ATP 3-37.2

Antiterrorism

June 2014

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies and their contractors only to protect operational information. This determination was made on 1 June 2010. Other requests for this document must be referred to Commandant, U.S. Army Military Police School, Attn: ATZT-CDC, 320 MSCoE Loop, Suite 270, Fort Leonard Wood, MO 65473-8929.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Headquarters, Department of the Army

***ATP 3-37.2 (FM 3-37.2)**

Army Techniques Publication
No. 3-37.2

Headquarters
Department of the Army
Washington, DC, 3 June 2014

Antiterrorism

Contents

Distribution Restriction: Distribution authorized to U.S. Government agencies and their contractors only to protect operational information. This determination was made on 1 June 2010. Other requests for this document must be referred to Commandant, U.S. Army Military Police School, Attn: ATZT-CDC, 320 MSCoE Loop, Suite 270, Fort Leonard Wood, MO 65473-8929.

Destruction Notice: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

*This publication supersedes FM 3-37.2, 18 February 2011.

Figures

Tables

Preface (U)

(U) ATP 3-37.2 establishes fundamental principles and techniques for antiterrorism applications across the range of military operations. It is based on lessons learned from terrorist attacks, wartime engagements, and existing and developing antiterrorism strategies (military, federal, state, and local), policies, and doctrine.

(U) The principal audience for ATP 3-37.2 is commanders, staffs, leaders, and antiterrorism officers at all echelons that will plan and employ the antiterrorism principles and techniques discussed within. Trainers and educators throughout the Army will also use this manual.

(U) Commanders, staffs, and subordinates ensure that their decisions and actions comply with applicable United States (U.S.), international and, in some cases, host nation laws and regulations. Commanders at all levels ensure that Soldiers operate according to the law of war and the rules of engagement. (See FM 27-10.)

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

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

(U) Appendix A contains a metric conversion chart for the measurements used in this manual. For a complete listing of preferred metric units for general use, see Fed-Std-376B.

(U) ATP 3-37.2 uses joint terms where applicable. Selected joint and Army terms and definitions appear in the text. For definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition.

(U) ATP 3-37.2 applies to Active Army, Army National Guard/Army National Guard of the United States, and U.S. Army Reserve unless otherwise stated.

(U) The proponent of ATP 3-37.2 is the Maneuver Support Center of Excellence (MSCoE). The preparing agency is the MSCoE Capabilities Development and Integration Directorate; Concepts, Organizations, and Doctrine Development Division; Doctrine Branch. Send comments and recommendations on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, MSCoE, ATTN: ATZT-CDC, 14000 MSCoE Loop, Suite 270, Fort Leonard Wood, MO 65473-8929; by e-mail to <usarmy.leonardwood.mscoe.mbx.cdidcodddengdoc@mail.mil>; or submit an electronic DA Form 2028.

Introduction (U)

(U) 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 and Red China to prevent communist expansion and promote democracy and free market economic systems in developing nations. The possibility of nuclear war limited direct confrontation between U.S. and Soviet forces; but the Soviet Union and its allies promoted national wars of liberation (acts of terrorism, insurrection, guerrilla warfare) as a means to destabilize and overthrow the governments of developing nations. Additionally, those communist governments and rogue nations (such as Cuba, Libya, and North Korea) sponsored terrorism, often acting in the name of religious or political causes and directed acts of terrorism against Israel, West Germany, and other Western countries. In foreign countries, American citizens, U.S. military personnel, and their families are often targets of state-sponsored terrorism from terrorist groups (Palestine Liberation Army, Red Brigade, Red Army Faction, al-Qaeda).

(U) Recent terrorist attacks against the United States and other nations represent a variety of terrorist organizations that have broken free from state direction and funding to accomplish their own criminal and radical goals. Some modern terrorists operate for global submission to their ideology. Throughout the world, international, transnational, and domestic terrorists continue to adapt and modify their tactics. They use new technology and communications to recruit supporters, enhance operations, and share lessons learned.

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

- (FOUO) 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 protect assets and preserve combat power.
- (FOUO) Understanding the impact of psychological and information deception tactics used by terrorists to defeat the support of the local populace and the global observer.
- (FOUO) Analyzing the threat, criticality, vulnerability, and risk beyond bases and units throughout the area of responsibility (AOR), extending antiterrorism protective measures into the local populace. This enhances local support and mission accomplishment, especially during stability operations and irregular warfare.

(U) ATP 3-37.2 contains six chapters and five appendixes as follows:

- (U) **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 range of military operations. It concludes with a brief evolution of terrorist tactics throughout history.
- (U) **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.

- (U) **Chapter 3.** Chapter 3 provides doctrine for the execution of antiterrorism tasks within the operational Army. It outlines the three tactical tasks and the supporting antiterrorism tasks to effectively plan and defend against the terrorist threat. It also introduces the antiterrorism principles and how these principles guide the unit to mitigate terrorist actions.
- (U) **Chapter 4.** Chapter 4 is about implementation. It shows how the steps to counter terrorist actions are applied during movement and throughout unified land operations.
- (U) **Chapter 5.** Chapter 5 discusses how antiterrorism is integrated within the operations process through the military decisionmaking process (MDMP), mission command, and the risk management process to assess and mitigate the risk associated with terrorist activity.
- (U) **Chapter 6.** Chapter 6 addresses the antiterrorism officer's role at various organizational levels. It concludes with an introduction to a variety of working groups to assist units in focusing antiterrorism planning efforts.
- (U) **Appendix A.** Appendix A provides a metric conversion chart.
- (U) **Appendix B.** Appendix B contains personal protection measures.
- (U) **Appendix C.** Appendix C contains information on the integration of antiterrorism tactics, techniques, and procedures into various exercises.
- (U) **Appendix D.** Appendix D contains information on antiterrorism measures in operational contract support requirements packets.
- (U) **Appendix E.** Appendix E contains guidance on completing a threat, criticality, and vulnerability assessment and conducting risk analysis.

(U) 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. ATP 3-37.2 establishes a common frame of reference for commanders and staffs to assess, detect, warn of, defend against, and recover from terrorist attacks. As an Army, strategies and ideas of what antiterrorism means have adapted and extended thinking beyond bases and entry control points. ATP 3-37.2 expresses the need to make every Soldier aware of their vulnerabilities to terrorist actions and their ability to trust their 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 unified land 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 (U)

(U) The Army operates in a world that faces complex challenges influenced by enduring trends, rising regional powers, emerging space and cyber threats, and man-made disasters. At the head of these challenges is the present and growing rise of violent international and transnational terrorist networks. This chapter addresses the presence of terrorist networks throughout the range of military operations, the impact on unified land operations, and the evolution of these tactics throughout history.

TERRORISM (U)

1-1. (U) Terrorists use violence or the threat of violence to impact multiple audiences. *Terrorism* is the unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political. (JP 3-07.2) Terrorism ranges from individual acts of damage or destruction to highly sophisticated operations conducted by organized extremist groups with varied agendas (social, environmental, religious, economic, or political).

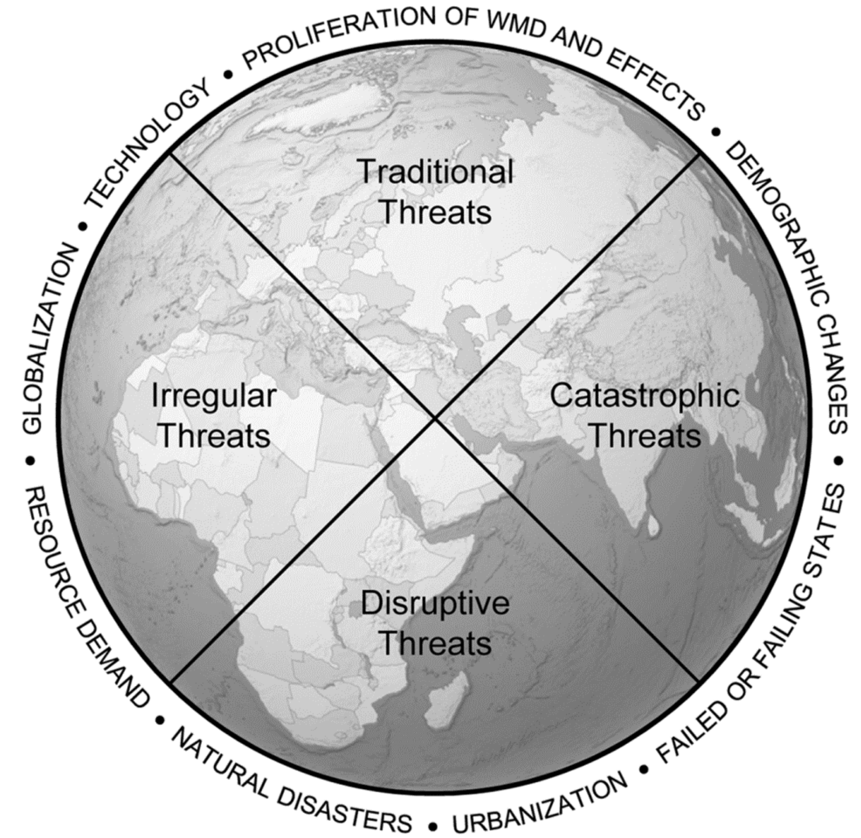
1-2. (U) Terrorists use violent and nonviolent acts to attract attention to their cause. Through the publicity that these acts generate, they communicate a message to their target audience. Terrorists seek to obtain the advantage, influence, and power that they lack and bring change on a local, regional,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

1-3. (U) 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 (JP 3-0). The operational environment includes enemy, friendly, and neutral elements. Understanding the operational environment includes the physical environment, governance, technology, local resources, and culture. The conventional military capabilities of the United States cause adversaries to pursue strategic victory through nontraditional strategies, tactics, capabilities, and methods. Adversaries will seek to circumvent or negate U.S. strengths while exploiting U.S. weaknesses. Due to the superior capability of U.S. forces, terrorists may—

- (U) Deny the United States easy access to a region.
- (U) Attack symbolic targets.
- (U) Degrade regional social and civil stability.
- (U) Disrupt regional security and economic confidence.
- (U) Seek catastrophic attack capabilities.
- (U) Distribute misinformation to a global audience.
- (U) Erode U.S. political resolve.
- (U) Promote protracted political conflict.
- (U) Use emerging media technologies.
- (U) Recruit domestically so that they blend in.
- (U) Employ women, children, and elderly or handicapped individuals to circumvent practices of profiling.

1-4. (U) Within the operational environment, Army forces face several global terrorist networks. 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) are more willing to use violence to pursue their goals in a less constrained international arena. This will result in an expanding set of actors and conflicts. Enduring trends intensify sources of conflict. (See figure 1-1.) These enduring trends include the following:

- (U) Globalization.
- (U) Technology.
- (U) Proliferation of weapons of mass destruction and effects.
- (U) Demographic changes.
- (U) Resource demands.
- (U) Natural disasters.
- (U) Urbanization.
- (U) Failed or failing states.
- (U) Religious fanaticism.



Legend:

WMD	weapons of mass destruction

Figure 1-1. (U) Challenges within persistent conflict

1-5. (U) These trends will create a future environment that presents a wide range of compound problems that occur unpredictably and perhaps simultaneously. These trends are not limited to natural disasters, terrorism, insurgency, civil war, state-on-state conflict, or multinational conflict. Shattered internal societies that are 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. (U) 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.*** (U) Adversaries in Iraq and Afghanistan presented traditional and irregular challenges. Terrorist groups (such as al-Qaeda) are irregular threats, but they also actively seek catastrophic capabilities.

1-7. (U) Terrorist networks may apply hybrid combinations to enhance the achievement of strategic terrorist objectives. Army forces will always have some degree of vulnerability to terrorist operations. Al-Qaeda specifically identifies military targets as a major priority to attack. The following contributing factors increase the danger to Army forces:

- (U) **Exposure.** Exposure increases as units and individuals are forward-deployed and internationally based. Increases in the operations tempo and the number of overseas deployments and periodic surge requirements in an operational area raise the opportunity for Army forces to operate in areas that are more accessible to terrorist groups.
- (U) **Symbolic value.** 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.
- (U) **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.

EVOLUTION OF TERRORISM (U)

1-8. (U) 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 sent 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, the use of the word *terrorism* became more prevalent. Loyalists and other opponents of the revolution employed terrorist tactics in resistance to the revolutionary agents.

1-9. (U) 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 used to defeat military and political machines gave many existing terrorist organizations and emerging resistance groups legitimacy to use a total war concept of fighting. New weapons and strategies targeted the civilian population of the enemy and destroyed its economic capacity, which 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.

1-10. (U) 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 or skill and exploit them. Some notable modern international terrorist actions that have led to the evolution and rise of antiterrorism thinking include the following:

- (U) **Provisional Irish Republican Army campaign (1969–1997).** The Irish Republican army engaged in an increasingly violent campaign against the British in Northern Ireland and England to influence public opinion in England and force the British government to withdrawal control from Northern Ireland.
- (U) **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. Their goal was to force the Israeli government to release other captured Black September members. The group killed 11 Israelis and 1 German police officer before being killed or captured.
- (U) **Beirut barracks bombing (1983).** In a coordinated suicide attack, two truck bombs driven by members of the Islamic Jihad targeted two Multinational Peacekeeping Force buildings. The terrorists targeted a U.S. military force barracks and a French military force barracks in Beirut, Lebanon. The truck drivers were able to penetrate security at both locations. In the attack on the U.S. military barracks, 241 American military personnel were killed and 60 were injured. In the attack on the French military barracks, 299 American and French military personnel and 6 civilians were killed.
- (U) **Subway sarin incident (1995).** In five coordinated attacks, perpetrators released sarin on several lines of the Tokyo subway, killing 13 people and severely injuring 50 others. The attacks also caused temporary vision problems for nearly 1,000 other people. The attack was directed against trains passing through Kasumigaseki and Nagatachō, home to the Japanese government.
- (U) **Khobar Towers bombing (1996).** Several members of the Hezbollah Al-Hijaz parked a sewage truck containing explosives equivalent to more than 20,000 pounds of trinitrotoluene (TNT) next to a fence that was approximately 72 feet from a building that housed U.S. Air Force personnel. The blast killed 19 military personnel and heavily damaged apartment complexes in the area.
- (U) **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-Qaeda network. The explosions killed approximately 223 people.
- (U) **Anthrax attacks (2001).** Over the course of several weeks, letters that contained anthrax spores were mailed to several news media offices and two Democratic U.S. Senators. These attacks killed five people and infected 17 others
- (U) **11 September attacks (2001).** Several coordinated attacks occurred in New York; near Washington, D.C.; and in Pennsylvania on the morning of 11 September 2001 when 19 al-Qaeda terrorists hijacked four commercial airliners and flew them into the World Trade Center towers, the Pentagon, and a field in Shanksville, Pennsylvania. These attacks killed 3,497 people and the 19 hijackers.
- (U) **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.
- (U) **Beslan school hostage crisis (2004).** Chechen rebels raided and took 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.
- (U) **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.

- (U) **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.
- (U) **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. When several of the agents moved to search him, al-Balawi detonated the explosives attached to his body.
- (U) **Moscow subway bombing (2010).** Two Chechen rebel female suicide bombers, known as the Black Widows, detonated explosives in Moscow subway stations during rush hour as trains pulled into the station. The suicide bombers killed 38 people.
- (U) **Pakistan suicide bombing (2011).** Two suicide bombers killed at least 80 people and injured 140 others at a military training center in Pakistan’s northwestern city of Charsadda. The Pakistan Taliban claimed responsibility for the attack, saying it was the first revenge for the killing of Osama bin Laden.
- (U) **Yemen suicide bombing (2012).** A suicide bomber dressed as a soldier blew himself up during a rehearsal for the annual Unity Day parade in the Yemeni capital, Sana’a. At least 120 people were killed and more than 350 people were injured. Al-Qaeda in the Arabian Peninsula claimed responsibility for the attack.
- (U) **Iraq bombings and shootings (2013).** On the 10th anniversary of the beginning of the Iraq War, a series of coordinated bombings and shootings killed 98 people and injured more than 200. At least 61 people were killed and 148 people were wounded in Baghdad, where most of the major attacks took place.
- (U) **Farah, Afghanistan, suicide bombing (2013).** A group of militants wearing suicide vests attacked a courthouse in Farah in an attempt to free Taliban fighters standing trial. At least 34 civilians and 12 security force members were killed, along with 9 of the insurgents. More than 100 others were injured in the attack. The attack was claimed by the Afghan Taliban.
- (U) **Boston Marathon bombing (2013).** Two bombs were detonated near the finish line of the Boston Marathon, killing 3 people and injuring more than 180 others. Two Chechen-American brothers were identified as the main suspects. One of the brothers died during a shootout with the police, and the other brother was taken into custody after being found nearly 18 hours later.

1-11. (U) The operational environment includes threats that blur the definitions of criminal, terrorist, and insurgent. Al-Qaeda is the best-known international example of such an organization. Its movement seeks to transform the Islamic societies and reorder their relationships with other nations and cultures. Al-Qaeda continues to participate in, take credit for, and support upstart organizations that execute violent and nonviolent actions that are compatible with al-Qaeda goals. Al-Qaeda’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-Qaeda’s media arm, As-Sahab, has shown significant advances in developing literature, Web sites, photographs, and movies that are created to segment and adapt the al-Qaeda propaganda message to particular groups and use the media as a weapon for countering U.S. goals.

1-12. (U) 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. missions around the globe.

1-13. (U) 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 each other'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.

1-14. (U) 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 targets on a regional level only; they also attack on a global scale, constantly trying to increase casualties and send stronger messages to their enemies. The 11 September 2001 attacks illustrated the possibility of unpredictable attacks, where anything and everything can become a weapon in the global terrorist campaign. The terrorist organization ability to influence citizens living within U.S. borders to execute attacks on behalf of the cause increases the level of complexity. Although 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.

TERRORISM AND IRREGULAR WARFARE (U)

1-15. (U) *Irregular warfare* is a violent struggle among state and nonstate actors for legitimacy and influence over the relevant population (JP 1). This broad form of conflict has insurgency, counterinsurgency, terrorism, and unconventional warfare as its principal activities. Irregular warfare favors indirect and asymmetric approaches, although it may employ the full range of military and other capabilities to erode enemy combat power, influence, and will. Enemies 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 forces cannot defeat unconventional and irregular threats, conventional Army forces may assume the lead role. During irregular warfare, Army forces may perform the following:

- (U) Foreign internal defense.
- (U) Insurgency support.
- (U) Counterinsurgency.
- (U) Combat terrorism.
- (U) Counterterrorism.
- (U) Unconventional warfare.

1-16. (U) Irregular warfare differs from conventional warfare dramatically in two aspects. First, it is domestic 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, irregular warfare also differs from conventional warfare by its emphasis on the indirect approach and the avoidance of direct military confrontation. Instead, irregular warfare 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. Irregular warfare 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 ability of civil authorities to provide security.

1-17. (U) Increasingly, the threats that U.S. forces face include 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, cyberwarfare, and low-tech weapons. Modern examples of these tactics include the following:

- (U) **Vietnam War (1959–1975).** 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, Pathet Lao, and Khmer Rouge.
- (U) **Soviet/Afghanistan War (1979–1989).** The Soviet military deployed a contingent set of forces, upwards of 108,000 personnel, into key bases, urban centers, and strategic locations throughout Afghanistan. The Soviets immediately faced a nationalistic guerilla force, called the *Mujahideen*, who fought the Soviet conventional force with varied asymmetric tactics and U.S.-supplied weapons and training until Soviet withdrawal in 1989.
- (U) **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.

1-18. (U) 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 instructional 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 area of operations is critical in knowing the threat capabilities and intentions.

1-19. (U) Terrorism and combating terrorism are activities conducted as part of irregular warfare and are frequent 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 counter-threat finance. Adversaries employing irregular warfare 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.

1-20. (U) During irregular warfare, the Army supports friendly states against hostile states and nonstate adversaries operating within nonbelligerent states. The following may take place during irregular warfare:

- (U) **Beginning** s**haping operations early.** Before and during shaping operations, commanders should assess the threat of terrorist activities and review antiterrorism guidance in anticipation of future operations.
- (U) **Employing integrated force packages that fuse military operations and intelligence activities at the tactical level**. When conducting irregular warfare, Army forces frequently conduct military operations to generate their own actionable intelligence and targeting data using human intelligence, signals intelligence, technical intelligence, counterintelligence, identity intelligence operations (biometrics, forensics, document and media exploitation), and cultural information to illuminate adversary networks and support activities and positively identify local populous (enemy or friendly) personalities. For example, commanders may establish teams in which military intelligence and law enforcement forces fuse operational intelligence on terrorist groups operating in their area of operations.

- (U) **Focusing tasks on enhancing or destabilizing the relationships between a political authority and the relevant populations.** Tasks in support of enhancing relationships include humanitarian assistance, civic action projects, effective governance promotion, counterinsurgency, counterterrorism, stability, and foreign internal defense. Tasks in support of destabilizing relationships include using unconventional warfare, training insurgent forces, and providing maneuver and sustainment support to partners. Security cooperation and security assistance missions significantly contribute to assisting the host nation government, military, and police forces in establishing or strengthening national capabilities and promoting stability to counter irregular warfare threats. 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 attacks.
- (U) **Reducing Army force presence after the security situation stabilizes.** Other government agencies and partners continue long-term, steady-state activities. The transition toward stability tasks and the ultimate handover to host nation security forces presents another opportunity for terrorists to attack the United States and partner nations as operations become more static and predictable.

UNIFIED LAND OPERATIONS (U)

1-21. (U) Unified land operations is the Army operational concept and contribution to unified action. *Unified land operations* describe how the Army seizes, retains, and exploits the initiative to gain and maintain a position or relative advantage in sustained land operations through simultaneous offensive, defensive, and stability operations in order to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution (ADP 3-0). The Army employs synchronized action (lethal and nonlethal) proportional to the mission and informed by a thorough understanding of all variables of the operational environment. A mission command that conveys intent and an appreciation of the situation guides the adaptive use of Army forces. (See ADP 3-0 and ADRP 3-0.)

1-22. (U) Unified land operations involve dynamic, continuous interaction between friendly forces and diverse groups throughout the area of operations. 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. Most 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.

ANTITERRORISM IN ARMY OPERATIONS (U)

1-23. (U) The Army is a critical component of unified action, employing landpower through unified land operations ranging from military engagement, security cooperation, and deterrence to major operations and campaigns. The effective employment of landpower requires securing and maintaining the initiative and combining types of operations. As a nonwarfighting functional element, antiterrorism is integrated throughout the operations process and across unified land operations. The application of antiterrorism measures is a supporting task of the protection warfighting function. (See ADRP 3-37.)

1-24. (U) Antiterrorism tasks play a critical role in the defense against terrorist acts and in how the force preserves combat power against actions by nonstate actors. Antiterrorism 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. Antiterrorism continues to serve as a foundation for unit security posture and how it applies actions within the protection warfighting function, even as the unit transitions to offense during major operations.

Note. (U) See JP 1 for additional information on the range of military operations, and see ADP 3-0 and ADRP 3-0 for additional information on unified land operations.

1-25. (U) Army forces operate across the range of military operations 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 less intensive missions (military engagements, security cooperation, deterrence) 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. Antiterrorism officers use proven measures within the antiterrorism 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 major operations and campaigns.

1-26. (U) 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 (JP 3-0). The threat of terrorism exists during all operations, including major operations.

1-27. (U) Antiterrorism planning and execution should consider a wider range of operational environments and the varying degree of terrorism risk. It is important for commanders and staffs to understand that terrorists can attack within any operational environment. 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. The traditional conflict continuum concept (the level of risk increases throughout the range of military operations) may no longer be true in respect to terrorism. Therefore, commanders should proactively conduct antiterrorism assessment, planning, and preparations across all operations to understand the terrorist threat and plan countermeasures.

1-28. (U) A change in the type of operation or task may require modification to the mission-essential task list and additional training for deploying units and units in the area of operations. The benefit of an antiterrorism program integrated throughout unit training (at home, camp station, and abroad) extends individual Soldier awareness and unit understanding of physical security measures without requiring new training. Antiterrorism training should be given the same emphasis as tactical task training; and as it 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 during any type of operation or task, anywhere they operate.

OPERATIONAL VARIABLES (U)

1-29. (U) 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 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.

1-30. (U) 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 ADRP 3-0. The information below is more specific to terrorism and terrorist organizations.

POLITICAL (U)

1-31. (U) 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 (such as tribal elders or 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. Antiterrorism 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.

1-32. (U) Antiterrorism officers also analyze how multinational and local political decisions within the area of operations impact, or are influenced by, other operational variables (economic, social, or 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, in some cases, political structures. Political ideology inconsistent with Islamic norms may be seen as a threat to Islamic societies. In this sense, the perceived encroachment of Western political ideology and cultures in Muslim majority societies is sometimes cited by Islamic terrorist groups as one of the reasons for their fight.

