incident in which local noncombatants are killed or wounded by multinational forces or terrorists, local media will often play and replay the images on television. A common terrorist tactic is to record an attack and then provide the video to the local news media afterwards. Frequently, civilian deaths are attributed to multinational or U.S. forces even when the terrorists were responsible for putting the civilians at risk or killing them. This endless-loop video technique is extremely effective in stirring strong emotions among people who otherwise would be indifferent. If multinational forces move too slowly and take too long to investigate and vet messages before engaging the media, the impressions of the event as portrayed by local media are already fixed in the minds of the target audience.

3-97. Army Public Affairs plays a leading role as the voice of the commander and has the mission to provide factual and timely information to the media without violating OPSEC. Psychological operations (as a core information operations element) are the primary means for the commander to communicate with the civilian populace in their own language. Public affairs, psychological operations, Soldier, and leader engagements should operate in concert with strategic communications guidance to achieve a proactive, integrated, counteradversary information message that is released to the broadest audience possible.

3-98. Public affairs, psychological operations, and information operation planners should have readily available contingency messages that are approved by the commander and well coordinated with operational staff elements (S-2, S-3, S-5, AT officer) in consequence management planning. The successful massing of information effects requires the commander to articulate his intent clearly for the integration of available elements of operations in the information domain. These messages need to be incorporated into consequence management exercises with scenario-driven battle drills to solidify their use and validity in reducing terrorist information activities. Public affairs officers actively involved in shaping consequence management message releases must ensure that they maintain an open dialogue with liaisons or points of contacts with units throughout the AO to acquire specific details about an event or incident when they are not in the immediate vicinity of an attack.

3-99. By analyzing audiences within the AO, public affairs is able to generate a plan to ensure that the message is broadcasted or distributed to the fullest capacity using the media means accessible to the civilian populace. Public affairs officers establish good working relationships with HN news media representatives in their AO to serve as critical contributors to the media management mission. Units should have a local contract media coordinator who provides understanding and insight into the local culture and media practices and provides translation and interpretation when needed. Deploying units should anticipate the need to interview and establish a contract with qualified local media personnel upon deployment. Having local media personnel onboard leads to successful engagement with HN media.

3-100. In the event of an attack, public affairs offices execute planned response statements with incorporated facts known at the time. The public affairs representatives should be located in the BDOC to keep abreast of incident activities. During the incident the public affairs officer should prepare media releases and conduct briefings at the media center, located away from the BDOC, , based on information that is received. The public affairs officer ensures that the information released is screened to maintain OPSEC. Media representatives should be given access to releasable information and to the scene as early as possible, with reasonable conditions and restrictions commensurate to the risk and gravity of the event. Media can assist in disseminating information about the incident to inform and mitigate additional harm. If in-person site visits are not possible, initiate action to push DOD imagery of the incident site to the media for immediate release.

3-101. Follow-on press releases, psychological operations products, and commander's interviews can be used as part of consequence management battle drills to emphasize the facts of the event and discredit terrorist disinformation. The incorporation of sterilized and approved photographic and video images and interviews with local and multinational force witnesses by public affairs and HN media sources aid in solidifying the multinational force statements while discrediting terrorist claims and denouncing or condemning their attack. By continually reducing terrorist claims and exploits through quick, consistent, and factual reporting, multinational forces effectively take the information offensive approach to the postattack phase and can be more effective at defeating terrorist support in the AO.

3-102. The advantages of having local or HN media cover noteworthy events and lead when publishing postattack messages are numerous. HN media can—

- Place an HN face on published works.
- Capture the ground truth in nearly real time.
- Counter antigovernment or anti-multi-national force information.
- Eliminate the language barrier when conducting interviews with other local nationals or witnesses to the event.
- Gain credibility and acceptance among the local population.

3-103. U.S. and multinational forces may never have enough initiative to overcome terrorists publishing information on what is a terrorist attack. Through informing, influencing, planning, and coordinating a consequence management response, the multinational force can inform the HN media about events that will likely impact and shape the information environment, influence cooperation of the civilian population, and reduce the terrorists' ability to successfully shape the local population's perceptions of an incident.

SUPPORT ANTITERRORISM TASKS

3-104. The deployed AT program is reinforced by AT tasks that support the execution of three tactical tasks discussed above (see figure 3-3, page 3-7). By establishing an AT program, increasing AT awareness, developing civil-military partnerships, and exercising AT plans and responses commanders enhance their units ability to defeat terrorist activities.

Antiterrorism Task 1. Establish an Antiterrorism Program

3-105. The AT program within a unit is a commander's program that is designed to protect personnel, infrastructure, and information. To accomplish these goals, commanders must plan, integrate, and apply all in-place programs (combating terrorism, physical security, security operations, and personnel protective services) and support this effort through the extensive use of available intelligence and CI services. Commanders communicate their intent on managing the terrorist threat to their subordinates, enhancing decentralized execution and adaptability to changing tactics at lower levels.

3-106. AT planning is conducted and documented in the form of an annex, to operation order or plan, or SOP for units (battalion or higher) while conducting training and operational deployments (50 or more personnel), training exercises (50 or more personnel), and special events (Iraqi police academy graduation, opening of a new HN government facility). Commanders and staffs coordinate their efforts with the appropriate HN authority and U.S. country teams. AT annexes should be flexible for use by a unit or base and can be adapted for any environment (in-transit, base, offense, or defense operations) and are coordinated through the appropriate geographic combatant command and U.S. embassy or consulate.

3-107. The purpose is to help the AT officer structure an AT appendix in a comprehensive and organized manner. The format is usually patterned after the standard five-paragraph military operations order (situation, mission, execution, sustainment, and C2) that can be issued as a standalone document or in support of a larger operations order. This format enables the synchronization of existing programs (physical security, AT, OPSEC, information security, HRP protection). AT considerations should be integrated into plans and separate annexes. Collaborative staff interaction is a crucial element in developing a realistic executable plan that provides amplified instructions as required. AT planning documentation should address—

- The application of AT measures.
- Terrorist threats and other threat activities.
- Measures to reduce vulnerabilities to terrorist acts and attacks.
- AT physical security measures.
- AT measures for critical asset security.
- ECP procedures.
- FPCON implementation measures, including site-specific AT measures.
- On-site security elements.
- Operations and information security.
- AT measures for HRP, when appropriate.
- Reaction to terrorist incidents.
- CBRNE plans and measures to deal with toxic industrial hazards.
- BDOC operations.
- Alert notification procedures.
- Incident response management procedures.
- AT construction and building considerations.
- AT measures for logistics and other contracting.
- AT measures for in-transit movements, when appropriate.

Antiterrorism Task 4. Increase Antiterrorism Awareness

3-108. *Situational awareness* is the immediate knowledge of the conditions of the operation, constrained geographically and in time (FM 3-0). Situational awareness emphasizes that Soldiers know what is happening around them. The knowledge and perceptions occur in the Soldier's mind; situational awareness is an ability to maintain a constant vigil over important information, understand the relationship among the various pieces of information monitored, and project this understanding into the near future to make critical decisions.

3-109. For this reason, AT awareness serves as a key component of a unit's ability to assess, detect, warn and defend against terrorist actions. To help combat complacency, commanders emphasize AT awareness by ensuring that personnel within their command are aware of the significance of the terrorist threat, reemphasize unit and personal protection measures, report suspicious activities, and review assessed vulnerabilities and RAM. By emphasizing and teaching Soldiers to recognize potential or actual threats early, they can take measures to avoid or counter threats before they occur.

3-110. AT awareness serves more as an attitude or mind-set than a hard skill. When an attack occurs, persons with a complacent or apathetic mind-set are taken completely by surprise, unable to respond due to freezing up from shock and denial as their minds try to assess the situation. The opposite is also true: Soldiers cannot be expected to operate in a state of heightened awareness for extended periods. The constant stream of adrenalin and stress leads to mental and physical fatigue and impairs the body's natural fight or flight response. AT awareness supports the Soldier's ability to remain at a balanced level of awareness. The knowledge, exposure, and experience a Soldier gets from training, information, lessons learned, exercises, and rehearsals causes the Soldier to function without added stress associated with maintaining this level of personal security posture indefinitely.

3-111. AT awareness influences a Soldier's ability to conduct surveillance detection and recognize information that could thwart a future attack or enhance other intelligence collection efforts. Paying close attention to simple details (time, environment, distance, and demeanor) can uncover a possible terrorist if that person is sloppy in his surveillance techniques. How much time a person spends in an area could give him away. The location or environment and the distance at which someone stays are also important. If someone is consistently spotted parked down the street at odd hours of the night, for instance, that might be reason to think the person is conducting surveillance. How a person acts, or his demeanor, can also give someone away. A frequently nervous individual could inadvertently show concern over getting caught. Demeanor can also account for indicators when dealing with suicide bombers (unseasonably warm clothing, odd bulges under clothing, mumbling, fidgeting, an obvious avoidance of security personnel).

3-112. To fill in the information gap and lessen the degree of uncertainty, terrorist information must flow from top to bottom and from bottom to top. Information collected by subordinate elements (patrols, ECPs, others in contact with locals) needs to be reported in a timely manner to the unit S-2. The information contained in patrol reports and debriefs can provide important details on the terrorist threat and will assist the staff and AT officer in developing a more detailed and realistic threat model for the commander. As discussed earlier in this manual, potential threat may involve terrorists, criminal organizations, or actors with unknown intentions. As part of an AT program, the staff works closely with psychological operations personnel to look at groups, cells, and individual elements. They collaborate and evaluate propaganda, graffiti, and gang symbols to determine likely propaganda or communications by threats operating in the area.

Antiterrorism Task 6. Establish Civil-Military Partnerships

3-113. Commanders will coordinate with defense attaches, regional service officers, and local civilian communities to establish relationships to formulate partnerships to combat and defend against terrorism. The formation of effective civil-military teams creates complementary capabilities that mitigate the inherent weaknesses of the U.S. Army and HN civilian agencies who are living and operating in the AO. Partnerships include the sharing of resources and information to enhance the safety of the Soldiers operating in the area and the local populace who become part of the commander's responsibility. The daily interaction between U.S. forces and the myriad of civilians and civil organizations in the supported

commander's AO can develop useful civil information, which can be fused or processed to increase situational awareness, situational understanding, or situational dominance.

3-114. Civil-military partnerships also exist to enhance a commander's capabilities in response to terrorist attacks. Assistance from HN assets can provide resources in the way of CBRNE response, security, construction, and mass casualty assistance to reduce the effects of terrorist attacks and assist in recovery efforts. Partnerships with local media help to broadcast the commander's message to the population, reducing the impact of terrorist misinformation. Military partnerships with HN media resources are crucial for disseminating psychological operations products that encourage postincident civilian cooperation and reporting to prevent or mitigate terrorist incidents.

Antiterrorism Task 8. Conduct Exercises and Evaluate/Assess the Plan

3-115. Exercises test and validate policies, plans, and operating procedures; test the effectiveness of response capabilities; and increase the confidence and skill levels of personnel. Because current and future deployments will consist of joint, multinational, and HN partners, it is important that agencies exercise together. These exercises enhance coordination among varying partners whether it is on a base or on patrol and help them work together. They also allow personnel to become familiar with other procedures and identify those areas needing further coordination. In the absence of actual operations, exercises are an important indicator of the preparedness of a unit or multinational force to deal with a variety of terrorist incidents.

3-116. Commanders institute exercise and training programs that develop, refine, and test the command's AT response procedures to terrorist threats or incidents and ensure that AT is an integral part of the unit's protection posture. Soldiers train to perform tasks while operating alone or in groups. Soldiers and leaders develop the ability to exercise mature judgment and initiative under stress. The Army requires agile and adaptive leaders who are able to handle the challenges of a terrorist threat that is present throughout the full spectrum of operations. Change and adaptation to an asymmetrical threat must be recognized, communicated, and implemented far more quickly than in the past. Solutions discovered in exercises or in real situations must be disseminated throughout the force and then adapted quickly and innovatively as the terrorists adapt to counter the newfound advantages.

3-117. Experiences from Iraq and Afghanistan demonstrated that Soldiers who are trained exclusively for offense and defense operations were not as capable of adapting to the requirements for stability operations or facing the challenges associated with dealing with an asymmetric threat. Commanders must find a balanced approach to the types of training essential to full spectrum operations, understanding that the terrorist threat is present throughout the spectrum of conflict. Incorporating AT training and awareness prepares Soldiers to operate more efficiently in any environment.

Chapter 4
Executing Antiterrorism Measures

This chapter further expands on the integration of AT in full spectrum operations as discussed in chapter 1 and the application of AT tactical tasks to protect Army forces from violent and nonviolent terrorist tactics in various deployed environments.

MOVEMENT

4-1. *Force projection* is the ability to project the military instrument of national power from the United States or another theater of operations, in response to requirements for military operations (JP 5-0). Through power generation platforms, installations provide continuous force generation, deployment, and training operations for active and reserve component forces to enhance the operational Army and accomplish strategic objectives. Force projection encompasses a range of processes, including mobilization, deployment, employment, sustainment, and redeployment.

4-2. Current and future global commitments will keep Army operational forces in a nearly constant rotation, traveling from one geographical location to another. The Army is expected to move a combat-capable brigade anywhere within 96 hours with forces capable of operating in any environment. The early introduction of credible, capable forces with the ability to fight at the outset is an important strategic factor and crucial in convincing a potential enemy that further aggression would be too costly. To do this, the Army must protect its assets against terrorist activities to preserve its combat power and ensure the sustainment of its land operations. AT thinking and planning integrated into every aspect of predeployment and in-transit operations ensures proficiency, especially under demanding time constraints.

4-3. Army units and activities are expected to deploy rapidly in support of force projection operations. Movement planning takes into consideration the movement of unit equipment, personnel, and accompanying supplies from one location to another. Unit movement operations are conducted during training exercises, mobilization, deployment, and redeployment. Unit movement operations are planned, coordinated, and executed by principal modes (rail, motor vehicle, air, and sea). The mode of movement determines AT TTP for preparing, planning, coordinating, and executing unit movements (see figure 4-1, page 4-2). The phases of deployment are—

- Planning.
- Predeployment.
- Movement.
- Reception, staging, onward movement, and integration.

PLANNING

4-4. To meet their responsibilities to support operational, exercise, and contingency plans, units develop movement plans. Normally, brigades and battalions create movement plans and companies use extracts from battalion movement plans in company operation orders. Unit movement plans are tailored to the requirements for mobilization, deployments, and exercises, which have specific goals and missions. The plans are written in operation order format and are usually an annex to an operation order. The unit plans the move using the movement plan and executes the move under an operation order. A unit may have several plans, each one supporting a different contingency or exercise and tailored to support the plan for it. Each plan makes unique demands on the unit and requires AT thinking throughout. This is the reason that separate plans are prepared and tailored to each requirement. (See FM 3-35 for guidance on developing a movement plan.)

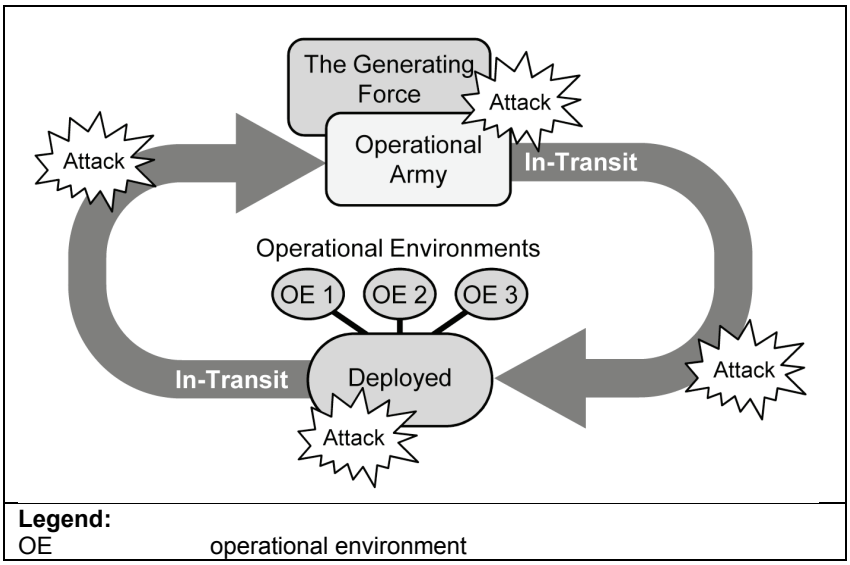


Figure 4-1. Threats to in-transit movements

4-5. In-transit movements have security seams created by operational handovers and a lack of situational awareness. Forces travel on vulnerable platforms with personal equipment and weapons stored for transport, reducing their ability to defend themselves against terrorist attacks. Commanders should focus on these security seams and conduct security planning with the responsible agencies for each phase to overcome vulnerabilities identified for the unit movement. Unit commanders must have the situational awareness required to implement effective security measures, guard against information leaks, and defend against terrorist surveillance and attack.

PREDEPLOYMENT

4-6. Army Commands, ASCCs, direct reporting units, U.S. Army Reserve Command, and the Army National Guard Bureau provide their respective unit commanders with an updated threat analysis and VA for the route and method of travel to the mobilization station. This includes intelligence that gives the unit commander up-to-date situational awareness. The unit commander incorporates these assessments into the unit movement order to support a common operational picture and to serve as a basis for security planning while intransit.

4-7. To help minimize the risk while intransit, units should conduct a leader's reconnaissance before moving the advance and main bodies. The leader's reconnaissance will include threat analysis, VA, and coordination to mitigate risks identified by the leader's reconnaissance. AT assessments should be conducted sufficiently in advance of deployments to allow and facilitate the development of security procedures, acquisition of necessary materials, obtainment of tailored and focused intelligence, organization necessary security support augmentation, and conduct of HN coordination.

4-8. Installation commanders within the U.S. Army Installation Management Command are charged to protect deploying forces as they conduct force projection operations. Units preparing for deployment interact with the installation staff through the corps and division protection cells and the installation ATWG. The unit AT officer serves as liaison between these groups and their respective commands to address security concerns throughout the entire movement into the joint operations area. Installation commanders ensure that unit training requirements are considered, especially during periods of heightened security concerns (increased threat, elevated FPCON, civil disturbances).

4-9. OPSEC and information protection are also key protection tasks during predeployment activities. Effective OPSEC keeps adversaries from exploiting friendly deployment and staging information. Commanders also ensure that rear detachment commanders and family readiness groups take appropriate OPSEC measures.

4-10. Relief-in-place planning should begin when the relieving unit is identified and a predeployment site survey has been conducted. Through constant surveillance by the local population, conversations with Soldiers, and open-source information, enemy combatants and terrorists can determine when units are expected to rotate. Improperly planned and rehearsed relief in place creates a seam in security that terrorists can exploit by increased terrorist attacks during a period of increased operational risk.

Site Survey

4-11. Brigade-size and above units conduct a leader's reconnaissance before the unit begins its collective training cycle in preparation for deployment. An effective predeployment site survey helps inform the unit about the AO and the combat tasks and missions the unit is expected to fulfill once deployed. The predeployment site survey helps commanders develop training plans and prioritize resources and time to accomplish predeployment activities. After the initial predeployment site survey, the commanders andstaff analyze the mission requirements, outline the training needed, and focus the leadership on the core issues and shortfalls that are critical for preparation.

4-12. The predeployment site survey is mission- and time-dependent and is normally conducted three to six months from the anticipated deployment. This time frame is close enough to deployment that the mission and AO are not expected to change significantly, yet far enough in advance to allow for programming resources and scheduling training. This schedule also provides the staff with sufficient time to review and adopt practices and products to use during the transfer of authority and initial phase of operations in the AO. The unit takes enough personnel to reasonably cover the areas concerned in the time allotted for the predeployment site survey. The predeployment site survey team should include the AT officer and representatives from each staff section. The predeployment site survey process should focus on staff functions and the transition, not exclusively on the commander.

4-13. Upon completion of the predeployment site survey, the commander and staff should have an increased knowledge base of the region they will operate in and the terrorist threat and identified actions in that area. With this knowledge, the commander can issue guidance and determine key training tasks. The predeployment site survey should give information on the—

- Requests for information and arrangements made to get follow-up information.
- Maintenance of digital pictures of key places, infrastructure, and local persons of importance or influence.
- Maintenance of information on the current enemy situation and specific terrorist threat, including current enemy tactics and practices, incidents, and experiences of enemy operations.
- Policies and practices for units dealing with contractors (U.S., local, and third-country nationals) working on the deployed FOB. The AT officer should obtain a clear understanding of how local nationals, third-country nationals, multinational forces, and contractors are cleared for access to U.S. bases and facilities.
- Copies of the outgoing unit's AT appendixes, ASCC AT guidance, SOPs, reports, and briefing formats, digitally if possible.
- Equipment, materials, and supplies staying behind or provided by the theater of operations that will pass from the outgoing unit to the arriving unit. Include maintenance status and identify equipment shortfalls.

Security Plans

4-14. Units use the results of the TA, criticality assessment, and VA to develop security plans for self-protection while in transit. Although emphasis must be on movements through high-threat areas, commanders should not discount appropriate security measures for movements in lower-threat areas.

4-15. Commanders must implement appropriate AT measures to reduce risk and vulnerability. Advanced or onboard security augmentation should be considered for travel through high-threat areas. Equipment (advanced surveillance cameras and monitors, explosive detection devices, blast mitigation equipment) can significantly enhance a transiting unit's posture against terrorist threats. Commanders should consider commercial-off-the-shelf or government-off-the-shelf products to meet near-term AT requirements.

4-16. Commanders and senior Army representatives accompanying the movement are responsible for ensuring that security measures sufficiently address vulnerabilities. Security measures taken to establish defense and protection must be continually reviewed and progressively updated to counter the changing threat and add an element of unpredictability to the terrorist calculation. This responsibility cannot be ignored. Local security must be vigilant 24/7 to provide observation, early warning and, if necessary, live-fire capability. Additionally, rest and recuperation facilities located within the operational-level commander's AO require close consideration. These facilities are frequently vulnerable due to their location and easy access. Movements may require tailored intelligence and CI support, HN assistance, or planned alternate routes based on the vulnerabilities associated with the movement. Commanders and staffs should consider the following to assist in mitigating their risk during movement:

- **Protective measures.** After estimating the threat and conducting a VA, the unit must take steps to ensure the security of its personnel, information, facilities, and equipment. During the determination process to establish appropriate protective measures, the unit commander must develop a set of proactive and reactive plans that are rooted in risk management and risk mitigation. The commander must oversee plan development and provide guidance continuously. The result must be plans that are realistic, effective, resourced, and coordinated.
- **Routine security operations.** Once the commander has approved plans that outline AT security measures, the unit must implement those measures. When possible, try to incorporate security considerations into facility selections and attempt to minimize the use of dedicated guards through the effective use of technology. Ensure that security measures are coordinated with tenant activities and U.S. forces within the AOR. Implement RAM and make use of supporting military police and other security force units. Commanders must be cognizant of the threat, identify and prioritize assets, and implement appropriate physical and procedural security measures to safeguard the unit.
- **Contingency operations.** After conducting planning and implementing basic security measures, the unit must be prepared to execute specific contingency plans within the AOR as required by the AOR commander. Augmentation support (first responders) that is provided by the unit must be officially identified, trained, and equipped to respond to conventional and CBRN attacks. Unit personnel must be familiar with the details of response plans requiring their participation. At a minimum, unit leaders and Soldiers should understand their involvement in mass-casualty triage and processing, decontamination, emergency evacuations, site security and control measures, and interagency support and coordination measures. At a minimum, commanders should exercise and test mass-casualty medical response and consequence management procedures, including C2 and CBRN response measures.

4-17. The terrorist threat remains one of the nation's most pervasive challenges. The USS Cole incident has shown that DOD personnel, facilities, and activities make high-value terrorist targets; and no change is predicted for the near future. Irregular threats use terrorism, insurgency, and guerrilla warfare to interdict U.S. forces attempting to enter foreign areas in crisis. These areas are often characterized by the presence of enemies, adversaries, supporters, and neutrals that are intermixed, with no easy method to distinguish one from another. AT officers oversee the execution of several actions at each stage of movement operations (see table 4-1).

Table 4-1. AT support to deployment operations

Planning for Deployment		
• Analyze the mission. • Structure the force. • Refine deployment data. • Prepare the force. • Schedule the movement.		
Predeployment Activities	***Movement***	***RSO&I***
• Provide Level I AT training. • Provide AOR-specific training.	• Submit the AT appendix to combatant commander. • Track all units during transit.	• Maintain contact with U.S. security advance personnel.
Identify Potential Terrorist Threats and Other Threat Activities		
• Coordinate with higher headquarters S-2 to obtain terrorist threat assessment for all movement. • Identify specific COAs for all movement phases.	• Continue to assess and update the original threat assessment.	• Brief the unit on threat levels. • Maintain situational awareness. • Receive updated threat and criminal activity reports.
Reduce Vulnerabilities to Terrorist Acts and Attacks		
• Conduct PDSS to identify potential unit vulnerabilities in each movement phase. • Wargame potential unit vulnerabilities. • Coordinate with lift provider to determine appropriate defensive measures. • Coordinate with the lift provider and HN regarding security of port of debarkation.	• Coordinate interagency security measures. • Develop HRP security measures. • Employ surveillance detection and counterintelligence resources. • Continuously assess overnight stops and refuel points.	• Conduct port vulnerability assessments. • Brief the unit on ROE. • Implement planned security measures. • Liaison with HN support.
React to Terrorist Incident		
• Plan unit responses to various threat COAs. • Develop communication plan to ensure that units can receive and transmit warnings/reports.	• Assemble port readiness committees. • Coordinate response plan during movement with applicable agency. • Respond to the incident.	• Obtain the local response plan guidance. • React to incident (if necessary).
Legend: AOR area of responsibility AT antiterrorism COA course of action HN host nation HRP high-risk person PDSS predeployment site survey ROE rules of engagement RSO&I reception, staging, onward movement, and integration		

Movement Coordination

A Stryker brigade combat team, conducting a unit movement from a post to a port of embarkation, received threat information through the garrison's protection cell. The unit deployment required the movement of 300 vehicles across 8 law enforcement jurisdictions. The garrison protection cell was uniquely skilled to provide threat information fusion because of established relationships and information from elements within DOD and outside law enforcement agencies. The garrison protection cell coordinated police information, intelligence, and civilian security with more than 22 local, federal, and DOD agencies. The fusion cell produced in-depth analysis of the threat to the team's movement and advised the team and garrison commanders on protection measures. The coordinated effort gave law enforcement the knowledge to identify and prevent disruptive actions by violent protesters while the equipment moved across multiple jurisdictions. These actions protected critical combat power through the successful shipment of equipment for use in a combat theater.

Fort to Port

4-18. The unit commander develops an in-transit security annex to the movement order that outlines security measures, which will mitigate or reduce suspected vulnerabilities during movement. The unit AT officer helps develop this annex and recommends appropriate security measures. The unit then files its request for movement authorization (movement credit), coordinates for security support from local authorities (as required), executes the movement once approval is obtained, and coordinates for additional security at the port of embarkation (as required). The installation monitors the execution of unit movement, tracks movement, and provides changes to threat information as required.

Port to Port

4-19. The operational responsibilities of unit movements from the aerial port of embarkation to the aerial port of debarkation are controlled by the U.S. Transportation Command, Air Mobility Command, and installation commander. These commands are primarily responsible to safeguard unit personnel while transiting by civilian and military aircraft.

4-20. The operational responsibilities of unit movements from the seaport of embarkation to the seaport of debarkation are controlled by the installation commander, Transportation Command, and Surface Deployment Distribution Command. These commands are primarily responsible for safeguarding unit equipment and personnel while transiting by civilian and/or military vessels.

4-21. The TA provides the unit commander with an updated threat analysis and assists the unit AT officer in conducting the VA for the route and method of travel from the seaport of embarkation to the seaport of debarkation. This includes intelligence that gives the unit commander up-to-date situational awareness. The Transportation Command and Surface Deployment Distribution Command make (through operations channels) a VA available for the mode of travel and locations through which the deploying unit will move. The VA should consider the terrorist threat and attack methodologies that may cause mass casualties.

4-22. The unit AT officer assists in developing this annex and recommends appropriate security measures. The in-transit security annex to the unit movement order may require specific measures that are tailored to shipboard security functions. Shipboard security is provided primarily for the security of the vessel. The secondary function of security personnel is to safeguard the unit's sensitive items and cargo. The vessel commander determines the priority for security personnel. The organization of shipboard security elements may vary, though two security squads per vessel is a general planning factor.