1-33. (U) Failed or failing states hold a number of attractions for terrorist organizations. Failed states retain the outward signs of sovereignty, although 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—

- (U) 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.
- (U) Permitting terrorist groups to engage in smuggling and drug-trafficking and establish transshipment points to raise funds for operations.
- (U) 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.
- (U) 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 (U)

1-34. (U) The military variable includes state and nonstate armed forces capabilities within the operational environment. Commanders analyze force capabilities to defend against and defeat terrorists operating within their area and to analyze terrorist capabilities to attack U.S. and multinational partners, high-risk personnel (HRP), critical infrastructure, and information networks. The antiterrorism officer reviews friendly force training cycles and schedules for periods of vulnerability, particularly while forces are massed, in recovery, or in-transit. The antiterrorism 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 antiterrorism 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. Antiterrorism officers assist in developing a plan to defend against these tactics and to mitigate their impact on the mission and strategic goals.

ECONOMIC (U)

1-35. (U) The economic variable encompasses individual and group behavior related to producing, distributing, and consuming resources. Antiterrorism officers help the commander to understand factors within economic behaviors that could or do influence and support terrorist actions or factors (unemployment, hiring practices, class delineation, and cultivation of alternative illegal enterprises [drugs]). The antiterrorism 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.

1-36. (U) 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. EO 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 tactics:

- (U) **Extortion and kidnapping.** Terrorist organizations engage in extortion and kidnapping as a means of getting ransom or blackmail money to finance future operations.
- (U) **Smuggling.** Organizations smuggle drugs, weapons, and people as a means of enhancing their current capabilities or for monetary compensation.
- (U) **Counterfeiting.** Reproducing currency or designer goods is an inexpensive way to generate financing and support operations.
- (U) **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.
- (U) **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.
- (U) **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.
- (U) **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 the religion of Islam and supporting the citizens of poverty-stricken countries, while some are created with the sole intention of funding terrorism. At times, al-Qaeda has received more than $30 million per year in presumed charitable donations. This same technique was used successfully during the Provisional Irish Republican army terrorist insurgency in Northern Ireland (1967–1998) when many bars in Boston and supposedly Catholic charities were fraudulently used to fund weapons for the Irish Republican army conflict.

SOCIAL (U)

1-37. (U) 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 antiterrorism 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 a 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 (U)

1-38. (U) Broadcast media sources (print, television, radio, the Internet, and social media networks) can rapidly disseminate views on military operations worldwide. Many organizations (such as al-Qaeda) have advanced their media production and development capabilities to rival U.S. film production companies. In turn, media coverage 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, the Internet, and propaganda to segment and influence their target audience.

1-39. (U) Antiterrorism 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 (U)

1-40. (U) 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 defense support of civil authorities tasks. 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.

1-41. (U) Planners analyze strengths and shortfalls. This helps determine critical assets for future protection or reflects 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 area of operations. Troop occupation or the defacement of cultural landmarks and structures is used as disinformation to fuel the terrorist cause and aid in recruitment. The sabotage of energy supplies, key bridges, water lines, and schools by terrorists reduces public confidence and influences mission success, especially during peacekeeping and stability.

PHYSICAL ENVIRONMENT (U)

1-42. (U) 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 means of supporting terrorist activities.

1-43. (U) 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 mission command and information collection 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 (U)

1-44. (U) 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 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.

1-45. (U) 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, antiterrorism officers seek to disrupt and defeat the time advantage of terrorists.

INFLUENCE ON MISSION VARIABLES (U)

1-46. (U) 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 understanding when terrorism is not the main threat in a particular area. Table 1-1 shows how these variables influence terrorism considerations at the tactical level through the 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 1-1. (U) Operational variables effects on mission variables

	Mission	***Enemy***	***Terrain and Weather***	***Troops and Support Available***	***Time Available***	***Civil Considerations***
Political						X
Military		X		X		
Economic						X
Social						X
Information				X		X
Infrastructure						X
Physical Environment			X			
Time						

This page intentionally left blank.

Chapter 2

Terrorist Tactics (U)

(U) Terrorism is a tactic. This chapter presents an overview of conditions that are a composite of capabilities and limitations which may be present in a complex operational environment that includes terrorism. Acts of terrorism demonstrate an intention to cause significant psychological and physical effects on a relevant population through the use or threat of violence. The terrorist threat to U.S. forces will continue for the near future. In antiterrorism, the principle of assess involves a continuous process to compile and analyze available information concerning potential terrorist activities within a commander's area of operations. (See chapter 3 for additional information on antiterrorism principles.) A comprehensive threat assessment using a DOD methodology that consists of four factors (operational capability, intentions, activity, and operational environment) can help commanders anticipate the possibility of attacks. This chapter describes the general categories of terrorist groups and their motivations and tactics as an integral step in identifying the probability of a terrorist attack. This chapter also addresses security challenges associated with people, motivations, and actions under the general topic of terrorism and the tactics that terrorists employ in contemporary incidents.

NONSTATE GROUPS (U)

2-1. (U) 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 as terrorists can also be categorized as insurgents, guerrillas, criminals, and other types of nonstate affiliates or adherents that use terrorism.

2-2. (U) Many armed nonstate groups purposely mask their activities within a relevant population. 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 battalion or brigade intelligence staff officer (S-2) should consider when developing an understanding of the operational capability characteristics of the threat are—

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

- (U) What are the group operational doctrine; strategies; and tactics, techniques, and procedures?
- (U) Are there linkages with the police, military, other criminal organizations, political parties or groups, major businesses, or other organizations?
- (U) What are the group goals?

INSURGENTS (U)

2-3. (U) *Insurgency* is the organized use of subversion and violence to seize, nullify, or challenge political control of a region. Insurgency can also refer to the group itself. (JP 3-24) The term insurgent broadly refers to types of unconventional forces and operations and can include guerrilla; insurgent; criminal; subversive; revolutionary; and affiliate, adherent, and similar actors, 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. (U) 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 (U)

2-5. (U) *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 the military-like organizational structure and normal operations. 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 operations.

PARAMILITARY FORCES (U)

2-6. (U) *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). 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. (U) 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. (U) 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 state 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 (U)

2-9. (U) Criminal organizations are normally independent of nation-state control. However, large-scale criminal organizations often extend beyond national boundaries to operate regionally, transnationally, 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. (U) By mutual agreement or when their interests coincide, criminal organizations may become affiliated with other actors (such as insurgents or individuals providing capabilities similar to a private army for hire). Criminal organizations controlling or operating in the same area as insurgents or guerrillas can provide security and protection to insurgent or guerrilla activities in exchange for financial assistance, intelligence, arms and materiel, or general logistic support. Criminal organizations can create diversionary actions or conduct reconnaissance and early warning, money laundering, smuggling, transportation, and civic actions on behalf of the insurgents or guerrillas. Their mutual interests can include preventing U.S. or government forces from interfering in their activities.

2-11. (U) 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. (U) At times, criminal organizations might also be affiliated with nation-state military or paramilitary actors. In a 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. (U) 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. (U) 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, work skills, or 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 recruitment 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, actions have expanded to include piracy in failed states (such as Somalia).

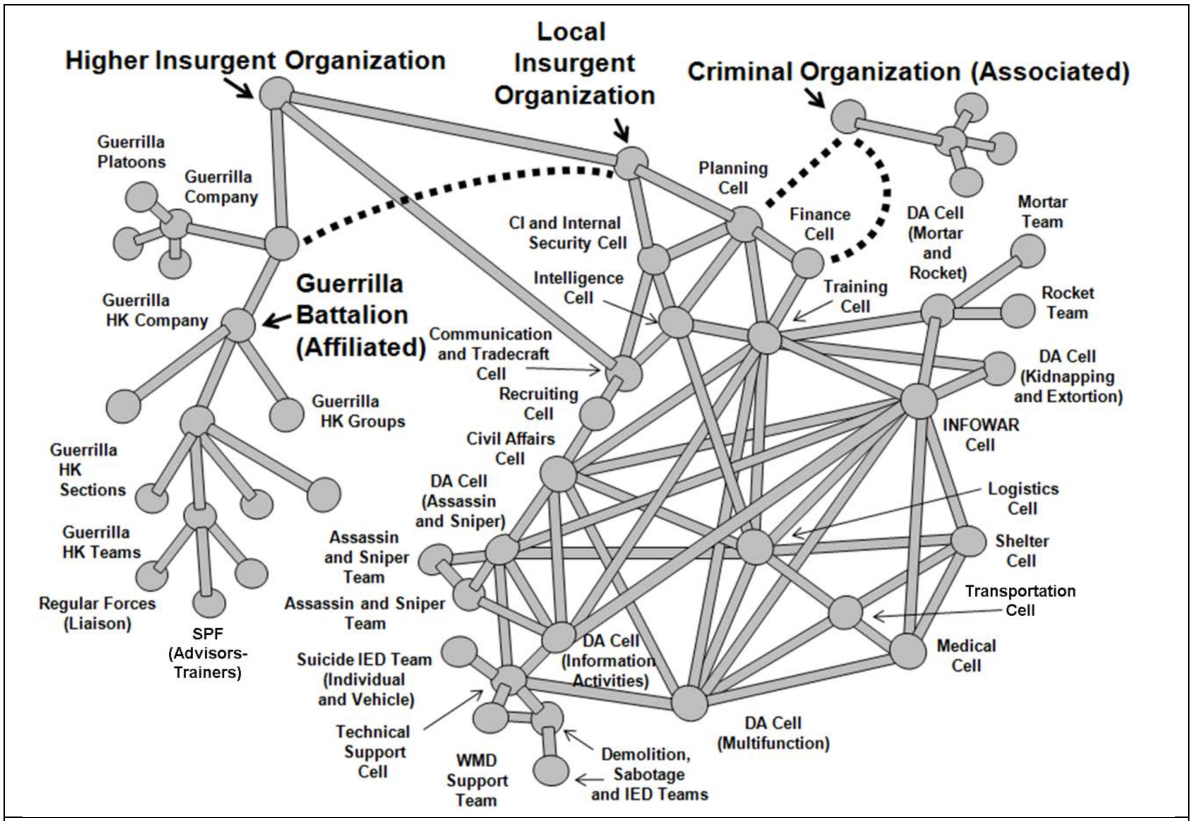
2-15. (U) Contemporary terrorism relies on networks of interrelated terrorist groups, social movements, and criminal organizations to conduct operations, secure funds, and influence audiences. Historically, terrorists and criminal organizations were local, regional, or occasionally, transnational threats. Rarely did terrorists challenge the nature of the nation-state or modern state authority and governance. 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 their activities often overlap.

TERRORIST NETWORKS (U)

2-16. (U) 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. These networks also aim to exhaust the will of the United States and its multinational partners who oppose them.

2-17. (U) Terrorist networks often oppose globalization, the expansion of democracy, and the freedom it often brings. Although 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 the following:

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



Legend:

CI	counterintelligence
DA	direct action
HK	hunter-killer
IED	improvised explosive device
INFOWAR	information warfare
SPF	special-purpose forces
WMD	weapons of mass destruction

Figure 2-1. (U) Terrorist network

2-18. (U) 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-Qaeda and its associated movements (such as al-Shabaab or Boko Haram) operate in more than 80 countries. They have conducted attacks around the world, including the attacks on 11 September 2001 in the United States. State sponsors of terrorism (Iran, Syria, Yeman, Lebanon, and Libya) 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 covert operatives create a network of safe houses, vehicles, equipment, finance, and local information.

2-19. (U) Historically, terrorist organizations prefer to attack soft 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 the 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 adversary strengths against U.S. weaknesses. The most devastating form of these attacks will be conducted with the use of chemical, biological, radiological, nuclear, and explosives (CBRNE) components.

OPERATIONAL CAPABILITY (U)

2-20. (U) Terrorist groups or operations align along national, transnational, and international areas of influence. National groups are typically composed of individuals from the same nation that operate within the boundaries of a single state or nation. Transnational groups are usually composed of members from various nations and operate across international borders. International groups operate in two or more nations and usually receive support from a foreign government.

2-21. (U) 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—

- (U) **Nonstate-supported.** These terrorist groups operate autonomously, receiving no support from any government.
- (U) **State-supported.** These groups generally operate independently, but receive some support (financial, logistic, intelligence) from one or more governments.
- (U) **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 (U)

2-22. (U) 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-term) generally demonstrate group intent as—

- (U) Demonstrating anti-U.S. sentiment.
- (U) Demonstrating anti-host nation sentiment.
- (U) Attracting publicity to the group cause.
- (U) Demonstrating group power.
- (U) Demonstrating government weakness.
- (U) Exacting revenge.
- (U) Obtaining logistic support.
- (U) Causing a government to overreact.

2-23. (U) Terrorists tend to align themselves with particular ideologies or political philosophies as a justification for their actions to host nation 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—

- (U) **Separatist.** These groups desire separation from existing entities through independence, political autonomy, or religious autonomy 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.
- (U) **Ethnocentric.** Groups of this identity view race or ethnicity as the defining characteristic of a society, and a select group is often perceived superior because of its inherent racial or ethnic characteristics. Ethnicity, therefore, becomes a basis of cohesion.
- (U) **Nationalistic.** The loyalty and devotion to a nation and the national consciousness derived from placing national culture and interests above those of other nations or groups are the motivating factors 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.
- (U) **Revolutionary.** These groups are dedicated to the overthrow of an established order and replacing it with a new political or social structure.

Ideological Categories (U)

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

- (U) **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.
  - (U) **Right wing.** These groups are associated with the reactionary or conservative side of the political spectrum and, in the extreme, 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, often their intent is to replace existing forms of government with a much smaller and more limited government.
  - (U) **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. Often their intent is to have a very large government that takes charge of every facet of life.
  - (U) **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 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, while leaning toward no government and few rules. 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.

- (U) **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 (Protestant and Catholic Christian) 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. Cults that adopt terrorism are often apocalyptic in their world view and are extremely dangerous, unpredictable, and difficult to penetrate and deter.
- (U) **Social.** Particular rules of law, social policies, or issues will often be so contentious that they will incite extremist behavior and terrorism. For example, the federal law on abortion rights (Roe versus Wade) focuses attention of antiabortionists who attack medical clinics and employees. This is frequently referred to as single-issue or special-interest terrorism.

INSIDER THREATS (U)

2-25. (U) Commanders must also be aware of Soldiers, Department of the Army (DA) civilians, contractors, and others operating within the vicinity of their area of operations who sympathize with extremist groups and terrorist organizations and their ideals. Attacks on Soldiers (such as the shooting attack at Fort Hood, Texas, in 2009) have raised the need for effective leadership and antiterrorism measures to protect the force, even from one another. Exposure to actions in the area of operations, in conjunction with challenged personal situations or crises that shake belief systems, can test a Soldier's loyalty to their unit, their fellow Soldiers, and their nation and make them 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—

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

2-26. (U) Another form of insider threat comes from host nation or allied military units that the Army is working in conjunction with or training. Individuals from within these foreign militaries may be insurgents who have infiltrated their country's military, or they could be members who are sympathizers of, or influenced by, a terrorist ideology from their country or region. Examples of this have been the numerous green on blue attacks during operations in Afghanistan.

SELF-RADICALIZATION (U)

2-27. (U) The number of U.S. extremists is growing as a number of unlikely militants throughout America become radicalized using the Internet. These U.S. extremists plot attacks at home and abroad. The influence of people 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-Qaeda and other terrorist groups spread their ideology into the United States and to other citizens of Western society. The distinct phases to radicalization are—

- (U) **Preradicalization.**
  - (U) Absence of a psychological profile.
  - (U) Identity crisis.
  - (U) Influence in meetings at religious institutions, on the Internet, at school, at home, at work, in prison, or through sports activities.
- (U) **Self-identification.**

> ***Note.*** (U) The trigger to transition an individual from a passive to active actor in terrorism can be a single emotional event or incident or a long-term, progressive rationalizing of why and how a perceived wrong must be corrected.

  - (U) Economy (lost a job, had a promotion blocked, received Uniform Code of Military Justice discipline from the military).
  - (U) Social alienation, discrimination, or racism (real or perceived).
  - (U) Politic (international conflicts involving a certain demographic, political wing, or religion).
  - (U) Death in the family or unit.
  - (U) Religion that is influenced by ideology.
- (U) **Indoctrination.**
  - (U) Withdrawal from normal functions, church or moderate mosques, and other social activities.
  - (U) Politicization of new beliefs (preaches or argues with other unit members).
  - (U) Increased training that may involve travel overseas.
  - (U) Role assignments.
  - (U) Group bonding or local training camps.
  - (U) Meetings with like-minded individuals in areas that are hard to detect (private homes, the countryside).
- (U) **Commitment to act.**
  - (U) Mission acceptance and a decision to carry out violent action in support of the mission.
  - (U) Training and preparation (actions on contact, rehearsals).
  - (U) Mental reinforcement activities.
  - (U) Attack planning (research, surveillance, intelligence gathering, resource acquiring).

2-28. (U) 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, DA civilians, and contractors 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 that unit members do 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 confines in which the individual lives and operates is the best gauge for detecting unusual, out-of-character, or questionable behaviors.

2-29. (U) 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 movements. The consensus view among analysts is that converts to religions and some ideologies, regardless of other demographic factors, bear an elevated risk of radicalization for two key reasons:

- (U) The desire to prove their conviction.
- (U) The general ignorance of the overall teachings and the complex, interpretive methodologies of religious traditions.

2-30. (U) Although many potential indicators are innocuous alone, when combined, they may paint a more sinister picture. These indicators include—

- (U) Advocating violence, the threat of violence, or the use of force to create fear and achieve goals that are generally political, religious, or ideological. (See AR 190-14 for additional information on use of force.)
- (U) Advocating support for international terrorist organizations or objectives.
- (U) Providing financial or other material support to a terrorist organization or to a suspected terrorist.
- (U) Having familial ties to known or suspected terrorists or terrorist supporters.
- (U) Associating with or having connections to a known or suspected terrorist.
- (U) Repeating expressions of hatred and intolerance of American society, culture, government, military, or the principles of the U.S. Constitution.
- (U) 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.
- (U) Expressing an obligation to engage in violence in support of international terrorism or inciting others to do the same.
- (U) Demonstrating shifts in personal relationships.

2-31. (U) Commanders and leaders should also be aware of, or attempt to discover, a Soldier's reliance on some sort of intermediary (an extremist cleric or a terrorist recruiter) to facilitate and catalyze the Soldier's radicalization. These communications often occur online (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 counterintelligence, personnel security, law enforcement, and information assurance capabilities to assess, detect, and mitigate insider threats within their units.

2-32. (U) A lone or independent actor, 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 (wives, parents, close friends, fellow Soldiers) of terrorists and extremists 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 (U)

2-33. (U) Geographic designations are sometimes used to categorize terrorist groups. (See figure 2-2, page 2-10.) In some instances, geography overlaps with ethnic, national, religious, or ideological aspirations. Geographical association with the area of the primary concern for the group will be made, although these designations are only relevant to the government or state that uses them.

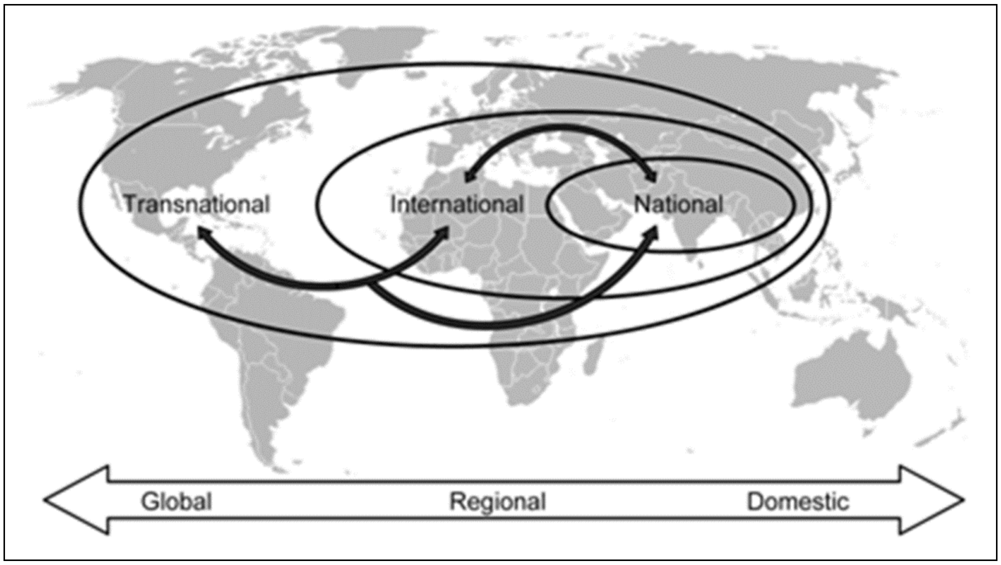


Figure 2-2. (U) Operational reach of terrorists

2-34. (U) Examples of geographically categorized terrorists are—

- (U) **National or domestic.** 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 efforts specifically on the sociopolitical arena of their nation.
- (U) **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 it 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.
- (U) **Transnational.** Transnational groups are usually active within a unique geographic continent. However, these groups cross over national or domestic boundaries to conduct operations and retreat back to their safe havens until the next opportunity or mission.

TERRORIST ACTIVITY (U)

2-35. (U) Terrorist activity includes actions during the planning process, as the specific attack forms, or as tactics are employed. The activities of the group may include—

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

2-36. (U) 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 (such as an attack on U.S. forces). The most common rationales for targeting U.S. military forces are to—

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

STRUCTURE (U)

2-37. (U) 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, time, or the need for survival. (See figure 2-3.)

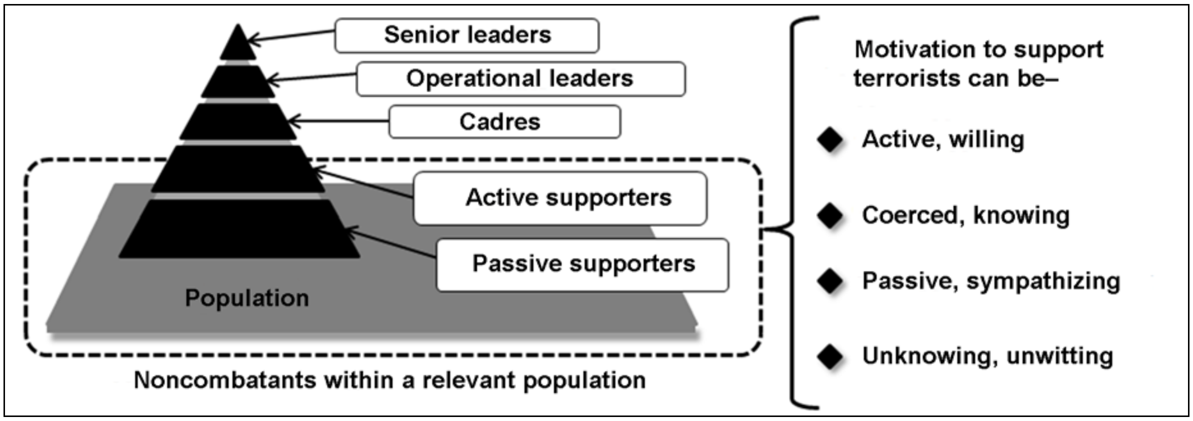


Figure 2-3. (U) Terrorist organizational support model

2-38. (U) 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:

- (U) **Leaders.** Leaders provide direction, approve goals and objectives, and give guidance for achieving the organization mission. Leaders are broken into two levels of command structure:
  - (U) **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.
  - (U) **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, operational leaders rise from within the ranks of an organization or splinter and create their own organization (such as Abu Musab al-Zarqawi).
- (U) **Cadres.** The cadres are active members of the terrorist organization. This echelon plans and conducts operations and manages intelligence, finances, logistics, propaganda, and communications. Mid-level cadres tend to be trainers and technicians (bomb makers, financiers, surveillance experts). Low-level cadres are inspired actors and recruits. They are the actual bombers and direct-action terrorists.

- (U) **Active supporters.** Active supporters are active in the political, fundraising, and information activities of the group. They may also conduct information collection 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.
- (U) **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, the fear of reprisal from terrorists (for overt noncompliance) is a compelling factor for passive supporters.

2-39. (U) 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.

2-40. (U) 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-Qaeda may take their inspiration for terrorism from ideological statements of senior al-Qaeda leaders, yet their direct actions are unilateral.

2-41. (U) A terrorist organization 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—

- (U) **Operations.** The operations function will determine the operational objectives of the attack, the participants, the specific target, the timing, and the attack method.
- (U) **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 intelligence capabilities or current and relevant knowledge of the target area. The security subfunction may also include countersurveillance security to prevent compromise of the group and its mission and counterintelligence to detect and neutralize insider threats to the terrorist organization.
- (U) **Support.** The support function normally fulfills requirements (recruitment and personnel support, media, financing, education, camp management, logistics, supplies, weapons, munitions, transportation, communications).
- (U) **Cadre or cell.** The cadre, or action element, is the heart of the organization and is manned by those who are trained to execute the attack or emplace the bombs.

2-42. (U) 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, fundraising, 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 targeted members with U.S. citizenship.

2-43. (U) 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 force cooperation.

2-44. (U) In addition to structure and the type of members, threat group capabilities include training, weapons, equipment, and threat tactics. Training seeks to achieve a proficiency level 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 who are willing to exchange training, there are also experts in the technical, scientific, operational, and intelligence fields who are willing to provide training or augment operational capabilities on a contract basis.

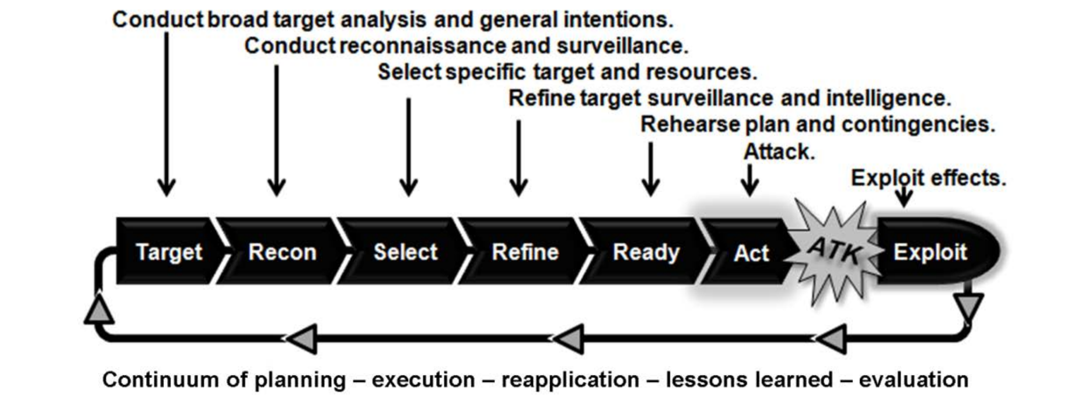
2-45. (U) The threat of domestic terrorism (groups or individuals whose activities are directed at the host nation government from where they originate) includes extremist groups, militia groups, and individual actors. Domestic terrorists can be motivated by grievances that include special interests, single issues, anarchy, sovereign rights, race-based hate, and self-preservation or personal rights. 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 terrorists identify with single-issue or special-interest groups who use terrorism to influence policy on a single issue (such as animal rights; abortion; ecology; the environment; an antigovernment stand; or ethnic, race, or minority rights).

2-46. (U) 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 the—

- (U) Los Angeles Times building bombing (1910).
- (U) Wall Street bombing (1920).
- (U) Bath school bombings (1927).
- (U) Unabomber attacks (1978–1995).
- (U) Murrah Federal Building, Oklahoma City, bombing (1995).
- (U) Centennial Olympic Park bombing (1996).
- (U) Anthrax attacks through the U.S. Postal Service (2001).
- (U) Fort Dix attack plot (2007).
- (U) Little Rock, Arkansas, recruiting station shooting (2009).
- (U) Times Square bombing attempt (2010).
- (U) Boston Marathon bombing (2013).

TERRORIST PLANNING CYCLE (U)

2-47. (U) 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.


Conduct broad target analysis and general intentions.
Conduct reconnaissance and surveillance.
Select specific target and resources.
Refine target surveillance and intelligence.
Rehearse plan and contingencies.
Attack.
Exploit effects.
Target
Recon
Select
Refine
Ready
Act
ATK
Exploit
Continuum of planning – execution – reapplication – lessons learned – evaluation

Legend:

ATK	attack
recon	reconnoiter

Figure 2-4. (U) Typical terrorist planning cycle

2-48. (U) The generic sequence and timing of terrorism depends on organizational capabilities and limitations, operational constraints, and the commitment level of an actor or organization. Understanding this underlying motivation is fundamental to appreciating the resolve to plan and act. Terrorists create conditions to optimize awareness, training, and mission readiness to achieve objectives that counter enemy forces. When advantageous to terrorist operations, coordination and cooperation can combine the capabilities of conventional military, paramilitary, criminal activities, and terrorism.

2-49. (U) Tactics, techniques, and procedures include creating conditions of instability in a particular operational environment, alienating the population from the governing authority of the region, and improving the irregular force influence on a designated populace and key leaders in that relevant population. In complex conditions, terrorists may be able to employ a range of organizational options from small, loosely affiliated cells to global networks to promote psychological effects and mission success. Such networks can be local, regional, international, or transnational affiliations; host simple or sophisticated media affairs programs; and acquire covert or overt financial, political, military, or social support in terrorist plans and operations.

2-50. (U) A terrorism planning cycle is actually a continuum. Terrorists typically plan, prepare, act, and apply experience and skill to achieve objectives. The concept of a spiral effect may be a more effective way to visualize and understand a planning cycle of terrorism. Even with periodic setbacks in acts of terror capabilities and execution, the resolve of terrorists to a compelling agenda is often progressive, adaptive, and long-term to achieve organizational objectives.

2-51. (U) Throughout a continuous planning cycle, terrorists gather information on potential targets, determine the likelihood of a successful attack, make decisions on tactics, commit resources, establish execution timelines, and train and rehearse for the operation. At any time throughout the cycle, attack planning can be halted or accelerated based on gathered information, friendly force actions, or changes in group intentions. U.S. forces can influence the terrorist planning cycle throughout the phases.

2-52. (U) Terrorist operations are typically prepared to minimize risk and achieve the highest probability of success by avoiding enemy strengths and concentrating attacks on enemy weaknesses. Emphasis is often placed on maximizing irregular force security and terrorism effects. Security measures usually include planning and operating with small numbers of irregular force members to more effectively compartment knowledge of a pending terrorism mission.

2-53. (U) Collection against potential targets may continue for years before an operation is decided upon. Detailed planning is normal, but it can be deliberately shortened when an opportunity arises. While some targets may be vulnerable enough with shorter periods of observation, the information gathering and analysis for intelligence will be intense. Operations planned or underway may be altered, delayed, or cancelled due to changes at the target or in local conditions. Tactical missions conducted by or for larger irregular forces complement operational objectives and strategic goals of the irregular force. The psychological impact on a targeted population is the overarching objective of any terrorist operation.

2-54. (U) Terrorists use their experience and expertise to effectively apply traditional principles for plans and operations and often exchange expertise in particular skill sets (recruitment, media affairs, and training on various forms of direct action in terrorism). Tactical methods and analysis of successful missions are often shared via the Internet and Web sites hosted by an irregular force. Adaptability, innovation, improvisation, and risk assessment are key components of plans and actions toward mission success.

PHASE I: BROAD TARGET SELECTION (U)

2-55. (U) This phase involves using available sources to collect information on potential targets. Collectors may be core members of the terrorist cell, sympathizers, or people providing information without knowledge of the intended purpose.

2-56. This phase also includes open-source and general information collection. Some types of information collection include the following:

- (U) Stories from newspapers and other media that provide background information.
- (U) Internet research that provides data (texts, pictures, blueprints, video information).
- (U) 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).

2-57. (U) 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 (U)

2-58. (U) This phase can be very short or span many years. Some elements of information that are typically gathered include the following:

- (U) **Practices, procedures, and routines.** This includes regularly scheduled deliveries, work schedules, identification procedures, and observable routines.
- (U) **Residences and workplaces.** This includes the physical layout and individual activities at the two places the target typically spends the most time.
- (U) **Transportation and travel routes.** This includes the mode of transportation, common travel routes (house, work, gym, school), ingress and egress points, vehicles allowed on the grounds, and public transportation.
- (U) **Security measures.** This includes security around the target, presence and 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.

2-59. (U) 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 need to be alert for activities that may be precursors to terrorist acts. These personnel are well trained and well disposed to be vigilant.

2-60. (U) The following are examples of activities or conditions that may be indicators of terrorist threats:

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

2-61. (U) The activities and conditions listed are not 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 (U)

2-62. (U) 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:

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

PHASE IV: PREATTACK SURVEILLANCE AND PLANNING (U)

2-63. (U) 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 current patterns of the target 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—

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

PHASE V: ATTACK REHEARSAL (U)

2-64. (U) 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 the following:

- (U) Equipment and weapons operational checks.
- (U) Communications and signals to be used in the mission.
- (U) Skills performance of all and/or particular specialists.
- (U) Final preparatory checks.
- (U) Preoperations inspection drills.
- (U) Deployment sequence of movements and maneuver into the target area.
- (U) Actions near or on the objective.
- (U) Primary and alternate escape routes.

- (U) Initial safe haven, hiding sites, or rally point actions.
- (U) Transfer plans from the initial safe haven to subsequent safe havens.

2-65. (U) Rehearsals for upcoming attacks have taken place at unpopulated weapons ranges, at paintball facilities, and near terrorist 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—

- (U) Target information gathered to date.
- (U) Target patterns of activities.
- (U) Physical layout of the target area for changes in routes or man-made features.
- (U) Time-distance factors from the assault position to the attack point.
- (U) Security force presence during varied states of alert.
- (U) Reaction response timing by security forces to a demonstration, feint, or threat.
- (U) Ability to pre-position or retrieve equipment or vehicles near the objective.
- (U) Ease of blocking and restricting an escape route at critical choke points.

PHASE VI: ACTIONS ON THE OBJECTIVE (U)

2-66. (U) 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—

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

2-67. (U) Simultaneous actions may include those taken by an assault element, security element, and support element. Some missions may require a breach element. Actions on the objective will sequence through several main tasks:

- (U) Isolate the objective site.
- (U) Gain access to the individual(s) or asset.
- (U) Control the target site.
- (U) Seize or destroy the individual(s) or asset at the objective.
- (U) Achieve the mission task.

PHASE VII: ESCAPE (U)

2-68. (U) Escape plans are usually well rehearsed and well executed. The exception is a suicide attack. However, even in suicide attacks, there are usually support personnel and handlers who must escape or evade response force personnel.

2-69. (U) 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.

TERRORIST NETWORKS, PLANNING, AND TACTICS (U)

2-70. (U) Terrorist tactics display common principles of armed conflict and propaganda with the intent to cause fear and tactical surprise 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 threat 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 through 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 tactics, techniques, and procedures.

2-71. (U) Incidents of terrorism can be the rogue action of a lone individual or the sanctioned activities of large organizations acting under nation-state directives. 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.

2-72. (U) 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 area of operations.

2-73. (U) 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. Examples of tactics, techniques, and procedures 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 (U)

2-74. (U) Terrorist tactics include defensive actions conducted to defeat an enemy attack, gain time, economize their capabilities, and 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. Terrorists can augment defensive actions with terrorism to—

- (U) Defeat an enemy attack.
- (U) Gain time.
- (U) Economize irregular force capabilities.
- (U) Develop conditions favorable for subsequent offensive operations.

2-75. (U) 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 area of operations. The retrograde is a transitional action 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 include the following:

- (U) Dispersing and hiding.
- (U) Using human shields.
- (U) Exploiting sensitive infrastructure.
- (U) Conducting inform-and-influence activities.

Dispersion and Hiding (U)

2-76. (U) Dispersion and hiding in complex terrain and urban environments degrade situational understanding 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 leadership and command of terrorist organizations is often decentralized. Terrorist operations are noncontiguous and dispersed.

2-77. (U) Within an area of operations, 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.

2-78. (U) Safe houses may be houses, apartments, mosques, stores, refugee camps, barracks, or other infrastructures that house individuals involved in criminal or terrorist activities. Al-Qaeda, 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, mosques, shrines, hospitals, and ruins) can be sensitive for political, religious, cultural, or historic reasons. Enemy forces have been known to deliberately occupy sensitive buildings under the assumption that U.S. forces will refrain from entering or returning fire. See the Hauge Convention for *Protection of Cultural Property in the Event of Armed Conflict*, 1954.

Human Shields (U)

2-79. (U) Terrorists deliberately use noncombatants as human shields. This limits forces to more stringent rules of engagement and limits 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. These groupings can conceal movements and be a means of escape for terrorists after executing an attack. Some terrorists purposely use the elderly, women, and children as human shields. Activities to create selective areas of human shields can include the following:

- (U) Orchestrating work strikes.
- (U) Fomenting mass rallies.
- (U) Coordinating peaceful-appearing demonstrations.
- (U) Coercing civilians to gather with and around an irregular force action, security, or support element.

2-80. (U) Types of withdrawal actions or repositioning through human shields causes terror for the noncombatants involved and may allow terrorists to regain a tactical initiative and renew offensive actions. Asymmetric techniques take advantage of typical restrictions on enemy rules of engagement and often reduce enemy capabilities to apply their full suite of weapon systems against an irregular force. Some defensive tactics are to—

- (U) Disperse within a relevant population of noncombatants.
- (U) Use noncombatants as a human shield during armed conflict with an enemy.
- (U) Exploit positioning in close proximity to infrastructure (hospitals, schools, places of religious worship).
- (U) Conduct information warfare manipulation of actions when enemy forces cause noncombatant casualties in combating the irregular force.

Enemy Information Activities (U)

2-81. (U) Enemy forces have used information to disrupt popular support for U.S. forces and multinational partners and to garner regional and international sympathy and support for insurgent forces, mainly from Europe and Muslim societies. Terrorists spread rumors or misinformation in marketplaces and cafes as a means to offset the official information from a host nation 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 military 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.

2-82. (U) 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 partner 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 U.S. and multinational partners of using excessive force.

OFFENSE (U)

2-83. (U) Attack is the primary type of offensive action that U.S. forces will experience from a terrorist. Tactics, techniques, and procedures 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 area of operations. Reconnaissance and surveillance aid in information and intelligence collection to provide this awareness and understanding, therefore, improving the terrorist ability to combine effects at a time and place for the optimum expectation of mission success.

2-84. (U) Terrorists employ a broad range of technology to support their tactics, techniques, and procedures. 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 U.S. forces and multinational partners develop countermeasures for terrorist tactics, terrorists adapt their tactics, techniques, and procedures in an attempt to remain elusive. As the terrorist use of advanced technologies is countered, terrorists may revert to previous low-tech tactics. Their cycles are not easily predicted, and the manner in which they adaptively operate attempts to counter or preempt unified land operations or unified action.

2-85. (U) Effective offensive tactics develop and use intelligence regarding a hostile force and terrain, 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 actions.

2-86. (U) Terrorist targeting of U.S. military forces spans the worldwide U.S. presence in 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.

2-87. (U) Terrorist tactics, techniques, and procedures 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—

- (U) Assassination.
- (U) Arson.

- (U) Bombing.
- (U) Kidnapping and hostage taking.
- (U) Raid and ambush.
- (U) Hijacking.
- (U) Seizure.
- (U) Sabotage.
- (U) Threat or hoax.
- (U) Environmental destruction.
- (U) Man-portable, air defense system use.
- (U) Chemical, biological, radiological, and nuclear (CBRN) threats and hazards.

2-88. (U) 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 antiterrorism awareness for individual and collective training, professional military education, and operational missions.

Assassination (U)

2-89. (U) 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 whom 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 (U)

2-90. (U) 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 its commitment to other missions.

Bombing (U)

2-91. (U) 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 IEDs and person-borne IEDs. Bomb techniques have also included aerial delivery, maritime delivery, ground surface implant, subsurface implant, and marine surface and subsurface mining.

2-92. (U) The 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 (if the action produces undesirable results) generates media interest and may lead to increased coverage of the terrorist group agenda.

Vehicle-Borne Improved Explosive Device (U)

2-93. (U) Vehicle-borne IEDs 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. These devices have been used against U.S. forces that operate in the area during combat patrols. Terrorists have also positioned these vehicular devices near a facility with the intent to kill forces, as in the Khobar Towers bombing. (See figure 2-5, page 2-22.) The bomb is then detonated by suicide initiation, time delay, or remote control.

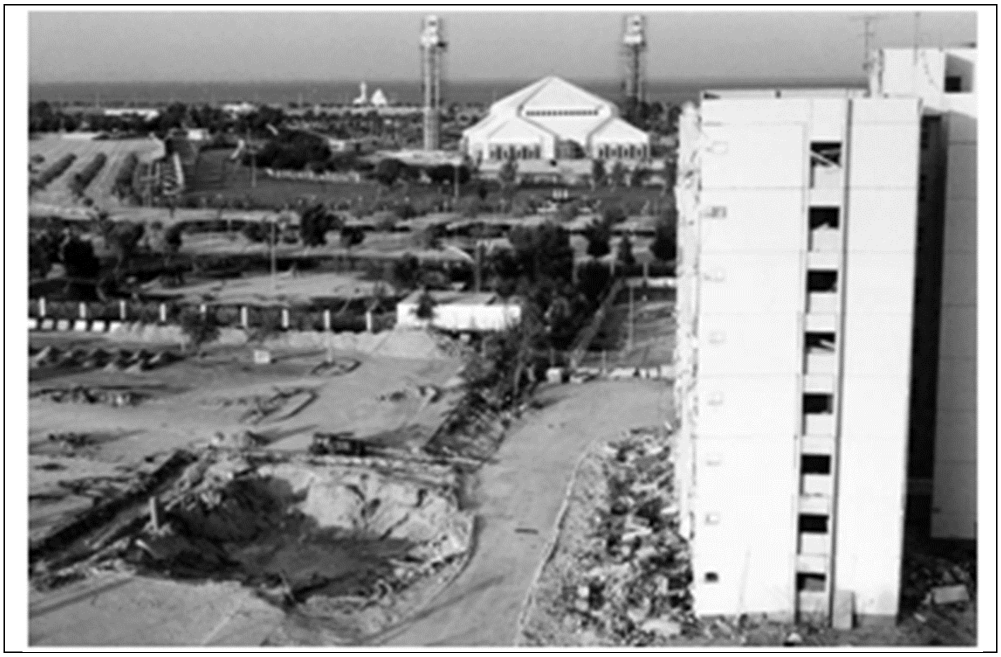


Figure 2-5. (U) Khobar Towers 1996 bombing incident

Person-Borne Improvised Explosive Device (U)

2-94. (U) 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. There have also been instances where the device was implanted into the body of the perpetrator to evade detection.

Delivered Device (U)

2-95. (U) 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 (known as 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. Some of the bombs contained nails and other fragments and performed like a claymore mine when they were opened. Kaczynski believed that the bombings were necessary to attract attention to the erosion of human freedom by modern technology.

Suicide Attack (U)

2-96. (U) A suicide attack can be the act of an individual or a tactic planned and conducted by an irregular force to spotlight a grievance with an intentional self-destruction and incidence of mass casualties, death, and mayhem. Mass media attention is often focused on an organizational grievance when such a sensational action occurs. As a tactic, a suicide attack seeks to degrade the resolve of a relevant population and obtain concessions from an enemy to an irregular force agenda. Organizational aims and ideological support to commit suicide in attacking an enemy is often complicated in motivations but is typically an action used when other more conventional means of combating an enemy are overmatched and produce no results. A suicide attack tactic can also be evaluated for an operational intent or strategy to obtain support for an irregular force agenda from state and nonstate actors who might be otherwise unwilling to get involved in a social or political conflict of an irregular force.

2-97. (U) In whatever means a suicide attacker uses, an irregular force member conducting such an act of terrorism has the ability to adjust actions until the moment of attack. This adaptive behavior makes a suicide attacker particularly dangerous. When the weapon is a suicide bomb, the moment to detonate a suicide vest or a vehicle-borne IED can be adjusted given conditions as they exist at the time and place of a planned attack. An attacker can estimate the degree of mayhem that will be caused by the explosion and change who and where to assault. In other instances, a handler of the suicide attack can command-detonate a bomb on a willing or unknowing individual carrying a bomb. The terrorist attack can be a deliberate assault on a specified target or can be an intentional, indiscriminate act to kill or maim combatants and noncombatants. A suicide attack is primarily a psychological assault on an enemy and its supporters.

2-98. (U) 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—

- (U) Bombings physically and psychologically impact society, tugging at humanitarian respect for innocence and life and undermining public confidence in its safety.
- (U) Bombings are inexpensive, costing as little as $150 for a simple attack.
- (U) Bombings are difficult to stop. Bombers take advantage of societies where the freedom of passage, hesitancy to conduct thorough body searches, or lack of technologically advanced screening devices increases the chance of success.
- (U) Bombings can be highly lethal and difficult to trace back to the responsible person or organization, limiting operations security (OPSEC) risks. The carnage resulting from the attack instantly gains media notoriety.

2-99. (U) Suicide bombings are normally composed of the following:

- (U) Recruiter.
- (U) Trainer.
- (U) Bomber.

2-100. (U) 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.

2-101. (U) 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 the conflict area (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.

2-102. (U) The briefcase, backpack, or carried form of an 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 an 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 following:

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

Maritime Delivery Tactic (U)

2-103. (U) Terrorists can use small, fast maritime vessels loaded with explosives and a team of suicide bombers to attack or cripple commercial or naval vessels. In 2000, two al-Qaeda members conducted a suicide attack on the United States Ship (USS) Cole, killing 17 military personnel. The terrorists made adjustments based on the failed attack against the USS The Sullivans earlier in the year. They 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 C-4 and detonating it. (See figure 2-6.)

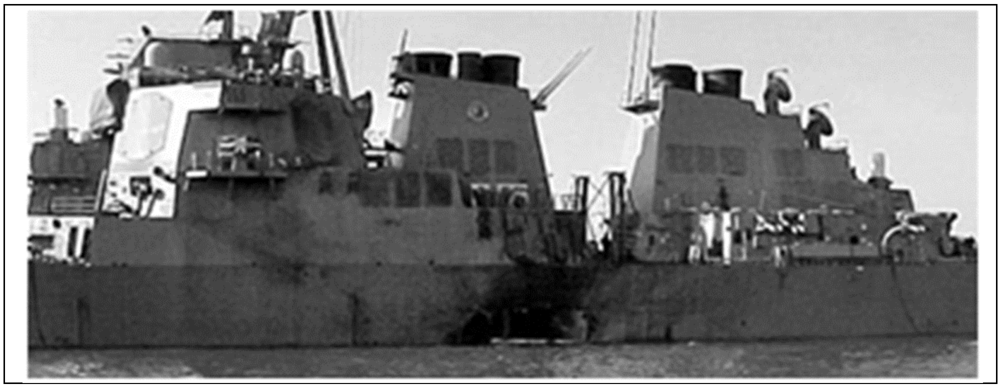


Figure 2-6. (U) Attack on the USS Cole

Kidnapping and Hostage Taking (U)

2-104. (U) 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, or 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 the chances of success in carrying out a mission, or can be exchanged 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 (U)

2-105. (U) A terrorist raid is similar in concept to a conventional military task, but is usually conducted with smaller forces against targets marked for 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.

Hijacking (U)

2-106. (U) 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 (U)

2-107. (U) Seizure is an act normally associated with the forceful occupation of a symbolic location or key facility (energy plant, cyber node, civil education center). Unlawful seizure can be associated with holding people in a location or facility as hostages, such as in the 2004 Beslan school siege by Chechen militants in North Ossetia (Russia).

Sabotage (U)

2-108. (U) 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 (U)

2-109. (U) 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 (U)

2-110. (U) 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 (U)

2-111. (U) 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—

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

Chemical, Biological, Radiological, and Nuclear Threats and Hazards (U)

2-112. (U) The means of a CBRN attack can range from a highly sophisticated weapon system (a nuclear bomb) to an improvised device (rudimentary improvised radiological device). The threat of chemical contamination or biological infection adds to the array of possible terrorist options. 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 proliferate and employ weapons of mass destruction.

2-113. (U) 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 the capability to weaponize chemical or biological material is 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.

2-114. (U) Terrorists could introduce CBRN material into the air or into a facility 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 direct insertion at the agent into facility outside air intakes. Internal release can be through the mail, by supply delivery, by direct release within a building or area, or by insertion into a ventilation system. Many chemical and biological agent precursors are commercially available, and instructions on building a device have been found on the Internet.

1995 Tokyo Subway Sarin Attack (U)

(U) 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 weapons in an attempt to generate a lethal airborne agent and the psychological and operational effect and use of CBRN weapons as a lucrative tactic for terrorists. First responders, hospital staffs, and hospital facilities became contaminated, increasing casualties and degrading emergency response and recovery. A postattack analysis and criminal case study of Aum Shinrikyo revealed a history of escalating violence and showed that the Japanese police suspected their experimentation with, and intent to use, chemical weapons before the attack.

THREAT VULNERABILITIES (U)

2-115. (U) Vulnerabilities exist in terrorist plans, operations, and support functions. The United States 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—

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

2-116. (U) 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 enable a process for improved leader education, training, and operations.

2-117. (U) Establishing alliances and multinational partnerships 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 other elements of national power (diplomacy, economy, and information).

2-118. (U) During the MDMP, the understanding and application of threat characteristic analysis increases the ability to know the threat and exploit threat vulnerabilities. Threat characteristics provide a construct from which to view the threat, to include personality targeting that rounds out the factors used for conventional warfare analysis. These factors include the following:

- (U) Composition.
- (U) Disposition.
- (U) Strength.
- (U) Tactics and operations.
- (U) Training.
- (U) Logistics.
- (U) Combat effectiveness.
- (U) Electronic technical data.

2-119. (U) The threat model allows the analyst to graphically depict the threat, which 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.

This page intentionally left blank.

Chapter 3

Foundations of Antiterrorism (U)

(U) This chapter explains antiterrorism as a tactical task and places antiterrorism into context with combating terrorism and the protection warfighting function. It introduces the five principles of antiterrorism: assess, detect, defend, warn, and recover. By understanding the principles of antiterrorism and the relationship of antiterrorism to combating terrorism and the protection warfighting function, antiterrorism planners will be better prepared to integrate antiterrorism into unified land operations.