4-23. Units should consider the following factors if tasked with rail or shipboard security planning: TA, rules of engagement and use of force; security detachment functions and responsibilities; support equipment; weapons qualification and proficiency; C2; and railhead, pier-side, and afloat security duties. Vehicle Movement

4-24. During movement to the port of embarkation, unit commanders and AT officers rely on their installation and deployment centers to provide the latest TA along the route of travel and coordinate with law enforcement to reduce the likelihood of domestic terrorist attack or civil protest. Commanders establish security measures and identify rest stops and safe havens along the route.

4-25. In the AO, the probability and severity of IED use in the operational environment make convoy operations an enticing element for terrorist attack. Commanders and leaders reduce their vulnerability to attack by supervising several key tasks before movement. Once the order to move is received commanders execute troop-leading procedures and verify route clearance, patrol frequency, and counter IED operations in the area with the S-2/S-3. Commanders ensure that each member of the convoy is briefed on the latest TA, disseminate contingency plans; conduct radio checks; ensure that the counter remote-controlled, IED electronic warfare (counter remote control improvised explosive device electronic weapon [CREW] system is operational; develop a medical plan; and verify weapon status. Checklists, precombat checks, and precombat inspections ensure that personnel and equipment are functional before movement. If possible, convoy commanders conduct a map drill and obtain photos of known checkpoints and safe havens along the routes.

Air Movement

4-26. The Army deploys personnel, supplies, and equipment by air through an aerial port of embarkation operated by the Air Force and through civilian airfields. Deploying unit commanders are responsible for AT planning for movement to the aerial of embarkation and in the marshaling area. Army and Air Force commanders jointly coordinate mutual defense while traveling by air.

4-27. Commanders and leaders keep arrival and departure dates and times on close hold and tell Soldiers to do the same to reduce the risk of terrorist incident. Man-portable air-defense systems create additional planning challenges for the security of aircraft. Army and Air Force commanders continue to assess the threat and plan refueling and layover locations where the risk of such tactics is minimal.

Rail Movement

4-28. The March 2004 Madrid, rail attacks and the July 2005 London subway bombings dramatically revealed the vulnerability of passenger rail to terrorist attack and demonstrated the need for increased focus on the security of transit systems. Certain characteristics of rail systems make them inherently vulnerable to terrorist attacks and, therefore ,difficult to secure. By design, passenger rail systems are open, have multiple access points, may have hubs serving multiple carriers and, in some cases, have no barriers so that they can move large numbers of people quickly. The openness of passenger rail systems can leave them vulnerable because operator personnel cannot completely monitor or control who enters or leaves the systems. Therefore, a variety of security precautions (HN support and security forces on the train) should be used to minimize vulnerabilities to attack when transiting by rail.

4-29. The Surface Deployment Distribution Command is responsible for planning and executing rail movements; however, the transiting unit commander retains responsibility for planning AT measures for rail movements. Rail security is vital for the operational Army since equipment must arrive intact and ready for integration at the joint reception, staging, onward movement, and integration site.

4-30. Cargo guards or escorts maintain surveillance over military equipment during the journey and notify railroad personnel of problems. They must be thoroughly trained regarding AT measures and provided with current terrorist threat information. The rail cargo escorts help railroad personnel protect and maintain the security of Army equipment loaded aboard trains and of U.S. Army interests.

Sea Movement

4-31. Ports and harbors are prime targets for terrorist activities. Perimeter areas of these facilities are more vulnerable because of the extensive distance and exposed waterside of pier areas. Terminal areas may include fully developed piers and warehouses or may be an unimproved beach where logistics-over-the-shore or roll-on/roll-off operations are conducted (see ATTP 3-39.32). Because the security activities that DOD may conduct outside its installations are limited, it must work closely with a broad range of federal,

state, and local agencies to ensure that adequate AT measures exist and are executed during deployments through strategic seaports. AT responsibilities for DOD deployments through commercial seaports are divided among a number of DOD organizations, including U.S. Transportation Command components, particularly the Surface Deployment Distribution Command Military Sealift Command, U.S. Army Forces Command, and individual deploying units. (See FM 3-35.)

4-32. The USS Cole incident indicates port vulnerability. Terrorists exploited access control measures and perimeter security vulnerabilities of waterside approaches to the naval ship while near the coastline. As a result, the Navy destroyer suffered a serious terrorist bomb attack that severely damaged the ship, killing 17 Sailors and injuring 39. The attack came in the form of a small boat laden with explosives that, according to some reports, was thought by the crew to have been a part of the scheduled contractor refueling support. The significance of this for commanders is that it reinforces the need for completing thorough vulnerability and risk analysis and identifying the right mix of physical security measures when intransit, using sea lines of communication. Units should consider irregular or asymmetric approaches that terrorists can employ to leverage their strength against perceived weakness.

4-33. Supercargos are unit personnel designated on orders to accompany, secure, and maintain unit cargo onboard ships. Supercargoes are the deploying unit commander's onboard representatives during the movement of unit equipment on a ship. They perform liaison during cargo reception at the seaport of embarkation, shipload, and discharge operations, and seaport of debarkation port clearance operations.

4-34. Upon arrival at the seaport of embarkation, supercargos are under the operational control of the port commander. While onboard a ship, they are under the C2 of the vessel's captain. Upon arrival at the seaport of debarkation, supercargos are under the operational control of the port commander and are normally released to the unit on completion of port clearance operations.

4-35. Terrorist TAs identify and evaluate potential threats on the basis of factors (capabilities, intentions, past activities). Unit commanders recommend the composition of supercargoes based on several factors, including the amount and types of equipment loaded aboard the ship and the number of units with equipment on the ship. However, the Military Sealift Command determines the actual number of supercargos permitted onboard, based on the berthing capacity on the ship. (See FM 3-35.)

RECEPTION, STAGING, ONWARD MOVEMENT, AND INTEGRATION

4-36. The operational responsibilities of unit movements from the aerial port or seaport of debarkation to the AO are controlled by the combatant or joint operations area commander and the deploying unit. These commands are primarily responsible for safeguarding unit equipment and personnel while intransit. Security is paramount during reception, staging, onward movement, and integration, security is paramount. Reception, staging, onward movement, and integration operations must be protected from the full range of threats, including espionage, local unrest, terrorist activities, and CBRN attacks. The reception, staging, onward movement, and integration process calls upon the full range of Army transportation support, from discharging ships and hauling cargo to providing information for force tracking. HN support plays a critical role and should be planned. The reception, staging, onward movement, and integration process is facilitated by the use of HN resources (ports; airfields; railways; land for staging, traffic convoy, and convoy escorts).

4-37. The combatant commander is responsible for establishing an FPCON baseline level and providing guidance on the employment of random AT measures and programs at the aerial port or seaport of debarkation for the arriving unit. The reception, staging, onward movement, and integration required of the arriving unit will be established before the unit movement (details should be determined during the leader's reconnaissance and predeployment site survey). This includes subsequent unit movements from the aerial or seaport of debarkation through assembly or staging areas and on to the final unit destination.

4-38. Upon arrival, the unit commander should receive an updated threat analysis and VA from the departure control group for the route and method of travel from the port of debarkation to the AO. This includes intelligence that gives the unit commander up-to-date situational awareness.

DEFENSIVE OPERATIONS

4-39. While defensive operations can serve as a temporary state until offensive operations can resume, commanders also conduct defensive operations to retain key terrain, provide secure C2 to a larger AO, deter or defeat terrorist offensive operations, or protect the local populace, critical assets, and infrastructure. AT measures naturally support the commander's protection requirements during defensive and stability operations.

4-40. AT measures should consider the entire operational area and take into account measures that are necessary to protect people and assets traveling in, around, and through the local area. Effective AT measures integrate a multitude of security programs, which ensure that U.S. personnel, information, infrastructure, installations, facilities, and forces are protected from adversary attack. Defensive measures are established based on an assessment of the full range of threats (enemy conventional forces, terrorists, insurgents, organized criminal elements, insiders). No matter which defensive task is performed, the survivability of C2 centers and key communications nodes in defensive operations is critical to success. Survivability and AT tasks and plans are essential during the defense and may require a deliberate and detailed approach to ensure that combat power is apportioned where it is most needed. Commanders may use decision support tools and analysis to assess critical assets and key vulnerabilities. Adversary attacks may be from conventional, irregular, or terrorist forces and drive changes in local FPCON. Incident management plans in execution are key components to a successful protection plan.

4-41. In a mobile defense or retrograde operation, commanders ensure that their forces understand the probability of terrorist actions against them as they maneuver across restricted terrain. The relatively low expense of asymmetric tactics make them ideal for use as a means to harass or destroy supply lines, channel forces, or impact combat power by trying to reduce manpower and equipment. Forces serving as a covering force to protect the main force or guard exposed flanks may find themselves operating without immediate support. Soldiers rely on predeployment AT training and updated TAs to gain an understanding for the likely tactics to be used against them in a certain area. They rely on increased situational awareness and ability to identify likely IED tactics to aid in protecting themselves and covered forces.

4-42. Effective and disciplined OPSEC and surveillance detection operations protect essential elements of friendly information, preventing enemy reconnaissance and other information collection capabilities from gaining an advantage through identifiable or observable pieces of friendly information or activities. These actions are critical during defensive and retrograde operations to prevent surprise and reduce the likelihood of a successful terrorist attack. OPSEC and information protection activities deny the enemy access to information systems and prevent network intrusion, degradation, or destruction through computer networks, thus protecting the commander's situational awareness and the secrecy of unit plans.

4-43. In an area defense and during area security operations, commanders understand the importance of protecting C2 nodes and the surrounding populace. AT supports the deliberate planning process necessary to mitigate risk through physical means and the portioning of combat forces to protect critical assets. Commanders and staffs use the various threat, vulnerability, and criticality assessments contained in this manual to aid in identifying the importance of key personnel, areas, and facilities with significant social, economic, and political value in tactical operations. Increased probability or the results of successful terrorist attacks drive the overall FPCON level or could result in the implementation of various RAM. Incident management plans to recover from terrorist actions and to maintain the continuity of operations are essential in the overall success of Army operations.

4-44. Within the operational themes of peacetime military engagement, limited intervention, peace operations, and IW, commanders establish locations to provide C2, sustain combat power, project forces in conducting operational tasks, and develop actionable intelligence to meet strategic goals. Commanders establish FOBs on key terrain to provide a secure environment and negatively influence the terrorist's ability to conduct violent and nonviolent attacks during U.S. military operations. Commanders can also extend protection to the local populace, critical assets, and key infrastructure to deny terrorists influence in that area and allow for the freedom of movement.

4-45. Because terrorists and U.S. forces are continuously striving for the support of the local populace, commanders engage the community to separate the identity, goals, and grievances of terrorist groups and the local community. *Community engagement* is the process of working collaboratively with and through groups of people affiliated by geographical proximity or special interest to enhance their understanding and support for military operations and activities (DODI 5400.13). Successful community engagement can assist in building positive perceptions of U.S. presence in an area and, through community interaction, can help the protection posture of the base itself.

FORWARD OPERATING BASES

4-46. *Bases* are a locality from which operations are projected or supported, an area or locality containing installations that provide logistic or other support or a home airfield or home carrier. (FM 3-90) Current national, defense, and military strategies require modular Army land forces to conduct operations anywhere from self-sufficient FOBs. FOBs can be part of traditional or nontraditional military missions, regional threats, AT actions, or counterdrug operations. Nearly all operational bases where U.S. military troops are deployed can be targets for terrorist attacks. Commanders, with assistance from the AT officer, ensure that bases are securable and defendable against this type of threat at all times.

4-47. Base commanders have overall responsibility for the security of everything within the base boundaries. Tenant units usually secure their own facilities within the base, while selected forces from the various commands are made available to the base commander, who will exercise tactical control over those forces for base defense and incident management. These forces will comprise an element that is able to meet the capabilities of the local threat, along with identified elements to reduce the damage to unit operations and critical infrastructure as a result of a successful terrorist attack.

4-48. FOB site selection and design layout are determined by competing demands and considerations (mission concerns, political constraints, HN requirements, Service regulations). AT measures should be deliberately integrated into the planning, design, and construction of FOBs. A FOB design that includes considerations for terrorist threat capabilities and countermeasures can greatly reduce the amount of materials, time, and energy required to protect the FOB and increase its defensive posture during increased threat or FPCON levels.

Base Selection

4-49. The early identification of AT and security requirements is essential to the base planning effort. Addressing protection and security concerns early helps ensure that site location and layout are compatible with security operations and mission accomplishment. The early development of AT and security requirements helps to reduce construction and manpower costs and ensures adequate protection of personnel and assets. It is easier and more cost-effective to establish AT security measures during the planning process rather than after the fact.

4-50. The key to the effective planning, design, and development of base protection requirements is a partnership between the unit AT officer or security planners and the engineers. This partnership helps ensure the development of integrated protective measures and security procedures that are consistent with base design. Commanders ask whether—

- AT measures will result in an acceptable level of risk to the force, considering funding restraints and mission requirements. The level of risk should be consistent with the commander's intent and applicable guidance.
- AT measures are within the capability of the unit.
- Resources are available to accomplish the task.
- AT measures provide maximum latitude for initiative.
- AT measures are within the bounds of legal, moral, and HN constraints.
- AT measures consider future operations, latitude for initiative, and flexibility to meet unexpected threats and opportunities.

4-51. For enduring or main operating bases, AT planning should also be incorporated into the framework of master planning. Master planning provides an integrated strategy for construction and maintenance of required facilities. The incorporation of protection and security concerns into the master planning process ensures cost-effective protection. Master planning requires regular coordination through the protection cell or ATWG and engineers.

Planning and Design Stages

4-52. Planners and designers can integrate AT measures into three planning and design stages that support FOB development:

- **Site selection.** Planning provides a framework to guide the development of the FOB. Consideration of AT measures during the site selection stage may preclude the need for applying more stringent AT measures to the FOB later. Site selection planning should make use of vegetation, topography, and natural barriers as protective measures.
- **Base layout and design.** Planning addresses methods for integrating perimeter security, standoff distances, ECPs, vehicle barriers, fences, and security lighting to diminish the potential threat to personnel and critical assets.
- **Base construction.** Planning considers protective design measures for structures, including the structural hardening of walls, roofs, floors, and windows to reduce the vulnerability of these structures, thereby making them less inviting targets.

Tactical Site Selection

4-53. Deployed-base site selection and design layout are determined by competing demands and considerations (mission concerns, political constraints, HN requirements, Service regulations). AT measures should be deliberately integrated into the planning, design, and construction of FOBs. Operating bases take many forms, depending on the location and length of time an operating base will be used. Examples of operating bases are—

- Contingency operating base.
- FOB.
- Combat outpost.
- Logistics support area.
- Joint contingency operating base.
- Joint forward operating base.
- Joint security stations.

4-54. While the terminology and purpose may be different, a base design that includes the considerations of terrorist threat capabilities and countermeasures can greatly reduce the amount of materials, time, and energy required to protect the base and increase its defensive posture during increased threat or FPCON levels. The unit AT officer should work closely with base planners and designers to ensure the integration of protection measures.

Planning Factors

4-55. Proper site selection and effective FOB layout helps to accomplish the objectives of protecting the force. Base camp planners are challenged with varying degrees of conditions, uncertainty in mission durations, and the fluctuation in troop strength and force repositioning that occurs as the mission or strategy adjusts. Commanders and AT officers work with base developers to ensure that a sufficient level of protection exists and is factored into further construction plans should base expansion or permanency be determined at a later date. Applicable AT requirements must be considered during the site layout and design of the controlled perimeter and protective structures for the FOB. Site layout and design must—

- Meet the minimum AT requirements of UFC 4-010-01.
- Meet applicable combatant command (command authority) AT requirements.

- Include requirements to defeat specific threats, based on input from the base commander and/or intelligence reports.
- Involve a risk analysis of the DOB assets to determine if additional AT design requirements are merited. Higher-risk assets may warrant higher levels of protection, more resources, and shorter timelines.

SITE SELECTION CONSIDERATIONS

4-56. Sites for FOBs are selected to facilitate the accomplishment of the primary operational mission. Even so, AT considerations must not be ignored. The location of a FOB should be chosen to facilitate protecting the force and make an enemy attack more difficult. Planners can facilitate this effort by first conducting a terrain analysis (observation and fields of fire, avenues of approach, key terrain, obstacles and movement, and cover and concealment is a tool) for a proposed FOB. This analysis should consider the military aspects of a location from the standpoints of the defenders and the enemy.

4-57. In selecting a site, FOB planners should consider the—

- **Threat.** Identify and characterize threats to the FOB. Understanding the threat assists commanders in determining the best location for a FOB.
- **Political considerations.** Consider the relationship with the local public, including—
  - ***HN political climate.*** Consider how the local situation influences FOB location, design, or land use decisions. Politically unpopular decisions may attract acts of aggression.
  - ***Adjacent landowners.*** Assess potential problems (the impact of traffic restriction, safety, other inconveniences). Identify restrictions that limit public access to the area of the proposed FOB.
  - ***Appearance.*** Consider the local perception of the appearance of a proposed FOB. For example, public perception of a fortress may be desirable or undesirable.
- **FOB mission.** Examine the FOB mission, planned facilities, and tenant units and organizations.
- **Available real estate and buildings.** Determine available real estate, existing facilities, infrastructure, and buildings. Assess off-base land and zoning plans for protection impacts. Assess occupancy requirements.
- **Communication capability.** Assess the ability to speak to higher headquarters and subordinate units operating in the AO using FM, satellite, and Internet capabilities.
- **Dispersion and standoff minimum requirements.** Provide minimum standoff requirements to the controlled perimeter, parking areas, living quarters, roadways, and buildings.
- **Defense in depth.** Select a site that provides defense in depth, requiring a terrorist to negotiate varied defense mechanisms to reach an ideal target. Do the location and layout of the FOB present a hardened image to a terrorist, one that will discourage an attack? Do the location and layout assist personnel in defending against vehicle-borne, improvised explosive devices and rockets, artillery, and mortars by allowing for use of natural barriers, standoff distance, dispersion, compartmentalization, and clear fields of fire?
- **Perimeter requirements.** Determine perimeter security requirements (standoff, barriers, ECPs, lighting). Does the location and layout assist security personnel in assessing the intentions of an unauthorized intrusion or activity? How do they affect the ability to raise and lower the FPCON level and implement RAMs?
- **Vehicle roadway considerations.** Design on- and off-base roadways. Keep bases from main thoroughfares and uncontrolled vehicle access. Minimize the number of access roads in the base.
- **Natural or man-made vantage points.** Avoid placing a FOB adjacent to higher surrounding terrain or buildings that provide easier surveillance of FOB activity or vegetation, drainage channels, and ditches, which can provide enemy concealment.
- **Potential enemy vantage points.** Situate the FOB to limit attacks by direct, line-of-sight weapons from potential vantage points.

- **Natural terrain (observation and fields of fire, avenues of approach, key terrain, obstacles, cover and concealment).** Do the location and layout of the FOB make use of the terrain and natural barriers to impede intruders in their efforts to reach the objective?
- **Open space.** Maximize the distance between the perimeter and surrounding developed areas. Provide as much open (clear) space as possible. Does the location and layout of the FOB facilitate the detection of possible threats and attempts at unauthorized entry?
- **Topographic areas.** Avoid low-lying topographic areas that can facilitate the effects of possible CBRNE attacks.

BASE LAYOUT CONSIDERATIONS

4-58. Personnel responsible for FOB layout, design, and AT must consider a multitude of challenges (FOB operational and functional issues, HN requirements, safety, fire protection). In general, these concerns and constraints will be unique to a specific FOB. Designers need to recognize conflicts and establish priorities during the planning stage so that they will work toward optimal solutions. Some layout considerations are similar to site selection considerations. The layout and design of a FOB should facilitate current operations; have a layered security approach; include ECPs tailored for large vehicles, personnel access, military access, or combinations; have facilities designed to support incident response and quick reaction; and include redundant utilities, protected critical assets, and accessible protective shelters throughout. In addition to the areas discussed above, those responsible for the FOB layout should also consider the following areas:

- **Terrain.** Consider available real estate, taking into account existing natural and man-made features and the availability of existing facilities and types of temporary structures.
- **DOB mission requirements.** This includes tenant unit and organization mission and space requirements.
- **Critical assets.** Identify assets to be protected, and determine the level of protection needed against an identified threat.
- **Dispersion and standoff requirements.** Maximize the distance from occupied structures to the FOB boundary.
- **HN, multinational force, and tenant-unit force security requirements.** This includes security restrictions, considerations, and sensitivities.
- **Construction considerations.** Assess the types and quantity of indigenous and other available construction materials, equipment, funding, labor, contractor support, and reverse-engineering considerations.
- **Ammunition storage.** Early in the planning stage, determine where to locate ammunition storage points or temporary ammunition holding areas, observation posts, ECPs, overwatch positions, and quick-reaction force, fire, security, and personnel stations.
- **Utilities and infrastructure.** Provide secure access for power and heating plants, gas mains, water supplies, water treatment plants and storage facilities, and electrical service. Provide underground, concealed, and protected utilities where possible. Locate storage tanks and operations facilities for petroleum, oil, and lubricants down-slope from other facilities and at the required separation distance from critical assets, occupied structures, and other utility plants.
- **Detainee holding area.** Early in the planning stage, determine the requirement to provide housing and security for detained personnel and enemy combatants.
- **Shelters and bunkers.** Ensure that survivability and defensive positions and protective shelters and bunkers are strategically located to benefit DOB personnel.

2009 Complex Attack on Combat Outpost Keating

On 3 October 2009, Soldiers of Troop Bravo, 3d Squadron, 61st Cavalry, repelled an enemy force of 300 anti-Afghan forces fighters, preserving their combat outpost and killing approximately 150 enemy fighters. U.S. forces sustained 8 killed in action and 22 wounded. All but 3 of the wounded returned to duty after the attack.

Combat Outpost Keating, originally established as a base for a Provincial Reconstruction Team in 2006, was located in Nuristan Province, surrounded by high ground, with limited overwatch protection from nearby Observation Post Fritsche. Combat Outpost Keating was used to engage and protect the local populace, but due to limited manpower and tactical reach of the compound, the mission devolved into one of base defense.

The delayed closing of Combat Outpost Keating contributed to a mind-set of imminent closure that served to impede improvements in force protection on the combat outpost. Over time, the enemy made numerous probing attacks, learning the TTP of Bravo Troop and pinpointing the location of weapons systems and key infrastructure and material (generators, barracks). Compounding the situation, U.S. intelligence assessments became desensitized to enemy actions over several months. During the 5 months of Bravo Troop's deployment to Combat Outpost Keating, the enemy launched approximately 47 attacks (triple the rate of attacks experienced by their predecessors).

On 3 October 2009, Troop Bravo Soldiers woke to a previously unseen volume of enemy fire, commencing at approximately 0558 hours, coming from the high ground surrounding the combat outpost. A simultaneous enemy attack against Observation Post Fritsche limited mortar fire support from that location. Enemy fighters applied the information gathered from probing attacks and immediately inflicted casualties on the combat outpost guard force and suppressed Combat Outpost Keating's primary means of fire support (60- and 120-millimeter mortars). Afghan National Army soldiers on the eastern side of the compound failed to hold their position, and enemy forces penetrated the Combat Outpost Keating perimeter at three locations.

Continuing to fight under the heavy enemy indirect and direct fire from superior tactical positions and suffering a loss of power to the tactical operations center when enemy forces destroyed the main power generator, Bravo Troop withdrew to a tight internal perimeter. With critical supporting fires from the U.S. Air Force close air support and AH-64 Apache helicopter close combat aviation fires (that took over 45 minutes to arrive), the junior officers and noncommissioned officers (NCOs) regained the initiative and fought back during the afternoon hours to regain control of Combat Outpost Keating. The Soldiers, aided by continuous fires from supporting aviation units, engaged the enemy fighters who had breached the compound and reestablished control of key buildings.

OFFENSIVE OPERATIONS

4-59. In offensive operations, commanders use AT measures and training to better prepare their combat patrols before mission execution. The asymmetric violent and nonviolent tactics used by terrorists are similar to those used by insurgents, guerillas, and unconventional forces. By training and preparing Soldiers to defend against the terrorist threat at camp and home station while deployed during stable and unstable peace, commanders are inherently preparing their force to defend against the threats to combat power faced in active insurgencies and during general war. Within the protection warfighting function,

commanders apply AT protection measures while weighing the risk involved, with bold initiative and control of the operational tempo.

4-60. During offensive operations, various military organizations may be involved in area security operations in an economy-of-force role to protect lines of communications, convoys, and critical fixed sites and radars. FOBs employ local security measures (assessments and recommendations, RAM, and increased FPCON), but may be vulnerable to nonstate actors used as an arm of a greater military engagement. Based on mission analysis and planning efforts, specific AT measures are identified to counter terrorist tactics.

4-61. Commanders, with the assistance of the AT officer and staff, assess the threat, vulnerabilities, and criticality associated with conducting combat patrols. The staff weighs the probability of attack by terrorist organizations on patrols en route to execute a movement to contact or attack while analyzing the susceptibility of FOBs to terrorist attacks with the reduction of available combat forces. The commander emplaces units to thwart identified threats and increases the overall FPCON or implements RAM to protect logistics lines, critical sites, and HN infrastructure and to identify vulnerabilities within his own forces to the asymmetric tactics associated with terrorist actions.

4-62. Level I AT training and AOR-specific training before deployment give the Soldier a level of awareness necessary to instinctually identify when something appears out of place during combat patrols. Training a Soldier to identify the signs of an IED or suicide bomber helps to preserve combat power while it operates in confined spaces found within most urban settings or en route to an objective in more rural settings. Personal protection training assists the Soldiers in preparing mentally in case of separation from their unit or being taken hostage by terrorist organizations operating in support of an active insurgency or conventional enemy force. This training helps to sustain the individual during personnel recovery operations and enhances the likelihood of the Soldier being recovered and returned to the fight.

4-63. Patrols obtain information about terrorist threats and capabilities before leaving the security of a FOB. The patrol leader establishes the patrol's posture in relation to the threat and briefs the unit on the travel route, safe havens, and mine and IED threat to increase situational awareness. The patrol leader also reviews battle drills, the use of electronic countermeasures, and the rules of engagement to reduce the impact of potential terrorist actions against the unit.

4-64. Because of the reliance on speed, audacity, and surprise in the offense, AT officers understand the importance of OPSEC and information security. Terrorist organizations have shown increased skill at utilizing technology and have demonstrated abilities at hacking into information centers. To protect the commander's availability of information and increased situational awareness, AT officers ensure that communication lines and information systems are protected from outside attack or surveillance to protect ongoing and future mission planning. AT officers also influence commander's guidance and operating procedures to ensure that Soldiers do not reveal mission-critical information across open-source Web sites or in e-mails to family members back home.

4-65. Leaders ensure that their Soldiers understand the rules of engagement before conducting operations, especially when units are transitioning from general war to peace enforcement. Actions on the battlefield can have a positive or negative effect on the overall U.S. mission. Terrorists understand the media cycle and try to use misinformation to sway local public support for U.S. or multinational operations. Terrorists in the past have conducted bombings in urban centers and edited film to give the appearance of a U.S. attack on innocent victims. Commanders should never underestimate how information and incidents in their AOR will be manipulated to achieve terrorist goals.

4-66. Leadership serves as a key component to effective combat power and offense operations. The AT officer ensures that critical HRP are provided with necessary protection against the violent asymmetric tactics associated with terrorists. The AT officer assists designated security teams and squads in obtaining the necessary training and equipment to best accomplish their duties. While the U.S. Army conducts operations through centralized planning and decentralized execution, AT officers understand the effect on unit morale after the loss of a key leader or commander to attack or assassination and, ultimately, works to preserve the unit's fighting spirit. Leaders operate and maneuver where they can best direct the fight, but they need protection. Security teams should move with, flank, and escort key leaders throughout the battlefield to preserve their ability to influence the operation and ensure mission success.

STABILITY OPERATIONS

4-67. Fragile and failing states serve as safe havens and breeding grounds for terrorist activity, providing an area to recruit, conduct training, and project attacks around the world. To engage this national security threat during the time of persistent conflict, the use of Army forces to provide a stabilizing influence is more critical than ever. (See FM 3-07.)

4-68. Stability operations require commanders to balance protection needs between military forces and civil populations; it is in this environment, that AT posture is at its greatest. Nonstate actors prey on civilians and other noncombatants as a means of weakening U.S. influence in the country and domestic U.S. political resolve and to promote their individual agendas. Because U.S. forces and the local population frequently interact, planning for their protection is important and should be integrated in local base threat, vulnerability, and criticality assessments. Attacks on critical infrastructure and reconstruction projects not only have an impact on mission success, but could also affect local base operations and popular support for U.S. forces. Nonstate actors are nearly indistinguishable from noncombatants and view U.S. forces and facilities as prime targets. For this reason, some Army functional capabilities are often retasked from their primary function to conduct or reinforce protection efforts (defending against a terrorist threat based on METT-TC).