3-1. (U) *Antiterrorism* is the defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces (JP 3-07.2). Antiterrorism is a consideration of forces during military operations as the Army defensive program to protect against terrorism. Army antiterrorism, at a minimum, focuses on risk management, planning (including the antiterrorism plan), training, exercises, resource generation, and comprehensive program review. Antiterrorism planning coordinates specific antiterrorism security requirements with the efforts of other security enhancement programs (intelligence support to antiterrorism, law enforcement, physical security, operations security, information security). Effective antiterrorism programs synchronize intelligence, risk management, and existing security programs to provide a holistic approach to defend against terrorist threats. The eight antiterrorism tasks that guide the commander in the development of a unit antiterrorism program are—

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

3-2. (U) 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. Antiterrorism is not a discrete task or the sole responsibility of a single branch—all branches bear responsibility. Antiterrorism must be integrated into unified land operations and considered at all times. Installations in the continental United States or outside the continental United States, U.S. Army Corps of Engineers projects, bases, and combat units should consider antiterrorism principles in every assigned mission.

COMBATING TERRORISM (U)

3-3. (U) *Combating terrorism* consists of actions, including antiterrorism and counterterrorism, taken to oppose terrorism throughout the entire threat spectrum (JP 3-26). As a strategy, program, and 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 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.

3-4. (U) *Counterterrorism* is the actions taken directly against networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks (JP 3-26). 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 tasks, not counterterrorism.

3-5. (U) The defensive element of combating terrorism (antiterrorism) overlaps with the commander's protection efforts. Combating terrorism also includes the following critical supporting functions:

- (U) Incident management (preparation for and response to a terrorist incident or event).
- (U) Intelligence support (collection and dissemination of terrorism-related information) taken to oppose terrorism throughout the entire threat spectrum).

PROTECTION WARFIGHTING FUNCTION (U)

3-6. (U) *Protection* is the preservation of the effectiveness and survivability 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 (JP 3-0). The Army keystone manual for protection (ADP 3-37) 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 (ADRP 3-0). The six Army warfighting functions are:

- (U) Movement and maneuver.
- (U) Intelligence.
- (U) Fires.
- (U) Mission command.
- (U) Sustainment.
- (U) Protection.

3-7. (U) Preserving the force includes protecting personnel (combatant and noncombatant) and physical assets of the United States and multinational partners. ADRP 3-37 discusses the tasks and systems of the protection warfighting function. It uses many of the other supporting tasks within the protection warfighting function for the sole purpose of preventing and recovering from terrorist acts. The supporting tasks are—

- (U) Conduct operational area security.
- (U) Employ safety techniques (including fratricide avoidance).
- (U) Implement operations security.
- (U) Provide intelligence support to protection.
- (U) Implement physical security procedures.
- (U) Apply antiterrorism measures.
- (U) Conduct law and order.
- (U) Conduct survivability operations.
- (U) Provide force health protection.
- (U) Conduct CBRN operations.
- (U) Provide explosive ordnance disposal and protection support.
- (U) Coordinate air and missile defense.
- (U) Conduct personnel recovery.
- (U) Conduct internment and resettlement.

3-8. (U) While antiterrorism 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. Employing antiterrorism measures 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 antiterrorism 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 unified land operations and their inherent responsibility to protect the force. (See figure 3-1.)

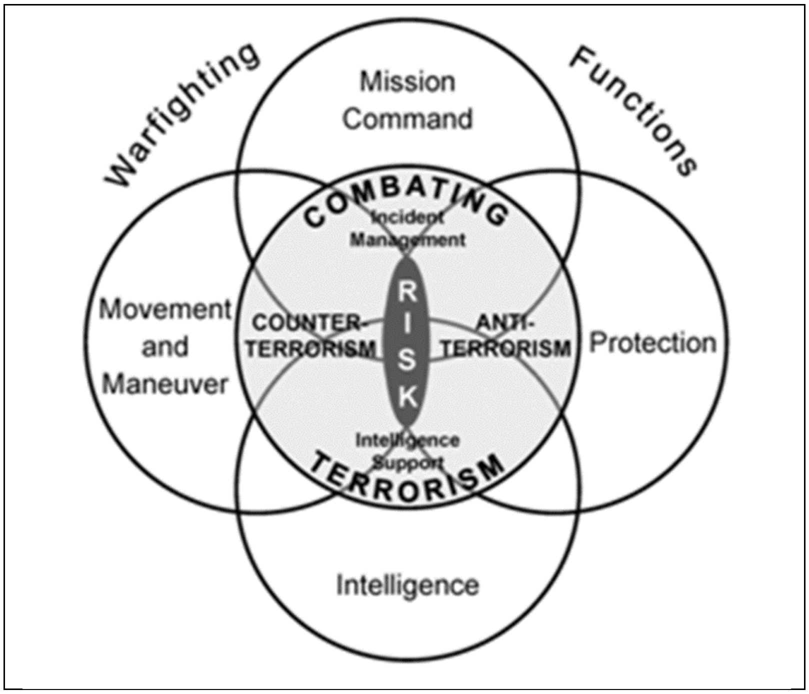


Figure 3-1. (U) Terrorism risk

3-9. (U) 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 unified action and host nation partners. Antiterrorism measures, within combating terrorism, are complementary or reinforcing to combat power generation. Complementary capabilities protect the weakness of one system or organization with the capabilities of a different warfighting function. Reinforcing capabilities combine similar systems or capabilities within the same warfighting function to increase the overall capabilities of the function.

3-10. (U) Through mission command, commanders and staffs introduce antiterrorism principles into the operations process, risk management, and mission orders to accomplish unified land operations. Commanders empower subordinate leaders and Soldiers to adapt to a tough and often elusive enemy and perform effectively in a complex and chaotic environment through authority, direction, intent, and information.

3-11. (U) The key elements of antiterrorism tasks are—

- (U) Assessment.
- (U) Force protection conditions (FPCONs).
- (U) Random antiterrorism measures.
- (U) Physical security.

3-12. (U) 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. 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 capabilities to safeguard bases, protect the local populace, and protect forces.

3-13. (U) The intelligence warfighting function provides timely and actionable terrorist threat information in support of combating terrorism. 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.

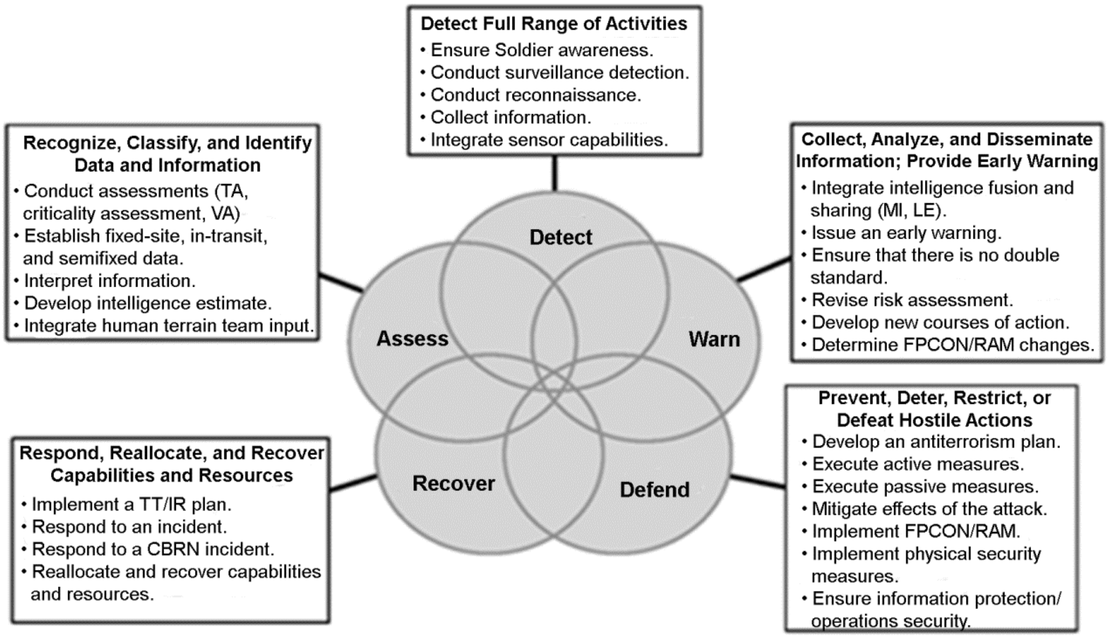
3-14. (U) Army counterintelligence is a key contributor in preventing and deterring terrorist activities and is responsible for identifying terrorist indications and warnings. Army counterintelligence personnel support the antiterrorism tasks through the execution of the counterintelligence functions (investigations, collection, analysis and production, and technical services and support). Army counterintelligence focuses on foreign intelligence and security services and international terrorist organization intelligence collection and targeting activities that are directed at Army equities. This focus provides indications and warnings of exploitation or potential attacks. Unless assigned to a counterterrorism unit, Army counterintelligence is continually engaged in an antiterrorism role to help detect, identify, and assess foreign intelligence and security services, international terrorist organization collection threats, and terrorism indications and warnings. To support antiterrorism, counterintelligence personnel—

- (U) Conduct foreign intelligence collection and counterintelligence activities to collect and disseminate information on foreign threats against the Army.
- (U) Sustain 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.
- (U) Maintain a capability to report and disseminate time-sensitive information concerning the foreign threat against Army personnel, facilities, and other assets.
- (U) Provide supported Army commanders with information concerning the foreign threat against personnel, facilities, and operations consistent with the provisions and limitations of AR 381-10 and other applicable regulations and directives, to include foreign threat information in briefings on counterintelligence according to AR 381-12.
- (U) Serve as the Army intelligence liaison representative to federal, state, and local agencies and host nation federal, state, and local agencies to exchange foreign threat information.

3-15. (U) The maneuver warfighting function supports combating terrorism and conducting unit antiterrorism 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 area of operations.

ANTITERRORISM PRINCIPLES (U)

3-16. (U) The five antiterrorism principles (assess, detect, warn, defend, and recover) represent the characteristics of successful antiterrorism 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. Antiterrorism is proactive, focused, and conducted by integrating military and cross-government capabilities against enemies. These principles guide the commander and antiterrorism officer to protect personnel (combatant and noncombatant), information, and physical assets by applying active and passive measures against the full threat spectrum. These principles are not a process and may be applied as the situation dictates. (See figure 3-2.) Army professionals apply these principles using their discretionary professional judgment under the philosophy of mission command and fully understanding the commander’s intent, mission, and resources available.


Detect Full Range of Activities
• Ensure Soldier awareness.
• Conduct surveillance detection.
• Conduct reconnaissance.
• Collect information.
• Integrate sensor capabilities.
Recognize, Classify, and Identify Data and Information
• Conduct assessments (TA, criticality assessment, VA)
• Establish fixed-site, in-transit, and semifixed data.
• Interpret information.
• Develop intelligence estimate.
• Integrate human terrain team input.
Collect, Analyze, and Disseminate Information; Provide Early Warning
• Integrate intelligence fusion and sharing (MI, LE).
• Issue an early warning.
• Ensure that there is no double standard.
• Revise risk assessment.
• Develop new courses of action.
• Determine FPCON/RAM changes.
Detect
Assess
Warn
Recover
Defend
Respond, Reallocate, and Recover Capabilities and Resources
• Implement a TT/IR plan.
• Respond to an incident.
• Respond to a CBRN incident.
• Reallocate and recover capabilities and resources.
Prevent, Deter, Restrict, or Defeat Hostile Actions
• Develop an antiterrorism plan.
• Execute active measures.
• Execute passive measures.
• Mitigate effects of the attack.
• Implement FPCON/RAM.
• Implement physical security measures.
• Ensure information protection/ operations security.

Legend:

CBRN	chemical, biological, radiological, and nuclear
FPCON	force protection condition
IR	incident response
LE	law enforcement
MI	military intelligence
RAM	random antiterrorism measures
TA	threat assessment
TT	terrorist threat
VA	vulnerability assessment

Figure 3-2. (U) Antiterrorism principles

ASSESS (U)

3-17. (U) Assessment is the method of monitoring and evaluating the current situation and progress of an operation, task, or mission. Assessing includes the analysis of the security environment, threat information, and 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 antiterrorism measures and force capabilities.

DETECT (U)

3-18. (U) 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 mission command elements. A detection system must provide all three of these capabilities to be effective. Detection may identify enemy movement via direct observation; information collection; or electronic security systems capabilities. Other examples of detection are perimeter patrols or security technology, unmanned aircraft systems, and reconnaissance and surveillance patrols.

DEFEND (U)

3-19. (U) Defense protects an asset from aggression by delaying or preventing enemy movement toward the asset or by shielding the asset from threat tactics, tools, weapons, and explosives. Defensive measures may be—

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

WARN (U)

3-20. (U) 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 enemy 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 (U)

3-21. (U) Recovery deals with the need to recover after a terrorist incident. In an almost seamless evolution, the emphasis on response changes to recovery operations. Within recovery, actions are taken to help military personnel, installations, facilities, and operating units return to a preincident operating status. Short-term recovery (hours to weeks) includes immediate measures that support crisis response activities. Examples of crisis response and recovery are—

- (U) Providing essential health and safety services.
- (U) Restoring interrupted utility and other essential services.
- (U) Reestablishing transportation routes.
- (U) Operating decontamination sites.
- (U) Providing food and shelter for displaced persons.

3-22. (U) During the crisis response and immediate aftermath of a terrorist incident, it is important to restore trust with the served community of command. When the safety, security, and well-being of civilians, noncombatants, and military forces have been shown to be vulnerable to acts of terror, the physical visibility of leaders and Soldiers responding in an efficient, ethical, and effective professional manner helps restore the trust and credibility of the host nation government and U.S. forces. Long-term incident management and recovery may also involve some of the same actions, but it 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 (U)

3-23. (U) Commanders communicate the spirit and intent of antiterrorism doctrine throughout the chain of command or line of authority by establishing antiterrorism 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.

3-24. (U) Commanders, with the assistance of antiterrorism officers, develop and maintain an antiterrorism appendix to the operation order or implementation guidance found in an annex. The antiterrorism appendix informs their units on how to defend against terrorist threats. The antiterrorism appendix usually pertains to battalion-size or greater units and to operational deployments (50 or more personnel) during training, deployment, and redeployment. This appendix 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 random antiterrorism measures. Antiterrorism planning includes the following:

- (U) Physical security measures.
- (U) Antiterrorism measures for HRP and high-risk billet.
- (U) Operational contract support actions (see appendix D).
- (U) Measures for in-transit movements.
- (U) Construction and building consideration.
- (U) Critical asset security.
- (U) FPCON implementation and measures for incident response and incident management.

3-25. (U) Units integrate antiterrorism 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, 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.

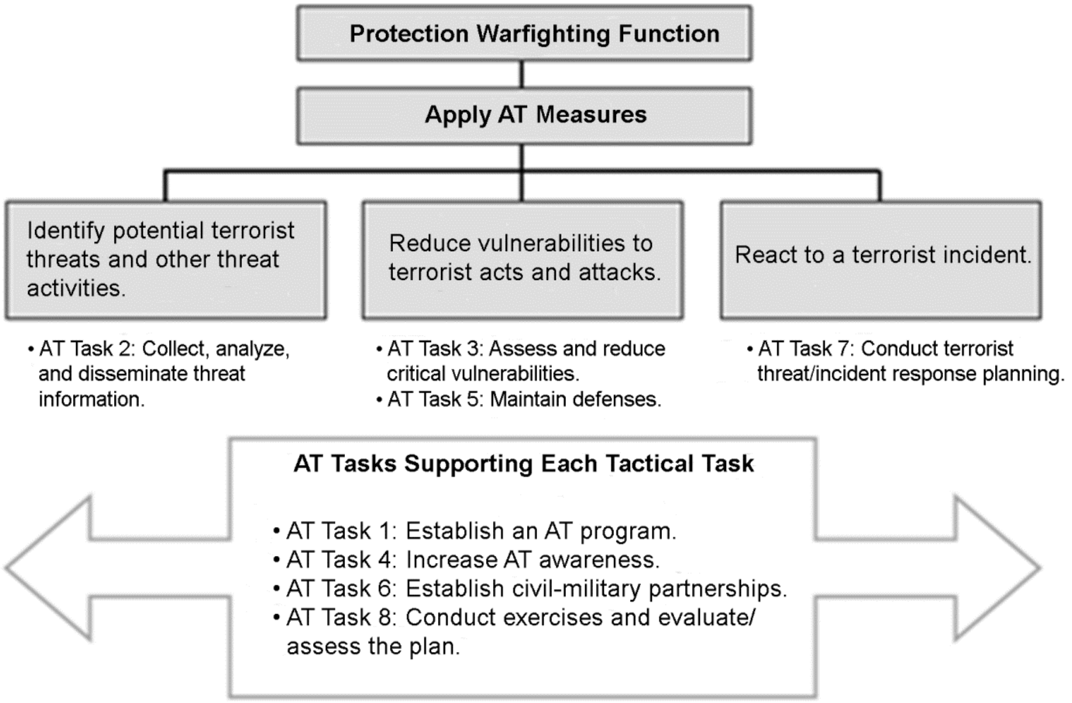
3-26. (U) Where functional cells are organized by warfighting functions, integrating cells coordinate and synchronize forces and warfighting functions within a specified planning horizon (long-, mid-, and short-term) and include the plans, future operations, and current operations integration cells. Units below the division level may not be resourced for three integration cells and may combine responsibilities into one integration cell or create working groups to assist in focusing efforts pertaining to a particular mission or threat.

3-27. (U) The preferred method (see DODI 2000.16) to focus antiterrorism efforts and planning is through the creation or inclusion of an antiterrorism working group (ATWG). Commanders and antiterrorism officers use the ATWG to oversee the implementation of the antiterrorism plan and tasks, develop and refine antiterrorism guidance, and address emergent or emergency antiterrorism 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 threat assessments 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.

3-28. (FOUO) Antiterrorism 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 (see FM 7-15):

- (FOUO) Identify potential terrorist threats and other threat activities.
- (FOUO) Reduce vulnerabilities to terrorist acts and attacks.
- (FOUO) React to a terrorist incident.

3-29. (FOUO) These primary tasks are supported by eight antiterrorism tasks (see AR 525-13) which commanders and antiterrorism officers should use to achieve objectives that deter terrorist incidents, employ countermeasures, mitigate effects, and conduct incident recovery. (See figure 3-3, page 3-8.)


Protection Warfighting Function
Apply AT Measures
Identify potential terrorist threats and other threat activities.
Reduce vulnerabilities to terrorist acts and attacks.
React to a terrorist incident.
• AT Task 2: Collect, analyze, and disseminate threat information.
• AT Task 3: Assess and reduce critical vulnerabilities.
• AT Task 5: Maintain defenses.
• AT Task 7: Conduct terrorist threat/incident response planning.
AT Tasks Supporting Each Tactical Task
• 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.

Legend:

AT	antiterrorism

Figure 3-3. (FOUO) Army tactical tasks and supporting antiterrorism tasks

IDENTIFY POTENTIAL TERRORIST THREATS AND OTHER THREAT ACTIVITIES (U)

3-30. (U) 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 antiterrorism officers empower their staffs and coordinate with multiple entities to identify terrorist risk to units operating within the United States, during in-transit movement to deployed locations, and while conducting unified land operations or unified action in a host nation.

Antiterrorism Task 2. Collect, Analyze, and Disseminate Threat Information (U)

3-31. (FOUO) The threat assessment is used to identify the terrorist threats that are posed to Army assets, the threats that could be encountered while executing a mission, and the threats that are inherent within the intelligence preparation of the battlefield or intelligence estimate process. The threat assessment is a product developed from the threat analysis. The threat analysis identifies and evaluates potential threats based on factors such as threat 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. (See UFC 4-010-01 for a list of assumed threats that must be considered when planning mitigations in the antiterrorism plan.)

3-32. (U) Terrorist threat information can be obtained from 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 threat assessment. 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 tasks while leading the direction of antiterrorism and defensive tasks to ensure mission success.

3-33. (U) Threats have 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, active shooters, information network attacks, mortars, asset thefts, air attacks, and the employment of CBRN weapons.

3-34. (U) Assessing the threat considers two main factors: the probability and severity 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 are assessed during mission analysis; course of action (COA) development, analysis, and rehearsal; and MDMP execution steps. The assessment must consider mission- and non-mission-related aspects that may have an impact. The result is a prioritized list of threats and an initial estimated level of risk for each identified threat, expressed in terms of low, moderate, or high for the commander. These factors are indicated as—

- (U) **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 the MDMP and risk management, there are five levels of probability:
  - (U) **Frequent.** Occurs very often, known to happen regularly. Examples are surveillance, criminal activities, cyber attacks, and small arms fire.
  - (U) **Likely.** Occurs several times, a common occurrence. Examples are IEDs, hostages, ambushes, and bombings.
  - (U) **Occasional.** Occurs sporadically, but is not uncommon. Examples are injury or death from attacks against aircraft, hijacking, or skyjacking.
  - (U) **Seldom.** Remotely possible, could occur at some time. Examples are the release of CBRN hazards or the employment of weapons of mass destruction.
  - (U) **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.
- (U) **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 the knowledge of the results of similar past events. There are four levels:
  - (U) **Catastrophic.** Complete mission failure or the inability to accomplish the mission, death or permanent total disability, the loss of major or mission-critical systems or equipment, major property or facility damage, mission-critical security failure, or unacceptable collateral damage.
  - (U) **Critical.** Severely degraded mission capability or unit readiness; permanent disability, partial disability, or temporary total disability exceeding 3 months; extensive major damage to equipment or systems; significant damage to property or the environment; security failure; or significant collateral damage.
  - (U) **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 3 months; or minor damage to property or the environment.
  - (U) **Negligible.** Little or no adverse impact on mission capability, first aid or minor medical treatment, slight equipment or systems damage (remain fully functional or serviceable), or little or no property or environmental damage.

3-35. (U) Threat analysis provides the staff with information to base warnings for locations, countries, or regions. The S-2 works in conjunction with the operations officer, antiterrorism 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:

- (U) Ensure that antiterrorism and threat information are distributed up and down the chain of command and laterally, as appropriate.
- (U) Implement effective processes to integrate and fuse the sources of available threat information.
- (U) Prepare specific terrorism threat assessments 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).
- (U) Integrate terrorism threat assessments into the risk management process; and be a major source of analysis and justification for recommendations to raise or lower FPCON levels, implement random antiterrorism measure enhancements (including physical security program changes and program and budget requests), and conduct terrorism vulnerability assessments.
- (U) Ensure that terrorism threat assessments are a part of the intelligence preparation of the battlefield, MDMP, and leader's reconnaissance in conjunction with deployments. Follow-on terrorism threat assessments are conducted for deployments as determined by the commander or as directed by higher headquarters.

3-36. (U) Threat analysis is a continuous process of compiling and examining information to develop intelligence indicators of possible terrorist activities. Intelligence, counterintelligence, and antiterrorism officers develop essential elements of information to focus the threat analysis and identify likely targets by using the following considerations:

- (U) Organization, size, and composition of groups operating in the AOR.
- (U) Motivation (religious, political, ecological).
- (U) Long- and short-range goals.
- (U) Religious, political, and ethnic affiliations.
- (U) International and national support (moral, physical, financial).
- (U) Recruiting methods, locations, and targets (students).
- (U Group leaders, opportunists, and idealists identity.
- (U) Group intelligence capabilities and connections with other terrorist groups.
- (U) Supply and support sources.
- (U) Important dates (religious holidays).
- (U) Ability to plan.
- (U) Internal discipline.
- (U) Preferred tactics and operations.
- (U) Willingness to kill.
- (U) Willingness for self-sacrifice.
- (U) Group skills (demonstrated or perceived) (sniping, demolition, masquerade, industrial sabotage, airplane or boat operations, tunneling, underwater or electronic surveillance, poisons or contaminants).
- (U) Equipment and weapons (on-hand and required).
- (U) Transportation (on-hand and required).
- (U) Medical support availability.
- (U) Means and methods of mission command.
- (U) Means and methods of communicating to the public.

Intelligence Support to Antiterrorism (U)

3-37. (U) Intelligence plays a crucial role in supporting antiterrorism efforts by assisting commanders and staffs in distinguishing preincident indicators to prevent attacks against the United States and multinational partners. Intelligence facilitates a greater understanding of the operational environment, with emphasis on the populace, criminal activity, host nation, and active terrorist organizations. Actionable intelligence provides a foundation that an antiterrorism 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 antiterrorism officer to better assess the terrorist threat, determine the appropriate protection conditions, mitigate the risk of terrorist actions, prepare combat patrols, and determine random antiterrorism measures. (See ADP 2-0, ADRP 2-0, FM 2-19.4, FM 2-22.2, FM 2-91.4, and FM 2-91.6.)

3-38. (U) 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 they will attack, their actions will always be difficult to predict. They have the advantage of time—time to select the target and choose the time of the attack. Human intelligence, criminal intelligence, and counterintelligence 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.

3-39. (U) 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, even years, so that the target's daily routine and those areas that affect their daily life are completely understood. Terrorists are most vulnerable to being caught or deterred from executing an attack during these surveillance and planning phases.

3-40. (U) Commanders (through their antiterrorism officers, staffs, protection cells, and working groups) develop a system to monitor, report, collect, analyze, and disseminate terrorist threat information. Intelligence supports the commander during unified land operations and is one of the warfighting functions. The intelligence warfighting function includes assets within the military intelligence branch and the assets of branches that can assist in the information collection 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 reach situational understanding (every Soldier is a sensor).

3-41. (U) 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 antiterrorism 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, smaller units and activities rely on solid analysis, synchronization, and fusion by higher headquarters to provide direction in implementing FPCON measures and random antiterrorism measure responses. Counterintelligence should be thoroughly integrated into the commander's operational planning and preparation. The counterintelligence mission makes it an ever-present antiterrorism enabler through the routine execution of its functions. However, counterintelligence can tailor its functions to provide support to antiterrorism and protection-specific operations, including—

- (U) Screening locally employed personnel working on military bases outside the continental United States.
- (U) Tailoring security education and awareness briefings and programs.
- (U) Conducting travel and foreign contact briefings and debriefing programs.
- (U) Supporting threat assessments and vulnerability assessments.
- (U) Providing foreign intelligence and security service and international terrorist organization threat analysis and products.
- (U) Conducting counterintelligence investigations and collection that impact antiterrorism and protection.

3-42. (U) Intelligence support to antiterrorism 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 methods of a threat in current 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 (U)

3-43. (U) 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 (U)

3-44. (U) Commanders continuously assess antiterrorism capabilities. These assessments review the overall program; individual, physical, and procedural security measures; and unit predeployment preparation. Commanders and antiterrorism officers analyze the threat assessment and implement physical protection measures according to known terrorists or potential capabilities.

Criticality Assessment (FOUO)

3-45. (FOUO) 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 specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the nation to continue to function effectively (JP 3-07.2). For antiterrorism purposes, the criticality assessment should also include high-population facilities (recreational activities, theaters, sports venues) that may not be mission-essential. Units conducting tactical tasks should focus on assets that are most critical to the operation and identify the most critical aspect of the mission.

3-46. (FOUO) 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.

3-47. (FOUO) The criticality assessment identifies assets supporting Army missions, units, or activities deemed critical by military commanders or civilian agency managers. Antiterrorism officers can assist leaders with conducting 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, 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. The criticality assessment addresses the impact of temporary or permanent loss of assets and examines costs of recovery and reconstitution, including time, expenditure, capability, and infrastructure support.

3-48. (FOUO) Critical assets at each command echelon must be determined and prioritized. The antiterrorism officer, protection cell, and staff gauge how quickly a lost capability can be replaced before giving a prioritized recommendation to the commander. The commander who is responsible for antiterrorism approves the prioritized list. The goals of a criticality assessment are to—

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

3-49. (FOUO) 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:

- (FOUO) Importance.
- (FOUO) Effect of loss.
- (FOUO) Recoverability.
- (FOUO) Mission functionality.
- (FOUO) Substitutability.
- (FOUO) Repairability.

3-50. (FOUO) Initial protection planning requires various assessments to support protection prioritization—threat assessment, vulnerability assessment, 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.

3-51. (FOUO) 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 antiterrorism measures while conducting unified land operations. Staffs, ATWGs, or selected individuals may find MSHARPP and CARVER assessment tools helpful. MSHARPP assesses potential targets from the inside out with a focus on the mission perspective of U.S. forces. CARVER assesses targets from the outside in with a focus on the mission perspective of terrorists. Appendix E discusses MSHARPP and CARVER in detail.

Vulnerability Assessment (FOUO)

3-52. (FOUO) A vulnerability assessment is a command or unit level evaluation to determine the potential weakness of an asset (personnel, installation, unit, exercise, residence, facility, network, infrastructure, information, or 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 threat assessment. Antiterrorism officers and other multidisciplinary experts in areas such as terrorist tactics, structural engineering, physical security, and installation preparedness conduct these assessments.

3-53. (FOUO) The vulnerability assessment 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 identifying and 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 vulnerability assessments are—

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

3-54. (FOUO) The antiterrorism 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, counterintelligence, law enforcement, communications, safety, fire, engineers, medical services, CBRN planning and response). At the unit level, the operations section should help the antiterrorism officer find subject matter experts to assist with the assessments.

3-55. (FOUO) Vulnerability assessments enable the commander to plan appropriate countermeasures to reduce the vulnerability and associated prudent 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 unit vulnerability. Tactics of terrorist organizations seek to use the element of surprise to obtain a greater advantage over more powerful forces. A commander's ability to thwart potential terrorist actions will be greatly enhanced through developing COAs, red teaming, and identifying force susceptibility to surprise. When assessing vulnerability to terrorism during unified land operations, the staff assists the commander by providing answers to the following questions:

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

3-56. (FOUO) Commanders and staffs assess the vulnerability of an asset based on its construction, accessibility, and recognizability. Staffs assess the asset construction and physical hardness to estimate how it would withstand the varying types of threats that could impact it. Staffs assess whether the asset is accessible and when a potential terrorist can reach the target with sufficient personnel and equipment to accomplish the mission. This analysis entails identifying and studying critical paths that the terrorist must take to achieve an objective and the unit means to impede terrorist tactics. Target recognizability is the degree to which it can be recognized by an operational element or intelligence collection and reconnaissance asset under varying conditions. Weather can influence target recognizability. Target size, complexity, and camouflaging can also influence recognizability. Through detailed surveillance, threats can distinguish the unit or personnel level of importance and choose to strike at those perceived to be most critical to their goals and objectives.

3-57. (FOUO) The end state of the vulnerability assessment is the identification of physical characteristics or procedures that render critical assets, areas, or special events vulnerable to a range of known or feasible threat capabilities. Vulnerability is determined partly by the commander's desired level of protection for the asset, area, or special event. Although performing an effective vulnerability assessment requires detailed analysis, the results quantifying and rating the effectiveness of protective measures are invaluable and provide a major tool for developing antiterrorism protective measures.

3-58. (FOUO) The vulnerability assessment methodology should follow this sequence:

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

Antiterrorism Task 5. Maintain Defenses (FOUO)

3-59. (FOUO) Commanders use specific antiterrorism security procedural and physical measures to protect personnel, information, and materiel from terrorist threats. Within the antiterrorism appendix of the operation order, commanders outline specific threat mitigation measures as part of developing controls during the risk management 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 random antiterrorism measures. The terrorist planning cycle can be interrupted, and an attack could possibly be prevented by the use of a comprehensive random antiterrorism measures program. Individual Soldier awareness and training are key elements in successfully detecting and thwarting terrorist acts.

Force Protection Conditions (FOUO)

3-60. (FOUO) 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 antiterrorism activities. The unit antiterrorism 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.*** (FOUO) 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 establishing procedures to ensure that FPCON measures are uniformly disseminated and implemented.

3-61. (FOUO) Although not completely applicable in a combat zone, these measures can be used as a template in developing protection guidance. Well-designed antiterrorism measures facilitate the antiterrorism principles of assess, detect, defend, and warn. FPCON measures include provisions for reinforced physical security; increased security personnel and inspections of vehicles, hand-carried items, and packages; random antiterrorism measures; 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 and the procedures for raising or lowering FPCON levels are prescribed in AR 525-13.

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

Random Antiterrorism Measures (FOUO)

3-62. (FOUO) A key component of an active operation order antiterrorism appendix is random antiterrorism measures that provide the commander with a flexible means to increase security and minimize or prevent the establishment of predictable patterns of security. Specified measures must be tailored for each location and for each FPCON. Commanders have 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, random antiterrorism measures convey an image of increased vigilance and awareness to observers who are external to the military site. Random antiterrorism measures, if properly implemented, present an ambiguous and confusing assessment of the military site security posture to terrorist groups and should ultimately disrupt the terrorist planning cycle.

3-63. (FOUO) The unit antiterrorism plan should contain detailed instructions on the implementation of random antiterrorism measures, 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. (See AR 525-13.) Random antiterrorism measures 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 random antiterrorism measures on terrorists is difficult to measure, but such programs introduce uncertainty and unpredictability to planners and organizers of terrorist attacks. Examples of random antiterrorism measures include the following:

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

High-Risk Personnel (FOUO)

3-64. (FOUO) 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, location, or a specific threat that requires additional security to reduce or eliminate risks. These personnel may be formally designated HRP or high-risk billets. A high-risk billet is an individual who has not been designated as a HRP, but by virtue of their job or position, may be at risk. For example, a deployed brigade commander would be considered a high-risk billet.

3-65. (FOUO) The commander of a geographical area is responsible for the safety and security of dignitaries and HRP traveling through the area. Corps and division commanders conducting unified land operations, through combatant command authorization, may be designated HRP or high-risk billets based on a threat in the area. Brigade and battalion commanders normally do not require the same level of protection as an HRP, but they may warrant a security detail taken from within the command or, at a minimum, a squad to enhance movement within the area of operations.

3-66. (FOUO) Principles of risk management should be employed in designating HRP and high-risk billets, approving protective support, and determining the number and type of assigned protective services detail personnel. Protective services detail 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 190-58, AR 525-13, ATP 3-39.35, and DODI O-2000.22. Technical assistance is also available from the supporting criminal investigation division unit.

Physical Security (U)

3-67. (U) *Physical security* is that part of security 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 3-0). In support of antiterrorism, physical security measures identify physical vulnerabilities to terrorist attacks on bases, personnel, and materiel and take actions to reduce or eliminate those vulnerabilities. Engineer 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 Physical Security Program supports antiterrorism through the coordinated efforts of policies, plans, and procedures specifically designed to achieve a strong physical security posture.

3-68. (U) 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, establishing 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 builds physical security into contingency, mobilization, antiterrorism, and wartime plans. The program goal is to safeguard personnel and protect property by preventing, detecting, and confronting unauthorized acts. (See ATP 3-39.32.)

3-69. (U) The physical security officer provides assistance to the antiterrorism officer and commander in the defensive planning, implementation, and control of antiterrorism efforts. 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 threat assessment, compliance with protection standards, and risk management. Physical security systems installed in and around installations, facilities, and units form the physical backbone of antiterrorism efforts. The facilities, equipment, and personnel that form the installation security force are critical resources that help defend against terrorist attacks.

Entry Control (U)

3-70. (U) Entry control ensures the proper level of access for Army personnel, visitors, contract personnel, and vehicle traffic. The objective of an entry control point 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 an entry control point. The design of an entry control point 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 ATP 3-39.32.) Entry control also prevents personnel from exiting the base, if necessary, as a means to contain and capture criminal or terrorist perpetrators.

3-71. (U) Entry control points 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. 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 deployed operating base. These procedures can also help detect contraband and mitigate the potential for sabotage, theft, trespass, terrorism, espionage, or other criminal activity.

3-72. (U) Entry control procedures are intended to accomplish the following objectives as part of in-depth defense for a deployed operating base:

- (U) Permit personnel, vehicles, and delivered materials to move through the deployed operating base without unduly interfering with day-to-day operations. Some interference will be necessary, depending on the security requirements.
- (U) Help maintain adequate security throughout the deployed operating base, and protect critical assets.
- (U) Contain and resolve actual and potential attacks, and apprehend perpetrators.
- (U) Delay attackers in reaching critical assets, and inhibit egress from the deployed operating base so that security personnel can sound the alarms and take immediate protective actions.

Information Protection (U)

3-73. (U) *Information protection* is those active or passive measures used to safeguard and defend friendly information and information systems (ADRP 6-0). Information protection denies enemies, adversaries, and others the opportunity to exploit friendly information and information systems for their own purposes. 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.

3-74. (U) Critical information is information that is vital to a mission. If an enemy 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 questions converted from critical information. The use of essential elements of friendly information is an effective way to ensure the widest dissemination of unit or organizational critical information while protecting classified and sensitive information.

3-75. (U) Counterintelligence support to OPSEC entails identifying enemy intelligence; tactics, techniques, and procedures; collection methods; analysis; and exploitation capabilities that target essential elements of friendly information and developing countermeasures. Conducting counterintelligence investigations, developing counterintelligence sources, debriefing Army personnel, and screening local nationals and contract linguists can be useful to determine what essential elements of friendly information are being targeted by foreign intelligence and what enemy collection methods and capabilities are being used to collect essential elements of friendly information. Additionally, cyber counterintelligence elements can perform Internet open-source collection and DOD network and systems analysis to determine OPSEC vulnerabilities and provide support to the Army network threat assessments and vulnerability assessments. The commander of the Intelligence and Security Command provides data on the foreign intelligence threat, terrorist threat, and counterintelligence support to OPSEC programs for Army units, Army Service component commands (ASCCs), and direct reporting units and above.

3-76. (U) Units use the critical information list to create a consolidated list of 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 unit or organizational critical information, while protecting it, is to convert it to essential elements of friendly information.

3-77. (U) OPSEC applies across the range of military operations. Units conduct OPSEC to preserve essential secrecy. *Operations security* is the process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities (JP 3-13.3). OPSEC may also be used to—

- (U) Identify those actions that can be observed by threat intelligence systems.
- (U) 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.
- (U) Select and execute measures that eliminate or reduce, to an acceptable level, the vulnerabilities of friendly actions to enemy exploitation. (See ADRP 3-37.)

3-78. (U) 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 ensure that—

- (U) Itineraries, travel plans, and personnel rosters are protected.
- (U) Established patterns are eliminated.
- (U) Building and base plans, billeting assignments, and very important person guest lists are protected.
- (U) Classified or sensitive information is discussed only on cryptographically secured telephone or radio circuits (such as automatic secure voice communications systems) approved by the National Security Agency.
- (U) Personal and family information is protected from strangers.
- (U) Physical security measures to protect personnel and prevent unauthorized access to facilities, materiel, and documents are coordinated.

3-79. (U) Communications technology provides the enemy and terrorists potential access to additional information sources. Soldiers deployed on military operations have included information about living situations, weaknesses in protection, and ongoing and future operations in e-mails, Internet blogs, and photographs on social sites. 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 (U)

(U) In March 2010, information pertaining to an upcoming raid was posted by an Israeli Defense Force member on a social networking site one day before an offensive operation 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 A TERRORIST INCIDENT (U)

3-80. (U) Commanders 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 ATTP 3-39.10 for additional information on critical incident response.) 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 infrastructure, and continue to progress toward mission success without drastic impacts on unit capabilities.

Antiterrorism Task 7. Conduct Terrorist Threat/Incident Response Planning (FOUO)

3-81. (FOUO) 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 bases and base camps use the antiterrorism 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 antiterrorism officers coordinate with friendly units, civil authorities, supporting contracting organizations, and selected contract service company managers (first responders, firefighter services) to plan for terrorism incident 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.

3-82. (FOUO) *Incident management* is a national comprehensive approach to preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies (JP 3-28). Incident management also acts as a deterrent to terrorist attacks by mitigating the 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 antiterrorism program.

Incident Management (U)

3-83. (U) Incident response measures to a terrorist attack include procedures to provide mission command, 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 may be present. First responders, in this case, refer to military, local, state, 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 management activities.

3-84. (U) *Crisis management* is measures, normally executed under federal law, to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or an act of terrorism (JP 3-28). This is predominantly a law enforcement response.

3-85. (U) The Army continues to support efforts to provide incident management capabilities worldwide through domestic incident management, DOD-led incident management and, in support of allies, foreign consequence management. The primary objective of antiterrorism 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.*** (U) 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 defense support of civil authorities' tasks in defense of the homeland and meet the requirements outlined in HSPD 5.

Incident Management Plan (U)

3-86. (U) 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 ability to perform mission-essential functions. To be effective, incident response measures must be fully coordinated, exercised, and evaluated. Attacks employing CBRN weapons may produce mass casualties or widespread destruction, which can quickly overwhelm organic resources. Command considerations for incident management include the following:

- (U) Knowing the response route.
- (U) Approaching uphill and upwind if possible.
- (U) Avoiding choke points.
- (U) Designating rally points.
- (U) Identifying safe staging locations for incoming units.
- (U) Ensuring the use of personal protective equipment and personnel accountability.
- (U) Assessing security continually.
- (U) Allowing the evacuation of noncombatants to safe areas and the injured to treatment facilities, while keeping open access to first responders.
- (U) Ensuring security and screening procedures for witnesses and preventing the escape of terrorists.
- (U) Evaluating the need for specialized units (explosive ordnance disposal).
- (U) 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.
- (U) Knowing mass casualty and first responder requirements.

3-87. (U) The operation order antiterrorism appendix should prepare for the most likely threats as identified through the threat assessment and maximize the use of existing plans and standing operating procedures that can be referenced in the antiterrorism appendix. Establishing a mechanism to respond to a terrorist incident is an essential element of antiterrorism. Within the boards, bureaus, centers, cells, and working groups of the Army construct, the ATWG acts as the principal planning agency. The antiterrorism officer, key unit staff (S-2, battalion or brigade operations staff officer [S-3], civil affairs operations staff officer), selected contracted first responders, supporting contracting office personnel, and personnel who make up the base defense operations center (BDOC) are part of the ATWG. 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.

3-88. (U) 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:

- (U) **Medical team.** This team is capable of triage, patient decontamination, and backup responder decontamination as necessary.
- (U) **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.
- (U) **Law enforcement.** This team is responsible for securing the crime scene, providing responder security, and controlling ingress and egress at the incident site.
- (U) **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.
- (U) **Explosive ordnance disposal.** The explosive ordnance disposal team is responsible for the detection, identification, on-site evaluation, safe, recovery, and initial disposition of unexploded ordinance.

Tenant Unit Responsibility (U)

3-89. (U) Tenant unit commanders must actively participate in the preparation of defense plans for bases and base camps 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 operational area 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 (U)

3-90. (U) 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 the 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:

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

3-91. (U) 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, by base defense guard or security forces, 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 antiterrorism appendix with on-scene command relationships and a clearly established chain of command. When responding to requests for support from civil authorities, the initial response force acts in a supporting role. However, the commander does not relinquish command responsibility and authority.

3-92. (U) 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 the 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 attack area. Response forces may be under constant observation so that responders must maintain a heightened level of security when exposed.

3-93. (U) 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 civil 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.

3-94. (U) 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, host nation police, and military forces responding to the incident according to the existing status-of-forces agreement.

Base Defense Operations Center (U)

3-95. (U) A BDOC is a mission command 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 operational area security efforts and coordinates and integrates area security operations with the base cluster operations center (if established) or other designated high-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 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.

3-96. (U) The nature of a BDOC depends on the combination of forces located at each particular base (Army units, unified action partners, multinational units, host nation agencies). 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:

- (U) Command.
- (U) Intelligence.
- (U) Operations.
- (U) Logistics.

Communications (U)

3-97. (U) 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.

FOB Marez Suicide Attack, Mosul, Iraq (U)

(U) A terrorist incident on 21 December 2004 in Iraq shows a well-planned base camp 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 the tables, and carried them outside. The BDOC took immediate action; medics were on scene 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 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. The suicide bomber was a 24-year-old man from Mosul who worked at the base for 2 months and provided information about the base camp to Ansar al-Sunna. Security at U.S. bases in Iraq was ordinarily extremely tight. Local Iraqi workers were typically searched before entering the base and monitored on the base. The only Iraqi nationals usually allowed in dining mess halls were Iraqi soldiers. This suggests that base facilities had been infiltrated by adversaries who were collecting and providing information on base vulnerabilities. Further, this attack was carried out in daylight against the largest facility on the base 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 (U)

3-98. (U) 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 the servicing 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 the following:

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

3-99. (U) Apprehended military personnel are handled according to the Uniform Code of Military Justice, DOD and Service regulations, and applicable installation standing operating procedures. In foreign incidents, persons employed by or accompanying the Armed Forces who engage in certain misconduct may be prosecuted under U.S. law and the Military Extraterritorial Jurisdiction Act. Certain civilian detainees may also be processed according to the status-of-forces agreement, diplomatic note, or other agreements with that particular country. Cases being considered for disposition under the Military Extraterritorial Jurisdiction Act require coordination through the staff judge advocate. Unless circumstances dictate otherwise, the staff judge advocate should also be consulted before releasing an individual to host nation authorities. The United States does not normally render its own nationals to the custody of a third party, including a host nation. 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 7 working days after termination of the detention of nonmilitary personnel for antiterrorism.

3-100. (U) 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 servicing judge advocate and law enforcement personnel should ensure that reports are submitted to higher headquarters in sufficient detail to meet prosecution requirements.

3-101. (U) 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, domestic civil authorities or host nation 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 (U)

3-102. (U) Employing irregular warfare tactics, the greatest weapon of the terrorist is the ability to influence operations and public opinion through the aggressive domination of the media information cycle. The rapid release of information as press releases (audio, video, or printed products) tied to an event (IEDs, suicide bombings, civilian casualties, attacks on U.S. forces) seizes the information initiative. Information is always secondary to the timing. The burden to disprove the information in a terrorist information product usually rests with the target of the attack. In the deployed joint operations area, units often face an adaptive and technologically savvy enemy which recognizes that the global information network is the most effective tool for attacking what is perceived to be the center of gravity—public opinion (domestic, and international). This type of information warfare increased the flow of money and aid from around the globe, influenced the civilian opinion of U.S. forces in occupied areas, and affected the public opinion within the United States.

3-103. (U) The release of timely information following a terrorist attack is critical to getting ahead of the media information cycle and terrorist attempts to influence the public opinion. In a deployed environment, planning for terrorist attacks requires coordination between the influence line of effort, to include planners, military information support operations (MISO) elements, and the inform line of effort with public affairs officers. Public affairs officers can provide quick statements from a commander concerning a terrorist incident to seize the media initiative. MISO can provide products (flyers, radio and television spots, coordinated host nation civilian key leader engagements) that highlight factual details surrounding a controversial incident or event to prevent distortion by terrorists. The timing of postevent public affairs releases and MISO products is critical. They are far less effective if not placed on the street within minutes to a few hours after an event.

3-104. (U) 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. Local media often plays and replays images on television following an incident in which local noncombatants are killed or wounded by U.S. forces, multinational partners, or terrorists. 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 partners or Army 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 U.S. and multinational partners move too slowly and take too long to investigate and vet messages before engaging the media, the impressions of the event as portrayed by the local media are already fixed in the minds of the target audience.

3-105. (U) Army public affairs officers play a leading role as the voice of the commander and have the mission to provide factual and timely information to the media without violating OPSEC. MISO (as a core information-related capability) is the primary means for the commander to communicate with the civilian populace in their own language. Public affairs, MISO, Soldier, and leader engagements should operate in concert with strategic communications guidance to achieve a proactive, integrated, counter threat information message that is released to the broadest audience possible.

3-106. (U) Public affairs, MISO, and inform-and-influence activity planners should have readily available contingency messages that are approved by the commander and well coordinated with operational staff elements (S-2, S-3, battalion or brigade plans staff officer, antiterrorism officer) during incident management planning. The successful massing of information effects requires the commander to articulate the intent clearly for the integration of available elements of operations in the information domain. These messages need to be incorporated into incident 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 incident management message releases must ensure that they maintain an open dialogue with liaisons or points of contacts with units throughout the area of operations to acquire specific details about an event or incident when they are not in the immediate vicinity of an attack.

3-107. (U) By analyzing audiences within the area of operations, public affairs officers are 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 host nation news media representatives in their area of operations 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 host nation media.

3-108. (U) In the event of an attack, public affairs officers 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.

3-109. (U) Follow-on press releases, MISO products, and commander interviews can be used as part of incident 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 witnesses by public affairs and host nation media sources aid in solidifying statements by the U.S. and multinational partners, while discrediting terrorist claims and denouncing or condemning their attack. By continually reducing terrorist claims and exploits through quick, consistent, and factual reporting, the Army and multinational partners effectively take the information offensive approach to the postattack phase and can be more effective at defeating terrorist support in the area of operations.

3-110. (U) The advantages of having local or host nation media cover noteworthy events and lead when publishing postattack messages are numerous. Host nation media can—

- (U) Place a host nation face on published works.
- (U) Capture the ground truth in near real time.
- (U) Counter antigovernment force information.
- (U) Eliminate the language barrier when conducting interviews with other local nationals or witnesses to the event.
- (U) Gain credibility and acceptance among the local population.

3-111. (U) The Army and multinational partners may never have enough initiative to overcome a terrorist publishing information about a terrorist attack. Through informing, influencing, planning, and coordinating an incident management response, the Army or multinational partners can inform the host nation media about events that will likely impact and shape the information environment, influence cooperation of the civilian population, and reduce the terrorist ability to successfully shape the local population perception of an incident.

SUPPORT ANTITERRORISM TASKS (U)

3-112. (U) The deployed antiterrorism program is reinforced by antiterrorism tasks that support the execution of the tactical tasks discussed earlier in this chapter (see figure 3-3, page 3-8). By establishing an antiterrorism program, increasing antiterrorism awareness, establishing civil-military partnerships, and conducting exercises and evaluating/assessing the plan, commanders enhance their unit ability to defeat terrorist activities.