4-69. Success in stability operations depends on military forces seizing the initiative. In fragile states, the sudden appearance of military forces typically produces a combination of shock and relief among the local populace. By quickly dictating the terms of action and driving positive change in the environment, military forces improve the security situation and create opportunities for civilian agencies and organizations to contribute. Immediate action to stabilize the situation and provide for the immediate humanitarian needs of the people begins the processes that lead to a lasting peace. Failing to act quickly may create a breeding ground for dissent and possible recruiting opportunities for terrorists or other adversaries.

4-70. In the absence of a conventional or militant force, a commander's greatest threat will derive from terrorist activities. As in offensive and defensive operations, commanders with the assistance of the AT officers use various assessments and AT measures to mitigate the vulnerabilities of their forces and bases to the violent tactics of terrorism. Commanders also expand their ring of AT protection to encompass the local populace, critical infrastructure, and heads of government to—

- Provide a safe and secure environment.
- Enhance freedom of movement.
- Establish rule of law.
- Create a stable government.
- Create a sustainable economy.

4-71. Terrorists use their ability to blend with local society and the cover of urban settings as means to attack U.S. efforts and escape undetected. Heightened awareness and community engagement by Soldiers increases their ability to separate the local populace from the terrorist network. Terrorists will sabotage rebuilding projects, kidnap members of nongovernmental organizations and relief agencies, directly strike military forces, and attack ethnicities and religious sects to disrupt U.S. efforts, force multinational partners to pull out, and create the impression that the newly formed government cannot provide basic social well-being.

4-72. Because stability operations are conducted among the people and with greater coverage by a global media network, commanders take steps to establish effective information tasks. Inform and influence activities enhance the success of each primary stability task, reinforcing and complementing actions on the ground with supporting messages. Through effective inform and influence activities, Army forces draw on cultural understanding and media engagement to achieve decisive results while reducing the terrorist effectiveness in misinformation. As much as practical, commanders provide the news media with information to facilitate prompt, accurate reporting. Gaps in information reporting or media engagement after an incident leave room for terrorist organizations to manipulate the scenes or the events to serve their goals of circumventing U.S.-led efforts.

CIVIL SUPPORT OPERATIONS

4-73. Civil support operations are conducted only within the United States and U.S. possessions and territories, not outside the United States. If DOD conducts disaster relief operations in support of a foreign nation, for example, it is a stability operation and is called *foreign humanitarian* assistance or *foreign consequence management*. The Department of State, not DOD, is the lead agency for this type of effort.

4-74. Within the framework of homeland security, Army forces, as part of a joint response at the state level, federal level, or both, will normally conduct civil support operations exclusively, often employing capabilities developed for other elements of full spectrum operations as part of civil support. Domestic operational environments are different from other tasks within full spectrum operations in terms of law, military chain of command, deadly force, and interagency process.

4-75. Civil support is provided to U.S. civil authorities under the auspices of the National Response Framework or defense support of civil authorities for domestic emergencies and designated law enforcement support missions. It includes operations that address the consequences of disasters, accidents, terrorist attacks, and incidents. Army forces conduct civil support operations when the size and scope of events exceed the capabilities of domestic civilian agencies. During Army civil support operations, AT measures are important to protect U.S. citizens and Soldiers from unknown hazards and threats. Army forces perform civil support tasks (see FM 3-28) under U.S. law, generally following a tiered-response concept. The National Guard is often the first military force to respond on behalf of state authorities. In this capacity, the National Guard functions under the authority of State Active Duty status and operates under Title 32, U.S. Code. In addition, the National Guard forces under state control have law enforcement authorities that Regular Army units do not have. The National Guard is well suited to conduct these missions. If the response requirements exceed state and National Guard capabilities, the governor may request assistance from federal authorities. AT planning considerations during civil support operations may include—

- Security support for national events and postdisaster recovery.
- Increased liaison with local law enforcement.
- Fusion of threat information for the AO.

Note. During Joint Task Force Rita (Fifth U.S. Army) support to the Federal Emergency Management Agency for Hurricane Katrina recovery operations, the Task Force designated FPCON Bravo to establish an appropriate security posture to protect U.S. citizens and Soldiers operating throughout the disaster area from the threat of terrorism.

This page intentionally left blank.

Chapter 5
Integration Into the Operations Process

This chapter focuses on AT integration throughout the operations process and its service to commanders as a combat multiplier. Terrorists use simple, low-tech methods to accomplish monumental results. Terrorists are patient, methodical, calculated, and bold in their surveillance and method of attack. To counter this enemy, U.S. forces must be equally patient and methodical in the process to defeat terrorist actions before and while they occur and to defend their AORs with vigilance and tenacity. Through an intelligence-led approach, commanders use the MDMP or troop-leading procedures into plan and defend against terrorist capabilities.

COMMAND AND CONTROL ACTIVITIES

5-1. The operations process consists of the major C2 activities performed during operations: planning, preparing, executing, and continuously assessing the operation. The commander drives the operations process through mission command as seen in figure 5-1. At the start of operations, the activities within the process move sequentially. Once operations have begun, activities within the process begin to operate simultaneously, planning and preparing the follow-on mission as initial tasks are being executed. Planning remains a continuous activity, while preparing is done simultaneously only when a unit is not conducting operations. Assessing is continuous throughout activities and is crucial to influencing activities and mission accomplishment.

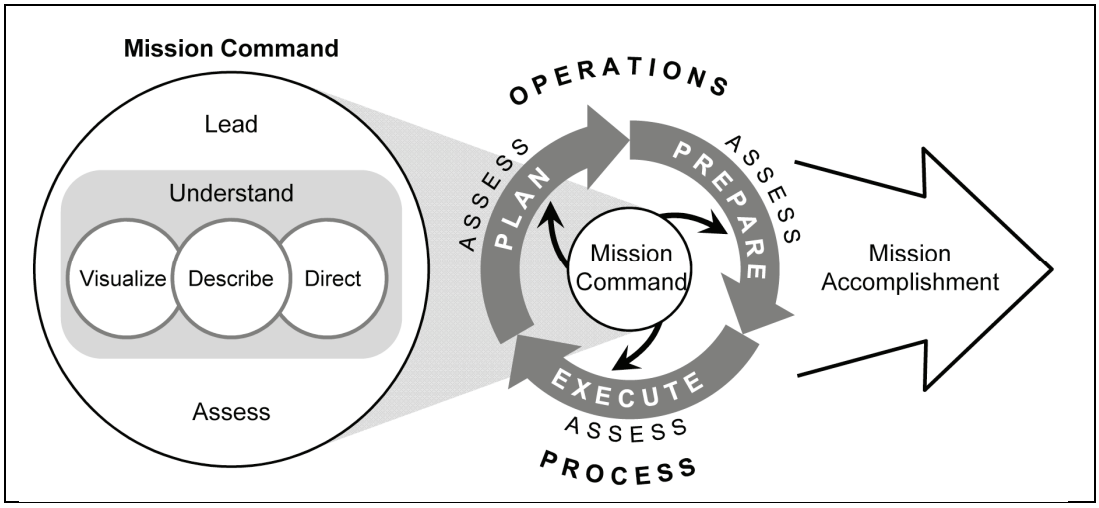


Figure 5-1. The operations process and mission command

5-2. AT is an integral part of the protection warfighting function, and commanders rely on their AT officers and staffs to assist them in understanding the terrorist threat, its capabilities, and the impact it has on their forces. Commanders visualize potential solutions to prevent terrorist acts through an understanding of how AT is integrated within the protection warfighting function and how it applies to the protection of forces throughout force generation and missions within the operational environment. As the commander begins visualizing AT solutions, he describes his concept and intent to the staff, helping to drive the planning process and COA development. Through constant assessment, the commander obtains enough

information to begin directing the staff to achieve those tasks necessary to protect the force based on the current and potential threat of terrorism.

5-3. Commanders and subordinate leaders will need to respond quickly and intelligently to constant change. Terrorists continue trying to sway local support and adapt their tactics from high tech to low tech to counter U.S. tactics. Commanders direct by effectively positioning and empowering key leaders. Leaders have the flexibility to adapt their roles to meet the demands of the environment changing from operational roles to that of politician and business developer. They operate more decentralized from the higher headquarters and exert their ability to make decisions and react to identify and seize opportunities without higher supervision. Commanders focus on mission accomplishment by understanding these requirements and empowering subordinate leaders and decisionmakers at the lowest level. Through decentralized operations, Army forces are empowered to defeat the fluidity and cellular operations of terrorist organizations.

PLANNING

5-4. *Planning* is the means by which the commander envisions a desired outcome, lays out effective ways of achieving it, and communicates to his subordinates his vision, intent, and decisions, focusing on the results he expects to achieve. (FM 3-0) Assessment during planning focuses on monitoring the current situation, establishing measures of effectiveness/measures of performance, and evaluating COAs.

5-5. Because AT is a defensive posture against terrorism, planning plays a crucial role in ensuring that the risks associated with terrorism have been addressed and that mitigation strategies have been implemented in protecting combat power. Planning supports decisionmaking by analyzing relevant information and providing context to develop situational understanding and a greater understanding of the terrorist threat. The outcome of planning is the commander's decision about how to execute the operation through the approved COA. Planning concludes with the production of orders, preparations, and execution.

5-6. During mission analysis, the AT officer, working with the G-2/S-2, develops running estimates to monitor and evaluate AT efforts throughout the operations process. These AT efforts may assist in the development of measures of performance and effectiveness. A *measure of performance* is a criterion used to assess friendly actions and is tied to measuring task accomplishment (JP 3-0). A *measure of effectiveness* is a criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect (JP 3-0).

5-7. The approved vulnerability reduction mitigation measures, commander's decisions for acceptable risk, critical-asset list, and defended-asset list represent running estimates that are incorporated into appropriate plans and orders. The staff or appropriate working groups identify the most probable terrorist threats the unit faces with the goal of preventing or deterring an occurrence, where possible, and then deliberately applying or deriving AT measures to reduce vulnerability and mitigate risk.

5-8. During the MDMP, planners receive guidance as commanders describe their visualization of the operational concept and intent. This guidance generally focuses on COA development by identifying decisive and supporting efforts, massing effects, and stating priorities. Effective planning guidance provides a broad perspective of the commander's visualization, with the latitude to explore additional options. Command guidance is often issued using the warfighting functions as criteria. A commander's initial AT guidance in planning may include the following information:

- Intelligence focus for AT efforts.
- Areas or events where risk is acceptable.
- Critical assets and high-value targets.
- FPCON status.
- RAM implementation.
- CBRNE risk guidance.
- Information operations condition.
- OPSEC risk tolerance.
- Rules of engagement and interaction.

5-9. Commanders typically determine their own commander's critical information requirements (CCIRs), but may select some from staff nominations. The AT officer recommends highest priority intelligence requirements and friendly force information requirements for the commander to designate as CCIRs. The following are examples of AT priority intelligence requirements:

- Discovery of or intent to conduct modifications to common systems—including clothing (suicide belts or vests), luggage, boats, aircraft, trucks, cars, motorcycles, bicycles, propane tanks—to enable the delivery of a bomb.
- Discovery of bomb-making factories, safe houses, safe havens, and weapons caches.
- Individuals with a suspected nexus to terrorism and training or background in explosives, blasting, electronics, electrical engineering, or chemistry.
- Unexplained presence of antidotes or bleaching material.
- Static surveillance (persons loitering: observing entry/exit/delivery protocols; access controls;, photographing, videotaping, or sketching diagrams of bases and critical facilities.
- Mobile surveillance (repeated slow vehicular drive-bys [typically with more than one occupant]; this may include videotaping or photographing facilities, perimeter security measures, and vehicle entry and exit clearance procedures).
- Suspicious attempts to gain employment at critical facilities, with their security units or with outside vendors with access to the base.
- Attempts to recruit insiders to support terrorist attack planning or execution.
- Prevalence of computer network attack or exploitation (scans, probes, downloads, Internet protocol mapping efforts into sector networks and systems by country and address).

THREAT, CRITICALITY, AND VULNERABILITY ASSESSMENTS

5-10. The AT officer, with the support of the various staff elements, specifically analyzes terrorist threat capability or the vulnerability and criticality of an asset to assist commanders in determining priorities for implementing AT measures. Because of the global threat of terrorism, commanders must be aware of the threat in phases of force generation operations, the movement to training or operational locations, and the threat against forces while maneuvering throughout the AO. Units are vulnerable in different ways and at different times throughout these phases. AT officers synchronize AT measures to enhance and support in-transit movement, the security of DOBs, and the maneuvering of forces in the AO.

5-11. Criticality assessments and VA are intended to be sequential. However, the criticality assessment can be conducted before, after, or concurrent with the TA. The VA should be conducted after the TA and criticality assessment to determine which critical assets are more vulnerable. Commanders can also use VA methodology for combat patrols and mission planning for assets that are not designated as critical, but that are still susceptible to terrorist actions. Staff officers incorporate these assessments as part of their running estimate.

CRITICAL ASSET LIST

5-12. The *critical-asset list* is a prioritized list of assets that should be protected; they are normally identified by phase of the operation and approved by the commander. These assets are of such extraordinary importance that their incapacitation or destruction would have a very serious, debilitating effect on operations (JP 3-07.2). Once the TA, criticality assessment, and VAs are complete, the staff presents the prioritized list of critical assets to the commander for approval. Competing demands for resources and mission requirements limit what is available to protect critical assets. Within a unit, the staff assists the commander in determining which assets are critical for mission success and recommends priorities for protection with available resources. The list will depend on the mission variables and should represent those assets that are most attractive to terrorist action. Critical assets can range from facilities barracks on a FOB to local infrastructure (HN power plants, wells, voting centers, government offices). Critical-asset list development may require establishing evaluation criteria (criteria associated with the CARVER analysis matrix) (see appendix E).

Defended-Asset List

5-13. The vulnerability and criticality assessments, when compared to the assessed threats, provide the commander with information to make decisions regarding which assets are most critical, which assets must have resources dedicated to their protection, and where the commander can accept risk. Not all assets listed on the critical-asset list will continuously receive protection. Critical assets with some protection from applied resources become part of the defended-asset list, which lists those assets from the critical-asset list prioritized by the commander to be defended with the resources available. (JP 3-01) This allows the commander to apply finite protection capabilities to the most vital assets. The defended-asset list is similar to mission-essential vulnerability areas on an installation or fixed-site facility and signifies those assets that could have a direct impact on mission failure or strategic setbacks. (See FM 3-37.)

COMPOSITE RISK MANAGEMENT PROCESS

5-14. CRM is the Army's primary decisionmaking process for controlling risk and the primary integrating process for all tasks within the protection warfighting function. To ensure that Army AT efforts operate in an environment that is as safe and efficient as possible, CRM is to be taken into account in AT protection planning, preparation, execution, and recovery (see DA Pamphlet 385-30 and FM 5-19). AT uses a holistic four-part assessment process (threat, criticality, vulnerability, and risk analysis) to outline potential protection gaps. Units assess threats, criticality, and vulnerability to provide the commander with a baseline to implement appropriate AT measures, and mitigate terrorist risk to unit operations, and enhance protection.

5-15. These assessments should be conducted sufficiently in advance of deployments to allow for updating AOR-specific training and developing security procedures, acquiring necessary materials, obtaining focused intelligence, coordinating necessary security augmentation forces, and requesting HN support. In addition to the operating base itself, assessments should address rest areas, refueling locations, and movement routes.

5-16. Leaders apply the CRM process (see table 5-1) by integrating the TA, criticality assessment, and VA to make conscious and informed decisions. These decisions may result in the commit of resources or enact policies and procedures that will mitigate the threat, define the residual risk level, or make risk decisions. Deliberate risk management allows the application of the complete process when time is not critical. Crisis risk management is conducted after or immediately preceding a terrorist attack by reviewing the situation using the CRM process. The key steps of CRM are—

- Identifying hazards (including the TA).
- Assessing hazards to determine threat capabilities (initial risk) and COAs (criticality assessment and VA).
- Developing controls and making risk decisions.
- Implementing controls to conduct activities that deter terrorist incidents, employing countermeasures to mitigate the effects of a terrorist incident and recovering from a terrorist incident.
- Supervising and evaluating.

5-17. Terrorists have demonstrated their ability to operate anywhere, and their actions against uniformed personnel are not limited to the battlefield. Soldiers and their families can become the victims of terrorist acts while enjoying block leave, conducting predeployment activities, or failing to comprehend their surroundings when navigating a foreign city. To mitigate terrorist opportunities, leaders must integrate the CRM process into every mission and operation and during all phases (planning, preparation, execution, and recovery).

5-18. Using the standard risk assessment matrix, probability and severity for each identified hazard are converted into a specified level of risk. This assessment is an estimate, not an absolute. It may not indicate the relative danger of a given operation, activity, or event. The overall levels of risk identified are listed on the bottom of DA Form 7566 (Composite Risk Management Worksheet) (see FM 5-19). Accepted residual risk should be approved at the appropriate level of command (see DA Pamphlet 385-30).

Table 5-1. CRM process

Step 1: Identify Hazards	*Step 2: Assess Hazards*	*Step 3: Develop Controls and Make Decisions*	*Step 4: Implement Controls*	*Step 5: Supervise and Evaluate*
• Mission analysis • Threat information collection ▪ UCC/ASCC/ DRU ▪ J-2/G-2/S-2 ▪ ISR plan ▪ Local • IPB process ▪ Define the battlefield environment ▪ Define the battlefield effects ▪ Evaluate the threat ▪ Determine threat COAs • Threat assessment ▪ Operational capability ▪ Intent ▪ Activity ▪ Operational environment ▪ Probability/ severity ▪ Threat matrix	• Criticality assessment ▪ Criticality matrix ▪ MSHARPP ▪ CARVER ▪ Prioritized list of assets ▪ Critical-asset list • Vulnerability assessment ▪ UFC guides ▪ Vulnerability matrix ▪ War-gaming ▪ METT-TC ▪ Threat/asset pairing • Risk analysis ▪ Evaluation of threat, criticality, and vulnerability ▪ Evaluation of response elements ▪ Risk analysis table ▪ Risk analysis graph	• Briefing to commander • Defended-asset list • AT plan/standing operating procedures • Physical security plan • Resourcing	• Force protection condition measures • Random antiterrorism measures • Rules of engagement • Suspicious activity • Reporting procedures • Incident management • AT exercises and training	• Situational/AT awareness • Leader involvement ▪ Precombat checks ▪ Rehearsals • Measures of performance • Measures of effectiveness
ASSESSMENT		**MANAGEMENT**		

Legend:

ASCC	Army service component command
AT	antiterrorism
CARVER	criticality, accessibility, recoverability, vulnerability, effect, and recognizability
COA	course of action
DRU	direct reporting unit
G-2	Deputy Chief of Staff for Intelligence
IPB	intelligence preparation of the battlefield
ISR	intelligence, surveillance, and reconnaissance
J-2	intelligence director (joint staff)
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civilian considerations
MSHARPP	mission, symbolism, history, accessibility, recognizability, population, and proximity
S-2	intelligence officer
UCC	unified combatant command
UFC	unified facilities criteria

MILITARY DECISIONMAKING PROCESS

5-19. The *military decisionmaking process* is a planning methodology that integrates the activities of the commander, staff, subordinate headquarters, and other partners to understand the situation and mission, develop and compare COAs, decide on a COA that best accomplishes the mission, and produce an operation plan or order for execution. The MDMP helps leaders to apply thoroughness, clarity, sound judgment, logic, and professional knowledge to understand situations, develop options to solve problems, and reach decisions (FM 5-0).

Note. The joint force headquarters uses processes similar to the MDMP (see JP 5-0).

5-20. Commanders initiate the MDMP upon receipt or in anticipation of a mission. Commanders and staffs often begin planning in the absence of a complete and approved higher headquarters operation plan or order. Depending on the situation—commanders conduct design before, in parallel with, or after the MDMP. By doing so, Commanders are able to apply critical thinking to understand and visualize the terrorist threat and modify unit tactics and approaches to solving the problem.

5-21. The MDMP consists of seven steps as shown in table 5-2. This manual outlines each step of the MDMP, the various inputs, a method to conduct it, how AT supports each method, and outputs. The outputs lead to an increased understanding of the situation facilitating the next step of the MDMP. Commanders and staffs generally perform these steps sequentially; however, they may revisit several steps as they learn more about the situation, and before producing the plan or order. The MDMP drives preparation. Since time is a factor in all operations, commanders and staffs conduct a time analysis early in the planning process. This analysis helps them determine what actions are required and when those actions must begin to ensure that forces are ready and in position before execution (see FM 5-0).

Table 5-2. AT support to MDMP

Key Inputs	*MDMP*	*AT Support Actions*	*Key Outputs*
• Higher headquarters plan or order or a new mission anticipated by the commander	**Step 1: Receipt of Mission** **Warning Order**	❖ Develop terrorist estimate based on country and historical data. • Perform an initial threat assessment. • Determine legal restrictions. • Determine theater requirements.	• Commander's initial guidance • Initial allocation of time
• Higher headquarters knowledge and intelligence products • Knowledge products from other organizations ❖ **Terrorist-specific intelligence** ❖ **COCOM theater-specific AT requirements**	**Step 2: Mission Analysis** **Warning Order**	• Enhance IPB (terrorism). • Determine key AT tasks. • Conduct VA and criticality assessment. • Determine AT resource constraints. • Perform CRM process. • Generate AT-specific CCIR/EEFI. • Enhance ISR to look for terrorist and criminal activity. • Brief commander on terrorist influences.	• Problem statement • Mission statement • Initial commander's intent • Initial planning guidance • Initial CCIR and EEFI • Updated IPB and running estimates ❖ **Terrorist threat assessment** ❖ **Criticality/vulnerability assessment**

Table 5-2. AT support to MDMP (continued)

Key Inputs	*MDMP*	*AT Support Actions*	*Key Outputs*
• Problem statement • Mission statement • Initial commander's intent, planning guidance, CCIR, and EEFI • Updated IPB and running estimate	**Step 3: COA Development**	• Determine CAL and DAL. • Determine risk tolerance and risk mitigation for each COA (probability versus severity). • Brief the commander on key AT tasks that can be applied across all COAs.	• COA statements and sketches • Revised planning guidance
• Updated running estimates • Revised planning guidance • COA statements and sketches	**Step 4: COA Analysis**	• Assist the S-2 in developing terrorist COAs. • Assist the S-3 in developing defenses.	• Refined COAs • Potential decision points • Wargame results • Initial assessment measures
• Updated running estimates • Refined COAs • Evaluation criteria • Wargame results	**Step 5: COA Comparison**	• Identify advantages and disadvantages. • Develop recommended COA. • Refine COAs.	• Evaluated COAs • Recommended COAs • Updated running estimates
• Updated running estimates • Evaluated COAs • Recommended COA	**Step 6: COA Approval** **Warning Order**	• Assist with CCIR and EEFI AT updates. • Determine required resources to conduct the AT plan in support of the COA.	• Commander's selected COA and any modifications • Refined commander's intent, CCIR, and EEFI
• Commander's selected COA with any modifications • Refined commander's intent, CCIR, and EEFI	**Step 7: Orders Production**	• Write the AT plan. • Develop the AT portion of Annex F. • Conduct training and exercises.	• Approved operation plan or order ❖ AT plan/annex ❖ FPCON measures ❖ RAM planning ❖ Threat dissemination and mass notification ❖ Terrorist incident response annex to AT plan
❖ **Specific to AT**			

Table 5-2. AT support to MDMP (continued)

Legend:	
AT	antiterrorism
CAL	critical-asset list
CCIR	commander's critical information requirements
COA	course of action
COCOM	combatant command
CRM	composite risk management
DAL	defended-asset list
EEFI	essential elements of friendly information
FPCON	force protection condition
IPB	intelligence preparation of the battlefield
ISR	intelligence, surveillance, and reconnaissance
RAM	random antiterrorism measures
S-2	intelligence officer
S-3	operations officer
VA	vulnerability assessment

PREPARATION

5-22. *Preparation* consists of activities performed by units to improve their ability to execute an operation. Preparation includes, but is not limited to, plan refinement; rehearsals; intelligence, surveillance, and reconnaissance; inspections; and movement (FM 3-0). Preparation requires commander, staff, unit, and Soldier actions. Preparation creates conditions that improve friendly forces' opportunities for success. Some primary functions of preparation include—

- Improving situational understanding and AT awareness.
- Developing a common understanding of the plan (terrorist threat/incident response).
- Practicing and becoming proficient in critical tasks.
- Integrating, organizing, and configuring the force.
- Ensuring that forces and resources are ready and positioned (FPCON, RAM).

5-23. Because the force is often most vulnerable to attack and surprise while preparing, the emphasis on AT increases during preparation and continues throughout execution. AT measures and tasks are executed to protect essential elements of friendly information and to reduce vulnerabilities associated with the physical exposure of units that are training, rehearsing, moving, or positioning for deployment or upcoming operations. Establishing civil-military partnerships with organizations early in planning is a key activity of preparation, and it continues throughout execution. Allies and civilian agencies and organizations, including HN organizations, are frequently present before forces arrive and remain after forces depart.

5-24. Working with the S-2/S-3, the AT officer synchronizes with the ATWG on the evolving threat information obtained from the intelligence preparation of the battlefield. Based on new information collected through the intelligence, surveillance, and reconnaissance plan and friendly force reporting, the AT officer assists the commander in maintaining situational understanding of the current and estimated terrorist threat. The AT officer focuses on each phase of the unit's mission movement from home station, layovers en route, and occupation and mission execution in the forward operating location. Commanders synchronize with subordinate commands and use liaisons to enhance information sharing with higher headquarters.

5-25. The AT officer assists the commander in identifying resources necessary to protect the force. Preparation begins in unit training with the completion of AT training, rehearsing access control procedures, exercising incident management plans, and ordering equipment necessary to enhance physical security measures. Soldiers selected for supercargo operations review the rules of engagement in the protection of unit equipment.

EXECUTION

5-26. *Execution* is putting a plan into action by applying combat power to accomplish the mission and using situational understanding to assess progress and make execution and adjustment decisions (FM 3-0). In executing full spectrum operations, commanders anticipate and balance priorities among offensive, defensive, and stability or civil support operations. The operational theme and the operation's general characteristics dictate how the elements of full spectrum operations are combined to accomplish the mission.

5-27. Commanders and staffs, implement AT measures (FPCON levels, RAM, physical security barriers and devices to protect the force during full spectrum operations) (see table 5-3). BDOC commanders coordinate with tenant units and support agencies within the FOB. Exercises during operations will test vulnerabilities and the base ability to respond effectively to a terrorist attack. During execution, the staff ensures that operations progress successfully, identifying variances in the terrorist situation. AT officers assist the staff in reassessing the threat and vulnerabilities to the unit's ability to maintain combat power. In response to an actual attack, the commander, with the assistance of the AT officer and subordinate units, manages the consequences and that crisis, recovers and sustains operations, and conducts information operations to minimize the effect of terrorist information activities.