Antiterrorism Task 1. Establish an Antiterrorism Program (U)

3-113. (U) The antiterrorism 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 counterintelligence services. Commanders communicate their intent on managing the terrorist threat to their subordinates, enhancing decentralized execution and adaptability to changing tactics at lower levels.

3-114. (U) Antiterrorism planning is conducted and documented in the form of an appendix to an operation order, operation plan, or standing operating procedure for units (battalion or higher) while conducting training and operational deployments (50 or more personnel), training exercises (50 or more personnel), and special events (host nation police academy graduation, opening of a new host nation government facility). Commanders and staffs coordinate their efforts with the appropriate civil authorities and U.S. teams. Antiterrorism appendixes should be flexible for use by a unit or base, can be adapted for any environment (in-transit, base, offense, or defense), and are coordinated through the appropriate geographic combatant command and U.S. embassy or consulate.

3-115. (U) The purpose is to help the antiterrorism officer structure an antiterrorism appendix in a comprehensive and organized manner. The format is usually patterned after the standard five-paragraph military operation order (situation, mission, execution, sustainment, and mission command) that can be issued as a stand-alone document or in support of a larger operation order. This format enables the synchronization of existing programs (physical security, antiterrorism, OPSEC, information security, HRP protection). Antiterrorism considerations should be integrated into plans and separate appendixes. Collaborative staff interaction is a crucial element in developing a realistic executable plan that provides amplified instructions as required. Antiterrorism planning documentation should address the following:

- (U) Application of antiterrorism measures, to include random antiterrorism measures.
- (U) Essential antiterrorism program elements according to AR 525-13.
- (U) Terrorist threats and other threat activities.
- (U) Measures to reduce vulnerabilities to terrorist acts and attacks.
- (U) Antiterrorism physical security measures.
- (U) Antiterrorism measures for critical asset security.
- (U) Entry control point procedures.
- (U) FPCON implementation measures, including site-specific antiterrorism measures.
- (U) On-site security elements.
- (U) OPSEC and information security.
- (U) Antiterrorism measures for HRP, when appropriate.
- (U) Reaction to terrorist incidents.
- (U) CBRNE plans and measures to deal with toxic industrial hazards.
- (U) BDOC operations.
- (U) Alert notification procedures.
- (U) Incident response management procedures.

- (U) Antiterrorism construction and building considerations.
- (U) Antiterrorism measures for logistics and other contracting.
- (U) Antiterrorism measures for in-transit movements, when appropriate.

Antiterrorism Task 4. Increase Antiterrorism Awareness (FOUO)

3-116. (FOUO) Soldiers need to be situationally aware and know what is happening around them. 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.

3-117. (FOUO) For this reason, antiterrorism awareness serves as a key component of the unit ability to assess, detect, warn, and defend against terrorist actions. To help combat complacency, commanders emphasize antiterrorism 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 random antiterrorism measures. By emphasizing and teaching Soldiers to recognize potential or actual threats early, they can take measures to avoid or counter threats before they occur.

3-118. (FOUO) Antiterrorism 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 position is debilitating also; 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. Antiterrorism 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 allow the Soldier to function without added stress associated with maintaining this level of personal security posture indefinitely.

3-119. (FOUO) Antiterrorism 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. 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, obvious avoidance of security personnel).

3-120. (FOUO) 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, entry control points, 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 antiterrorism 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 antiterrorism program, the staff works closely with MISO 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 (FOUO)

3-121. (FOUO) Through the conduct of civil-military operations, commanders may coordinate with defense attachés, regional service officers, indigenous populations, and institutions that can be used to combat and defend against terrorism. The formation of effective and integrated civil-military teams creates complementary capabilities that mitigate the inherent weaknesses of the Army and civilian agencies that are living and operating in the area of operations. 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 area of operations can develop useful civil information, which can be fused or processed to increase situational awareness, situational understanding, or situational dominance. It is critical for commanders to understand the integrated process, intricacy, and mission requirements of conducting civil-military operations that develop effective civil-military partnerships in support of antiterrorism tasks.

3-122. (FOUO) Civil-military partnerships also exist to enhance a commander's capabilities in response to terrorist attacks. Assistance from civil authorities can provide resources in the way of CBRN 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 media resources are crucial for disseminating MISO products that encourage postincident civilian cooperation and reporting to prevent or mitigate terrorist incidents. Civil-military partnerships result from the civil-military operations conducted by the units within the area of operations. These relationships will assist in the integration of military and civilian resources, developing a whole government approach and building a unity of effort during the execution of antiterrorism tasks. (For additional information on the integration of civil-military operations across the range of military operations, see JP 3-57 and FM 3-57.)

Antiterrorism Task 8. Conduct Exercises, and Evaluate/Assess the Plan (FOUO)

3-123. (FOUO) 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 unified action and/or multinational 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 of multiple units within the Army or within unified action or multinational partners to deal with a variety of terrorist incidents.

3-124. (FOUO) Commanders establish exercise and training programs that develop, refine, and test command antiterrorism response procedures to terrorist threats or incidents and ensure that antiterrorism is an integral part of the unit 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 Army 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. (For additional information on antiterrorism exercises, see Standard 23 in AR 525-13.)

3-125. (FOUO) Experiences from Iraq and Afghanistan demonstrated that Soldiers who are trained exclusively for offensive tasks were not as capable of adapting to the requirements for stability tasks or facing the challenges associated with dealing with an asymmetric threat. Commanders must find a balanced approach to the types of training essential to unified land operations, understanding that the terrorist threat is present throughout the range of military operations. Incorporating antiterrorism training and awareness prepares Soldiers to operate more efficiently in any environment.

This page intentionally left blank.

Chapter 4

Execution of Antiterrorism Measures (U)

(U) This chapter further expands on the integration of antiterrorism in unified land operations as discussed in chapter 1 and the application of antiterrorism tactical tasks to protect Army forces from violent and nonviolent terrorist tactics in various deployed environments.

MOVEMENT (U)

4-1. (U) *Force projection* is the ability to project the military instrument of national power from the United States or another theater, in response to requirements for military operations (JP 3-0). Through power generation platforms, installations provide continuous force generation, deployment, and training 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.

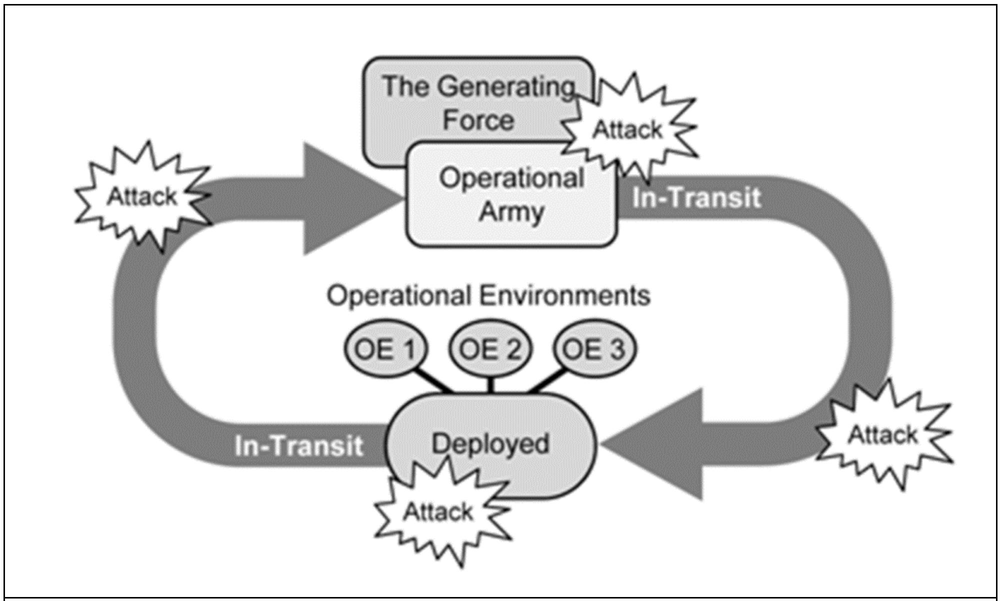
4-2. (U) Current and future global commitments will keep Army operational forces in a nearly constant rotation, traveling from one geographic location to another. The Army is expected to move a combat-capable brigade anywhere within 96 hours with forces capable of operating in any environment. The early 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. Antiterrorism thinking and planning integrated into every aspect of predeployment and in-transit movement ensures proficiency, especially under demanding time constraints.

4-3. (U) Army units and activities are expected to deploy rapidly in support of force projection. 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 (vehicle, rail, air, and sea). The mode of movement determines antiterrorism tactics, techniques, and procedures for preparing, planning, coordinating, and executing unit movements. (See figure 4-1, page 4-2.) The phases of deployment are—

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

PLANNING (U)

4-4. (U) 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 antiterrorism 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.)



Legend:
OE operational environment

Figure 4-1. (U) Threats to in-transit movements

4-5. (U) 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 (U)

4-6. (U) Army commands, ASCCs, direct reporting units, the U.S. Army Reserve Command, and the Army National Guard Bureau provide their respective unit commanders with an updated threat analysis and vulnerability assessment 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 in transit.

4-7. (U) To help minimize the risk while in transit, unit leaders should conduct reconnaissance before moving the advance and main bodies. The leader’s reconnaissance will include a threat analysis, vulnerability assessment, and coordination to mitigate risks identified by the leader’s reconnaissance. Antiterrorism assessments should be conducted sufficiently in advance of deployments to develop security procedures, acquire necessary materials, obtain tailored and focused intelligence, organize the necessary security support augmentation, and conduct host nation coordination.

4-8. (U) Installation commanders within the U.S. Army Installation Management Command are charged to protect deploying forces as they conduct force projection. Units preparing for deployment interact with the installation staff through the corps and division protection cells and the installation ATWG. The unit antiterrorism officer serves as the 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. (U) 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. (U) Relief-in-place planning should begin when the relieving unit is identified and a predeployment site survey has been conducted. Enemy combatants and terrorists can determine when units are expected to rotate through constant surveillance by the local population, conversations with Soldiers, and open-source information. 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 (U)

4-11. (U) 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 area of operations 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 and staffs 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. (U) The predeployment site survey is mission- and time-dependent and is normally conducted 3 to 6 months from the anticipated deployment. This time frame is close enough to deployment that the mission and area of operations are not expected to change significantly, yet far enough in advance to allow for the programming of 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 during the initial phase of operations in the area of operations. 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 antiterrorism 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. (U) Upon completion of the predeployment site survey, the commander and staff should have an increased knowledge of the region they will operate in and of the terrorist threat and identified actions in the area. With this knowledge, the commander can issue guidance and determine key training tasks. The predeployment site survey should include the following:

- (U) Requests for information and arrangements for follow-up information.
- (U) Maintenance of digital pictures of key places, infrastructure, and local persons of importance or influence.
- (U) Maintenance of information on the current enemy situation and specific terrorist threat, including current enemy tactics and practices, incidents, and experiences of enemy operations.
- (U) Policies and practices for units dealing with contractors (U.S., local, and third-country nationals) who are working on the deployed FOB. The antiterrorism officer should obtain a clear understanding of how local nationals, third-country nationals, foreign forces, and U.S. contractors are cleared for access to U.S. bases and facilities.
- (U) Outgoing unit antiterrorism appendixes, ASCC antiterrorism guidance, standing operating procedures, reports, and briefing formats (digital copies if possible).
- (U) 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 (U)

4-14. (U) Units use the results of the threat assessment, criticality assessment, and vulnerability assessment 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 low-threat areas.

4-15. (U) Commanders must implement appropriate antiterrorism 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 the posture of a transiting unit against terrorist threats. Commanders should consider commercial, off-the-shelf or government, off-the-shelf products to meet near-term antiterrorism requirements.

4-16. (U) 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 area of operations require close consideration. These facilities are frequently vulnerable due to their location and easy access. Movements may require tailored intelligence and counterintelligence support, host nation or domestic civil authorities assistance, or planned alternate routes based on the vulnerabilities associated with the movement. Commanders and staffs should consider the following to assist in mitigating risk during movement:

- (U) **Protective measures.** After estimating the threat and conducting a vulnerability assessment, the unit must take steps to ensure the security of its personnel, information, facilities, and equipment. When establishing 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.
- (U) **Routine security operations.** Once the commander has approved plans that outline antiterrorism 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 random antiterrorism measures 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.
- (U) **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 incident management procedures, including mission command and CBRN response measures.

4-17. (U) 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. Antiterrorism officers oversee the execution of several actions at each stage of movement. (See table 4-1.)

Table 4-1. (FOUO) Antiterrorism 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 1 AT training. • Provide AOR-specific training.	• Submit the AT appendix to the combatant commander. • Track 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 a terrorist threat assessment for movement. • Identify specific COAs for 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. • War-game potential unit vulnerabilities. • Coordinate with the lift provider to determine appropriate defensive measures. • Coordinate with the lift provider and HN or domestic civil authority regarding the security of the 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 the rules of engagement. • Implement planned security measures. • Liaison with HN or domestic civil authority support.
React to Terrorist Incidents		
• Plan unit responses to various threat COAs. • Develop a communication plan to ensure that units can receive and transmit warnings/reports.	• Assemble port readiness committees. • Coordinate the response plan during movement with the applicable agency. • Respond to the incident.	• Obtain the local response plan guidance. • React to an incident (if necessary).

Legend:

AOR	area of responsibility
AT	antiterrorism
COA	course of action
HN	host nation
HRP	high-risk personnel
PDSS	predeployment site survey
RSO&I	reception, staging, onward movement, and integration
S-2	battalion or brigade intelligence officer
U.S.	United States

Fort to Port (U)

4-18. (U) The unit commander develops an in-transit security annex to the movement order which outlines security measures that will mitigate or reduce suspected vulnerabilities during movement. The unit antiterrorism 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 (U)

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

4-20. (U) The threat assessment provides the unit commander with an updated threat analysis and assists the unit antiterrorism officer in conducting the vulnerability assessment 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 U.S. Transportation Command and Surface Deployment Distribution Command make (through operations channels) a vulnerability assessment available for the mode of travel and locations through which the deploying unit will move. The vulnerability assessment should consider the terrorist threat and attack methodologies that may cause mass casualties.

4-21. (U) The unit antiterrorism officer assists in developing this appendix 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 unit sensitive items and cargo. The vessel commander determines the priority for security personnel. The organization of shipboard security elements may vary, although two security squads per vessel is a general planning factor.

4-22. (U) Units should consider the following factors if tasked with rail or shipboard security planning:

- (U) Threat assessment.
- (U) Rules of engagement and rules for the use of force. (See AR 190-14 for additional information on use of force.)
- (U) Security detachment functions and responsibilities.
- (U) Support equipment.
- (U) Weapons qualification and proficiency.
- (U) Mission command.
- (U) Railhead, pier side, and afloat security duties.

MOVEMENT (U)

4-23. (U) During movement to the port of embarkation, unit commanders and antiterrorism officers rely on their installation and deployment centers to provide the latest threat assessment 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.

4-24. (U) In the area of operations, the probability and severity of IED use in the operational environment make convoy missions 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 threat assessment, disseminate contingency plans, conduct radio checks, ensure that the radio-controlled counter IED electronic warfare 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 photographs of known checkpoints and safe havens along the routes.

Air Movement (U)

4-25. (U) 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 antiterrorism planning for movement to the aerial port of embarkation and in the marshaling area. Army and Air Force commanders jointly coordinate mutual defense while traveling by air.

4-26. (U) 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 (U)

4-27. (U) 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 (host nation support and security forces on the train) should be used to minimize vulnerabilities to attack when transiting by rail.

4-28. (U) The surface deployment distribution command is responsible for planning and executing rail movements; however, the transiting unit commander retains responsibility for planning antiterrorism 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.

4-29. (U) Cargo guards or escorts maintain surveillance over military equipment during the journey and notify railroad personnel of problems. They must be thoroughly trained regarding antiterrorism 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 Army interests.

Sea Movement (U)

4-30. (U) 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 ATP 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 antiterrorism measures exist and are executed during deployments through strategic seaports. Antiterrorism 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.)

4-31. (U) Supercargoes 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.

4-32. (U) Upon arrival at the seaport of embarkation, supercargoes are under the operational control of the port commander. While onboard a ship, they are under the mission command of the vessel captain. Upon arrival at the seaport of debarkation, supercargoes are under the operational control of the port commander and are normally released to the unit upon the completion of port clearance operations.

4-33. (U) Terrorist threat assessments identify and evaluate potential threats on the basis of capabilities, intentions, past activities, and operational environment. 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 supercargoes permitted onboard, based on the berthing capacity on the ship. (See FM 3-35.)

RECEPTION, STAGING, ONWARD MOVEMENT, AND INTEGRATION (U)

4-34. (U) The operational responsibilities of unit movements from the aerial port or seaport of debarkation to the area of operations 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 in transit. Security is paramount during reception, staging, onward movement, and integration. 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. Host nation support plays a critical role and should be planned. The reception, staging, onward movement, and integration process is facilitated by the use of host nation resources (ports; airfields; railways; land for staging, traffic convoy, and convoy escorts).

4-35. (U) The combatant commander is responsible for establishing an FPCON baseline level and providing guidance on the employment of random antiterrorism 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 port or seaport of debarkation through assembly or staging areas and on to the final unit destination.

4-36. (U) Upon arrival, the unit commander should receive an updated threat analysis and vulnerability assessment from the departure control group for the route and method of travel from the port of debarkation to the area of operations. This includes intelligence that gives the unit commander up-to-date situational awareness.

DEFENSE (U)

4-37. (U) While defensive tasks can be conducted temporarily until offensive tasks can resume, commanders also conduct defensive tasks to retain key terrain, provide secure mission command to a larger area of operations, deter or defeat terrorist offensive actions, or protect the local populace, critical assets, and infrastructure. Antiterrorism measures naturally support the commander’s protection requirements during defensive and stability tasks.

4-38. (U) Antiterrorism 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 antiterrorism measures integrate a multitude of security programs, which ensure that U.S. personnel, information, infrastructure, installations, facilities, and forces are protected from enemy 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 mission command centers and key communications nodes in defense is critical to success. Survivability and antiterrorism 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. Enemy 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.

4-39. (U) In a mobile defense or retrograde mission, 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 antiterrorism training and updated threat assessments to gain an understanding for the tactics likely to be used against them in a certain area. They rely on increased situational awareness and the ability to identify IED tactics to aid in protecting themselves and covered forces.

4-40. (U) Effective and disciplined OPSEC and surveillance detection missions 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 missions 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.

4-41. (U) In an area defense and during area security, commanders understand the importance of protecting mission command nodes and the surrounding populace. Antiterrorism 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. The increased probability or results of successful terrorist attacks drive the overall FPCON level or could result in the implementation of various random antiterrorism measures. Incident management plans to recover from terrorist actions and to maintain the continuity of operations are essential in the overall success of unified land operations.

4-42. (U) Commanders establish locations to provide mission command, 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 ability to conduct violent and nonviolent attacks during unified action. Commanders can also extend protection to the local populace, critical assets, and key infrastructure to deny terrorist influence in that area and allow for the freedom of movement.

4-43. (U) 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 engagements* are those public affairs activities that support the relationship between military and civilian communities (JP 3-61). 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.

BASES AND BASE CAMPS (U)

4-44. (U) A *base* is a locality from which operations are projected or supported, an area or locality containing installations which provide logistic or other support, or a home airfield or home carrier (JP 4-0). Current national, defense, and military strategies require modular Army land forces to conduct operations anywhere from self-sufficient FOBs. Nearly all operational bases where U.S. military troops are deployed can be targets for terrorist attacks. Commanders, with assistance from the antiterrorism officer, ensure that bases are securable and defendable against this type of threat at all times.

4-45. (U) Base commanders have the overall responsibility for the security 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.

4-46. (U) Site selection and design layout are determined by competing demands and considerations (mission concerns, political constraints, host nation requirements, Service regulations). Antiterrorism measures should be deliberately integrated into the planning, design, and construction of base camps. A base camp design that includes considerations for terrorist threat capabilities and countermeasures can greatly reduce the amount of materials, time, and energy required to protect the base camp and increase the defensive posture during increased threat or FPCON levels.

Base Selection (U)

4-47. (U) The early identification of antiterrorism 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 and mission accomplishment. The early development of antiterrorism and security requirements helps to reduce construction and manpower costs and ensures the adequate protection of personnel and assets. It is easier and more cost-effective to establish antiterrorism security measures during the planning process rather than after the fact.

4-48. (U) The key to the effective planning, design, and development of base protection requirements is a partnership between the unit antiterrorism 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—

- (U) Antiterrorism 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.)
- (U) Antiterrorism measures are within the capability of the unit.
- (U) Resources are available to accomplish the task.
- (U) Antiterrorism measures provide maximum latitude for initiative.
- (U) Antiterrorism measures are within the bounds of legal, moral, and host nation constraints.
- (U) Antiterrorism measures consider future operations, latitude for initiative, and flexibility to meet unexpected threats and opportunities.

4-49. (U) Antiterrorism planning should also be incorporated into the framework of master planning. Master planning provides an integrated strategy for the 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 (U)

4-50. (U) Planners and designers can integrate antiterrorism measures into three planning and design stages that support FOB development:

- (U) **Site selection.** Planning provides a framework to guide the development of the FOB. The consideration of antiterrorism measures during the site selection stage may preclude the need for applying more stringent antiterrorism measures to the FOB later. Site selection planning should make use of vegetation, topography, and natural barriers as protective measures.
- (U) **Base layout and design.** Planning addresses methods for integrating perimeter security, standoff distances, entry control points, vehicle barriers, fences, and security lighting to diminish the potential threat to personnel and critical assets.
- (U) **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 (U)

4-51. (U) Deployed-base site selection and design layout are determined by competing demands and considerations (mission concerns, political constraints, host nation requirements, Service regulations). Antiterrorism measures should be deliberately integrated into the planning, designing, and constructing 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—

- (U) Contingency operating base.
- (U) FOB.
- (U) Combat outpost.
- (U) Logistic support area.
- (U) Joint contingency operating base.
- (U) Joint FOB.
- (U) Joint security stations.

4-52. (U) 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 antiterrorism officer should work closely with base planners and designers to ensure the integration of protection measures.

Planning Factors (U)

4-53. (U) 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 antiterrorism 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 antiterrorism 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—

- (U) Meet the minimum antiterrorism requirements of UFC 4-010-01.
- (U) Meet applicable combatant command (command authority) antiterrorism requirements.
- (U) Include requirements to defeat specific threats, based on input from the base commander and intelligence reports.
- (U) Involve a risk analysis of the deployed operating base assets to determine if additional antiterrorism design requirements are merited. Higher-risk assets may warrant higher levels of protection, more resources, and shorter timelines.

SITE SELECTION CONSIDERATIONS (U)

4-54. (U) The FOB site is selected to facilitate the accomplishment of the primary operational mission. Even so, antiterrorism considerations must not be ignored. The location of a FOB should be chosen to facilitate force protection 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) for a proposed FOB. This analysis should consider the military aspects of a location from the standpoints of the defenders and the enemy.

4-55. (U) In selecting a site, FOB planners should consider the following:

- (U) **Threat.** Identify and characterize threats to the FOB. Understanding the threat assists commanders in determining the best location for a FOB.
- (U) **Political considerations.** Consider the relationship with the local public.
  - (U) **Host nation political climate.** Consider how the local situation influences FOB location, design, or land use decisions. Politically unpopular decisions may attract acts of aggression.
  - (U) **Adjacent landowners.** Assess potential problems, to include the impact of traffic restriction, safety, and other inconveniences. Identify restrictions that limit public access to the area of the proposed FOB.
  - (U) **Appearance.** Consider the local perception of a proposed FOB. For example, public perception of a fortress may be desirable or undesirable.
- (U) **FOB mission.** Examine the FOB mission, planned facilities, and tenant units and organizations.
- (U) **Real estate and building availability.** Determine available real estate, existing facilities, infrastructure, and buildings. Assess off-base land and zoning plans for protection impacts. Assess occupancy requirements.
- (U) **Communication capability.** Assess the ability to speak to higher headquarters and subordinate units operating in the area of operations using frequency modulation, satellite, and Internet capabilities.
- (U) **Dispersion and standoff minimum requirements.** Provide minimum standoff requirements to the controlled perimeter, parking areas, living quarters, roadways, and buildings.
- (U) **Defense in depth.** Select a site that provides defense in depth, requiring a terrorist to negotiate varied defense mechanisms to reach an ideal target. Does the location and layout of the FOB present a hardened image to a terrorist, one that will discourage an attack? Does the location and layout assist personnel in defending against vehicle-borne IEDs, rockets, artillery, and mortars by allowing for use of natural barriers, standoff distance, dispersion, compartmentalization, and clear fields of fire?
- (U) **Perimeter requirements.** Determine perimeter security requirements (standoff, barriers, entry control points, 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 random antiterrorism measures?
- (U) **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.
- (U) **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.
- (U) **Potential enemy vantage points.** Situate the FOB to limit attacks by direct, line-of-sight weapons from potential vantage points.
- (U) **Natural terrain (observation and fields of fire, avenues of approach, key terrain, obstacles, cover and concealment).** Does 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?
- (U) **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?
- (U) **Topographic areas.** Avoid low-lying topographic areas that can facilitate the effects of possible CBRNE attacks.