Table 5-3. Expanded operations process with AT support tasks

<table>
<tr><th></th><th>Plan</th><th>Prepare</th><th>Execute</th></tr>
<tr><td rowspan="2">AT Planning Tasks</td><td>AT Task 2. Collect, analyze, and disseminate threat information.</td><td>AT Task 3. Assess and reduce critical vulnerabilities.
AT Task 5: Maintain defenses.</td><td>AT Task 7. Plan terrorist threat/incident response planning.</td></tr>
<tr><td colspan="3">AT Task 1. Establish an AT program.
AT Task 4. Increase AT awareness.
AT Task 6. Establish civil-military partnerships.
AT Task 8. Conduct exercises, and evaluate/assess the plan.</td></tr>
<tr><td>AT Measures (AUTL 6.6)</td><td>Identify potential terrorist threats and other threat activities (AUTL ART 6.6.1).</td><td>Reduce vulnerabilities to terrorist acts and attacks (AUTL ART 6.6.2).</td><td>React to a terrorist incident (AUTL ART 6.6.3).</td></tr>
<tr><td>Integrating Process</td><td colspan="3">Composite Risk Management →</td></tr>
<tr><td>Control Measures</td><td colspan="3">Command and Staff Actions</td></tr>
<tr><td rowspan="3">• Operational design
• Commander's intent
• Planning guidance
• CCIR
• Assignment of missions
• Plans and orders
• ISR plan
• Graphic control measures
• Unit SOPs
• Information requirements
• SOFAs
• Legal considerations and constraints</td><td>MDMP/TLP
• Threat assessments
• METT-TC analysis
• Terrain analysis
• Task organization/ personnel requirements
• Resourcing</td><td>• Vulnerability and criticality assessment and risk analysis
• Probability versus severity
• Movement
• Predeployment site survey
• CAL and DAL
• Training/rehearsals</td><td>Rapid decisionmaking and synchronization process
• Mitigate terrorist acts
• Adjust CCIR
• Physical security and entry control</td></tr>
<tr><td colspan="3">Continuous Assessment
(Monitor and Evaluate Measures of Effectiveness/Performance)</td></tr>
<tr><td colspan="3">Warfighting Functions →
Supporting Processes →
• IPB • Targeting • ISR synchronization • Knowledge management
Continuing Activities →
• Security operations • Information tasks • Liaison and coordination</td></tr>
</table>

Table 5-3. Expanded operations process with AT support tasks (continued)

Legend:	
ART	Army tactical task
AT	antiterrorism
AUTL	Army universal task list
CAL	critical-asset list
CCIR	commander's critical information requirements
DAL	defended-asset list
IPB	intelligence preparation of the battlefield
ISR	intelligence, surveillance, and reconnaissance
MDMP	military decisionmaking process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
SOFA	status-of-forces agreement
SOP	standing operating procedure
TLP	troop-leading procedure

ASSESSMENT

5-28. *Assessment* is the continuous monitoring and evaluation of the current situation, particularly the enemy, and progress of an operation (FM 3-0). Assess is a continuous activity of the operations process and an activity of mission command. Assessment plays a critical role in the AT program and is supported by assessments (TA, criticality assessment, VA, and risk [see chapter 3]) to evaluate a unit's security posture when dealing with a terrorist or irregular threat. Commanders, assisted by their AT officer and staff, continuously assess the operational environment and the progress of operations. Based on updates or changes to the threat, vulnerability, or criticality assessment, commanders direct adjustments, thus ensuring that the operation remains focused on accomplishing the mission while protecting the force, information, and equipment. Examples of change indicators within AT are—

- Indicators of enemy CBRNE use.
- Escalation of force incidents reports or other indicators of enemy IED use.
- Increased criminal activity in a given AO.
- Reports of the enemy targeting critical HN infrastructure.
- Identification of a threat to the base or sustainment facilities.

5-29. Commanders also assess the progress of the operations through the operation order, the common operational picture, observations of other friendly forces, running estimates, and the assessment plan that evaluates the measure of effectiveness, measures of performance, and reframing criteria. Because assessment is continuous, it requires prioritization, monitoring, and evaluation to ensure that required changes are implemented effectively without distracting the staff's ability to support ongoing operations.

5-30. Commanders can also assess their use of AT measures in protecting the force through evaluated measures of effectiveness and performance. A measure of performance helps determine whether a commander has applied enough, correct resources to an operation. A measure of effectiveness is useful in determining success and deciding whether a commander must maintain, adjust, or reallocate resources. Through a variety of mechanisms commander's can determine changes to their unit's AT posture, no matter how slight, to help in reducing vulnerabilities and aiding in Soldier vigilance.

5-31. To enhance assessment within brigades, battalions, and companies, the ATWG assembles key staff to consolidate and discuss emerging trends, issues, and impacts relating to events over various planning horizons. The group examines the assessment plan to ensure that measures of effectiveness, measures of performance, and indicators are still valid; determine whether updates to the TA, criticality assessment, VA, or risk analysis are necessary; and develop new measures and indicators as required.

5-32. Comprehensive AT program reviews determine the ability to protect personnel, information, and critical resources by detecting or deterring threat attacks or, failing that, to protect by delaying or defending against threat attacks. Commanders should conduct a self-assessment of their AT programs and the programs of their subordinate units after assuming command in conjunction with predeployment VAs, after

occupying a new base, when completing a change of responsibility, or when there are significant changes in threat, vulnerabilities, or asset criticality.

5-33. The self-assessment can use the Management Control Evaluation Checklist found in AR 525-13 or can use a locally developed checklist that meets the approval of the unit's higher headquarters (Army commands, ASCC, direct reporting units, or ARNG). The AT program review should focus on the essential AT elements and, as a minimum, assess the following functional areas:

- Physical security.
- Engineering.
- Plans, operations, training, and exercises.
- Resource management.
- Military intelligence.
- Criminal intelligence.
- Information operations.
- Law enforcement.
- Threat options.
- OPSEC.
- Medical.
- Protection of executives and HRP.

5-34. Vulnerabilities discovered by these assessments identify the areas to mitigate risk or enhance their security posture. Commanders and staffs should develop a mechanism to track program vulnerabilities, with a plan to reduce their exposure, and report their findings to their higher headquarters or by populating the Core Vulnerability Assessment Management Program where applicable.

This page intentionally left blank.

Chapter 6
Antiterrorism Officer in the Force

This chapter examines the roles and responsibilities of the AT officer within the Army, focusing on the support to the operational Army and synchronization with the protection warfighting function. Because the types of threats faced by expeditionary units vary greatly from one geographic location to another and throughout full spectrum operations, AT plays a critical role in the protection of assets (people, infrastructure, information) within the commander's AOR. The AT officer serves as the lead in assisting the commander and in preparing the unit to defend against acts of terrorism while intransit or on deployment.

ROLES AND RESPONSIBILITIES

6-1. The AT officer serves as the commander's principal staff assistant for matters concerning potential terrorist activities against the unit. As a member of the operations section, the AT officer serves as the focal point and subject matter expert for coordinating plans and procedures governing AT, including physical, informational, operational, personal, and infrastructure security. Within the commander's intent, the AT officer directs the development, implementation, and operation of an integrated AT program, helps fuse intelligence and criminal information, and guides crisis management planning and execution in the event of a terrorist attack. The AT officer also serves as a member of the Installation Design Team in support of organizational decisions affecting real property and security engineering requirements in support of new construction projects and 50 percent renovation, addition, or conversion-of-use projects. (See UFC 4-020-01.)

6-2. As the lead for the ATWG, the AT officer provides planning advice to the commander on the resolution of complex vulnerabilities, crisis management, and possible threats to the unit based on information from the meetings. The AT officer evaluates the effectiveness of the command AT program and prepares the foundation for enhancing the relationship among Army forces, HN civil authorities, and units within the AO. In conjunction with the planning cell, the AT officer formulates and coordinates matters pertaining to the protection and security of personnel, property, and materiel against terrorist threats.

6-3. As an effective staff officer, the AT officer provides the commander with accurate, timely, and relevant information and well-analyzed recommendations in regard to FPCON and RAM. This helps the commander minimize unnecessary risk. The AT officer assesses hazards related to terrorist activity and recommends controls to reduce or eliminate unnecessary risks through the proper posturing of subordinate units.

6-4. The AT officer should be a graduate of an AT officer Level II training course certified by Army Training and Doctrine Command and is responsible for providing the commander with information and recommendations within the parameters of the AT program. In most units or activities, being an AT officer is an additional duty for personnel serving in the operations section, but should be considered a full-time position at higher levels and during major operational deployments. The AT officer assists the commander in accomplishing the tasks associated with AT, using the AT principles as a framework to guide his efforts (see figure 6-1, page 6-2).

6-5. The AT officer relies on the combined expertise of the entire headquarters staff to develop effective AT plans and to coordinate and integrate AT measures throughout the command's units and actions. Such expertise includes the command public affairs office, which can assist in community awareness; the

command intelligence staff, which supports understanding of the specific terrorist threat throughout the AOR and AO; and the command logistics, maintenance, and contracting staffs, which ensure that AT measures are included in mission areas and support functions.

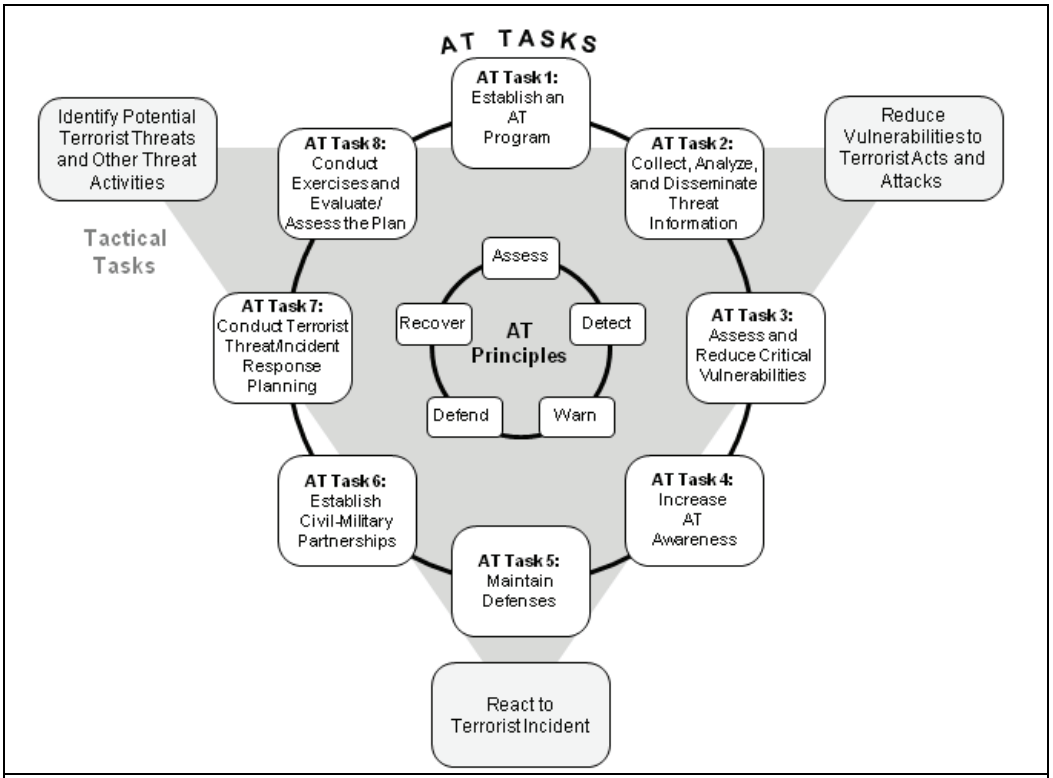


Figure 6-1. AT tasks and principles

ECHELONS ABOVE CORPS

6-6. Army commands, ASCCs, and select direct reporting units contribute to the Title 10, U.S. Code, and support of Army organizations through a variety of controls that allow these headquarters to better anticipate the needs of commanders and prepare forces before their deployment or the execution of missions in the AO. Their authority includes the ability to assess, deter, detect, defend against, prevent, and mitigate terrorist activities. (See FM 3-0.)

6-7. The combatant command (command authority) exercises tactical control for force protection, which may be further delegated to ASCCs that are over DOD elements and personnel within the combatant commander's AOR. ASCCs typically exercise authority for force protection over Army personnel (including their dependents) assigned, attached, transiting through, or training in the ASCC AO, except those for personnel or units over which the combatant commander retains security responsibility. This authority enables the ASCC to change, modify, prescribe, and enforce protection measures for covered forces according to the combatant commander's guidance.

> ***Note.*** Transient forces do not come under the chain of command of the area commander solely by their movement across operational area boundaries, except when the combatant commander or ASCC is exercising tactical control authority for force protection purposes.

6-8. ASCCs play a critical role in the fight against global terrorism. The theater of operations is the first level of command with a dedicated AT and protection division that adds an in-theater source of staff

support for subordinates. Combatant command (command authority) and the ASCCs typically resource the protection warfighting function to support Army forces in the theater of operations and joint and multinational forces. ASCCs facilitate regional counterterrorism operation and consequent management efforts with little notice to engage terrorist forces offensively in a suspected safe haven or to respond to the results of a catastrophic terrorist attack. ASCCs provide terrorist threat situational awareness to deploying forces, and they provide operational experience in the area to assist in solving ground force issues. More critical to successful land force operations is the ASCCs' partnerships within their geographic area that facilitate the protection and use of key infrastructure and facilities (ports, airbases) to support inbound force projection and areas to launch future operations.

6-9. At theater command and ASCC levels, AT planning and actions focus on understanding and tracking the terrorist threat and terrorist activities—including regional and transnational groups—and coordinating with the HN to leverage the full support of the HN security forces. Theater and ASCC orders and directives for AT focus on information sharing, AOR-specific AT training and readiness requirements, and resources required to meet the urgent needs of operational forces.

6-10. The AT officer within the protection division supports the ASCC's inherent AT responsibilities by integrating the Army universal task list tasks, AT tasks, and AT principles into the command operations and intelligence processes to support forces operating within their AO by—

- Ensuring that AT programs and procedures include specific prescriptive standards to address specific terrorist capabilities and geographic settings, particularly regarding infrastructure critical to mission accomplishment and other DOD-owned, -leased, or -managed mission-essential assets.
- Providing AT planning information (airfield, port, and movement route information and threat; vulnerability and criticality assessment data) to deploying units to enable them to manage risk and develop a tailored AT appendix within Annex F of the operations order.
- Incorporating AT into plans, orders, and publishing guidance to subordinate elements for the execution of AT measures, including FPCON and RAM implementation.
- Developing and implementing site-specific FPCON measures for stationary and in-transit units. The development of site-specific FPCON measures must account for sufficient time and space to determine hostile intent while considering constraints imposed by the standing rules of engagement and the standing rules for the use of force.
- Ensuring that FPCON procedures are in place to notify organic, tenant, and supported units of FPCON changes and transition procedures.
- Ensuring that policies and procedures are in place to identify and designate incumbents of high-risk bullets and HRPs (see DODI O-2000.22), providing supplemental training, as required, to personnel and their families assigned to high-risk bullets or designated HRPs.
- Assessing and reviewing (periodically) the AT programs of assigned and attached DOD components in their AOR.
- Tracking movements of 50 or more personnel into or through significant or high-threat areas and providing terrorist threat information, indications, and warnings.
- Ensuring that Soldiers, Army civilians, and Army contractors authorized to accompany the force have received applicable AT training and briefings upon arrival in their AOR.
- Establishing command relationships and policies for subordinate commands, including joint task forces, to ensure that effective mechanisms are in place to maintain protective posture commensurate with the terrorist threat.
- Assessing the terrorist threat and providing TA information to the DOD components and the commanders in the AOR.
- Developing risk mitigation measures and maintaining a database of those measures and the issues that necessitated their implementation.

- Keeping subordinate commanders informed of the nature and degree of the threat, ensuring that commanders are prepared to respond to changes in threats and local security circumstances, and ensuring that the commanders are fully and currently informed of threat information relating to the security of those DOD elements and personnel under their responsibility, but not under the command of the combatant commander.
- Ensuring that a capability exists to collect, receive, evaluate, analyze, and disseminate relevant data on terrorist activities, trends, and indicators of imminent attack, and developing and implementing the capability to fuse biometrics-enabled intelligence and suspicious activity reports from military security, law enforcement, and CI organizations with national intelligence, surveillance, and reconnaissance collection activities.
- Assembling AT program review assessment teams comprised of individuals with sufficient functional expertise to satisfactorily assess and evaluate (using measures of performance and effectiveness) the effectiveness and adequacy of AT program implementation within their subordinate commands.

CORPS AND DIVISIONS

6-11. Corps and divisions serve as modular entities designed to control forces tailored for specific joint operations. Corps serves as a command headquarters, a joint task force, or an intermediate tactical headquarters within large groupings of land forces. Divisions are structured for the tactical control of brigades during land operations or, with appropriate joint augmentation, can serve as a joint task force or land component command headquarters for small contingencies. This modularity creates the ideal C2 for the unified action necessary in IW and combating terrorism.

6-12. AT planning and actions at the corps level and below are tailored to the specific terrorist threat and operational environment. Staffs at this level provide focus and direction for AT by integrating the AT tasks and principles throughout their operations and by employing their organizational capabilities and assets.

6-13. Corps and divisions have established protection cells designed around the protection warfighting function. The AT officer supports the corps and division chiefs of protection by integrating the Army universal task list tasks, AT tasks, and AT principles into the command's operations and intelligence processes by—

- Exercising operational control or tactical control for force protection responsibilities by establishing AT guidance and programs for assigned Army or DOD elements and personnel, including the assessment and protection of facilities and the appropriate level of AT training and briefings.
- Planning, coordinating, synchronizing, and integrating AT capabilities and guidance with joint, interagency, and multinational assets within the protection cell for assigned organic Army elements (or DOD elements when acting as a joint task force).
- Coordinating with the geographic combatant commanders to ensure the adequate AT protection of in-transit and deployed forces operating in the combatant command's AOR; receiving terrorist threat reporting assessed by the combatant command and ASCC; and providing TA information and designated FPCON to the DOD components, multinational forces, and commanders in the AOR.
- Raising the local FPCON above the higher-level commander's FPCON for personnel and assets for which they have AT responsibility. AT officers cannot lower the local FPCON below the higher-level FPCON without the commander's written concurrence.
- Developing and implementing site-specific FPCON measures for stationary and in-transit units. The development of site-specific FPCON measures must account for sufficient time and space to determine hostile intent, while considering constraints imposed by the standing rules of engagement and the standing rules for the use of force.
- Ensuring that FPCON procedures are in place to notify organic, tenant, and supported units of FPCON changes and transition procedures.

- Ensuring that a capability exists to collect, receive, evaluate, analyze, and disseminate relevant data on terrorist activities and trends and provide indications and warnings of imminent attack.
- Identifying potential protection requirements for those corps or division commanders who are designated a high-risk bullet or HRP during operations.
- Informing the commander of changes or terrorist threats to critical-asset lists and defended-asset lists.
- Monitoring OPSEC actions at all levels.
- Reviewing terrorist threat/incident response plans, especially in regard to mitigating the effects of CBRNE.
- Overseeing the construction of FOBs and overseeing physical and area security operations in relation to the terrorist and nonstate actor threat.

BRIGADES AND BATTALIONS

6-14. The brigade combat team (BCT) is the basic building block of the Army's tactical formations, complemented by the addition of modular support brigades to create tailored, readily available expeditionary force packages that enhance the Army's flexibility and responsiveness. Battalions compose BCTs or serve in direct support of corps, divisions, and Army headquarters, serving as the lowest support headquarters to maneuver forces. These elements execute early-entry operations to close with the enemy; and they assist in preventing, containing, stabilizing, or resolving conflicts. Brigades and battalions are not organized with dedicated protection cells, but are still responsible for integrating protection functions and AT measures into operations.

6-15. The AT officer, serving in the brigade or the battalion S-3 section, works with higher and lower echelons to integrate the eight AT tasks within the three tactical tasks outlined in chapter 3 and may perform duties as a protection coordinator, bringing together other protection activities to support brigade and battalion operations. To provide AT focus to operations, the AT officer—

- Focuses on AT measures throughout the AO and establishes the common operating picture for AT awareness and execution.
- Submits movement operations to higher headquarters for review and seeks threat, FPCON, and infrastructure guidance.
- Establishes local AT measures in support of security for FOBs, logistic bases, and staging areas in support of the current operation.
- Raises the local FPCON above the higher-level commander's FPCON for those personnel and assets for which he has AT responsibility. He cannot lower the local FPCON below the higher-level commander's FPCON without the commander's written concurrence.
- Ensures that FPCON procedures are in place to notify organic, tenant, and supported units of FPCON changes and transition procedures.
- Serves as a member of the division protection cell, the division protection working group, and the base ATWG.
- Highlights the commander's AT concerns and responds to taskings in support of division or base AT or incident response plans.
- Obtains the commander's intent and works with the deputy brigade commander or battalion executive officer and staff elements to procure equipment in support of the brigade or battalion AT measures and in support of brigade or battalion AT requests.
- Ensures that subordinate battalions have a functioning AT program within their units and disseminates analyzed and unit tailored AT or threat-related information from higher headquarters.
- Heads the ATWG and coordinates with the brigade or battalion staff to analyze vulnerability and critical infrastructure identified by the brigade or battalion (using critical-asset lists and defended-asset lists) within their AOR. Informs the commander of changes or terrorist threats to critical-asset lists and defended-asset lists.

- Coordinates locally with HN and government agencies (State Department and embassy or consulate personnel) when operating abroad.
- Works with the staff judge advocate to ensure that the legal considerations in response to AT measures are met; and helps develop consequence management battle drills and themes with the public affairs officer, foreign counterintelligence officer (S-7) sections and attached psychological operations detachments.

COMPANIES

6-16. The company's effectiveness increases with the synergy of its subordinate elements. These components have a broad array of capabilities; individually, however, they also have vulnerabilities. Companies are often colocated with their respective battalions for support, while others may be operating independently on a FOB or as part of a logistics base separated from their headquarters.

6-17. At the company level, there is no documented requirement for an AT officer or AT program, but a company does have the lowest staff level possible to appoint AT responsibilities as an additional duty. Companies receive AT guidance and terrorist threat information from their higher headquarters. The company supports the higher headquarters AT planning guidance and program and provides elements to support base defense, RAM, and incident response operations. The company implements measures when operating alone on FOBs through the FOB AT annex, but still receives threat updates and analysis, logistic support, and assessment support from its higher headquarters.

6-18. An enhanced, platoon-size element of 50 or more serves as the minimal planning factor for AT measure considerations, especially intransit to a deployed location, during training exercises, or operating independently on a FOB or COP. At the platoon and squad levels, AT awareness plays a crucial role in their survivability while operating in the AO. Because platoons and squads are not resourced with the same barrier or physical security measures to enhance their own security, they rely more heavily on an individual's ability to detect, deter, and defeat a potential terrorist act. Soldiers incorporate what they learn and are exposed to during individual training at home station; enhance their skills through team, squad, and company training; and test their ability to react to terrorist attacks during battalion exercises.

PROTECTION CELLS

6-19. At the division level and higher, the protection cell is generally responsible for integrating or coordinating the tasks and systems that fall under the protection warfighting function. Protection cells, through the designated protection chief, participate in MDMP and translate command guidance and the terrorist TA into protection strategies that are reflected in the essential elements of friendly information, critical-asset list, and defended-asset list. The protection cell advises commanders on the priorities for protection and coordinates the implementation and sustainment of protective measures to protect assets according to the commander's priorities. (See FM 3-37.)

WORKING GROUPS

6-20. Working groups are types of meetings and are included on the unit's battle rhythm. A working group is a grouping of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function. Working groups are cross-functional by design to synchronize the contributions of multiple cells and staff sections. For example, the ATWG brings together representatives of all staff elements concerned with AT. It synchronizes the contributions of all staff elements with the work of the protection cell.

PROTECTION WORKING GROUP

6-21. The protection working group is led by the protection coordinator. It normally consists of an air and missile defense officer, an AT officer, a CBRN officer, an engineer, an explosive ordnance disposal officer, an electronic warfare officer, an OPSEC officer, the provost marshal, an intelligence representative, and a representative of the assistant chief of staff, signal (G-6). The commander may add

staff officers from safety, inform and influence activities section, medical, and civil affairs offices, depending on the operational environment or type of operation. At the division level, subordinate units normally provide a liaison officer to the working group meetings. The protection cells in division, corps, and Army headquarters integrate protection functions into the operations process. In the BCT, division or corps orders specify protection requirements and tasks. Since no protection cell exists in the BCT, commanders normally designate a lead staff element, S-3, to perform these functions. (See FM 3-37.)

ANTITERRORISM WORKING GROUP

6-22. The ATWG is formed to oversee the implementation of the AT planning guidance; refine terrorism TAs; coordinate and disseminate threat warnings; conduct VA, criticality assessment, and CRM; refine the AT annex to the operations order; and address emergent or emergency AT issues. Within the operational Army, the ATWG can be incorporated at the battalion level and above and its functions are integrated into unit staff planning and operations sections. During the planning process, the ATWG provides input to the commander's MDMP by integrating the TA with the commander's essential elements of friendly information, critical-asset list, and defended-asset list. The intent is to identify and recommend refinements to the COA that are necessary to reduce vulnerability and ensure mission success. The ATWG provides vulnerability mitigation measures to help reduce risks associated with a particular COA and conducts planning and oversight for full spectrum operations that are specific to irregular threats. ATWGs are led by the commander or AT officer, staff representatives, CBRNE expertise, tenant unit representatives, and HN and/or multinational partners.

THREAT WORKING GROUP

6-23. The threat working group is organized and meets based on the level of terrorist threat activity to develop and refine terrorism TAs and coordinate and disseminate threat warnings, reports, and summaries. In light of the enduring threat of terrorism and the expeditionary nature of Army forces crossing combatant command (command authority) boundaries, formal ATWGs may be appropriate at the ASCC, but the organic operations and intelligence elements and processes replace the need for a separate organization at the tactical level unit.

This page intentionally left blank.

Appendix A

Metric Conversion Chart

This appendix complies with AR 25-30 which states that weights, distances, quantities, and measures contained in Army publications will be expressed in both U.S. standard and metric units. Table A-1 is a metric conversion chart.

Table A-1. Metric conversion chart

U.S. Units	*Multiplied By*	*Equals Metric Units*
Feet	0.3048000000	Meters
Pounds	0.4535900000	Kilograms
Metric Units	***Multiplied By***	***Equals U.S. Units***
Milliliters	0.0338140227	Fluid ounces
Millimeters	0.0393700000	Inches
Kilograms	2.2046000000	Pounds
Kilometer	0.6213700000	Miles

This page intentionally left blank.

Appendix B

Personal Protection Measures

Soldiers, contractors, and civilians play important roles in the success of the AT program. They are potential targets and victims of terrorist violence and are educated on personal security measures that help create a safe environment while they are working, traveling abroad, or residing at home. Personnel asset protection incorporates the AT principles of assess, defend, and warn. This appendix emphasizes measures that assist in protecting the strategic force for mission success in joint operation theaters.

INDIVIDUAL PROTECTIVE MEASURES

B-1. Terrorists generate fear through intimidation, coercion, and acts of violence (bombings, hijackings, kidnappings). Recent events have proven that terrorists have reached new levels of organization, sophistication, and aggression. Their tactics and techniques are constantly changing and continue to be a challenge.

B-2. Various operational environments have displayed well-calculated actions and planning, with U.S. personnel as the specific target. Individual protective measures are executed by Soldiers, civilians, and contractors to protect against terrorist attacks. (See Chairman, of the Joint Chiefs of Staff [CJCS] Guide 5260.)

B-3. Soldiers and civilian employees should not dress or behave in a manner that attracts the attention of criminals or terrorist elements. They should avoid publicity, refrain from going out in large groups, reduce the amount of American or military-specific clothing and displays of patriotic tattoos when traveling outside the United States, and evade civil disturbances and demonstrations. While overseas, Soldiers must learn and practice key survival phrases (*I need a police officer*, *I need a doctor*) in the local language.

B-4. While training, preparing for deployment, or serving overseas, personnel should vary their routes and departure/return times. The surveillance a subject or an installation can be difficult to accomplish if movements appear random and unpredictable. Physical training and personal exercise should be conducted with a partner or in a group at varying times and places each day. Deserted streets, running trails, and country roads should be avoided. Individuals should inform others of where they are going, what they are doing, and approximately how long they will be gone.

B-5. Personnel should remain alert to anything that appears suspicious or out of place. Personal information will not be provided over the telephone. Individuals who suspect that they are being followed should go to a preselected, secure area (such as a military base or police station) and immediately report the incident to the security force, law enforcement agency, or military police. In overseas areas without these agencies, suspicious incidents should be reported to the security officer or military attaché at the U.S. embassy. Personal details should only be given to individuals with verified identities. Suspicious persons loitering near offices or unauthorized areas should be reported, and complete descriptions of the persons and vehicles should be provided. Photographs may be discreetly taken with cellular phone cameras. Associates and unit members should be advised of destinations and anticipated arrival times.

ACTIVE-SHOOTER RESPONSE

B-6. Soldiers are more equipped to handle active-shooter and post terrorist incidents than average civilians and local nationals. Active shooters are individuals who are engaged in killing or attempting to kill people in confined and populated areas. In most cases, active shooters use firearms. There is usually no

pattern or method of victim selection. Active-shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm. Because active-shooter situations often occur for 10 to 15 minutes, individuals must be mentally and physically prepared to cope with them before law enforcement personnel arrive on the scene.

B-7. AT awareness training measures, warrior task training exercises, basic first aid techniques, and battle drills facilitate a difference on and off the battlefield. Soldiers who survive an active shooter or terrorist incident or are in proximity of the aftermath of either incident may notify first responders and assist in providing detailed information to investigators. Soldiers can apply basic first aid to victims and use cellular telephones to call for assistance or to photograph criminal evidence before the area is disturbed. The dispatcher or law enforcement personnel should be informed of the—

- Active-shooter locations.
- Number of shooters involved.
- Active-shooter physical descriptions.
- Number and types of weapons involved.
- Number of potential victims.