BASE LAYOUT CONSIDERATIONS (U)

4-56. (U) Personnel responsible for planning bases and base camps must consider a multitude of challenges. In general, these concerns and constraints will be unique to the lay of the land. Base camp design is an extension of planning. Base camp layout is the process of calculating, mapping, and planning the allocation of land. Some key measures for base camp layout are:

- (U) Design the FOB to facilitate current operations.
- (U) Design the FOB to have a layered security approach.
- (U) Position the perimeter zone immediately in front of or behind the base camp. The perimeter zone consists of operations, fighting positions, and entry control points.
- (U) Provide adequate standoff distance.
- (U) Direct the positioning and construction of operations, guard posts, fighting positions, entry control points, and command posts in conjunction with protective positions.
- (U) Direct positioning and construction of emergency entry and exit points to ensure the mobility efforts of the response forces so that they are not constrained by entry control point locations.
- (U) Position the inner security area inside the base camp. The inner security area consists of interior barrier plans and traffic control measures to further halt or impede threats.
- (U) Provide barriers within the base camp for areas identified as critical assets due to the high concentration of people (dining facilities).
- (U) Provide hardening of facilities for vulnerable assets (storage areas, communication nodes, mission command nodes).
- (U) Deny hiding places within the base camp.

OFFENSE (U)

4-57. (U) During offensive tasks, commanders use antiterrorism measures and training to better prepare 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 prepare their force to defend against threats to combat power that are faced in active insurgencies and during general war. Within the protection warfighting function, commanders apply antiterrorism protection measures while weighing the risk involved, with bold initiative and control of the operational tempo.

4-58. (U) During offensive tasks, various military organizations may be involved in area security in an economy-of-force role to protect lines of communications, convoys, and critical fixed sites and radars. The FOB employs local security measures (assessments and recommendations, random antiterrorism measures, and increased FPCON), but it may be vulnerable to nonstate actors used as an arm of a greater military engagement. Based on mission analysis and planning efforts, specific antiterrorism measures are identified to counter terrorist tactics.

4-59. (U) Commanders, with the assistance of the antiterrorism 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 random antiterrorism measures to protect logistic lines, critical sites, and host nation infrastructure and to identify vulnerabilities within their own forces to the asymmetric tactics associated with terrorist actions.

4-60. (U) Level I antiterrorism 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 operating in confined spaces found within most urban settings or en route to an objective in more rural settings. Personal protection training prepares Soldiers mentally in case they are separated from their unit or are 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 and enhances the likelihood of the Soldier being recovered and returned to the fight.

4-61. (U) Patrols obtain information about terrorist threats and capabilities before leaving the security of a FOB. The patrol leader establishes the patrol 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.

4-62. (U) Because of the reliance on speed, audacity, and surprise in the offense, antiterrorism officers understand the importance of OPSEC and information security. Terrorist organizations have shown increased skill at using technology and have demonstrated abilities at hacking into information centers. To protect the commander's availability of information and increased situational awareness, antiterrorism officers ensure that communication lines and information systems are protected from outside attack or surveillance to protect ongoing and future mission planning. Antiterrorism 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.

4-63. (U) Leaders ensure that their Soldiers understand the rules of engagement before conducting missions. 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 Army or multinational partner operations. In the past, terrorists have bombed 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.

4-64. (U) Leadership serves as a key component to effective combat power during the offense. The antiterrorism officer ensures that critical HRP are provided with necessary protection against the violent asymmetric tactics associated with terrorists. The antiterrorism officer assists designated security teams and squads in obtaining the necessary training and equipment to best accomplish their duties. While the Army conducts operations through centralized planning and decentralized execution, antiterrorism officers understand the effect on unit morale after the loss of a key leader or commander to an attack or assassination and, ultimately, work to preserve the unit 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 (U)

4-65. (U) 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 ADP 3-07 and ADRP 3-07.)

4-66. (U) Stability tasks require commanders to balance protection needs between military forces and civil populations; it is in this environment that antiterrorism posture is at its greatest. Nonstate actors prey on civilians and other noncombatants as a means of weakening U.S. influence in the country, weakening domestic U.S. political resolve, and promoting their individual agendas. Because U.S. forces and the local population frequently interact, planning for their protection is important and planning should be integrated into local base threat, vulnerability, and criticality assessments. Attacks on critical infrastructure and reconstruction projects have an impact on mission success, local base operations, and 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).

4-67. (U) Success in stability 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.

4-68. (U) In the absence of a conventional or militant force, a commander's greatest threat will derive from terrorist activities. As in offensive and defensive tasks, commanders (with the assistance of antiterrorism officers) use various assessments and antiterrorism measures to mitigate the vulnerabilities of their forces and bases to the violent tactics of terrorism. Commanders also expand their ring of antiterrorism protection to encompass the local populace, critical infrastructure, and heads of government to—

- (U) Provide a safe and secure environment.
- (U) Enhance freedom of movement.
- (U) Facilitate the rule of law.
- (U) Enable a stable government.
- (U) Facilitate a sustainable economy.

4-69. (U) 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 increase 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 government cannot provide basic social well-being.

4-70. (U) Because stability is 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 events to serve their goals of circumventing U.S.-led efforts.

DEFENSE SUPPORT OF CIVIL AUTHORITIES (U)

4-71. (U) Defense support of civil authorities is conducted only within the United States and U.S. possessions and territories, not outside the United States. If DOD conducts disaster relief missions in support of a foreign nation, it is a stability task and is called foreign humanitarian assistance or foreign consequence management. The Department of State, not DOD, is the lead agency for this type of stability tasks.

4-72. (U) Within the framework of homeland security, Army forces, as part of a joint response (at state level, federal level, or both) will normally conduct defense support of civil authorities tasks exclusively, often employing capabilities developed for other elements of unified land operations as part of defense support of civil authorities. Conducting domestic operational environment tasks are different from other tasks within unified land operations in terms of law, military chain of command, use of force, and interagency process.

4-73. (U) Defense support of civil authorities is provided to U.S. civil authorities under the auspices of the *National Support Framework* for domestic emergencies, designated law enforcement support missions, national special security events, and other missions. It includes addressing the consequences of disasters, accidents, terrorist attacks, and incidents. Army forces conduct defense support of civil authorities when the size and scope of events exceed the capabilities of domestic civilian agencies. During defense support of civil authorities, antiterrorism measures are important to protect U.S. citizens and Soldiers from unknown hazards and threats. Army forces perform defense support of civil authorities tasks under U.S. law, generally following a tiered-response concept. (See ADRP 3-28.)

4-74. (U) The Army National Guard is often the first military force to respond on behalf of state authorities. In this capacity, the Army National Guard functions in the state active duty status or federally funded status under Title 32, U.S. Code (32 USC). In addition, the Army National Guard forces under state control have law enforcement authorities that Regular Army units do not have. The Army National Guard is well suited to conduct these missions. If the response requirements exceed state and Army National Guard capabilities, the governor may request assistance from federal authorities. Antiterrorism planning considerations during defense support of civil authorities may include—

- (U) Security support for national events and post disaster recovery.
- (U) Increased liaison with local law enforcement.
- (U) Fusion of threat information for the area of operations.

Note. (U) 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.

Chapter 5

Integration Into the Operations Process (U)

(U) This chapter focuses on antiterrorism integration throughout the operations process and its service to commanders as a combat multiplier. Terrorists often 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 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 to plan and defend against terrorist capabilities.

MISSION COMMAND ACTIVITIES (U)

5-1. (U) The operations process consists of the major mission command activities performed during operations: planning, preparation, execution, and assessment. The commander drives the operations process through mission command. (See 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 preparation are conducted as initial tasks are being executed. Planning remains a continuous activity, while preparation is done simultaneously only when a unit is not conducting operations. Assessment is continuous throughout activities and is crucial to influencing activities and mission accomplishment.

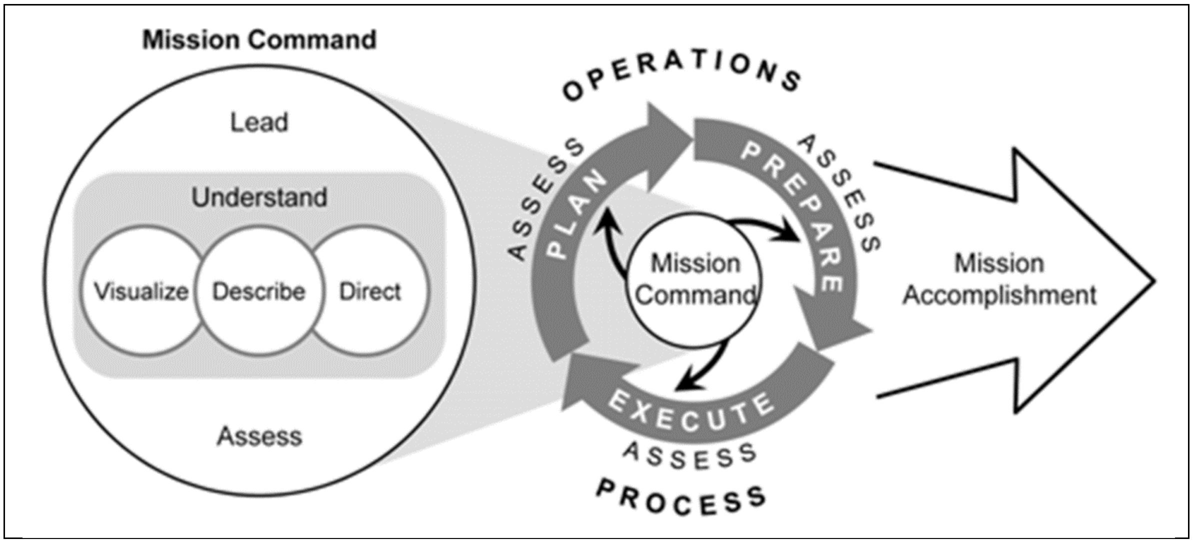


Figure 5-1. (U) Operations process and mission command

5-2. (U) Antiterrorism is an integral part of the protection warfighting function, and commanders rely on their antiterrorism 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 antiterrorism 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. The commander begins visualizing antiterrorism solutions, describes the concept and intent to the staff, and helps 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. (U) 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 respond 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 a politician or 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 (U)

5-4. (U) *Planning* is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about (ADP 5-0). Assessment during planning focuses on monitoring the current situation, establishing measures of effectiveness and measures of performance, and evaluating COAs.

5-5. (U) Because antiterrorism 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, preparation, and execution.

5-6. (U) During mission analysis, the antiterrorism officer, working with the G-2/S-2, develops running estimates to monitor and evaluate antiterrorism efforts throughout the operations process. These antiterrorism efforts may assist in the development of the measure of performance and effectiveness. A *measure of performance* is a criterion used to assess friendly actions that 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. (U) 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 antiterrorism measures to reduce vulnerability and mitigate risk.

5-8. (U) 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 antiterrorism guidance in planning may include the following information:

- (U) Intelligence focus for antiterrorism efforts.
- (U) Areas or events where risk is acceptable.
- (U) Critical assets and high-value targets.
- (U) FPCON status.
- (U) Implementation of random antiterrorism measures.
- (U) CBRNE risk guidance.
- (U) Information environment characteristics.

- (U) OPSEC risk tolerance.
- (U) Rules of engagement and interaction.

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

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

THREAT, CRITICALITY, AND VULNERABILITY ASSESSMENTS (U)

5-10. (FOUO) The antiterrorism 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 antiterrorism measures. Because of the global threat of terrorism, commanders must be aware of the threat in phases of force generation, the movement to training or operational locations, and the threat against forces while maneuvering throughout the area of operations. Units are vulnerable in different ways and at different times throughout these phases. Antiterrorism officers synchronize antiterrorism measures to enhance and support in-transit movement, the security of deployed operating bases, and the maneuvering of forces in the area of operations.

5-11. (FOUO) Criticality assessments and vulnerability assessments are intended to be sequential. However, the criticality assessment can be conducted before, after, or concurrent with the threat assessment. The vulnerability assessment should be conducted after the threat assessment and criticality assessment to determine which critical assets are more vulnerable. Commanders can also use vulnerability assessment 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 (U)

5-12. (FOUO) The *critical asset list* is a prioritized list of assets or areas, normally identified by phase of the operation and approved by the joint force commander that should be defended against air and missile threats (JP 3-01). These assets are of such extraordinary importance that their incapacitation or destruction would have a very serious, debilitating effect on operations. Once the threat assessment, criticality assessment, and vulnerability assessments 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 (host nation 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 for additional information.)

DEFENDED ASSET LIST (U)

5-13. (U) 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. A *defended asset list* is a listing of those assets from the critical asset list prioritized by the joint force 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 ADRP 3-37.)

ANTITERRORISM RISK MANAGEMENT PROCESS (U)

5-14. (U) Commanders will employ the antiterrorism risk management process as outlined in DODI 2000.16 and AR 525-13 in operational planning and decisionmaking. This must be accomplished to develop an effective antiterrorism plan and to enable commanders to assess and control risks associated with a mission or operation.

MILITARY DECISIONMAKING PROCESS (U)

5-15. (U) The *military decisionmaking process* is an interactive planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). The MDMP combines the conceptual and detailed aspects of planning and integrates the activities of the commander, staff, subordinate headquarters, and other partners throughout the planning process. 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.

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

5-16. (U) 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 design before, in parallel with, or after the MDMP. By doing so, commanders are able to understand and visualize the terrorist threat and modify unit tactics and approaches to solving the problem.

5-17. (U) The MDMP consists of seven steps as shown in table 5-1. This manual outlines each step of the MDMP, the various inputs, a method to conduct it, how antiterrorism 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 operations, commanders and staffs conduct a time analysis early in the planning process. This analysis helps determine what actions are required and when those actions must begin to ensure that forces are ready and in position before execution. (See ADRP 5-0.)

Table 5-1. (U) Antiterrorism 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 the Mission Warning Order	❖ Develop a 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 a VA and criticality assessment. • Determine AT resource constraints. • Perform the risk management process. • Generate AT-specific CCIR/EEFI. • Enhance information collection to look for terrorist and criminal activity. • Brief the 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** ❖ **VA/Criticality assessment**
• Problem statement • Mission statement • Initial commander's intent, planning guidance, CCIR, and EEFI • Updated IPB and running estimate	Step 3: COA Development	• Determine the CAL and DAL. • Determine the 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 • War-gaming results • Initial assessment measures
• Updated running estimates • Refined COAs • Evaluation criteria • War-gaming results	Step 5: COA Comparison	• Identify advantages and disadvantages. • Develop the recommended COA. • Refine COAs.	• Evaluated COAs • Recommended COA • 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 modifications • Refined commander's intent, CCIR, and EEFI
• Commander's selected COA with modifications • Refined commander's intent, CCIR, and EEFI	Step 7: Orders Production, Dissemination, and Transition	• 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 the AT plan

Table 5-1. (U) Antiterrorism support to MDMP (continued)

Key:	
❖	Specific AT tasks that are supported by MDMP
Legend:	
AT	antiterrorism
CAL	critical asset list
CCIR	commander’s critical information requirements
COA	course of action
COCOM	combatant command
DAL	defended asset list
EEFI	essential elements of friendly information
FPCON	force protection condition
IPB	intelligence preparation of the battlefield
MDMP	military decisionmaking process
RAM	random access measures
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
VA	vulnerability assessment

PREPARATION (U)

5-18. (U) *Preparation* consists of those activities performed by units and Soldiers to improve their ability to execute an operation (ADP 5-0). Preparation includes, but is not limited to, plan refinement, rehearsals, information collection, inspections, and movement. Preparation requires commander, staff, unit, and Soldier actions. Preparation creates conditions that improve friendly force opportunities for success. Some primary functions of preparation include—

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

5-19. (U) Because the force is often most vulnerable to attack and surprise while preparing, the emphasis on antiterrorism increases during preparation and continues throughout execution. Antiterrorism 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. Ally, civilian, and host nation agencies and organizations are frequently present before forces arrive and remain after forces depart.

5-20. (U) The S-2, S-3, antiterrorism officer, and ATWG synchronize the evolving threat information obtained from the intelligence preparation of the battlefield. Based on new data collected through the information collection plan and friendly-force reporting, the antiterrorism officer assists the commander in maintaining the situational understanding of the current and estimated terrorist threat. The antiterrorism officer focuses on each phase of the unit 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.

5-21. (U) The antiterrorism officer assists the commander in identifying resources that are necessary to protect the force. Preparation begins with unit training on antiterrorism, rehearsing access control procedures, exercising incident management plans, and ordering equipment necessary to enhance physical security measures. Soldiers selected for supercargo missions review on the rules for the use of force and the rules of engagement, as applicable, in the protection of unit equipment.

EXECUTION (U)

5-22. (U) *Execution* is putting a plan into action by applying combat power to accomplish the mission (ADP 5-0). It also involves using situational understanding to assess progress and to make execution and adjustment decisions. In executing unified land operations, commanders anticipate and balance priorities among offensive, defensive, and stability or defense support of civil authorities tasks. Operational variables and operational general characteristics dictate how the elements of unified land operations are combined to accomplish the mission. (See ADP 3-0 and ADRP 3-0.)

5-23. (U) Commanders and staffs implement antiterrorism measures (FPCON, random antiterrorism measures, physical security barriers and devices to protect the force during unified land operations). (See table 5-2.) 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. Antiterrorism officers assist the staff in reassessing the threat and vulnerabilities to the unit ability to maintain combat power. In response to an actual attack, the commander, with the assistance of the antiterrorism officer and subordinate units, manages the consequences, recovers and sustains operations, and conducts inform-and-influence activities to minimize the effect of terrorist information activities.

Table 5-2. (U) Expanded operations process with antiterrorism support tasks

AT Planning Tasks	***Plan***	***Prepare***	***Execute***
	AT Task 2. Collect, analyze, and disseminate threat information.	AT Task 3. Assess and reduce critical vulnerabilities. AT Task 5: Maintain defenses.	AT Task 7. Conduct terrorist threat/incident response planning.
	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.		
AT Measures (AUTL 6.6)	Identify potential terrorist threats and other threat activities (AUTL ART 6.6.1).	Reduce vulnerabilities to terrorist acts and attacks (AUTL ART 6.6.2).	React to a terrorist incident (AUTL ART 6.6.3).
Integrating Process	Risk management →		
Control Measures	***Command and Staff Actions***		
• Operational design • Commander's intent • Planning guidance • Commander's critical information requirements • Assignment of missions • Plans and orders • Information collection plan • Graphic control measures • Unit standing operating procedures • Information requirements • Status-of-forces agreements • Legal considerations and constraints	**MDMP/TLP** • Threat assessments • Mission variable analysis • Terrain analysis • Task organization/ personnel requirements • Resourcing	**Vulnerability and criticality assessment and risk analysis** • Probability versus severity • Movement • Predeployment site survey • CAL and DAL • Training/rehearsals	**Rapid decisionmaking and synchronization process** • Mitigate terrorist acts • Adjust commander's critical information requirements • Conduct physical security and entry control
	Continuous Assessment (Monitor and Evaluate Measure of Effectiveness/Performance)		
	Warfighting functions → Supporting processes → ▪ IPOE ▪ Targeting ▪ Information collection synchronization ▪ Knowledge management Continuing activities → ▪ Security operations ▪ Information tasks ▪ Liaison and coordination		

Table 5-2. (U) Expanded operations process with antiterrorism support tasks (continued)

Legend:	
ART	Army tactical task
AT	antiterrorism
AUTL	Army universal task list
CAL	critical asset list
DAL	defended asset list
IPOE	intelligence preparation of the operational environment
MDMP	military decisionmaking process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
TLP	troop-leading procedures

ASSESSMENT (U)

5-24. (U) *Assessment* is the determination of the progress toward accomplishing a task, creating a condition, or achieving an objective (JP 3-0). Assessment is a continuous activity of the operations process and an activity of mission command. Assessment plays a critical role in the antiterrorism program and is supported by other assessments (threat assessment, criticality assessment, vulnerability assessment, and risk assessment [see chapter 3]) to evaluate the unit security posture when dealing with a terrorist or irregular threat. Commanders, assisted by antiterrorism officers and staffs, 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 antiterrorism are—

- (U) Indicators of enemy CBRNE use.
- (U) Escalation-of-force incident reports or other indicators of enemy IED use.
- (U) Increased criminal activity in a given area of operations.
- (U) Reports of the enemy targeting critical host nation infrastructure.
- (U) Identification of a threat to the base or sustainment facilities.

5-25. (U) Commanders also assess the progress of 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, measure of performance, and reframing criteria. Assessments are continuous; prioritization, monitoring, and evaluation are required to ensure that required changes are implemented effectively without distracting the ability of the staff to support ongoing operations.

5-26. (U) Commanders can also assess their use of antiterrorism 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 antiterrorism posture, no matter how slight, to reduce vulnerabilities and aid Soldier vigilance.

5-27. (U) To enhance assessment within brigades, battalions, and companies, the ATWG assembles key staff to consolidate and discuss emerging trends, issues, and impacts related to events over various planning horizons. The group examines the assessment plan to ensure that the measures of effectiveness, measures of performance, and indicators are still valid; determine if updates to the threat assessment, criticality assessment, vulnerability assessment, or risk analysis are necessary; and develop new measures and indicators as required.

5-28. (U) Comprehensive antiterrorism 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 must conduct a self-assessment of their antiterrorism programs and the programs of subordinate units after assuming command in conjunction with predeployment vulnerability assessments; after occupying a new base; when completing a change of responsibility; or when there are significant changes in threat, vulnerabilities, or asset criticality.

5-29. (FOUO) 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 higher headquarters (Army command, ASCC, direct reporting unit, Army National Guard, garrison, tenant unit/activity, or stand-alone activity). The antiterrorism program review should focus on the essential antiterrorism elements and, as a minimum, assess the following functional areas:

- (FOUO) Physical security.
- (FOUO) Engineering.
- (FOUO) Plans, operations, training, and exercises.
- (FOUO) Resource management.
- (FOUO) Military intelligence.
- (FOUO) Criminal intelligence.
- (FOUO) Inform-and-influence activities.
- (FOUO) Law enforcement.
- (FOUO) Threat options.
- (FOUO) OPSEC.
- (FOUO) Medical.
- (FOUO) Protection of executives and HRP.

5-30. (U) 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 (U)

(U) This chapter examines the roles and responsibilities of the antiterrorism 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 unified land operations, antiterrorism plays a critical role in the protection of assets (people, infrastructure, information) within the commander's AOR. The antiterrorism officer serves as the lead in assisting the commander and in preparing the unit to defend against acts of terrorism while in transit or on deployment.

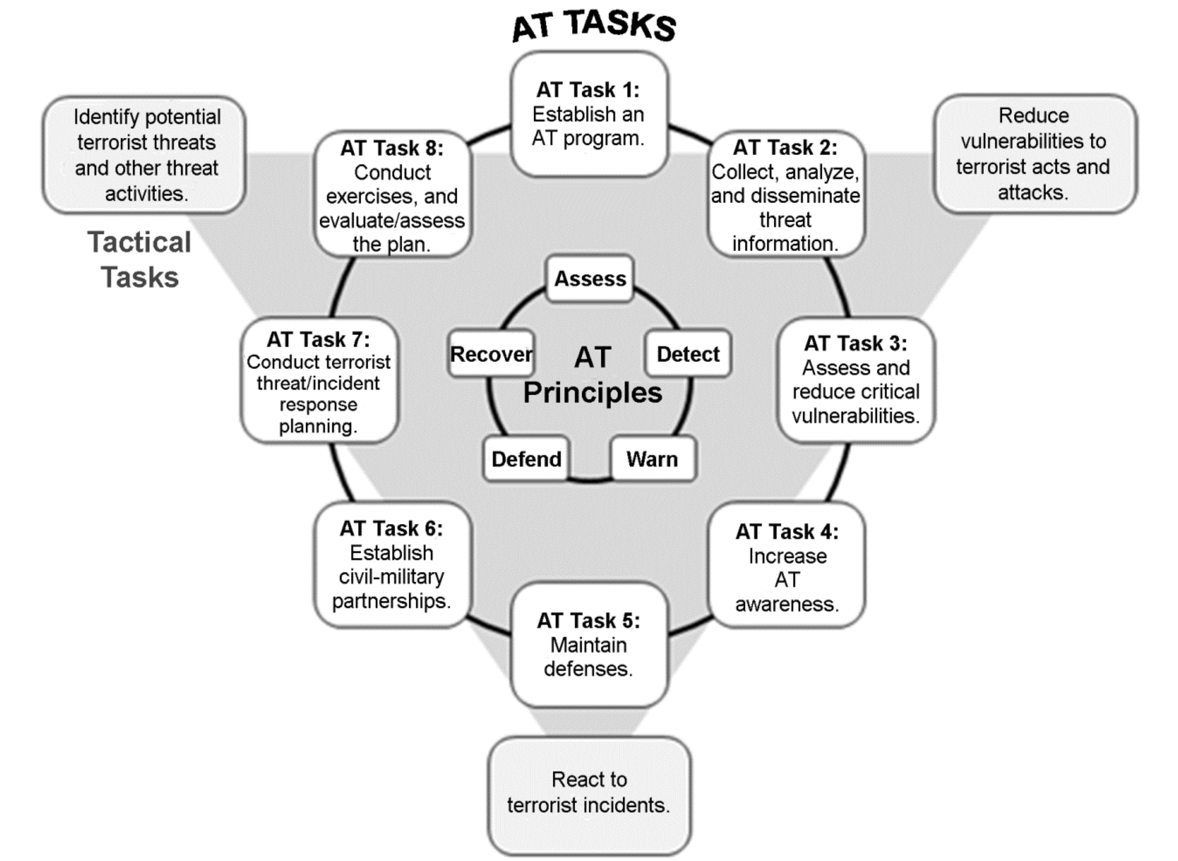
ROLES AND RESPONSIBILITIES (U)

6-1. (U) The antiterrorism officer serves as the commander's principal staff member concerning terrorist activities within the commander's AOR. The antiterrorism officer must be appointed, in writing, by the commander and must be antiterrorism Level II-certified. As a member of the S-2 or S-3 section, the antiterrorism officer serves as the focal point and subject matter expert for coordinating plans and procedures that govern antiterrorism, including physical, information, operation, personal, critical-asset, and infrastructure security. Within the commander's intent, the antiterrorism officer directs the development, implementation, and operation of an integrated antiterrorism program; helps fuse intelligence and criminal information; and guides crisis management planning and execution in the event of a terrorist attack. The antiterrorism officer also serves as a member of the installation design team in support of organizational decisions that affect 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. (U) As the lead for the ATWG, the antiterrorism 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 antiterrorism officer evaluates the effectiveness of the command antiterrorism program and prepares the foundation for enhancing the relationship among Army forces, host nation civil authorities, and units within the area of operations. In conjunction with the planning cell, the antiterrorism officer formulates and coordinates matters pertaining to the protection and security of personnel, property, and materiel against terrorist threats.