B-8. Effective practices for coping with an active shooter or a terrorist situation include—

- Being aware of the environment and possible danger.
- Noting the two closest exits.
- Remaining in offices or rooms and securing the doors.
- Taking the active shooter down as a last resort.

Note. When the shooter is at close range and escape is not an option, survival chances are greater if the shooter is incapacitated.

B-9. Lead officers and NCOs must quickly determine the most reasonable way to protect their own lives. When dealing with active-shooter or terrorist events, lead officers and NCOs should—

- If evacuation is possible—
  - Establish an escape route.
  - Evacuate the premises.
  - Leave belongings behind.
  - Help others escape.
  - Prevent individuals from entering areas where the active shooter may be present.
  - Keep hands visible.
  - Follow police officer instructions.
  - Do not move wounded individuals.
  - Notify law enforcement personnel when safety is reached.
- If evacuation is not possible, shelter in place by securing a hiding place that—
  - Is out of the active shooter's view.
  - Provides protection from gunfire.
  - Does not restrict movement.
  - Can be locked or blockaded against entry.
- If the active shooter is nearby—
  - Lock the doors.
  - Silence cellular telephones and pagers.
  - Turn off radios and televisions.
  - Hide behind large items (cabinets, desks).
  - Remain quiet.

- If evacuation and hiding are not possible—
  - Remain calm.
  - Dial 911 if speaking is impossible, leave the line open and allow the dispatcher to listen.
  - Adapt responses to the types of weapons used by the attacker.
  - Take action against the active shooter as a last resort and when life is in imminent danger.
  - Act aggressively against the shooter.
  - Throw items and improvised weapons.
  - Yell.
  - Commit to his actions.
  - Cooperate with first responders.
  - Remain calm, and follow instructions.
  - Put down items in your hands.
  - Raise your hands, and spread your fingers.
  - Avoid quick movements.
  - Do not cling to emergency personnel.
  - Do not point, scream, or yell.
  - Evacuate in the direction in which the first responders are entering.
  - Provide key information (the location of the active shooter, the number of shooters, a physical description of the shooter, the number and type of weapons held by the shooter, and the number of potential victims).

CULTURAL AWARENESS

B-10. Cultural awareness is essential to the basic mission of every individual and unit that operates OCONUS. Being familiar with HN customs facilitates better communication and understanding and reduces the likelihood of criminal and terrorist attacks spurred by actions that foster hatred toward the United States. Cultural awareness benefits military personnel and their families as they live and operate OCONUS and protects Soldiers and units that conduct operations, visits, and reconnaissance.

B-11. Knowing some of the basic tenets of a foreign culture is a critical component of ongoing contemporary operations. Commanders and staffs who understand and incorporate cultural considerations into planning and operations significantly improve unit effectiveness during operations. Cultural awareness is similar to situational awareness. Situational awareness can lead to situational understanding, and cultural awareness can lead to cultural understanding.

B-12. Situational awareness is to know what is happening around you, and situational understanding is to understand why things are happening around you. The key variable leading from situational awareness to situational understanding is experience. An observer, analyst, or operator who maintains situational awareness will develop situational understanding over time. The same relationship between cultural awareness and cultural understanding is possible if individuals, leaders, and units prepare and incorporate cultural considerations into all aspects of training for, planning, and conducting operations in the AO. Commanders and staffs deployed to Iraq, Afghanistan, and throughout Africa validated the necessity of cultural predeployment training and the need to incorporate cultural aspects into planning and conducting operations. Commanders and staffs prepare Soldiers for operations in environments through TAs, intelligence, crime data, and historical research. When operating in austere environments, Soldiers must remain in a heightened state of alert. The use of buddy teams when living and traveling in these environments assists in protecting personnel from potential terrorist and criminal attacks.

B-13. Culture is a shared set of traditions, belief systems, and behaviors. It is shaped by factors (history, religion, ethnic identity, language, nationality) and evolves in response to various pressures and influences. It is not inherent; it is learned through socialization. A culture provides a lens through which its members see and understand the world. Religion, perception, and language help military planners find centers of gravity and critical vulnerabilities. They also assist in operation planning and resource allocation.

B-14. Cultural awareness is the ability to recognize and understand the effects of culture on values and behaviors. In the military context, cultural awareness can be defined as the cognizance of cultural terrain for military operations and the connection between culture and warfighting. Cultural awareness involves considering cultural terrain in military operations, knowing the cultural factors that influence a given situation, and obtaining a specified level of understanding for a target culture.

B-15. Commander and staffs must consider cultural awareness when conducting training for Soldiers. This includes—

- Using basic language skills to help Soldiers gain the respect and trust of local citizens.
- Using appropriate greetings and interrogatives to build relationships.
- Understanding ethnic and sect differences to help Soldiers interpret daily events.

HOSTAGE PREVENTION

B-16. U.S. Army personnel participate in worldwide operations that can result in detention by unfriendly governments or captivity by terrorist groups. There has been a significant increase in recent years of American and foreign kidnappings by terrorist and insurgent organizations. In many cases, the victims were eventually released, but gruesome images of torture and execution strengthen the realization that hostage prevention must be taken seriously. (See CJCS Guide 5260, DOD Directive (DODD) 1300.7, DODI 1300.21, and DODI 1300.23.)

B-17. U.S. Army personnel who are captured by terrorists or detained by hostile foreign governments are often held for individual exploitation, U.S. government influence, or both. Each form of exploitation is designed to assist foreign-government or terrorist captors. In the past, terrorists and governments exploited detainees for adversary information, including confessions to crimes that were never committed. Governments have also been exploited to make damaging statements about themselves or to cause them to appear weak when compared to other governments. Governments have paid ransoms for terrorist captives. These payments have amplified terrorist finances, supplies, and operations, often prolonging the terror created by terrorist groups. Ransom payments have become extremely popular for recent Somali pirates, who have taken critical supply ships hostage to obtain large ransom payments. The U.S. government policy states that it will not negotiate with terrorists.

B-18. The U.S. government makes every good-faith effort to obtain the earliest release of U.S. Army Soldier, civilian, and contractor detainees and hostages. Faith in one's country and its way of life, faith in fellow detainees and captives, and faith in oneself are critical to surviving with honor and resisting exploitation. The destruction of this faith is the assumed goal of captors who are determined to utilize a detention or hostage situation to maximize their advantage.

B-19. U.S. Army personnel must take every reasonable step to prevent exploitation of themselves or of the U.S. government. If exploitation cannot be prevented, the captive must take every step to limit exploitation as much as possible. Detained personnel are often responsible for their own release. Detainers may become disinterested in further attempts to exploit individuals who continually and successfully resist exploitation efforts. Detainees and hostages must determine which actions will increase their probability of returning home with honor and dignity. Military members who have done their utmost to resist exploitation in a detention or hostage situation uphold DOD policies, the founding principles of the United States, and the highest traditions of military service.

B-20. U.S. Army personnel should maintain their military bearing, regardless of the captivity or harshness of treatment. They should remain calm and courteous and project personal dignity, especially during capture and the early stages of internment. Discourteous, nonmilitary behavior seldom benefits the long-term interest of a detainee or hostage and often results in unnecessary punishment that serves no useful purpose. In some situations, this type of behavior jeopardizes survival and complicates efforts to gain the release of the detainee or hostage.

B-21. There are no circumstances in which a detainee or hostage should voluntarily give classified information or materials to those unauthorized to receive them. U.S. Army personnel held as detainees or hostages will protect classified information to the utmost of their ability. An unauthorized disclosure of

classified information does not justify further disclosure. Detainees and hostages must resist each attempt by their captor to obtain this information.

B-22. The Geneva Conventions of 1949 are the recognized standard of treatment for all captives during armed conflict, regardless of the characterization of the conflict. The Geneva Conventions offer agreed international standards for protection to civilians, contractors, correspondents, and others who have authority to accompany and support multinational forces. The basic protections available to prisoners of war under the Geneva Convention Relative to the Treatment of Prisoners of War may not be required during operations outside of a declared war. The provisions of the Geneva Conventions affording prisoner-of-war protection apply only during declared war or international armed conflict. In conflicts not of an international character, combatants receive only the minimum protection specified in Common Article 3 of the Geneva Conventions. DODI 1300.23 provides for isolated personnel training DOD civilians and contractors supporting U.S. military operations. This summary provides some techniques and behaviors that complement those used by military personnel with whom they may be held.

B-23. U.S. military personnel detained by a hostile force or a terrorist during personal travel or military operation may be subject to the domestic criminal laws of the detaining nation. Lost, isolated, or captive Service members must be prepared to assess the dangers associated with being taken into captivity by local authorities. Their assessment of the dangers should dictate which efforts to take and what measure of force may be required to avoid capture, resist apprehension, and resist cooperation once captured. U.S. Army personnel must be aware of the following:

- Detained personnel must be extremely cautious of their captors. In addition to asking for a U.S. representative, detainees should provide their name, rank, Service number, date of birth, and the circumstances leading to their detention.
- Hostage takers have historically attempted to engage military captives in conversations concerning seemingly innocent, useless topic, and provocative issues. Discussions should be limited to, and revolve around health and welfare concerns, conditions of fellow detainees, and release efforts.
- Detainees should avoid providing information that can be exploited by the detaining government. Detainees who are forced to make statements or sign documents must provide as little information as possible and then continue to resist to the utmost of their ability.

CAPTIVITY BY TERRORISTS

B-24. Capture by terrorists is generally the least predictable form of captivity. The captor may qualify as an international criminal. The possible forms of captivity vary from a spontaneous kidnapping to a carefully planned and well-orchestrated hijacking. Hostages help determine their own fate. Terrorists often expect or receive no reward for providing good treatment of prisoners or for releasing victims unharmed. If U.S. military personnel are uncertain of whether captors are genuine terrorists or surrogates of another government, it should be assumed that they are terrorists. Tension levels are extremely high during the initial seizing of hostages. Both terrorists and hostages are most vulnerable at this point. Hostages should reduce tension by controlling emotions, following instructions, and avoiding physical confrontations. A sudden movement or action could precipitate a deadly response.

B-25. Obtain a passport to assist in blending in with other travelers and to delay the initial identification process in a hostage situation. Surrender the tourist passport if the terrorists demand identification during the initial stage, or delay providing identification as a U.S. military or official traveler by claiming an inability to locate the requested documents. However, do not lie when directly confronted about DOD status. The purpose of the initial delay is only to maximize survival during the initial stage.

- Portray yourself as an actual person (not merely an object) by conveying personal dignity and sincerity. Discuss nonsubstantive topics to convey human qualities and build rapport.
- Introduce commonalties such as family, clothes, sports, hygiene, and food.
- Listen to captors discuss their cause or boast.
- Address captors by name.
- Refrain from whining or begging.

- Introduce benign topics at critical times (impasses, demands) to reduce tension.
- Avoid emotionally charged topics (religion, economics, politics).
- Avoid being singled out as a result of being argumentative or combative.
- Circumvent escalating tension by avoiding stress-inducing language (*gun, kill*, *punish*).

B-26. Avoid signing confessions, making propaganda broadcasts, or conducting news interviews that could embarrass U.S. or host governments. Propaganda has been avoided by presenting logical reasons; however, the threat of death by terrorists for noncompliance is more realistic than in governmental detention. Do not mistake pride for inappropriate resistance. If forced to sign or make statements, degrade the propaganda and provide minimum information. Hostages should plan to be rescued. Hostages should—

- Leave fingerprints whenever and wherever possible.
- Inconspicuously deposit deoxyribonucleic acid (DNA) (in the form of drops of blood or hair strands with roots).
- Not hide their faces if photographs are taken because photographs provide positive identification and information.

B-27. In a rescue situation, hostages should—

- Seek safe areas that provide protection (under desks, behind chairs).
- Avoid doors, windows, and open areas.
- Drop to the floor if shelter cannot be reached.
- Keep his hands visible.
- Not attempt to help rescue forces.
- Not make sudden movements.
- Follow instructions that are given by the rescuers and expect rough treatment until rescue is fully accomplished.
- Relay information about the terrorists and other hostages to the rescue party.
- Keep faith with fellow hostages and behave accordingly.

B-28. Hostages and kidnapped victims who consider escape to be the only hope are authorized to make attempt. Escape from terrorists is risky, but may become necessary if conditions deteriorate to the point that the risks of remaining captive outweigh the risks associated with escape. These risks include torture, death, or the credible threat of death or torture. Hostages and kidnapped victims should begin planning for an escape as soon as possible to improve their chances of survival. This planning should include the passive collection of information on the captors, the strengths and weaknesses of the facility and its personnel, the surrounding area and conditions that could impact an escape attempt, and the items and materials within the detention area that may support an escape effort. The decision to escape should be based on careful consideration of the unique circumstances of the terrorist situation (an assessment of the current detention conditions, the potential for success, the risk of violence during the escape attempt, the potential retaliation if recaptured, the consequences for detainees who remain behind).

PREPARATION FOR EXTENDED ISOLATION

B-29. Soldiers, civilians, and contractors who operate within potentially hostile environments should protect themselves from kidnapping and extended isolation. Commanders and staffs must ensure that every Soldier, civilian, and contractor authorized to accompany the force are aware of the basic risk mitigation steps that can be taken for personal protection to accomplish the mission. These steps may include—

- Following local protection guidance to avoid hazardous situations.
- Developing a plan to communicate, flee, and fight.
- Developing a plan of action (including several backup plans) before departing a secure area.
- Being familiar with routes and maps.
- Ensuring that vehicles are reliable and have the necessary emergency equipment.

- Studying local customs and being alert to situations and changes in local behavior.
- Having a grab-and-go kit that includes a communications device (cellular telephone, radio), water, and basic first aid supplies.

Note. Consider including local clothing to assist in improvised disguises. A weapon with extra ammunition may also be appropriate if local conditions permit lawful possession.

- Having personal affairs in order.
- Preparing for potential isolation.
- Developing the will to survive and resist.
- Working with local military officials to—
  - Develop an emergency communications plan that provides connectivity to military or government support units. Include potential emergency contact ground-to-air signals, and ensure that personnel know how to implement the plan.
  - Maintain situational awareness. Blocked streets or individuals directing traffic down a side street could be funneling efforts for an ambush or an IED attempt.

PERSONNEL RECOVERY

B-30. Personnel recovery is the sum of military, diplomatic, and civil efforts to prepare for and execute the recovery and reintegration of isolated personnel. JP 3-50 is the overarching term for operations that focus on recovering isolated or missing personnel before becoming detained or captured and on extracting detained or captured personnel through coordinated and well-planned operations. Army component, corps, and division commanders establish a personnel recovery coordination cell to provide personnel recovery expertise within their AOs and with other components. Personnel recovery officers perform personnel recovery coordination functions at brigade level and below. Their responsibilities include—

- Ensuring reliable communications with subordinate units.
- Coordinating immediate recoveries for units.
- Gathering personnel recovery-specific information and disseminating it to subordinate units.
- Coordinating unit fire support and control measures.
- Ensuring that subordinate units have access to SOPs.
- Identifying subordinate unit personnel recovery equipment shortfalls to the personnel recovery coordination cell.
- Ensuring that sufficient evasion aids are available within subordinate units. (See FM 3-50.1.)

This page intentionally left blank.

Appendix C

Antiterrorism Exercises

Preparing for AT exercises is an important task that requires dedication and planning. Exercises are conducted to give leaders, staffs, Soldiers, and civilians realistic experiences to better accomplish tasks that are associated with AT. Realistic exercises allow personnel to be placed in fluid environments where critical decisionmaking is practiced to broaden the experience base and to identify areas or plans that need improvement. The commander should exercise physical security procedures by implementing AT measures. AT measures—

- Assist the organization in maintaining operational readiness.
- Provide the organization with a means to document and measure operational readiness.
- Validate capabilities identified in plans.
- Confirm training adequacies.
- Provide a means to assess and identify vulnerabilities and resources.
- Demonstrate a commitment to continuous AT improvement.
- Increase AT awareness.
- Provide a means to identify and prioritize AT and protection resources.
- Enable participants to fine-tune applicable skill sets.

PURPOSE OF EXERCISES

C-1. Limited training time requires leaders to select the most important tasks to sustain or improve, such as tasks that are essential to mission accomplishment and perishable without frequent practice. Because AT awareness and tasks support and protect units throughout full spectrum operations, it becomes critical to rehearse these tasks as part of regular unit training.

C-2. Commanders institute an exercise program that develops, refines, and tests AT response procedures to terrorist threats and incidents. This program ensures that AT is an integral part of unit operations and brings together multiple forces living and operating on one FOB under the direction of a single command, each with a responsibility to protect the force and aid in the recovery and functionality of that base after an attack. Exercises test the ability of small unit leaders to oversee the increase and decrease of FPCON measures, implement an effective RAM schedule, direct and coordinate response forces, and conduct incident management functions.

C-3. Conducting exercises allows commanders to achieve and sustain those mission-essential tasks associated with their AT guidance. Exercises create the ability to train commanders and staffs at all echelons in order to synchronize combat arms operations and implement mission command. Exercises also provide commanders with the ability to evaluate subordinates and subordinate units, test plans prior to real-world action or contact with terrorist elements, recognize shortfalls, and correct shortfalls prior to an attack. Through exercises, commanders enforce nested concepts and develop adaptive and agile leaders within their organization.

C-4. Commanders consider several key questions when selecting training exercises. As shown in figure C-1, page C-2, commanders refer to their training assessment before they start the exercise selection process to determine the following:

- What are the specific AT training tasks?
- What is the training audience for each specific AT training task?
- What is the overall training objective?

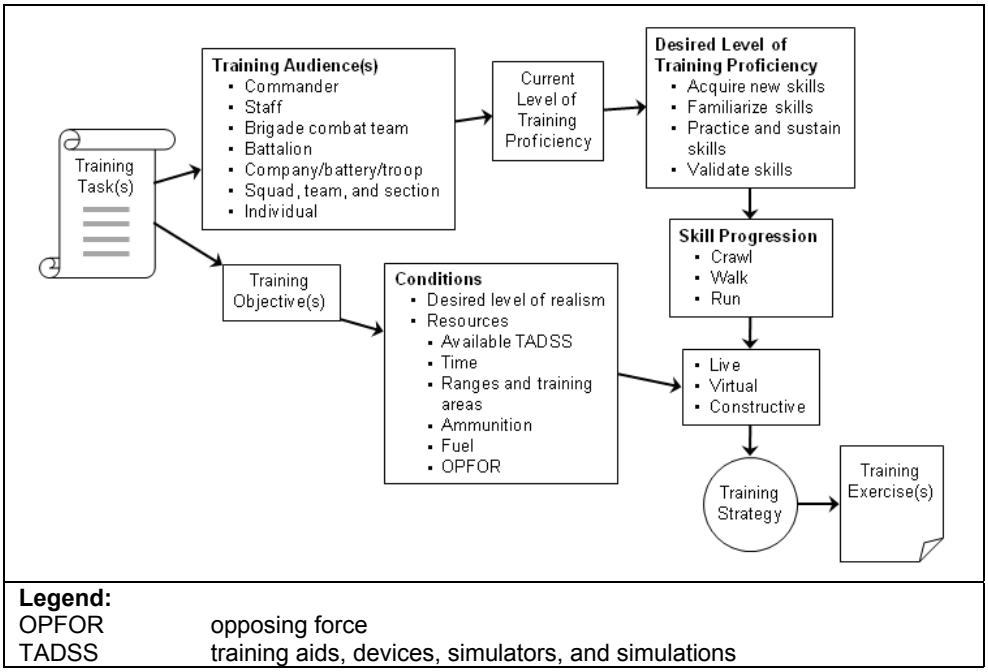


Figure C-1. Training exercise selection process

C-5. Once commanders identify the training audiences, they again refer to the training assessment to answer the following questions that help determine the training approach for any training exercise:

- What is the training audience's current level of proficiency?
- What is the required level of training proficiency for this training audience on this particular task? Is it to—
  - Acquire new skills?
  - Familiarize skills?
  - Practice and sustain skills?
  - Validate skills?

C-6. The crawl-walk-run technique is an objective, incremental, standards-based approach to training. Tasks are initially taught at a very basic level (crawl), then become increasingly difficult (walk), and finally approach the level of realism expected in combat (run). Training starts at the crawl stage. However, leaders first assess individual and unit training levels. Some individuals and organizations may be ready for the walk or run stage, depending on their experience.

C-7. Crawl stage events are simple to perform and require minimal support. This stage focuses on the basics of the task and proceeds as slowly as needed for individuals and the organization to understand task requirements. Walk stage training becomes incrementally more difficult. It requires more resources from the unit and home station and increases the pace and the level of realism. At the run stage, the level of difficulty for training intensifies. Run stage training requires the resources needed to create the conditions expected in the projected operational environment. Progression from crawl to run for a particular task may occur during a one-day training exercise or may require a succession of training periods.

C-8. In crawl-walk-run training, tasks and standards remain the same; however, the conditions under which they are taught change. Live, virtual, constructive, and gaming training enablers help provide the variable conditions for supporting a crawl-walk-run training strategy. Some ways to change conditions are—

- Increasing the difficulty of conditions under which tasks are being performed.
- Increasing the tempo of the training.
- Increasing the number of tasks being taught.
- Increasing or decreasing the number of personnel involved.

C-9. Trainers use the crawl-walk-run approach to determine the amount of detail to include in practice. If individuals or organizations are receiving initial training on a task, trainers emphasize basic conditions. If individuals are receiving sustainment training, trainers raise the level of detail and realism until conditions replicate an actual operational environment as closely as possible. Trainers challenge those with considerable experience to perform multiple training tasks under stressful conditions.

EXERCISE TYPES

C-10. Mission command requires competent, confident, adaptive leaders and Soldiers. It requires commanders to teach their subordinate commanders, leaders, and units how to train for mission command. Training for mission command requires the commander to train on the following elements of mission command:

- Commander's intent.
- Mission orders.
- Subordinates' initiative.
- Resource allocation.

C-11. A technique to train subordinates to understand the commander's intent (two echelons up) is to design training scenarios using nested concepts. Nested concepts provide the means to achieve unity of purpose, where each succeeding echelon's concept is nested in the other. Commanders who use nested concepts in training exercises provide an opportunity for subordinates to—

- Practice decentralized decisionmaking and execution.
- Exercise initiative within the commander's intent.

C-12. The nested concept method gives commanders—

- The opportunity to engage and exploit the talents and initiative of subordinate commanders and Soldiers at every level.
- An effective technique to train their subordinates in the use of the elements of mission command.

C-13. Training for mission command requires commanders and leaders to emphasize the use of mission orders along with nested concept training scenarios. Mission orders train subordinates to exercise initiative within the commander's intent. Commanders develop an environment of mutual trust and understanding that sponsors and fosters decentralized decisionmaking and execution. Additionally, commanders must—

- Underscore each subordinate's responsibility for the assigned mission in the context of the commander's mission, intent, and concept of operation.
- Help subordinates understand the leadership effect of combat power. Leaders decide where and when to generate the effects of maneuver, firepower, and protection.

C-14. AT exercises are similar in planning, preparation, execution, and evaluation to other training events and exercises conducted at various levels. The various types of exercises generally increase in the level of involvement and cost (see figure C-2).

- **Tactical exercise without troops.** A tactical exercise without troops is an exercise conducted in the field, on actual terrain suitable, for training units for specific missions. It is used to train subordinate leaders and staffs in terrain analysis, unit and weapons emplacement, and planning and executing the unit mission. This exercise would include the BCT commander and staff, subordinate battalion commanders and staffs, and separate BCT company commanders and senior NCO leaders.
- **Communications exercise.** A communications exercise to ensures that all units can communicate with one another across various types of communications equipment. It identifies shortfalls in communications equipment, especially when working with HN, multinational, and other partners who are not frequently assigned or attached to the higher headquarters. This exercise includes BCT and all battalion tactical command post (CP), main, and rear CPs and BCT separate company CPs and any HN, multinational, or attached units.

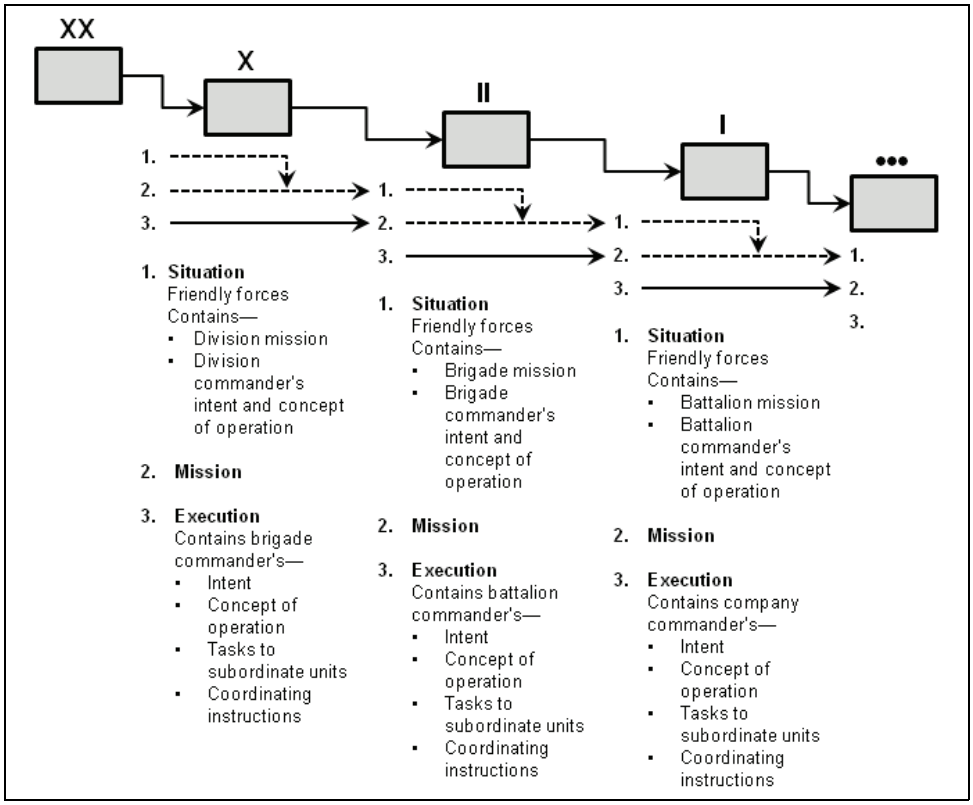


Figure C-2. Nested concepts within mission command

- **Command post exercise.** A command post exercise has simulated forces; it may be conducted from garrison locations or in between participating headquarters. This exercise includes BCT and battalion tactical CPs, main and rear CPs, and BCT separate company CPs. The training focuses on full staff interaction with higher, adjacent, supporting, and subordinate unit staffs, critical interactive staff processes, and Army Battle Command System and Force XXI battle command–brigade and below systems operator training.

- **Command field exercise.** A command field exercise is a conducted with reduced troop and vehicle density, but with full C2 and support units. The BCT executes AT measures developed during tactical exercises without troops and rehearsed during CP exercises. Participation includes—
  - Battalion leaders, down to and including platoon sergeants.
  - Battalion participation.
  - Criminal Investigation Division personnel (hostage negotiations, investigations).
  - First responders (medical and fire).
  - Quick-reaction forces.
  - Military intelligence and signal companies.

- **Tabletop exercises.** Also known as a *rock drill* or *sand table* exercise, this exercise involves the key leaders and staff officers of an organization or installation, gathered in one room or area. It is a scenario-driven discussion led by a facilitator and can be used to exercise specific portions of an AT appendix or the entire operation order itself. This exercise, depending on the scenario, can last for an hour or a full day. A tabletop exercise should be used when an AT appendix is new, as refresher training, or to familiarize new leaders with the AT appendix.
- **Drills.** Drills are collective training events that focus on selected functions, procedures, or portions of an AT appendix. For example, portions of an AT appendix that can be exercised to achieve limited objectives are CP exercises, notification drills, first-responder drills, and evacuation drills. Drills are scenario-driven events and are usually limited to specific organizations or functions in order to test, assess, and validate specific portions of a plan. They can last from 1 to 8 hours even longer, if necessary.
- **Full-scale exercise.** A full-scale exercise is the most complex AT exercise and will normally involve the entire organization and operating base. For many key organizations and tenant units, this event will be the major focus of training for the days and weeks leading up to it, as units activate portions or all parts of their AT measures. The exercise should be designed to test the elevation and reduction of FPCON measures and the planning and incorporation of RAM, including the operation of an access control point and barrier plan. The day-to-day functions of the operating base will most likely be impacted. To ensure a successful full-scale exercise, commands are encouraged to conduct a tabletop exercise and appropriate drills before conducting a full-scale exercise. This exercise requires the most planning and should be used to validate the AT appendix and timelines, assess functional capabilities and skills, identify gaps in security, and test equipment. It can last as long as several days.

ANTITERRORISM MISSION-ESSENTIAL TASKS

C-15. The Army universal task list assists commanders in mission-essential task list (METL) development by providing all the collective tasks possible for a tactical unit of company-size (and above) and staff sections. Commanders use the Army universal task list as a cross-reference for tactical tasks. They use it to extract METL tasks only when there is no current mission training plan for that echeloned organization, when there is an unrevised mission training plan to delineate tasks, or the current mission training plan is incomplete. For the tasks from the Army universal task list that are associated with AT (see figure C-3, page C-6).

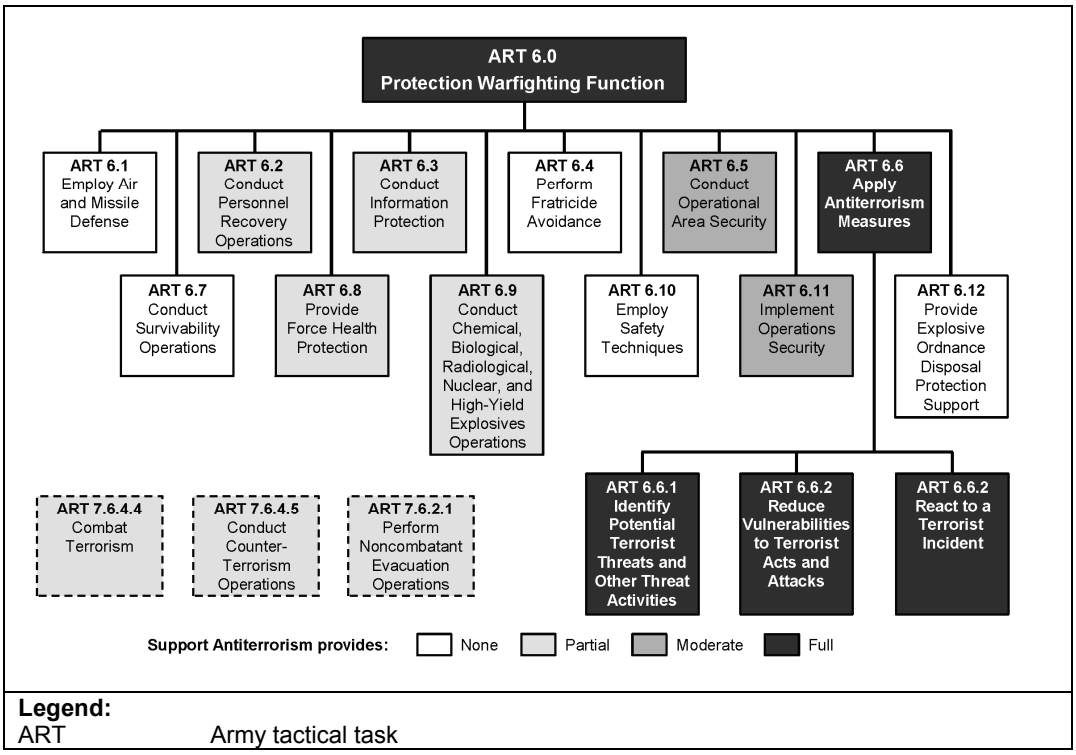


Figure C-3. Protection tasks within the Army universal task list

C-16. AT consists of defensive measures that are used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces. It is an element of protection. AT is a consideration for forces during military operations. To perform this function and mitigate risk and damage from terrorist attacks, the AT officer and commander implement AT measures to protect the force. These actions are fully supportive to tasks listed in Army Tactical Task 6.6 and are moderately and partially supportive to tasks found in other protection warfighting functions and operational themes.

C-17. Doctrine and other sources can provide additional information relating to a directed mission. These include—

- FM 7-15.
- CJCS Manual 3500.04E.
- AR 350-1.
- Combined arms training strategies and proponent-developed collective tasks and drills.
- Proponent-developed core METLs approved by Headquarters, Department of the Army.

EXERCISE PREPARATION

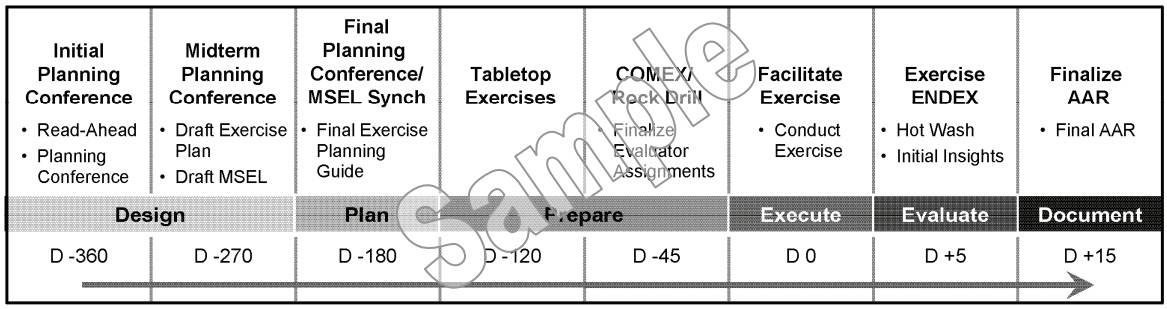
C-18. A successful AT exercise, like any other exercise or training event, requires thorough planning. Commanders and staffs should use Service-specific doctrine to plan an AT exercise. It is important to plan the training event far enough in advance so that it is does not conflict with other mission requirements, operations, and training events. Commanders must find ways to train while conducting current operations and to exercise forces in order to protect vulnerabilities, close security gaps, and reduce complacency. If the event is to achieve worthwhile training objectives, the commander must be involved in key decision points in the planning process, the first of which is to get the training event placed on the long-range training calendar. Some characteristics of an AT exercise include—

- Successful AT exercises are threat scenario-driven, guided by exercise controllers, with commander involvement and support.

- Drills may or may not have a threat scenario, depending on which function or portions of an AT appendix are being exercised. Commands must examine which key functions or portions of an AT appendix are key tasks that need to be exercised. They must ensure that tenant organizations, staffs, or subordinate units have properly trained and equipped those organizations to accomplish the tasks using Service-specific training methodology. Drills are excellent tools to train for and evaluate key functions and to validate the plan.
- Observer/controllers (O/Cs) are key players during exercises and should be identified and trained prior to the event. O/Cs should be able to move about freely during an exercise, to ensure that participants stay focused on the scenario, that they abide by the exercise rules, and that they assist in meeting the exercise objectives. In playing the role of the white hat, O/Cs will be in an excellent position to capture lessons learned and facilitate the AAR process.

ANTITERRORISM EXERCISE DESIGN

C-19. To have a successful AT exercise, commanders and planners should assign a planning team, and designate an officer in charge. This team should receive the commander's guidance to develop the scope of the exercise and the training objectives. Once the objectives are determined, the team should develop a work plan, with milestones to develop the exercise (see figure C-4). The format of the exercise, with corresponding staff and organizational responsibilities, should be tasked as early as possible to allow time to prepare. It is very important to plan the assessment process and means during the planning stages so that shortcomings can be identified and improvements can be tracked and accomplished. It is also important that the planning team and exercise developers not be participants in the actual exercise in order to maintain the level of surprise necessary for realistic training.



Legend:

AAR	after-action review
COMEX	communications exercise
ENDEX	end of exercise
MSEL	master scenario event list

Figure C-4. Sample timeline for exercise development

SCENARIO DEVELOPMENT

C-20. The operations/AT officer and intelligence officers work together to develop a realistic scenario that will set the conditions to achieve the training objectives. The threat scenario must be realistic and pertinent to the local TA. HN assistance can make significant contributions to scenario and threat development. Ensuring that valuable AT injects are developed is probably the most important task for action officers during the planning phase. That allows the training audience to experience a fluid operation that requires key AT staffing and decisions by leaders. The current TA should be used to develop a realistic scenario. For full-scale exercises, commands should consider a "red team" to fill the role of a terrorist organization. Identifying the red team early is critically important so that they can properly prepare and train for the event. Other considerations for scenario development are—

- The scenario development phase should produce several products, including a narrative, a timeline, and injects. Injects can be in many forms, some of which are messages, radio calls, or even physical actions. Creativity limited by realism during the inject development process should lead to a well-developed, challenging, and worthwhile exercise.
- Logistics and administrative coordination is essential to the success of the exercise. The staging of the event may require resources not normally on hand or may require initiative to acquire. Staging of events and the logistics associated with a terrorist act need to be considered and planned. Visual/audio support, access control to key O/C areas, and the control cell setup should be arranged. Finally, it is important to plan for basic items such as food, water, and latrine facilities for players and O/Cs. All of these requirements should be tasked to subordinate organizations or staffs.

CAUTION

Commanders and staffs must use extreme caution when conducting exercises or training in an operational environment, especially when making use of individual or crew-served weapons for realism.

C-21. The scenario should be articulated into a well-written exercise directive, with identified purposes of clear, focused tasks and predefined evaluation criteria. The directive is the foundation of the exercise. It must be produced far enough in advance for units to digest, plan, and train and to ensure that the exercise is worthwhile.

C-22. Once the scenario and directive have been developed, planners should create an exercise manual. It should contain the schedule, scope, objectives, inject timeline and implementation schedule, and ground rules of engagement. It should also contain scenario materials, contact information for key leaders and participants, the exercise directive for task organizations and units, and any other forms and records needed. Injects and some scenario materials should not be available to player units, or the exercise will lose realism. Portions of the exercise manual should be close-held documents, available only to key leaders, planners, and white-hat O/Cs.

THREAT RESOURCE

C-23. The Army Training and Doctrine Command G-2 Intelligence Support Activity (TRISA) produces a wide array of products and series of terrorism handbooks, available on digital video disc (DVD), that contain doctrinal information on contemporary threats and enemies in today's operational and institutional Army missions. The products support military members in operational units and installation/institutional activities. The threat material is intended to help commanders—

- Understand the operational environment and threat and emerging techniques of contemporary adversaries.
- Appreciate the operational threat across the Army community (leaders, Soldiers, DA civilians, families, and contractors, including those in institutional locations).

- Use the products to support training and awareness for the operational Army, forces intransit, and installation support activities.
- Integrate realistic threats into roleplaying, training readiness, institutional missions, and professional military education.

Note. A Military Guide to Terrorism in the Twenty-First Century is a primary Army reference guide prepared under the direction of TRISA. The guide is a capstone document for understanding the depth and breadth of the terrorist threat to U.S. forces. The guide should be used in conjunction with this chapter and the full series of threat products developed by TRISA.

EXERCISE CONDUCT

C-24. Exercises will have many players. The exercise coordinator (head O/C), other O/Cs, player units, and role players or red teams are key players. The exercise coordinator has overall responsibility for running the exercise and monitors the pace of events according to the scenario. The O/Cs observe individuals and unit or staff players to ensure that objectives are being met and to assess player responses to the scenario to compare them with expected responses and the predefined evaluation criteria. The O/Cs should also assist in tracking AARs.

Note. TRISA provides a standardized orientation and lessons for actors and roleplayer training. The target audiences is instructors and trainers of U.S. military forces and opposing forces, and other applicable trainers for interagency, intergovernmental, civilian-contractors, nongovernmental, private-volunteer and humanitarian-relief activities in training exercise design. The handbook presents an understanding of the operational environment, training unit mission, tools for trainers, outfitting and materiel, media affairs, and a training program concept for the training and development of role-players.

C-25. Before the exercise starts, several briefings occur to get everyone immersed in the training. Players are briefed on the scope of the exercise, the rules for the exercise, safety, and the roles of the controllers. Control cells are briefed and trained to run injects by message, telephone, simulators, or other predetermined means. Finally, role-players need to understand when their roles start and end and the purpose of their role-playing event.

C-26. Once the briefings are accomplished, it is time to start the exercise. The injects should be initiated according to the timeline and monitored by the exercise controller. Know who will need assistance in keeping track of time so that players are continually challenged. The planned timeline may need to be slowed down or sped up to keep the players constantly involved and engaged. A real AT event would be extremely engaging, and the exercise should attempt to simulate those conditions. The AT exercise ends when all injects have occurred, player units have accomplished responses, and training objectives have been met.

EXERCISE EVALUATION

C-27. The evaluation phase actually begins concurrently with the exercise. The exercise coordinator receives input on the enemy from the G-2/S-2. The enemy's perspective is critical to identifying why a unit succeeded or not. During formal AARs, the G-2/S-2 briefs what is known of the enemy's plan and intent to set the stage for discussing what happened and why it happened. Obtaining this data after operations is extremely difficult; therefore, these observations are often treated as assumptions rather than facts.

C-28. During their AAR, O/Cs accurately record what they learn about events (by time sequence) to avoid losing valuable information and feedback. O/Cs use any recording system that is reliable (notebooks and laptops, among others), and ensure that events are sufficiently detailed (identifying times, places, and names), and consistent. O/Cs and players should continually note and track AAR comments for consideration later. After the exercise, each echelon should conduct its own "hot wash" to capture lessons

learned and AAR comments. If the exercise lasts more than one day, it is usually a good idea to have a hot wash at the end of each day.

C-29. The exercise controller is responsible for collecting O/C input for the exercise AAR. The AAR is where significant execution shortcomings of the exercise and scenario is identified and discussed and a concept plan of action to fix each item developed.

C-30. AARs are the dynamic link between task performance and execution to standard. What actually occurred is placed against effective TTP, doctrine, and unit SOPs to correct deficiencies, sustains strengths, improve on weaknesses, and focus on performance of specific METL training objectives. Through the professional, candid discussion of events, Soldiers can identify what went right and what went wrong during the operation (using measure of effectiveness). When appropriate, they can evaluate their performance of tasks (using measures of performance).

C-31. The discussion helps Soldiers and leaders identify specific ways to improve unit proficiency. Units achieve the benefits of AARs by applying the results of them. Applications may include organizing observations, insights, and lessons; revising how the unit executes TTP; and developing future training. AARs may reveal problems with unit SOPs. If so, unit leaders revise the procedures and ensure that the unit implements the changes during future operations. Leaders can use the knowledge that AARs provided to assess performance, correct deficiencies, and sustain demonstrated task proficiency. These improvements will enhance unit performance in future operations (see FM 7-0, FM 6-01.1, and the Homeland Security Exercise and Evaluation Program for more detailed information on the AAR process).

C-32. Effective AARs require planning and preparation. During planning for an operation, commanders allocate time and resources for conducting AARs and assign responsibilities for them. The amount and level of detail needed during planning and preparation depend on the type of AAR and the resources available. The AAR process has the following:

- Plan.
- Prepare.
- Execute.
- Follow up (using AAR results).

C-33. AARs during operations differ from those during training. During operations, there are no dedicated collectors for data and observations. Instead, assessments of the operation's progress generated by the unit form the basis for the AAR. The AAR can be conducted in a variety of ways and depends on the size and unit level of the exercise participants. There are two primary methods of conducting an AAR:

- **Informal evaluations.** Informal evaluations occur when leaders evaluate unit training against established standards. Leaders follow an informal evaluation with an AAR or a critique, depending on the nature of the feedback to be provided. The informal AAR process is perfect during frequent stops in the exercise or action to serve as an on-the-spot coaching tool and to evaluate immediate performance measures during critical individual or collective tasks. Ideas and solutions gathered as a result of informal AARs can be immediately applied to the exercise as the unit continues training, enhancing Soldier understanding and aiding in unit proficiency.
- **Formal evaluations.** Formal evaluations involve dedicated evaluators and are scheduled in training plans. Normally, formal evaluations are highlighted during short-range training briefings. As much as possible, the headquarters that in two echelons higher performs formal external evaluations. For example, division commanders evaluate battalions, brigade commanders evaluate companies, and battalion commanders evaluate platoons. Feedback usually takes the form of an AAR followed by a written report. During and after formal evaluations, evaluators prepare their findings and recommendations. They provide these evaluations to the evaluated unit commander and higher commanders as required by the headquarters directing the evaluations. Formal AARs are usually accomplished after subordinate units have had an opportunity to conduct their own AARs and provide feedback during the backbrief to the unit commander. At the formal AAR, the facilitator reviews the collaboration that took place prior to the exercise and the METL tasks and goals that the unit had coming in the event. From there, the facilitator monitors the discussion by giving key

personnel the opportunity to speak and provide information relevant to determining unit strengths and shortfalls for further training development. The facilitator and staff propose recommendations to help strengthen the unit's performance in follow on exercises or during real-world deployments. Once the formal AAR is complete, the exercise staff officer should prepare a written AAR, complete with milestones and suspense dates to complete the required retraining, revision of the AT appendix, and resource acquisitions.

C-34. An AT exercise program for a unit conducting annual training, preparing for deployment, or participating in current operations can yield great benefits. AT exercises improve the AT appendix, AT SOPs, RAM execution, resource acquisition, program review, and increase awareness. Conducting an exercise is the best way to enhance base or organization AT programs and measures.

This page intentionally left blank.

Appendix D

Antiterrorism Measures in Operational Contract Support

The incorporation of AT considerations into commercial relationships with U.S. and foreign service providers is essential to enhancing the AT posture of operational forces in deployed environments. Contractors provide vital support and are part of the contingent for AT planning. Therefore, during the process to define contracted support requirements and during the contracting award, execution, and evaluation process, AT measures and actions should be considered, particularly when the contracted support could affect the security of DOD personnel. Contracting for goods and services is a normal, ever-expanding function within DOD. Contracted support presents AT security challenges that, if not addressed, could create seams and gaps in a unit's overall security profile. The federal acquisition regulations and associated supplements provide legal guidance used to establish federal government contracts and provide explicit directions for contract requirements, award, execution, and evaluation. AR 715-9 contains current policy and detailed how-to doctrine regarding operational contract support. At OCONUS locations, a status-of-forces agreement, memorandum of agreement, or other document prescribes guidance for the contracting process with regard to HN service providers. It is the responsibility of the requiring activity (for example, the command requesting commercially provided support) to incorporate AT security considerations into contract support requirements packages and local protection and base access plans. Unit AT officers should work closely with the higher-level unit AT officer, base security officer, and/or BDOC to ensure that AT-related security considerations are properly and legally incorporated into the base security policies and procedures and conveyed to the supporting contracting office. In turn, the contracting officer will ensure that there is a standard (base access) AT clause in each applicable contract. Each ASCC should enforce AT security guidance specific to the combatant commander AOR and/or joint operations area for the contract request process based on individual threat concerns and agreements with HNs.

ANTITERRORISM REQUIREMENTS DEVELOPMENT PROCESS

D-1. The decision to use contractors in an AO requires an assessment of the risks posed to the contractor and its employees and the potential impacts on the operation itself. Commanders must also consider the difficulties facing contractors when hostile action against them is likely. If failure of the contractor to provide the required support could jeopardize the overall success of the operation, contractor support may not be suitable.

D-2. Commanders must also consider the risk (insider threat) that a contractor could pose to the operation in terms of potential sabotage or other intentional overt or covert action (information gathering) by the contractor's employees. Commanders should consider the real possibility of direct or indirect actions taken against U.S. forces by contractor employees or individuals posing as contractor employees.

D-3. The requiring activity (the unit requesting contract support) commanders are responsible for ensuring that AT security measures are considered in the requirements development process. Each commander should develop area-specific AT security guidance and incorporate it into the AT appendix. This commander's guidance forms the core AT security criteria that is incorporated into local protection,

security, and base access policies and procedures. In turn, the supporting contracting office will incorporate these procedures via a standard contract clause requiring all contractors (including associated subcontractors) performing services on a military installation or near U.S. forces to follow local command protection, security, and base access measures.

D-4. Requiring activities need to closely consider any special AT security considerations related to contract support during the development of the requirements package. This risk assessment process related to contract support normally will lead to one of the following results:

- Acceptance of a level of AT risk and parameters.
- Change to the protection, security, and base access policies and procedures.
- Contract-specific AT measures (in some cases).

D-5. In the last case, the requiring activity may incur additional costs related to enhanced security measures. The requiring activity should follow the contract request support process as outlined in AR 715-9.

D-6. It is recommended that commanders develop an informal AT contract coordination and review team similar to the ATWG to manage contract development. The step-by-step process for incorporating AT security into contracts is discussed below and outlined in table D-1.

Table D-1. AT security measures in the contract support process

Step	*Major Task*	*OPR*
Step 1. Determine requirements.	• Determine contract support requirements. • Comply with applicable command guidance for requirements development. • Develop an acquisition-ready requirements package. • Obtain funding and approval for the requirements package.	Requiring activity and contracting officer
Step 2. Perform AT risk analysis.	• Conduct AT risk analysis. • Leverage local risk analysis information. • Determine risks associated with the contract. • Determine if current protection and base access procedures are sufficient to mitigate the risk of the contract. • Develop logistic alternatives, balanced with mission accomplishment.	Requiring activity support staff and AT officer
Step 3. Adjust AT security measures and/or develop contract-specific AT security measures in the requirements package.	• Develop specific AT security measures. • Leverage and/or modify security measures. • Develop a range of security measures, normal to advanced readiness postures. • Include AT security requirements in the performance work statement/statement of work and on DD Form 254 (Department of Defense Contract Security Classification Specification). • Consider linkage with the local FPCON system. • Balance security with the cost and benefits. • Ensure that the supporting contracting offices have current FPCON, security, and base access information applicable to contractors who are providing service on the base or near Army forces.	Requiring activity, commander, and AT officer

Table D-1. AT security measures in the contract support process (continued)

Step	*Major Task*	*OPR*
Step 4. Build and award the contract.	• Ensure that the AT risk assessment form is part of the requirements package, if required by the local command policy. • Incorporate contract requirements and security measures into the written contract via a standard clause and reference to appropriate contractor employee security and base access procedures. • Ensure that contract companies are vetted according to the local command policy before awarding the contract. • Award the contract.	Supporting contracting officer
Step 5. Perform contract oversight.	• **AT Officer.** Incorporate contract security requirements into the unit AT plan. • **COR.** Notify the AT officer that the contract is activated. • **AT Officer and COR.** Ensure that all AT security measures are in place before execution. • **COR and Contracting Officer.** Ensure contractor compliance with AT measures in the contract. • **AT officer and COR.** Periodically inspect AT security measures. • **AT Officer.** Review AT security measures if the local threat changes. • **All.** Conduct an annual, formal review upon contract renewal.	Supporting contracting officer/unit COR and AT officer

Legend:

AT	antiterrorism
COR	contracting officer representative
DD	Department of Defense
FPCON	force protection condition
OPR	Office of primary responsibility

STEP 1. DETERMINE THE REQUIREMENTS

D-7. The unit requiring the goods or service (the requiring activity) is responsible for identifying the specific contract requirement. The requiring activity works with the supporting contracting officer to ensure that the framework of the contract and scope of work are properly constructed in coordination with DOD, Service command, federal acquisition regulations, and contracting guidance. At this step, the unit should determine how essential this contract service is to mission accomplishment. The following questions are asked:

- Are there alternative means to providing the goods or service without assuming the increased risk of contracted support?
- Which units will be affected by the scope of the contract, when will it be executed (timeframe), and where it will be executed?
- Are there special area or building access requirements?
- Are there any specific contract employee restrictions (security clearance requirements, restrictions on the use of non-U.S. citizen employees)?

- Are current base access and security badging requirements sufficient to address the AT risks of this particular contract support request?
- Is the requiring activity or designated supported unit prepared to provide contract oversight assistance in the form of contracting officers and AT officer technical oversight?

D-8. The concern during this step is to determine the relevant AT security considerations along with the specific services being requested.

STEP 2. PERFORM ANTITERRORISM RISK ANALYSIS

D-9. The unit conducts an AT risk analysis process by using locally prepared AT assessments (threat, criticality, vulnerability, and risk). The use of these products helps the unit assess and identify the potential AT risks associated with the contract and incorporate specific AT security countermeasures into the contract. Part of this process is to consider alternative means of fulfilling the contract requirement as a means to mitigate or eliminate risks. The AT officer assists in the AT risk analysis process, ensuring that local security measures are leveraged and/or modified against risks and vulnerabilities associated with the contract.

STEP 3. PERFORM CONTRACT OVERSIGHT

D-10. During this step, the AT officer assists the unit in developing specific AT security measures. AT security measures should be based on the outcome of the CRM process and reflect the commander's overall AT risk management strategy. There should be a balance between effective security measures and costs and benefits. The unit and the AT officer should apply the commander's AT security considerations during this step. In coordination with the appropriate protection and security staff, the AT officer should design AT security strategies that complement the existing security profile of the location from a normal security posture through advanced readiness postures. Flexibility should be incorporated into the base AT and security procedures to allow for random schedules, access and/or search requirements, and changes in the local threat. For example, contractor personnel may be directed to enter the location through certain access points where they can best be identified and searched. The presence of contractor personnel may be prohibited from certain portions of the location and during advanced readiness postures. Any site-specific requirements that may impact the overall base or command protection, security, and procedures or policies should be immediately communicated to the appropriate base or command protection or security section and/or BDOC. The requiring activity must understand that these types of flexible AT measures may lead to increased cost, which may have to be justified to the approving official.

D-11. Prior to submitting the requirements package for review and approval, commanders and their contract development team should—

- Incorporate AT considerations into commercial relationships in order to develop a vested interest, on the contractor's part, for ensuring the safety and security of U.S. and coalition forces. They should also develop local contract company and employee screening policies (normally done at the joint force command level in overseas contingencies).
- Ensure that the performance work statement or statement of work requires contract personnel to comply with local base or command AT policies and procedures, including changes to schedules and access procedures. The appropriate base access and security procedures must be referenced in each requirements package.
- Identify suggested, unique AT quality assurance and surveillance plan measures for inclusion in the contract.
- Develop a risk mitigation and backup plan for mission-essential contractor services.
- Prepare contingency plans for obtaining essential services from other sources in the event that the contractor does not perform in a crisis or accept the risk attendant with a disruption in service.
- Be prepared to offer Level I AT awareness training for contractors authorized to accompany the force.
- Include contracted services and personnel in threat assessments and VAs.

Note. Contracts written to arm contractors for self-defense or security or mission purposes require additional legal, political, and civil analysis that must be addressed to ensure that the decision is consistent with the commander's intent.

STEP 4. BUILD AND AWARD THE CONTRACT

D-12. This step involves combining the overall contract services requirements with the AT security measures into an acquisition-ready requirements package. As a minimum, the requirements package should be staffed through the ATWG, legal officer, and commander. All Army requirements packages include a commander's formal AT review endorsement, which certifies that the AT security measures are satisfactory and that the commander has accepted the AT risk associated with this contracted support. Additionally, all requirements packages for services performed on base must include contractor employee site access information. This information is normally included by reference to the appropriate base policy or as a separate tab to the requirements package. Table D-2 identifies some of the specific AT security measures that should be considered for inclusion in service contracts that have an area of performance on a military base or near U.S. forces.

Table D-2. AT security measures for service contracts

AT Security Area	*AT Security Measure*
Contractor screening	• Vet preapproved, reputable companies through the contracting office, chief of mission, DOD. • Limit announcements for contractors to trusted sources based on the sensitivity of the mission. • Conduct a background check (law enforcement, HN). • Screen company and prospective workers. • Define the process for replacing workers. • Establish a central contractor database that is accessible only to U.S. and non-HN security forces and contains contractor ID with pictures. • Limit the work area. Clearly identify restricted or exclusion areas where contractor personnel are not authorized without specific permission or an escort.
Access control	• Ensure that access control roster (personnel and vehicles), names and vehicles verified by the company and received background screening and/or HN certification, substitutes receive the same vetting process prior to work. • Check badge systems and exchange badge system. • Check personal identification systems (for example, work uniform and vehicle marking). • Check biometrics systems such as fingerprint, retinal, facial feature reading device. • Ensure that large vehicles (such as, trash trucks) arrive empty before entering the location. • Arrange vehicle loads to facilitate searching. • Verify contents of large vehicles at distribution points and/or using an electronic vehicle-screening device. • Consider an alternative access control point for screening and searching contractor personnel and vehicles, especially oversize vehicles. • Consider an unloading zone away from protected assets. • Ensure that HN language translation support is provided. • Coordinate HN security requirements.

Table D-2. AT security measures for service contracts (continued)

AT Security Area	*AT Security Measure*
Circulation control	• Designate authorized work areas and travel routes. • Provide easily identifiable coding for badges and vehicles. • Assign a unit escort (armed as required) to the contractor. • Deny access during increased readiness conditions.
Special security concerns	• Include contract services as part of the local risk analysis and management process. • Ensure that AT security measures already in place are leveraged and complemented. • Consider all possible alternatives to fulfilling the required service; and determine if the service is required to accomplish the mission. • Consider time and space factors to determine hostile intent into AT security measures. • Consider incorporating contractor security measures into the local FPCON system. • Monitor contractors at the work site as required by the security environment. • Review contracts annually or when the local threat changes. • Establish food and water testing protocols. • Identify and monitor food, water, and petroleum distribution points (on and off location). • Ensure that delivery schedules are random and unpredictable. • Consider periodic interviews of contractors by security force personnel. • Provide contractor training and procedures for reporting suspicious activity and stolen equipment. • Determine what risks remain after AT security measures are applied and determine acceptance of risk. • Conduct frequent, random patrols, inspections, and spot checks. • Establish a security response force. • Ensure that HN agreements allow adequate AT security considerations during the logistics contracting process.
Legend: AT antiterrorism DOD Department of Defense HN host nation	

D-13. The contracting officer will ensure that the contract solicitation includes appropriate AT measures identified in the requirements package; this is normally done by referencing base or site access procedures. Contract- or site-specific AT requirements will be included in the solicitation as applicable. If local national contract company screening policies are in place, the contracting officer will also coordinate with the appropriate intelligence staff to ensure that only prescreened and approved companies are considered for the contract award. Finally, the contracting officer will normally consider AT-related past performance as part of the contract bid evaluation process. Once the contract is awarded by the supporting contracting officer, security requirements in the contract become binding to the contract company (and any related subcontractor), and government-provided security measures should be in place. The contracting officer and the unit should notify the unit contracting officer prior to the start of contract services to ensure that all required AT security measures are in place.

STEP 5. PERFORM CONTRACT OVERSIGHT

D-14. Contract oversight is a shared responsibility between the contracting officer and the unit. The unit contracting officer should follow the quality assurance and surveillance plan, which should contain specific AT measures as identified in the requirements package. The quality assurance and surveillance plan is used to periodically review the effectiveness of the contract, both in terms of services rendered and AT security measures in place. Contract oversight includes day-to-day contracting officer inspection and evaluation of services rendered, periodic inspection of access controls to ensure that control procedures are not being abused, and a formal annual review process to renew or cancel the contract. The requiring activity should be prepared to develop a contract modification request if the local threat changes or there is a requirement to modify and renegotiate the terms of the contract due to other changes in AT procedures. These change requests should be closely coordinated with the unit AT officer prior to sending them forward to the supporting contracting office for action.

Note. Commanders, contracting officers, and AT officers must be cautious in dealing with contract companies to ensure that they do not create unauthorized commitments. Only warranted contracting officers can change the terms and conditions of a contract.

D-15. Where applicable, contracting officers will consider past performance, including AT performance, in awarding future contracts. Other service providers that are not under contracts governed by the federal acquisition regulations, such as HN port and airport personnel and some transportation providers, should be vetted where feasible.

CONTRACTOR PERSONNEL PROTECTION

D-16. Protection measures for contracted services performed on military bases or near U.S. forces must be based on battlefield location decisions and the associated threat level made by the combatant commander and subordinate joint and Army commanders. Protecting service contractors who are in direct support of Army forces is the ARFOR commander's responsibility, via the G-3 staff.

D-17. When contractors provide services on Army bases or near Army forces in potentially hostile areas, the supported Army unit must assure the protection of the contractor's operations and personnel. Commanders and planners must determine the need for contractor protection early in the planning process and identify forces to provide security. Contractor employees cannot be required to perform protection functions and cannot take an active role in hostilities, but they retain the inherent right to self-defense. Commanders understand that contractors are subject to the same threat as Soldiers and must plan accordingly.

D-18. Commanders have legal responsibilities to provide security for contractors who are authorized to accompany the force, similar to the security provided for Army civilian employees. Contractors authorized to accompany the force are required to comply with the specific AT guidance directed by the Army and the combatant commander. Commanders may also be required to offer AT training to contractors authorized to accompany the force under the terms specified in the contract. It is also DOD and Army policy that all contractors (including contractors who are not authorized to accompany the force) and local national workers who are working within a U.S. military facility or in proximity to U.S. forces receive incidentally the benefits of measures undertaken to protect U.S. forces.

This page intentionally left blank.

Appendix E

Antiterrorism Assessments

Assessments form the foundation of every AT program and risk management approach used to defend against terrorist attacks that threaten infrastructure, personnel, and information. The following information and examples expand on the direction that is given in chapter 3 and provide guidance for commanders, leaders, and staff to prepare assessments that weigh risk and defend against potential attacks.

THREAT ASSESSMENT

E-1. A terrorism TA is developed by performing a thorough, in-depth threat analysis. It should be conducted at least annually on personnel and assets for which a commander has AT responsibility. A terrorist threat analysis consists of a continuous process of compiling and examining information and intelligence concerning potential terrorist actions in a given AOR. DOD has developed the following factors to assist leaders and staffs with threat analyses that are conducted country by country:

- **Operational capabilities.** Operational capabilities are acquired, assessed, or demonstrated levels of the capability to conduct terrorist attacks.
  - ***Group tactics.*** What type of attack has the group conducted in the past? Has the group conducted large- or small-scale bombings, kidnappings, assassinations, drive-by shootings, or other assaults? Has there been an indication that the group has new capabilities? Has the group been notably unsuccessful in an attack?
  - ***Mass-casualty capabilities.*** Does the group have the capability and willingness to conduct a mass-casualty attack? Has the group conducted mass-casualty attacks in the past? Has the group shown an interest in CBRNE material?
  - ***Targeting techniques.*** Does the group conduct attacks that are intended to maximize casualties? Does the group attempt to damage only property by placing IEDs after business hours or in remote locations?
  - ***State sponsorships.*** Does the group have state sponsorship? Who is the state sponsor? What type of intelligence, logistics, training, or funding is provided? Is support issued from one or more governments? If so, which ones?
  - ***Group operating areas.*** Is the group indigenous, regional, or transnational? Can indigenous groups operate regionally or internationally?
  - ***High-technology accesses.*** Does the group have access to high technology? Does the group use computers? If so, to what extent? Can the group conduct sophisticated, technical surveillance or employ advanced IEDs? What type of equipment is used? Where did the group get the equipment? Who trained the group?
  - ***Operational methods.*** What is the group's method of operation? (A group will usually continue to use TTP that have been successful in the past.)
  - ***Professional representations.*** What is the group's overall professionalism? Has the group consistently carried out successful, sophisticated attacks? Has the group demonstrated a high or low degree of tradecraft?

Note. Different tactics result in different degrees of threat. Groups that have conducted only property attacks present less threat than those that have conducted assassinations or attacks with large, vehicle-borne improvised explosive devices.

- **Intentions.** Intentions are stated purposes and/or actual attacks on U.S. interests.
  - ***Recent attacks.*** Has the group conducted a recent terrorist attack? If so, what type of attack? Which weapons were used? Were preincident indicators noted? Was outside support used? Did the group take credit for the attack?
  - ***Anti-U.S. ideologies.*** Does the group have an anti-U.S. ideology? Is the ideology stated publicly? What are the group's grievances against the United States? What trigger events could entice the group to act?
  - ***Anti-HN ideologies.*** Does the group have an anti-HN ideology? Does the group consider U.S. aid or support to be a hindrance to its goals? At what point would the group consider attacking U.S. interests because of this support?
  - ***Attacks in other countries.*** Has the group conducted a terrorist attack in another country? If so, where? What type of attack? Which type of support network was in place?
  - ***Responses to current, international events.*** Has the group responded to an international event with a terrorist attack? If so, what was the event? What type of response did it carry out? Has the group ever publicly denounced an international event involving the United States? Did it threaten U.S. interests?
- **Activities.** A terrorist group's activities may not always be related to operational planning or present a threat to U.S. or HN interests. Many groups use countries as support bases and may not want to jeopardize their status by conducting terrorist acts in those countries. Analysts must determine the group's activity by examining influential elements and by remembering that the situation is always fluid and subject to change. Key elements in evaluating activity include—
  - ***Presence.*** Is a group present, but inactive?
  - ***Fundraisers and safe havens.*** Does the group use the country for fundraising? If so, what type of fundraising? How much money is generated? What is its intended use? Is any of the money funneled to other locations or groups? Does the group use a country as a safe haven?
  - ***Suspected surveillance, threats, and suspicious incidents.*** Has the group conducted surveillance? Is the group proficient at surveillance? What does the group do with surveillance information? Has the group threatened DOD or U.S. interests? How does the group conduct surveillance? Have suspicious events been linked to the group?
  - ***Philosophy changes.*** Has the group shown signs of changing philosophies? Does the philosophical change include targets? Is DOD affected?
  - ***External cells.*** How does local leadership interact with external leadership? How much contact is normal? Does the group have connections with other cells? Do the cells train together? Do they share intelligence?
  - ***Key operative movements.*** Has there been noted movement of key operatives? If so, from where to where? Was the movement covert? Was there a reaction from other cells? What was the purpose of the movement? Were code words used?
  - ***Contingency planning.*** Has contingency planning been noted? Who or what were the targets? How were past plans executed? Who conducted the planning? Was outside help used or requested? Did any of the attacks occur after planning was noted? How much time elapsed?
  - ***U.S. or HN security element disruptions.*** Have U.S. or HN security forces disrupted group activities? Does the group perceive U.S. involvement? What caused the disruption? What was uncovered by security? How does it affect the group's operational capability in the country?
  - ***Weapons caches.*** Have weapons caches been uncovered? If so, what weapons were found? Are the weapons consistent with the group's past weapons usage? Who supplied the weapons?
  - ***Cell activities.*** What type of activity does the group primarily conduct in country? Operational? Support? Size of cells? Number of cells?

  - ***U.S.-targeted asset indicators***. Is there an indication that the group is targeting U.S. assets? If so, at which stage of the targeting process was the plan uncovered? What is the timing, specific target, and location of the plan?
  - ***Terrorist activity intelligence report assessments***. What type of intelligence is being reported? What is the source, reliability, and access of the reports?
- **Operational environments**. The overall environment influences a terrorist group's ability and motivation to conduct an attack. Influencing factors include—
  - ***Army presence***. What are the size, location, and duration of DA presence in the country? What are DA personnel doing in the country? What is the terrorist perception of DA significance? How politically sensitive is the DA presence? What could entice the terrorists to attack DA interests?
  - ***External influence***. Is the host country at war? Could this influence a terrorist group to attack? Is there active insurrection? Is the terrorist group involved in the insurrection?
  - ***HN security and cooperation***. Can HN security (including national law enforcement, paramilitary, and military institutions) maintain social order? How well are security forces trained to respond to terrorist incidents? What equipment is available for security forces? How are forces dispersed around the country? Does the HN cooperate with U.S. authorities? Does the HN share information?
  - ***Political influence***. What political influences are affecting the group's motivation to attack? Did HN strategies become more stringent after previous terrorist acts occurred?

E-2. CI support to the conduct of AT and protection VAs consists of producing a TA and making countermeasure recommendations in the final VA report concerning specific areas related to countering or negating known or suspected collection targeting of the supported command. A TA is a stand alone document that is produced from existing intelligence analysis and information that is developed through CI functions and liaisons with security, intelligence, and law enforcement agencies.

E-3. The Office of the Under Secretary of Defense, Counterintelligence, and Security developed a standardized TA that could be used to define the threat and inform the force of terrorist capabilities. The TA provides a series of executive summaries and detailed discussions to inform units of the terrorist threat within a particular AO. The TA can be as broad or as specific as necessary to prepare units in training for an upcoming deployment or to provide a continuous update during current operations. The TA should include—

- Terrorist threats.
  - Operational capabilities.
  - Intentions.
  - Activities.
  - Operational environments.
- Foreign intelligence and security service threats.
- Crimes.
- Civil disturbances.
- Medical and safety threats.
- Weapons of mass destruction.
- Security environments.
- Incident reporting and feedback points of contact.

THREAT CHARACTERISTICS

E-4. Intelligence plays a critical role in the AT program. Another approach that is available to the commander and AT officer for compiling a TA is to utilize the information obtained from the intelligence preparation of the battlefield process. In step 3 of the intelligence preparation of the battlefield, the G-2/S-2 and staff analyze the command's intelligence holdings that were identified in step 1 of the intelligence preparation of the battlefield to determine how the terrorist normally conducts operations under similar

circumstances. When operating against a new or less defined threat or terrorist, the G-2/S-2 may need to develop or expand intelligence databases and terrorist models, concurrently. To accomplish this, the G-2/S-2 should analyze threat characteristics for each group identified when defining the operational environment. (See FM 2-01.3 for more information.) Using this methodology, terrorists are evaluated on—

- Composition.
- Disposition.
- Tactics.
- Training.
- Logistics.
- Operational effectiveness.
- Communications.
- Intelligence.
- Recruitment.
- Support.
- Local support.
- Regional support.
- National support.
- International support.
- Popular support.
- Finance.
- Reach.
- National agencies.
- Law enforcement agencies.
- International, intergovernmental, and nongovernmental organizations.
- Personality.
- Other threats or adversaries.

THREAT MATRIX

E-5. The threat matrix tool uses available sources of information to identify and prioritize current threats so that the commander can start a counterplanning process and focus or reallocate resources based on the likeliness of occurrence and severity of the threat. The threat matrix does not replace the TA, but it does enhance and clarify the information contained in the analysis. Threat analysts gather information from various sources of intelligence, open-source information, and information collected through conversations with the local populace. Analysts gather this information and differentiate between threats that are likely to be used inside and outside the perimeter to aid in developing future vulnerability countermeasures.

E-6. Threat models depict how threat forces prefer to conduct operations under ideal conditions. They are based on what U.S. forces know about terrorist organizations, equipment, capabilities, and previous attack scenarios and how they "doctrinally" fight. Because terrorist organizations have shown their ability to quickly adapt to U.S. countermeasures and defenses, the threat models developed from the intelligence preparation of the battlefield before deployment require continuous updating as commanders and AT officers evaluate the threat, shift resources, and implement RAM. Threat modeling may also help commanders determine organizational tools (local support, recruitment capabilities, ideology) and operational tools (funding, training, CBRN capabilities, small arms).

E-7. Figure E-1 is a sample terrorist threat for an airfield. Threat probability and severity are initially assessed on a scale, based on the number of threats likely to be used against the unit or base. In this example, there are 10 possible threats to the airfield; therefore, the scale is 1 to 10, with 10 being the most probable or most severe.

Threat Capability	*Weapon*	*Delivery Method*	*Threat Probability*	*Threat Severity*	*Threat Priority (Probability x Severity)*	*Threat Priority (Inside Perimeter)*	*Threat Priority (Outside Perimeter)*
Vehicle bomb	220 lb	Vehicle (motorcycle, car, truck, boat, plane)	10	5	50	1	2
	1,000 lb		9	7	63	NA	1
	20,000 lb		4	10	40	NA	4
Sniper	7.62 mm/ .308 cal	Sniper	7	1	7	7	9
Standoff weapons	Mortar	Hasty attack	8	3	24	3	NA
	RPG	Hasty attack	5	2	10	5	5
Suicide bomber	25 lbs	Personal	6	4	24	2	3
MANPADS	SA7, SA16	Attack against aircraft in arrival or departure	3	6	18	NA	6
CBRN	Nerve agent/ toxic industrial chemical	Dispersed upwind of event or train derailment	1	9	9	6	7
	Chem/bio poison	Food or water	2	8	16	4	8

Legend:

bio	biological
cal	caliber
chem	chemical
CBRN	chemical, biological, radiological, and nuclear
lb	pound
MANPADS	man portable air-defense system
mm	millimeter
NA	not applicable
RPG	rocket-propelled grenade

Figure E-1. Sample threat matrix

CRITICALITY ASSESSMENT

E-8. A *criticality assessment* identifies key assets and infrastructure that support Department of Defense missions, units, or activities and are deemed mission-critical by military commanders and civilian-agency managers. It addresses the impact of temporary or permanent loss of key assets or infrastructures to the installation or a unit's ability to perform its mission. It examines costs of recovery and reconstitution costs that including time, dollars, capability, and infrastructure support (JP 3-07.2). The following criteria assists in standardizing the process of determining asset criticality:

- **Importance**. Importance measures the value of the area or the value of the assets located in the area. Considerations include function, inherent nature, and monetary value.
- **Effect**. Effect measures the ramification of a terrorist incident in the area. Considerations include psychological, economic, sociological, and military impacts.
- **Recoverability**. Recoverability measures the time required for the function that is occurring at the area to be restored. Considerations include resources, parts, expertise, manpower, and

redundancies. Even an injured, damaged, or destroyed DA asset may have future value in the accomplishment of other DA missions or be of symbolic value to the DOD, U.S. government, or American people. Considerations include resources that must be expended to recover or repair assets.

- **Mission functionality**. Mission functionality measures key positions, special facilities, and specialized equipment used to fulfill assigned missions.
- **Substitutability**. Are there substitutes available for personnel, facilities, or materiel? Can assigned missions be performed using substitutes? If the substitutes are less capable, can the mission still be accomplished successfully?
- **Reparability**. If a DA asset is injured or damaged, can it be repaired and rendered operable? How much time is required? How much will it cost? Can repairs be accomplished in a timely manner? Will repairs degrade asset performance? If so, can the mission be accomplished in the degraded condition?

CRITICALITY ASSESSMENT MATRIX

E-9. The criticality assessment matrix determines the criticality of each asset. The assessment team assigns a subjective value for criteria based on a scale (1 to 10) and determines the criteria to use. When all of the asset values are tallied, they are usually rank-ordered. The highest score is the most critical, and the lowest score is the least critical. However, not all assets in the matrix are essential for mission accomplishment. Figure E-2 shows an example of a criticality assessment matrix.

Asset	*Importance*	*Effect*	*Recoverability*	*Mission Functionality*	*Substitute/ Repair*	*Other*	*Total*
Base exchange	8	7	5	3	5		28
Corps headquarters	9	10	9	7	7		42
Soldier barracks	10	10	9	10	10		49

Figure E-2. Sample criticality assessment matrix

MISSION, SYMBOLISM, HISTORY, ACCESSIBILITY, RECOGNIZABILITY, POPULATION, AND PROXIMITY TOOL

E-10. Facility commanders are encouraged to use a criticality assessment tool that is simple yet has some measure of quantifiable logic to help in decisionmaking. Assessment teams use the methodology to determine terrorist options against specific targets. MSHARPP is a targeting analysis tool that is geared toward assessing personnel vulnerabilities, but it also has application in conducting a broader analysis. Assessment team members should be cognizant of potential gaps when choosing one methodology over another.

E-11. The purpose of the MSHARPP matrix is to analyze likely terrorist targets and assess their vulnerabilities from the inside out. Consideration is given to local threats, probable means of attacks, and variables that affect dispositions of potential targets. After developing a list of potential targets, MSHARPP selection factors are used to assist in further refining the assessment by associating a weapon or tactic with a potential target to determine the efficiency, effectiveness, and plausibility of the attack method and to identify vulnerabilities related to the target. When the MSHARPP values for each target or component are assigned, the sum of the values indicates the highest-value target (for a particular mode of attack) within the limits of the enemy's known capabilities.

E-12. The MSHARPP risk prioritization matrix allows leaders to identify target criticality, determine corresponding risk, and prioritize security assets. The matrix is based on the seven MSHARPP criteria and is produced for each critical asset that is listed in the critical-asset list. To complete the matrix, AT officers—

- Identify and reevaluate key structures, capabilities, organizations, and individuals in the AO that terrorists may target.
- Record the information from the seven MSHARPP criteria worksheets into the MSHARPP prioritization matrix for each asset being assessed, and compare this target to others that are considered critical to the commander and mission to determine the priority of assets. (See figure E-3.) After prioritization is complete and the commander determines the assets that will be resourced, the defended-asset list is updated.
- Evaluate the potential target using the sample MSHARPP evaluation tool shown in figure E-4, page E-8.
- Choose a risk statement that corresponds to a risk level. Explain how and why the risk level was assessed, record the assigned value for each criterion, and identify control and mitigation measures for each assessment.

Prioritization Matrix for _____at _____

MSHARPP	*Why and How*	*Value*	*Controls or Mitigation*	*Priority*
Mission				
Symbolism				
History				
Accessibility				
Recognizability				
Population				
Proximity				
Total Value (lower is better; maximum value is 35)				

Legend:
MSHARPP mission, symbolism, history, accessibility, recognizability, population, and proximity

Figure E-3. Sample MSHARPP prioritization matrix

Mission Criteria. The mission focuses primarily on the threat to the situations, activities, capabilities, and resources on an installation that are vulnerable to a terrorist attack. The mission components consist of the equipment, information, facilities, and operations or activities that are necessary to accomplish the unit/base mission. When assessing points in this area, determine whether an attack on mission components would cause degradation by assessing the component's— • **Importance.** This measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value. • **Effect.** This measures the ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts. • **Recuperability.** This measures the time required for the function occurring at that area to be restored, considering the availability of resources, parts, expertise, and manpower, and redundancies.	
The unit/base cannot continue to carry out its mission until the attacked asset is restored.	Catastrophic Risk (5)
The ability to carry out a primary mission of the unit/base would be significantly impaired if this asset were successfully attacked.	Critical Risk (4)
Half of the mission capability remains if the asset were successfully attacked.	Moderate Risk (3)
The unit/base could continue to carry out its mission if this asset were attacked, albeit with some degradation in effectiveness.	Negligible Risk (2)
Destroying or disrupting this asset would have no effect on the ability of the unit/base to accomplish its mission.	No Risk (1)

Why and How	Value	Controls and Mitigation

Symbolism Criteria. Consider whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (symbolic of U.S. military, government, and authority). Assess points in this area based on the symbolic value of the target to the enemy.	
The location is associated with personnel or organization leaders who are involved in actions to which the attacker is directly opposed.	Catastrophic Risk (5)
The target has historical, religious, or other symbolic significance to defender.	Critical Risk (4)
The target is regarded as an invulnerable strongpoint by the defender.	Moderate Risk (3)
The target is associated with the economic or production capability of the defender.	Negligible Risk (2)
The target is a popular social gathering area for the defender populace.	No Risk (1)

Why and How	Value	Controls and Mitigation

Historical Criteria. Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities.	
Attacks against this type of target are conducted routinely by most known threats (majority of all attacks).	Catastrophic Risk (5)
Attacks against this target are conducted routinely by primary threat.	Critical Risk (4)
Attacks against this type of target have occurred.	Moderate Risk (3)
Attacks against this type of target have been threatened.	Negligible Risk (2)
Attacks against this type of target fit the threat's method of operation.	No Risk (1)

Why and How	Value	Controls and Mitigation

Figure E-4. Sample MSHARPP criteria tool

Accessibility Criteria. A target is accessible when an operational element can reach it with sufficient personnel and equipment to accomplish the mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives and measuring those things that aid or impede access. The enemy must not only be able to reach the target, but must also remain there for an extended period.		
Easily accessible, standoff weapons can be employed.		Catastrophic Risk (5)
The target is inside a perimeter but outdoors.		Critical Risk (4)
The target is inside a building, but on ground floor.		Moderate Risk (3)
The target is inside a building, but on the second floor or in the basement.		Negligible Risk (2)
The target is not accessible or is only accessible with extreme difficulty.		No Risk (1)
Why and How	Value	Controls and Mitigation
Recognizability Criteria. A target's recognizability is the degree to which it can be recognized by an operational element and/or intelligence collection and reconnaissance asset under varying conditions. Weather has an obvious and significant impact on visibility (friendly and enemy). Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. The distance, light, and season must be considered. Other factors that influence recognizability include the size and complexity of the target, existence of distinctive target signatures, presence of masking or camouflage, and technical sophistication and training of the enemy.		
The target is clearly recognizable under all conditions and from a distance; it requires little or no training.		Catastrophic Risk (5)
The target is easily recognizable at small arms range and requires a small amount of training for recognition.		Critical Risk (4)
The target is difficult to recognize at night or, in bad weather; or it might be confused with other targets or target component; requires some training for recognition.		Moderate Risk (3)
The target is difficult to recognize at night, or in bad weather (even at small arms range), it is easily confused with other targets or target components and it requires extensive training for recognition.		Negligible Risk (2)
The target cannot be recognized under any conditions except by experts.		No Risk (1)
Why and How	Value	Controls and Mitigation

Figure E-4. Sample MSHARPP criteria tool (continued)

Proximity Criteria. Is the potential target located near other personnel, facilities, or resources that, because of their intrinsic value or "protected" status and a fear of collateral damage, afford it some form of protection? Examples include being located near national monuments or protected/religious symbols that the enemy holds in high regard. It is important to consider whether the target is in close proximity to other likely targets. Just as the risk of unwanted collateral damage may decrease the chances of attack, a "target-rich" environment may increase the chances of attack.		
The target is in close proximity; serious injury, damage, or death, or total destruction of protected personnel/facilities likely.		Catastrophic Risk (5)
The target is in close proximity: serious injury, damage or death, partial destruction of protected personnel/facilities likely.		Critical Risk (4)
The target is in close enough proximity to protected personnel and facilities; injury or damage, but not destruction is likely.		Moderate Risk (3)
The target is partially isolated; unwanted collateral damage to protected symbols or personnel is likely.		Negligible Risk (2)
The target is isolated; no chance of unwanted collateral damage to protected symbols or personnel is possible.		No Risk (1)
Why and How	Value	Controls and Mitigation
Population Criteria. Population addresses two factors, quantity of personnel and their demography. Demography asks the question: who are the targets? Depending on the ideology of the terrorist group(s), being a member of a particular demographic group can make someone (or some group) a more likely target. When assessing points in this area, determine whether group(s) have a history of, or are predicted to target military personnel, family members (U.S. citizens in general), civilian employees of the U.S. government (including local nationals), senior officers, or other high-risk personnel, or a member of an ethnicity (racial, religious, or regionally defined).		
Extremely large population center, attack causes mass casualties (1000+), Significant impact on international policy with the highest level of stress on infrastructure.		Catastrophic Risk (5)
Large number of people, attack causes mass casualties (500+), known target group present; Significant impact on international policy; significant stress on infrastructure.		Critical Risk (4)
Moderate number of people, attack causes extensive casualties (100+), known target group may be present; Significant impact on national policy; major stress on infrastructure.		Moderate Risk (3)
Sparsely populated, attack causes casualties of (10+); prone to having small groups or individuals, little target value based on demographics of occupants.		Negligible Risk (2)
No people present or attack on very few people (1-10); contains people that the terrorist group considers desirable to avoid harming.		No Risk (1)
Why and How	Value	Controls and Mitigation

Figure E-4. Sample MSHARPP criteria tool (continued)

E-13. Another way to reflect the results of the criticality assessment is by filling out an MSHARPP matrix (see figure E-5.) The values from (1 to 5) are assigned to each factor based on the associated data for each target taken from the MSHARPP worksheets. The number 5 represents the highest vulnerability, and the number 1 represents the lowest. The higher the total score, the more critical the target. The MSHARPP analysis assesses the present protection and enhanced postures proposed for escalating FPCONs. Specific target vulnerabilities are combined with exploitable perimeter control vulnerabilities. If access routes are well protected and not exploitable, a vulnerable building becomes a less likely target. The commander has an overall visual of assets listed in the critical-asset list with numerical data to assist in making risk decisions during CRM.

TARGET	*M*	*S*	*H*	*A*	*R*	*P*	*P*	*TOTAL*
Corps headquarters	5	4	5	1	3	4	1	23
Soldier barracks	2	4	5	4	4	4	2	25
Communication center	5	4	2	3	5	3	1	23
Fuel storage	4	3	1	5	4	1	3	21
Helicopter hangar	5	5	3	2	5	5	4	29
Weapon storage	5	5	1	1	5	3	1	21
Electric transformer	5	2	3	5	5	0	4	24
Legend: MSHARPP mission, symbolism, history, accessibility, recognizability, population, and proximity								

Figure E-5. Sample MSHARPP matrix

CRITICALITY, ACCESSIBILITY, RECUPERABILITY, VULNERABILITY, EFFECT, AND RECOGNIZABILITY MATRIX

E-14. The CARVER matrix is a valuable tool in determining criticality and vulnerability. For criticality purposes, CARVER helps assessment teams and commanders rank the assets that they are responsible for to determine the assets that are more critical to the success of the mission. This also helps determine which resources should be allocated to protect critical assets (personnel, infrastructure, information). CARVER assesses a potential target from a terrorist's perspective to identify what the enemy might perceive as a good (or soft) target. Commanders and AT officers may address—

- **Criticality.** How rapidly will the impact of asset destruction affect the unit's essential functions? What percentage of output and essential functions is curtailed by asset damage? Are there substitutes for the output product or service? What is the number of assets, and what is their position in the system or in the complex flow diagram? How critical is the facility to mission accomplishment?
- **Accessibility**. How easily can an enemy gain access to weapons?
- **Recuperability**. How long will it take to repair or replace the asset?
- **Vulnerability**. Is the asset hardened or guarded? Are measures in place to mitigate the threat?
- **Effect**. Will reprisals against allies result? Will national psychological operations themes be contradicted or reinforced? Will evasion be helped or hurt? Will the enemy population be alienated from its government, or will it become supportive of the government? What is the effect on the local population?
- **Recognizability**. Can the enemy recognize the target and its importance?

E-15. Target selection requires detailed intelligence and thorough planning, and it is based on the CARVER factors identified above. Establishing criteria allows the individual to better determine the criticality of a particular location or piece of equipment over a broader spectrum of analysis. The guidelines for completing the criteria and matrix include—

- Listing systems and subsystems for strategic analysis.
- Listing complexes or components of subsystems and complexes.

Note. The scale can be adjusted for tactical analysis.

E-16. The CARVER risk prioritization matrix allows leaders to identify target criticality, determine corresponding risk, and prioritize security assets. The matrix is based on the criteria discussed above and is produced for each critical-asset listed in the critical-asset list.

E-17. To complete the matrix, AT officers identify and reevaluate key structures, capabilities, organizations, and individuals in the AO that terrorists may target. They—

- Evaluate the potential target by using a criteria evaluation tool (figure E-6).
- Choose an appropriate risk statement in the criteria evaluation tool. Explain why and how the risk level was assessed, record the assigned value for each criterion, and identify control and mitigation measures for each assessment.
- Record the information into the CARVER prioritization matrix for each asset being assessed (see figure E-7, page E-14). Compare this target to other targets that are considered critical to the commander and mission to determine the priority of assets. When the prioritization is complete and the commander determines which assets will be resourced, update the defended-asset list.

Criticality Criteria. Determine the importance of a system, subsystem, complex, or component. A target is critical when its destruction or damage has a significant impact on the output of the targeted system, subsystem, or complex (at the highest level) on the unit's ability to make war or perform essential functions.		
Immediate halt in output, production, or service; target cannot function without it.		Catastrophic Risk (5)
Halt within 1 day or 66 percent curtailment in output, production, or service.		Critical Risk (4)
Halt within 1 week or percent curtailment in output, production, or service.		Moderate Risk (3)
Halt within 10 days or 10 percent curtailment in output, production, or service.		Negligible Risk (2)
No significant effect on output, production, or service.		No Risk (1)
Why and How	Value	Controls and Mitigation
Accessibility Criteria. A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives and measuring those things that aid or impede access. The enemy must be able to reach the target and remain there for an extended period.		
Easily accessible; standoff weapons can be employed.		Catastrophic Risk (5)
Inside a perimeter, but outdoors.		Critical Risk (4)
Inside a building, but on the ground floor.		Moderate Risk (3)
Inside a building, but on the second floor or in a basement.		Negligible Risk (2)
Not accessible or only accessible with extreme difficulty.		No Risk (1)
Why and How	Value	Controls and Mitigation

Figure E-6. Sample CARVER criteria evaluation tool

Recoverability Criteria. A measure of time required to replace, repair, or bypass, the destruction or damage inflicted on the target. Recoverability varies with the sources and ages of targeted components and with the availability of spare parts.		
Replacement, repair, or substitution requires 1 month or more.		Catastrophic Risk (5)
Replacement, repair, or substitution requires 1 week to 1 month.		Critical Risk (4)
Replacement, repair, or substitution requires 72 hours to 1 week.		Moderate Risk (3)
Replacement, repair, or substitution requires 24 to 72 hours.		Negligible Risk (2)
Same day replacement, repair, or substitution.		No Risk (1)
Why and How	Value	Controls and Mitigation
Vulnerability Criteria. A measure of terrorist ability to damage the target using available assets (people and material). A target (asset) is vulnerable if the terrorist has the means and expertise to successfully attack it.		
Vulnerable to long-range target designation, small arms, or charges of 5 pounds or less.		Catastrophic Risk (5)
Vulnerable to light antiarmor weapons fire or charges of 5 to 10 pounds.		Critical Risk (4)
Vulnerable to medium antiarmor weapons fire, bulk charges of 10 to 30 pounds, or very careful placement of smaller charges.		Moderate Risk (3)
Vulnerable to heavy antiarmor weapons fire, bulk charges of 30 to 50 pounds, or requires special weapons.		Negligible Risk (2)
Invulnerable to all but the most extreme targeting measures.		No Risk (1)
Why and How	Value	Controls and Mitigation
Effect Criteria. Estimate the positive or negative influence on the population as a result of the action taken. The effect considers the public relation near the target, but also considers the domestic and international reaction as well.		
Overwhelming positive effects for the terrorist; no significant negative effects.		Catastrophic Risk (5)
Moderately positive effects for the terrorist; few significant negative effects.		Critical Risk (4)
No significant effects; neutral.		Moderate Risk (3)
Moderately negative effects for the terrorist; few significant positive effects.		Negligible Risk (2)
Overwhelming negative effects for the terrorist; no significant positive effects.		No Risk (1)
Why and How	Value	Controls and Mitigation

Figure E-6. Sample CARVER criteria evaluation tool (continued)

Recognizability Criteria. A target's recognizability is the degree to which it can be recognized by an operational element or intelligence collection and reconnaissance asset under varying conditions. Weather has an obvious and significant impact on visibility (friendly and enemy). Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. The distance, light, and season must be considered. Other factors that influence recognizability include the size and complexity of the target, existence of distinctive target signatures, presence of masking or camouflage, and the technical sophistication and training of the enemy.		
The target is clearly recognizable under all conditions and from a distance, it requires little or no training for recognition.		Catastrophic Risk (5)
The target is easily recognizable at small-arms range and requires a small amount of training for recognition.		Critical Risk (4)
The target is difficult to recognize at night, or in bad weather, it might be confused with other targets or target component, and it requires some training for recognition.		Moderate Risk (3)
The target is difficult to recognize at night or in bad weather (even within small arms range), and it is easily confused with other targets or components; it requires extensive training for recognition.		Negligible Risk (2)
The target cannot be recognized under any conditions except by experts.		No Risk (1)
Why and How	Value	Controls and Mitigation

Figure E-6. Sample CARVER criteria evaluation tool (continued)

Prioritization Matrix for _____at _____				
CARVER	***Why and How***	***Value***	***Controls or Mitigation***	***Priority***
Criticality				
Accessibility				
Recoverability				
Vulnerability				
Effect				
Recognizability				
Total Value (lower is better; maximum value is 30)				
Legend: CARVER criticality, accessibility, recoverability, vulnerability, effect, and recognizability				

Figure E-7. Sample CARVER prioritization matrix

E-18. The CARVER matrix is a decision tool for rating the relative desirability of potential targets and for allocating attack resources (see figure E-8). It reflects the results of the checklist above, compared to the criticality of other assets within a unit's responsibility.

Potential Targets	***C***	***A***	***R***	***V***	***E***	***R***	***Total***	***Priority***
Police station	3	3	2	3	3	3	17	1
Corps headquarters	2	0	1	2	1	2	8	3
Soldier barracks	3	1	2	2	2	1	11	2
Legend: CARVER criticality, accessibility, recoverability, vulnerability, effect, and recognizability								

Figure E-8. Sample CARVER matrix

E-19. After completing the matrix, total the scores in the right column and then rank-order the totals to prioritize vulnerabilities to assist commanders in determining which assets require resources to ensure mission success. These assets are defended and added to the unit defended-asset list. The following are basic mitigation tips that address CARVER components:

- **Reduce criticality**. Have a backup device, system, or tested plan to allow mission accomplishment without the asset. Create redundancy (physically or operationally), have a tested and viable continuation of operations, and have a fall-back site for conducting the same mission from another location.
- **Reduce accessibility**. Control pedestrian and vehicle movements. Employ barriers, barricades, fences, remote motion sensors, and remote video surveillance equipment.
- **Reduce vulnerability**. Harden the structure and the immediate environment by using window treatments, structural reinforcements, and shatterproof and fireproof building materials. Maneuver vehicle parking and accesses sufficiently away from personnel massing facilities.
- **Reduce recognizability**. Delete the location and purpose of the facility from base maps, and remove building signs that describe the function or give the title of a unit in the facility. Instruct telephone operators to refrain from revealing information about the facility. Use plant cover (trees and bushes) to partially conceal the facility, particularly from roads.

VULNERABILITY ASSESSMENT

E-20. A VA is used by the commander to determine the susceptibility of assets to attack from threats identified by the TA, intelligence preparation of the battlefield, and/or war-gaming. A VA is also used to determine the vulnerability of critical assets (Soldiers, HRP, Internet communications, facilities). It identifies areas of improvement to prevent, withstand, mitigate, or deter threats based on the current threat and likely COA for enemy success. A VA helps address resource needs and the physical security focus. Even with a successful AT appendix, vulnerabilities can be discovered, especially during AARs of large-scale exercises; during war-gaming within the MDMP; and after enemy contact. The VA is usually conducted after a TA and criticality assessment. Commanders can use VA methodology for combat patrols and mission planning.

VULNERABILITY MATRIX

E-21. A VA matrix is used to determine the vulnerability of each asset. CARVER and MSHARPP tools are not always conducive to vulnerability analysis for tactical unit operations or base activity and primarily serve to determine criticality. However, certain factors and the definitions within those tools (recognizability, accessibility, vulnerability, recoverability, effect on population) can assist commanders in determining vulnerability by providing a metric to evaluate assets. The assessment team assigns values for each criterion based on a scale from 1 to 5. The number 5 represents the highest vulnerability, and the number 1 represents the lowest. After the asset values are tallied, they may be rank-ordered; however, the most vulnerable asset is not necessarily the highest risk. For example, equipment that is located in a storage warehouse near the perimeter of an installation may be vulnerable to a vehicle bomb on an adjacent public access road, but the criticality of the equipment or the likelihood that it is a terrorist target may be very low, resulting in an overall rating of low risk.

E-22. The AT officer uses the matrix in figure E-9, page E-16, and scales the various assets against the identified vulnerability areas to determine an overall vulnerability score. This score may be used to determine resource requirements or to help decide which critical assets are most vulnerable and require greater protection.

Asset	Recognizability	Accessibility	Vulnerability	Recoverability	Effect on Population	Total
Dining facility	4	4	4	2	4	18
Corps headquarters	5	2	3	3	5	18
Soldier barracks	2	4	4	2	3	15

Figure E-9. Sample vulnerability matrix

WAR-GAMING VULNERABILITY ASSESSMENT METHODOLOGY

E-23. The MDMP provides an established and effective methodology to conduct vulnerability analyses through war-gaming. When the S-2 initiates an attack against friendly forces, the staff should consider *who, what, when, where, why,* and *how* to help identify friendly unit vulnerabilities, determine appropriate countermeasures, and assess the degree of residual risk. Details regarding likely unit vulnerabilities and how they can be reduced or eliminated should become apparent. Specific questions and discussion points shown in table E-1 are not intended to be definitive; they are suggested techniques for identifying vulnerabilities during COA analysis or war-gaming. Unit personnel should supplement these questions and discussions as appropriate.

Table E-1. War-gaming vulnerability analysis

Event	Action	Reaction	Counteraction
Course-of-Action, War-Gaming and Antiterrorism Vulnerability Analysis			
• Most likely course of terrorist action	• Improvised explosive device attack	• Respond to the attack (secure the area, assess the situation, treat/evacuate the casualties) • Abort or continue the mission	• Follow-on attack targeting first responders • Information operation exploitation of attack

Table E-1. War-gaming vulnerability analysis (continued)

Event	*Action*	*Reaction*	*Counteraction*
Unit Vulnerability Analysis Questions/Discussions			
• Who was involved in the terrorist event?	• Who initiated the attack? How many personnel were involved?	• Who or what was the target of the terrorist attack? • Why was the unit element targeted? • Is the target a critical asset?	NA
• What type of terrorist event occurred?	• What was the attack mechanism? • What are the specific details regarding the weapons used in the attack (maximum effective range, burst radius, method of initiation)?	• What is the targeted element doing when the attack occurs? • What is the expected result (severity) of the terrorist attack based on the weapon/target pairing? • What is the expected number of casualties/level of damage based on the weapon/target pairing? • What is the impact on the unit mission?	NA
• When did the terrorist event occur?	• When is the attack initiated? • Why is the attack initiated at this time? • How long does the attack take?	• How long until the unit recovers from the attack and aborts/continues the mission? • How long until needed assistance arrives on site?	

Table E-1. War-gaming vulnerability analysis (continued)

Event	*Action*	*Reaction*	*Counteraction*
Unit Vulnerability Analysis Questions/Discussions (continued)			
• Where did the terrorist event occur?	• Where is the attack initiated? • Why is the attack initiated at this location?	• Does the location of the attack limit the ability of the unit to respond? • Is the unit vulnerable to continued attack at the location of the attack?	
• What was the purpose/ intent of the terrorist event?	• Why was the attack initiated? • What are the intended/desired effects of the attack?	• Did the attack achieve the desire results?	
• Discussion regarding the planning and execution of the terrorist event.	• How is attack the initiated? • What has to happen for the attack to occur?	• Was the attack self-initiated?	

TACTICAL UNIT VULNERABILITY ASSESSMENT METHODOLOGY

E-24. Tactical units assess their own vulnerability based on the environment in which they operate. While traveling from home station to a forward-deployed area or while operating in the AO, units must continuously evaluate their vulnerability to terrorist actions regardless of the mission. Units should remain cognizant of the fact that most terrorist attacks rely on the element of surprise. Terrorists take advantage of limited roadways, urban infrastructures, and planned IED emplacements; and they are willing to die while executing an attack. Therefore, units must identify tactics and battle drills that reduce the threat.

E-25. Leaders can utilize the following METT-TC framework to assist in conducting unit VA:

- **Mission**. Units consider the nature, location, and timeframe of the mission. They consider routes and movement techniques and identify chokepoints, communication capabilities, limited visibilities, and previous attack frequencies. Units also consider other elements of the mission and the capabilities (or lack of them) that make the overall unit more vulnerable.
- **Enemy**. Leaders assess the most likely and most dangerous COA based on the unit intelligence preparation of the battlefield and updated TA. Weapon and target pairing is critical in understanding unit vulnerability. Some unit elements are vulnerable to specific enemy weapons and tactics, but others are not. Questions concerning why and how a potential attack was conducted against a unit can help the commander identify additional opportunities to reduce unit vulnerability and mitigate the effects of attacks. (Why was the attack initiated? What were the intended or desired effects of the attack?) If the commander distinguishes the enemy's desired attack results, he can concentrate the unit response on preventing the intended effects. (How was the attack initiated? What had to happen for the attack to occur?)

- **Terrain and weather**. Leaders assess factors of terrain (observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment) and forecasted weather conditions to determine enemy and friendly advantages when operating in the environment. They pinpoint areas where the enemy will most likely attack. The unit S-2 and supporting engineer coordinator can develop terrain visualization tools to assist commanders and staff in identifying terrain that supports the enemy use of IEDs and other common terrorist tactics.
- **Time**. Available leaders assess when the enemy is most likely to attack and when the unit is most vulnerable. The VA can help predict specific environmental triggers that cause a potential unit vulnerability to become an actual attack. The transition from vulnerability to attack could be event-driven, time-driven, or location-driven. (Can the unit vary its start and return times? How long will it take for air or area unit supports to respond if they are attacked? Are there established curfews that reveal potential terrorist attacks?)
- **Troops and support available**. Leaders determine what organic equipment does the unit retains to reduce its vulnerability to various attacks? They also determine if the unit trained or rehearsed actions on contact or actions on the objective. Unit personnel in vehicles are more vulnerable to small arms fire and rocket-propelled grenade attacks than personnel in heavy, armored vehicles. Some unit elements (scouts, snipers) routinely operate separately from the main body; this may make them more susceptible to ambush. (Does everyone know how to summon fire or air support and medical evacuation? How many people know about the mission? Has the mission been discussed in unsecured web conversations?)
- **Civil considerations**. Determine if the populace is supportive of U.S. efforts in the area. (Are they reliable sources of intelligence on terrorist activity? What are the rules of engagement? Could civilians serve as shields or additional casualties if a terrorist attack takes place?)

RISK ANALYSIS

E-26. The risk analysis combines threat, criticality, and vulnerability ratings for each asset and develops a quantifiable assessment of risk (see table E-2). (*Risk Analysis = Criticality x Vulnerability x Threat Probability*) Risk is based on the value of the asset in relation to the threats and vulnerabilities that are associated with it. Risk is derived by combining the relative impact of loss or damage to an asset with the relative probability of an unwanted event.

Table E-2. Risk analysis table

Asset	*Attack Means*	*C (C) (1-10)*	*V (V) (1-10)*	*TP (TP) (1-10)*	*Risk Analysis Total C*V*TP*
Command Post					
	Car/truck bomb	9	8	6	432
	Suicide bomber	9	4	3	108
	Rocket/mortar	9	8	7	504
	Small arms fire	9	1	9	81
	CBRN attack	9	8	1	72
Legend:					
C	criticality				
TP	threat probability				
CBRN	chemical, biological, radiological, and nuclear				
V	vulnerability				

E-27. The risk analysis should quantify existing risks and make recommendations to reduce risk levels to mitigate damage (see figure E-10). Risk mitigation lessens the impact of loss from a successful terrorist attack and develops COA to plan for consequence management.

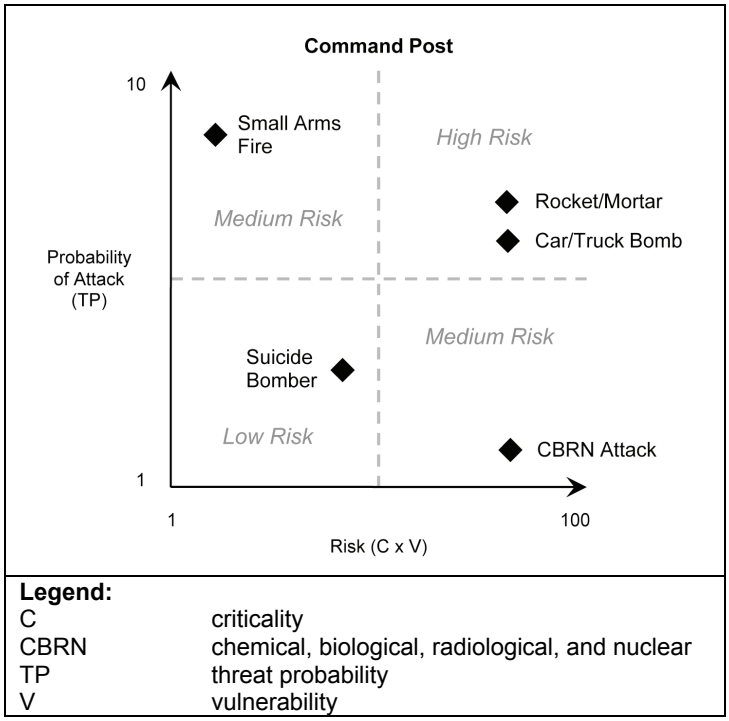


Figure E-10. Risk analysis graph

E-28. During risk analysis, the commander must consider the preceding elements and make well-informed decisions when planning FPCON measure implementation and terrorist incident response measures. The risk analysis management process does not dictate how to conduct the assessment or identify deficiencies and vulnerabilities; however, it outlines what type of information to collect and how to organize and display the information for decisionmaking. Information on vulnerabilities and deficiencies can be entered into the CRM process as outlined in chapter 5.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

AAR	after-action review
AO	area of operation
AOR	area of responsibility
AR	Army regulation
ARFOR	Army forces
ARNG	Army National Guard
ASCC	Army Service component command
AT	antiterrorism
ATTN	attention
ATWG	antiterrorism working group
BCT	brigade combat team
BDOC	base defense operations center
C2	command and control
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosive
CCIR	commander's critical information requirement
CI	counterintelligence
CIA	Central Intelligence Agency
CJCS	Chairman of Joints Chiefs of Staff
COA	course of action
CP	command post
CREW	counter remote control improvised explosive device electronic warfare
CRM	composite risk management
DA	Department of the Army
DNA	dioxyribonecleic acid
DOB	deployed operating base
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DVD	digital video disc
ECP	entry control point
FM	field manual
FOB	forward operating base

FORSCOM	U.S. Army Forces Command
FPCON	force protection condition
G-2	assistant chief of staff, intelligence
G-6	assistant chief of staff, signal
HN	host nation
HRP	high-risk personnel
IED	improvised explosive device
IRA	Irish Republican Army
IW	irregular warfare
JP	joint publication
MANSCEN	Maneuver Support Center
MDMP	military decisionmaking process
METL	mission-essential task list
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MSHARPP	mission, symbolism, history, accessibility, recognizability, population, and proximity
NCO	noncommissioned officer
O/C	observer/controller
OCONUS	outside the continental United States
OPSEC	operational security
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time
RAM	random antiterrorism measure
S-2	intelligence officer
S-3	operations and training officer
S-5	civil affairs officer
S-7	foreign counterintelligence officer
SOP	standing operating procedure
TA	threat assessment
TNT	trinitrotoluene
TRISA	Army Training and Doctrine Command G-2 Intelligence Support Activity
TTP	tactics, techniques, and procedures
UFC	united facilities criteria
USS	United States Ship
VA	vulnerability assessment

References

SOURCES USED

These are the sources quoted or paraphrased in this publication.

ARMY PUBLICATIONS

AR 25-30. *The Army Publishing Program.* 27 March 2006.

AR 350-1. *Army Training and Leader Development.* 18 December 2009.

AR 381-10. *U.S. Army Intelligence Activities.* 3 May 2007.

AR 381-12. *Threat Awareness and Reporting Program*. 4 October 2010.

AR 525-13. *Antiterrorism*. 11 September 2008.

AR 715-9. *Contractors Accompanying the Force*. 29 October 1999.

ATTP 3-39.32. *Physical Security.* 3 August 2010.

DA Pam 385-30. *Mishap Risk Management*. 10 October 2007.

FM 2-0. *Intelligence*. 23 March 2010.

FM 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace*. 15 October 2009

FM 2-19.4. *Brigade Combat Team Intelligence Operations*. 25 November 2008.

FM 2-22.2. *Counterintelligence*. 21 October 2009.

FM 2-91.4. *Intelligence Support to Urban Operations*. 20 March 2008.

FM 2-91.6. *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection*. 10 October 2007.

FM 3-0. *Operations*. 27 February 2008.

FM 3-07. *Stability Operations*. 6 October 2008.

FM 3-11.21. *Multiservice Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Consequence Management Operations.* 1 April 2008.

FM 3-13. *Information Operations: Doctrine, Tactics, Techniques, and Procedures.* 28 November 2003.

FM 3-19.12. *Protective Services*. 11 August 2004.

FM 3-24. *Counterinsurgency*. 15 December 2006.

FM 3-28. *Civil Support Operations*. 20 August 2010.

FM 3-35. *Army Deployment and Redeployment*. 21 April 2010.

FM 3-37. *Protection*. 30 September 2009.

FM 3-50.1. *Army Personnel Recovery*. 10 August 2005.

FM 3-90. *Tactics*. 4 July 2001.

FM 4-02.7. *Multiservice Tactics, Techniques, and Procedures for Health Service Support in a Chemical, Biological, Radiological, and Nuclear Environment.* 15 July 2009.

FM 5-0. *The Operations Process*. 26 March 2010.

FM 5-19. *Composite Risk Management*. 21 August 2006.

FM 6-0. *Mission Command: Command and Control of Army Forces*. 11 August 2003.

FM 6-01.1. *Knowledge Management Section.* 29 August 2008.

FM 7-0. *Training Units and Developing Leaders for Full Spectrum Operations*. 23 February 2011.

FM 7-15. *The Army Universal Task List*. 27 February 2009.

FM 19-10. *The Military Police Law and Order Operations*. 30 September 1987.

FORSCOM Regulation 190-58. *FORSCOM High Risk Personnel Security Program*. 1 September 2000.

DEPARTMENT OF DEFENSE PUBLICATIONS

DOD 0-2000.12-H. *DoD Antiterrorism Handbook*. 9 February 2004.

DODD 1300.7. *Training and Education to Support the Code of Conduct(CoC)*. 8 December 2000.

DODD 2000.12. *DoD Antiterrorism (AT) Program*. 8 August 2003.

DODI 0-2000.22. *Designation and Physical Protection of DoD High Risk Personnel (HRP)*. 22 January 2008.

DODI 1300.21. *Code of Conduct(CoC) Training and Education*. 8 January 2001.

DODI 1300.23. *Isolated Personnel Training for DoD Civilian and Contractors*. 20 August 2003.

DODI 2000.16. *DoD Antiterrorism (AT) Standards*. 2 October 2006.

DODI 5400.13. *Public Affairs (PA) Operations*. 15 October 2008.

UFC 4-010-01. *DoD Minimum Antiterrorism Standards for Buildings*. 8 October 2003.

UFC 4-010-02. *DoD Minimum Antiterrorism Standoff Distances for Buildings*. 8 October 2003.

UFC 4-020-01. *DoD Security Engineering Facilities Planning Manual*. 11 September 2008.

JOINT PUBLICATIONS

CJCS Guide 5260. *A Self-Help Guide to Antiterrorism.* 1 September 2010.

CJCSM 3500.04E. *Universal Joint Task Manual*. 25 August 2008.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 8 November 2010.

JP 3-0. *Joint Operations.* 17 September 2006.

JP 3-01. *Countering Air and Missile Threats*. 5 February 2007.

JP 3-05.1. *Joint Special Operations Task Force Operations.* 26 April 2007.

JP 3-07.2. *Antiterrorism*. 24 November 2010.

JP 3-13. *Information Operations*. 13 February 2006.

JP 3-13.3. *Operations Security*. 29 June 2006.

JP 3-24. *Counterinsurgency Operations*. 5 October 2009.

JP 3-26. *Counterterrorism*. 13 November 2009.

JP 3-28. *Civil Support.* 14 September 2007.

JP 3-50. *Personnel Recovery*. 5 January 2007.

JP 5-0. *Joint Operations Planning*. 26 December 2006.

JP 6-0. *Joint Communications System.* 10 June 2010.

OTHER PUBLICATIONS

Executive Order 13224. *Blocking Property and Prohibiting Transactions With Persons Who Commit, Threat to Commit, or Support Terrorism*. 23 September 2001.

U.S. Army TRADOC G2 Handbook No. 1. *A Military Guide to Terrorism in the Twenty-First Century*. 15 March 2008.

Geneva Conventions. < http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp>.

Homeland Security Exercise and Evaluation Program. https://hseep.dhs.gov/pages/1001_HSEEP7.aspx.

Homeland Security Presidential Directive 5. *Management of Domestic Incidents*. 28 February 2003.

Title 10, United States Code. *Armed Forces*.

Title 32, United States Code. *National Guard*.

DOCUMENTS NEEDED

DA Forms are available on the APD web site (www.apd.army.mil). DD forms are available on the OSD web site (www.dtc.mil/whs/directives/infomgt/forms/formsprogram.htm).

DD Form 254. *Department of Defense Contract Security Classification Specification*.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

DA Form 7566. *Composite Risk Management Worksheet*.

READINGS RECOMMENDED

These sources contain relevant supplemental information for Army leaders to help them increase their knowledge of the terrorist threat. Reading what others have written provides a foundation that leaders can use to assess situations and make appropriate decisions. The books and articles that follow are not the only good ones on these subjects. The field is vast and rich. They are, however, some of the more useful readings for Soldiers.

Brachman, Jarret. *Global Jihadism: Theory and Practice*. New York, Taylor and Francis, Ltd. 2008

Pape, Robert A. *Dying To Win – The Strategic Logic of Suicide Terrorism.* New York, Random House. 2005

Poole, H. John. *Militant Tricks: Battlefield Ruses of the Islamic Insurgent.* North Carolina, Posterity Press. 2005

Speckhard, Anne. *"Defusing Human Bombs: Understanding Suicide Terrorism," in Jeff Victoroff ed. Tangled Roots: Social and Psychological Factors in the Genesis of Terrorism*. Netherlands, IOS Press. 2006

Venzke, Ben, and Aimee Ibrahim. *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets.* Tempest Publishing, LLC. 2003

This page intentionally left blank.

Index

This page intentionally left blank.

This page intentionally left blank.

FM 3-37.2
18 February 2011

By order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
1102103

DISTRIBUTION:
Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with the initial distribution number (IDN) 116011, requirements for FM 3-37.2.