6-3. (U) As an effective staff officer, the antiterrorism officer provides the commander with accurate, timely, and relevant information and well-analyzed recommendations in regard to FPCON and random antiterrorism measures. This helps the commander minimize unnecessary risk. The antiterrorism officer assesses threats related to terrorist activity and recommends controls to reduce unnecessary risks through the proper posturing of subordinate units.

6-4. (U) The antiterrorism officer should be a graduate of an antiterrorism officer Level II training course that is certified by the U.S. Army Military Police School. The antiterrorism officer is responsible for providing the commander with information and recommendations within the parameters of the antiterrorism program. In most units or activities, being an antiterrorism officer is an additional duty for a person serving in the operations section but should be considered a full-time position at higher levels and during major operational deployments. The antiterrorism officer assists the commander in accomplishing the tasks associated with the protection warfighting function and antiterrorism, using the antiterrorism principles as a framework to guide their efforts. (See figure 6-1, page 6-2.)


AT TASKS
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.
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.
Identify potential terrorist threats and other threat activities.
Reduce vulnerabilities to terrorist acts and attacks.
React to terrorist incidents.
Tactical Tasks
AT Principles
Assess
Detect
Warn
Defend
Recover

Legend:

AT antiterrorism

Figure 6-1. (U) Antiterrorism tasks and principles

6-5. (U) The antiterrorism officer relies on the combined expertise of the entire headquarters staff to develop effective antiterrorism plans and to coordinate and integrate antiterrorism measures throughout command units and actions. Such expertise includes the command public affairs office (assists with community awareness); the command intelligence staff (supports understanding of the specific terrorist threat throughout the AOR and area of operations); and the command logistics, maintenance, and contracting staffs (ensures that antiterrorism measures are included in mission areas and support functions).

ECHELONS ABOVE CORPS (U)

6-6. (U) Army commands, ASCCs, and select direct reporting units contribute to the 10 USC 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 area of operations. Their authority includes the ability to assess, deter, detect, defend against, prevent, and mitigate terrorist activities.

6-7. (U) 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) that are assigned, attached, transiting through, or training in the ASCC area of operations (except personnel or units for 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.*** (U) 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. (U) ASCCs play a critical role in the fight against global terrorism. The theater of operations is the first level of command with a dedicated antiterrorism 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 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. (U) At theater command and ASCC levels, antiterrorism planning and actions focus on understanding and tracking the terrorist threat and terrorist activities—including regional and transnational groups—and coordinating with the host nation to leverage the full support of the host nation security forces. Theater and ASCC orders and directives for antiterrorism focus on information sharing, AOR-specific antiterrorism training and readiness requirements, and resources required to meet the urgent needs of operational forces.

6-10. (U) The antiterrorism officer within the protection division supports the ASCCs inherent antiterrorism responsibilities by integrating the Army universal task list, antiterrorism tasks, and antiterrorism principles into the command operations and intelligence processes to support forces operating within their area of operations. The antiterrorism officer does this by—

- (U) Ensuring that antiterrorism 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.
- (U) Providing antiterrorism 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 antiterrorism appendix within annex F of the operation order.
- (U) Incorporating antiterrorism into plans, orders, and publishing guidance to subordinate elements for the execution of antiterrorism measures, including FPCON and implementation of random antiterrorism measures.
- (U) 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 applicable rules of engagement or the rules for the use of force.
- (U) Ensuring that FPCON procedures are in place to notify organic, tenant, and supported units of FPCON changes and transition procedures.
- (U) Ensuring that policies and procedures are in place to identify and designate incumbents of high-risk billets and HRP positions. (See DODI O-2000.22.)
- (U) Providing supplemental training (as required) to personnel and their families assigned to high-risk billets or designated HRP.
- (U) Assessing and reviewing (periodically) the antiterrorism programs of assigned and attached DOD components in the AOR.

- (U) Tracking movements of 50 or more personnel into or through significant or high-threat areas and providing terrorist threat information, indications, and warnings.
- (U) Ensuring that Soldiers, Army civilians, and Army contractors authorized to accompany the force have received applicable antiterrorism training and briefings before arrival into the area of operations.
- (U) 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.
- (U) Assessing the terrorist threat and providing threat assessment information to DOD components and the commanders in the AOR.
- (U) Developing risk mitigation measures and maintaining a database of those measures and the issues that necessitated their implementation.
- (U) 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.
- (U) Ensuring that a capability exists to collect, receive, evaluate, analyze, and disseminate relevant data on terrorist activities, trends, and indicators of imminent attack.
- (U) Developing and implementing the capability to fuse biometric-enabled intelligence and suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national information collection activities.
- (U) Assembling antiterrorism program review assessment teams that are composed of individuals with sufficient functional expertise to satisfactorily assess and evaluate (using a measure of performance and effectiveness) the effectiveness and adequacy of antiterrorism program implementation within their subordinate commands.

CORPS AND DIVISIONS (U)

6-11. (U) Corps and divisions serve as modular entities designed to control forces that are tailored for specific joint operations. A corps serves as a command headquarters, a joint task force, or an intermediate tactical headquarters within a large group of land forces. A division is 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 mission command for the unified action necessary in irregular warfare and combating terrorism.

6-12. (U) Antiterrorism 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 antiterrorism by integrating the antiterrorism tasks and principles throughout their operations and by employing their organizational capabilities and assets.

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

- (U) Exercising operational or tactical control for force protection responsibilities by establishing antiterrorism guidance and programs for assigned Army or DOD elements and personnel, including the assessment and protection of facilities and the appropriate level of antiterrorism training and briefings.
- (U) Planning, coordinating, synchronizing, and integrating antiterrorism 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).
- (U) Coordinating with geographic combatant commanders to ensure adequate antiterrorism protection of in-transit and deployed forces operating in the combatant command AOR.

- (U) Receiving terrorist threat reporting assessed by the combatant command and ASCC.
- (U) Providing threat assessment information and designated FPCON to the DOD components, multinational forces, and commanders in the AOR.
- (U) Raising the local FPCON level above the FPCON level set by the higher-level commander for personnel and assets within their antiterrorism responsibility. (Antiterrorism officers cannot lower the local FPCON below the high-level FPCON without the commander's written concurrence.)
- (U) 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 applicable rules of engagement or the rules for the use of force.
- (U) Ensuring that FPCON procedures are in place to notify organic, tenant, and supported units of FPCON changes and transition procedures.
- (U) 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.
- (U) Identifying potential protection requirements for those corps or division commanders who are designated a high-risk billet or HRP during operations.
- (U) Informing the commander of changes or terrorist threats to critical asset lists and defended asset lists.
- (U) Monitoring OPSEC actions at all levels.
- (U) Reviewing terrorist threat and incident response plans, especially in regard to mitigating the effects of CBRNE.
- (U) Overseeing the construction of FOBs and overseeing physical and area security in relation to the terrorist and nonstate actor threat.

BRIGADES AND BATTALIONS (U)

6-14. (U) The brigade combat team is the basic building block of Army tactical formations, complemented by the addition of modular support brigades to create tailored, readily available expeditionary force packages that enhance Army flexibility and responsiveness. Battalions compose brigade combat teams 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 antiterrorism measures into operations.

6-15. (U) The antiterrorism officer works with higher and lower echelons to integrate the eight antiterrorism 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 antiterrorism focus to operations, the antiterrorism officer—

- (U) Focuses on antiterrorism measures throughout the area of operations and establishes the common operational picture for antiterrorism awareness and execution.
- (U) Submits movement operations to higher headquarters for review and seeks threat, FPCON, and infrastructure guidance.
- (U) Establishes local antiterrorism measures in support of security for FOBs, logistic bases, and staging areas in support of the current operations.
- (U) Raises the local FPCON level above the FPCON level set by the higher-level commander for personnel and assets within their antiterrorism responsibility. (Antiterrorism officers cannot lower the local FPCON below the higher-level commander's FPCON without the commander's written concurrence.)
- (U) Ensures that FPCON procedures are in place to notify organic, tenant, and supported units of FPCON changes and transition procedures.

- (U) Serves as a member of the division protection cell, the division protection working group, and the base ATWG.
- (U) Highlights the commander's antiterrorism concerns and responds to taskings in support of division or base antiterrorism or incident response plans.
- (U) 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 antiterrorism measures and in support of brigade or battalion antiterrorism requests.
- (U) Ensures that subordinate battalions have a functioning antiterrorism program within their units and disseminates analyzed and unit-tailored antiterrorism or threat-related information from higher headquarters.
- (U) 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.
- (U) Coordinates locally with host nation and government agencies (State Department and embassy or consulate personnel) when operating abroad.
- (U) Works with the brigade judge advocate or servicing judge advocate to ensure that the legal considerations in response to antiterrorism measures are met.
- (U) Helps develop incident management battle drills and themes with the public affairs officer, foreign counterintelligence officer sections, and attached MISO detachments.

COMPANIES (U)

6-16. (U) The company 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 logistic base separated from their headquarters.

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

6-18. (U) An enhanced, platoon-size element of 50 or more serves as the minimal planning factor for antiterrorism measure considerations, especially in transit to a deployed location, during training exercises, or when operating independently on a FOB or common operational picture. At the platoon and squad levels, antiterrorism awareness plays a crucial role in personnel survivability while operating in the area of operations. Because platoons and squads are not resourced with the same barrier or physical security measures as companies 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 (U)

6-19. (U) 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 the MDMP. These protection cells translate command guidance and the terrorist threat assessment 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 ADP 3-37 and ADRP 3-37.)

WORKING GROUPS (U)

6-20. (U) Working groups are a type of meeting. Working groups are included on the unit battle rhythm. A working group consists 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 antiterrorism. It synchronizes the contributions of all staff elements with the work of the protection cell.

PROTECTION WORKING GROUP (U)

6-21. (U) The protection working group is led by the protection coordinator. It normally consists of an air and missile defense officer, an antiterrorism 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. The commander may add staff officers from safety, the inform-and-influence activities section, and medical and civil affairs offices depending on the operational environment or the type of operation. At the division level, subordinate units normally provide a liaison officer for the working group meetings. The protection cells in division, corps, and Army headquarters integrate protection functions into the operations process. In the brigade combat team, division or corps orders specify protection requirements and tasks. Since no protection cell exists in the brigade combat team, commanders normally designate a lead staff element (S-3) to perform these functions. (See ADP 3-37 and ADRP 3-37.)

ANTITERRORISM WORKING GROUP (U)

6-22. (U) The purpose of the ATWG is to review threats, identify vulnerabilities, recommend countermeasures, recommend FPCONs and position of response forces, review tasks to components, monitor corrective actions, and direct special studies (force protection assessment teams). Commanders will establish an ATWG that meets semiannually or more frequently, depending on the level of threat activity, to oversee the implementation of the antiterrorism program, to develop and refine antiterrorism plans, and to address emergent or emergency antiterrorism program issues. (See AR 525-13 for additional information on the ATWG.)

THREAT WORKING GROUP (U)

6-23. (U) The threat working group meets at least quarterly but more frequently, as required, based on the level of terrorist threat activity. The threat working group is organized to develop and refine terrorism threat assessments 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 threat working groups 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 (U)

(U) This appendix complies with AR 25-30 which states that weights, distances, quantities, and measurements contained in Army publications will be expressed in both U.S. standard and metric units. Table A-1 is a metric conversion chart for the measurements used in this manual. For a complete listing of preferred metric units for general use, see Fed-Std-376B.

Table A-1. (U) Metric conversion chart

U.S. Units	***Multiplied By***	***Equals Metric Units***
Feet	0.3048	Meters
Metric Units	***Multiplied By***	***Equals U.S. Units***
Meters	3.2808	Feet
Legend: U.S. United States		

This page intentionally left blank.

Appendix B

Personal Protection Measures (U)

(U) Soldiers, contractors, and civilians play important roles in the success of the antiterrorism 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 antiterrorism 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 (U)

B-1. (U) 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. (U) 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 CJCS Guide 5260.)

B-3. (FOUO) 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. (FOUO) While training, preparing for deployment, or serving overseas, personnel should vary their routes and departure and return times. The surveillance of 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. (U) 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 (military base, 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 taken discreetly with cellular telephone cameras. Associates and unit members should be advised of destinations and anticipated arrival times.

ACTIVE-SHOOTER RESPONSE (U)

B-6. (U) Soldiers are more equipped to handle active-shooter and 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.

B-7. (U) 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-8. (U) Antiterrorism 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 an 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 following key information:

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

B-9. (U) Effective practices for coping with an active-shooter or terrorist situation include—

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

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

B-10. (U) Personnel must quickly determine the most reasonable way to protect their own lives. When dealing with active-shooter or terrorist events—

- (U) If evacuation is possible, personnel should—
  - (U) Establish an escape route.
  - (U) Evacuate the premises.
  - (U) Leave belongings behind.
  - (U) Help others escape.
  - (U) Prevent individuals from entering areas where the active shooter may be present.
  - (U) Keep hands visible when in contact with police personnel.
  - (U) Follow police officer instructions.
  - (U) Not move wounded individuals.
  - (U) Notify law enforcement personnel when safety is reached.
- (U) If evacuation is not possible, personnel should shelter in place by securing a hiding place that—
  - (U) Is out of the active shooter's view.
  - (U) Provides protection from gunfire.
  - (U) Does not restrict movement.
  - (U) Can be locked or blockaded against entry.

- (U) If the active shooter is nearby, personnel should—
    - (U) Lock the doors.
    - (U) Silence cellular telephones and pagers.
    - (U) Turn off radios and televisions.
    - (U) Hide behind large items (cabinets, desks).
    - (U) Remain quiet.
- (U) If evacuation and hiding are not possible right away, personnel should—
    - (U) Remain calm.
    - (U) Dial 911 even if speaking is impossible; leave the line open and allow the dispatcher to listen.
    - (U) Adapt responses to the types of weapons used by the attacker.
    - (U) Take action against the active shooter only as a last resort and when life is in imminent danger.
    - (U) Act aggressively against the shooter.
    - (U) Throw items and improvised weapons.
    - (U) Yell.
    - (U) Commit to actions.
    - (U) Cooperate with first responders.
    - (U) Remain calm and follow instructions.
    - (U) Put down items in your hands.
    - (U) Raise your hands and spread your fingers.
    - (U) Avoid quick movements.
    - (U) Not cling to emergency personnel.
    - (U) Not point, scream, or yell.
    - (U) Evacuate in the direction in which the first responders are entering.
    - (U) Provide key information (see paragraph B-7).

CULTURAL AWARENESS (U)

B-11. (U) Cultural awareness is essential to the basic mission of every individual and unit that operates outside the continental United States. Being familiar with host nation 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 outside the continental United States and protects Soldiers and units that conduct military engagements, visits, and reconnaissance.

B-12. (U) 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-13. (U) Situational awareness is to know what is happening in the surrounding area, and situational understanding is to understand why things are happening in the surrounding area. 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 training, planning, and conducting operations. Commanders and staffs deployed to Iraq, Afghanistan, and throughout Africa learned that cultural predeployment training and incorporation of cultural aspects into planning and conducting operations is beneficial. Commanders and staffs prepare Soldiers for operations in different environments through threat assessments, intelligence, crime data, and historical research.

B-14. (U) 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 protects personnel from potential terrorist and criminal attacks.

B-15. (U) Culture is a shared set of traditions, belief systems, and behaviors. It is shaped by history, religion, ethnic identity, language, and nationality. Culture 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 operational planning and resource allocation.

B-16. (U) 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-17. (U) Humans develop a world view through their own socioeconomic and cultural development. It influences their attitudes, beliefs, and character and, thus, affects their behavior. American Soldiers and Army civilians view the culture of other peoples and nations from the perspective of America's Army—its values, customs, traditions, laws, technology, equipment, doctrine, tactics, and command authorities. Training, education, and socialization must mitigate the tendency of Americans to view other cultures in a negative light (ethnocentrism), while developing cultural awareness, understanding, and tolerance in Soldiers and Army civilians,. Respect for the individual, human rights, and humanitarian concerns are the basis for the Law of Armed Conflict. Soldiers, even in the most trying of circumstances, are bound to treat others with dignity and respect. Developing such an understanding is part of developing character. Members of the Army profession must actively seek opportunities to better understand other cultures, see other perspectives, and appreciate what others find important.

B-18. (U) Commanders and staffs must consider cultural awareness when conducting training for Soldiers, to include—

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

HOSTAGE PREVENTION (U)

B-19. (U) 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, DODD 1300.7, DODI 1300.21, and DODI 1300.23.)

B-20. (U) 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 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-21. (U) The U.S. government makes every good-faith effort to obtain the earliest release of 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 use a detention or hostage situation to maximize their advantage.

B-22. (U) Army personnel must take every reasonable step to prevent exploitation of themselves and 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 code of conduct, and the highest traditions of military service.

B-23. (U) Army personnel should maintain 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-24. (U) There are no circumstances in which a detainee or hostage should voluntarily give classified information or materials to those unauthorized to receive them. 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-25. (U) The Geneva Conventions of 1949 are the internationally recognized standard of treatment for all captives (civilians, contractors, correspondents, and others who have authority to accompany and support multinational forces) during international armed conflict. The basic legal protections available to prisoners of war under Geneva Convention III, *Relative to the Treatment of Prisoners of War (GPW),* does not apply during operations outside of an international armed conflict. In conflicts not of an international character, captured combatants receive only the minimum legal protection specified in Common Article 3 to Geneva Convention I.

B-26. (U) DODI 1300.23 provides for the isolated personnel training of DOD civilians and contractors who are 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-27. (U) U.S. military personnel detained by a hostile force or a terrorist during personal travel or a military operation may be subject to the domestic criminal laws of the detaining nation. Lost, isolated, or captive Military personnel 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. Army personnel must be aware of the following:

- (U) 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.
- (U) Hostage takers have historically attempted to engage military captives in conversations concerning seemingly innocent, useless topics and provocative issues. Discussions should be limited to, and revolve around, health and welfare concerns, conditions of fellow detainees, and release efforts.
- (U) 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 (FOUO)

B-28. (FOUO) 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; 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-29. (FOUO) 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.

- (FOUO) 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.
- (FOUO) Introduce commonalties (family, clothes, sports, hygiene, food).
- (FOUO) Listen to captors discuss their cause or boast.
- (FOUO) Address captors by name.
- (FOUO) Refrain from whining or begging.
- (FOUO) Introduce benign topics at critical times (impasses, demands) to reduce tension.
- (FOUO) Avoid emotionally charged topics (religion, economics, politics).
- (FOUO) Avoid being singled out as a result of being argumentative or combative.
- (FOUO) Circumvent escalating tension by avoiding stress-inducing language (gun, kill, punish).

B-30. (FOUO) 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—

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

B-31. (FOUO) In a rescue situation, hostages should—

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

B-32. (FOUO) Escape from terrorists is risky, but escape 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 (U)

B-33. (U) 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—

- (U) Following local protection guidance to avoid hazardous situations.
- (U) Developing a plan to communicate, flee, and fight.
- (U) Developing a plan of action (including several backup plans) before departing a secure area.
- (U) Being familiar with routes and maps.
- (U) Ensuring that vehicles are reliable and have the necessary emergency equipment.
- (U) Studying local customs and being alert to situations and changes in local behavior.
- (U) Having a grab-and-go kit that includes a communications device (cellular telephone, radio), water, and basic first aid supplies.

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

- (U) Having personal affairs in order.
- (U) Preparing for potential isolation.
- (U) Developing the will to survive and resist.
- (U) Working with local military officials to—
  - (U) 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.)
  - (U) 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 (U)

B-34. (U) *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). It 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 areas of operations and with other components.

B-35. Personnel recovery officers perform personnel recovery coordination functions at brigade level and below. Their responsibilities include:

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

Appendix C

Antiterrorism Exercises (U)

(U) Preparing for antiterrorism 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 antiterrorism. 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 antiterrorism measures. Antiterrorism measures—

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

PURPOSE (U)

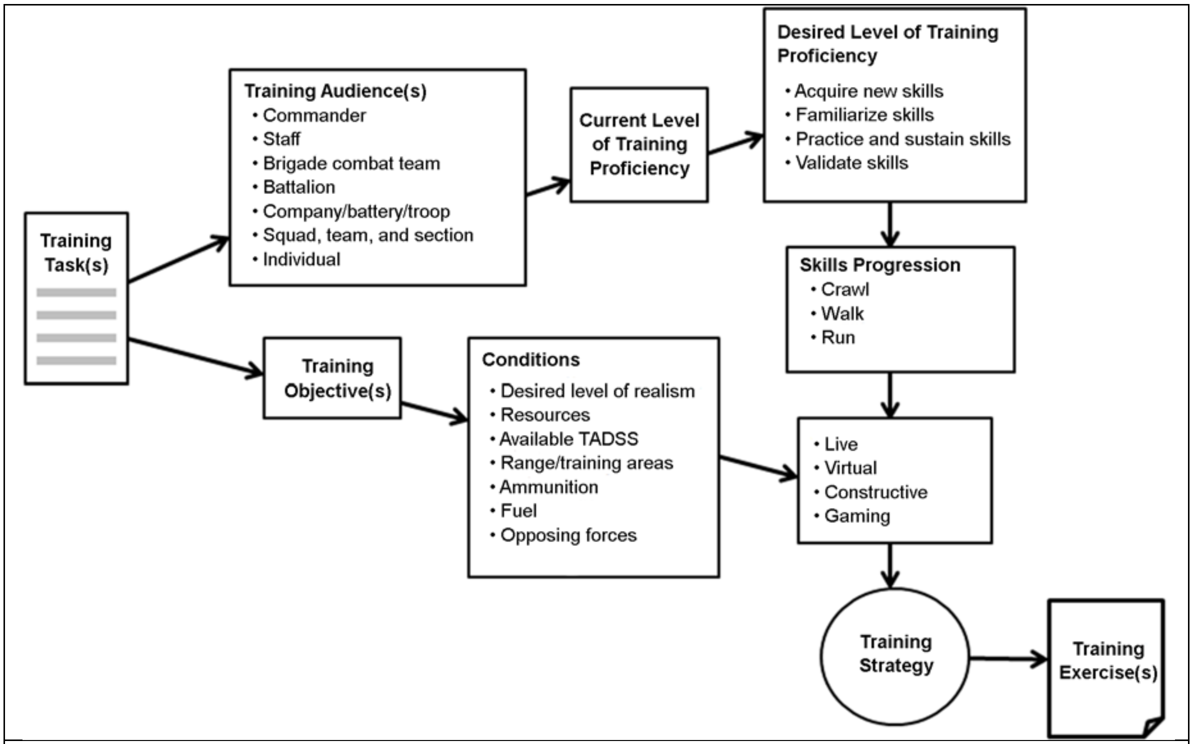
C-1. (U) Limited training time requires leaders to select the most important tasks to sustain or improve (tasks that are essential to mission accomplishment and perishable without frequent practice). Because antiterrorism awareness and tasks support and protect units throughout unified land operations,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

C-2. (U) Commanders institute an exercise program that develops, refines, and tests antiterrorism response procedures to terrorist threats and incidents. This program ensures that antiterrorism 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 random antiterrorism measures schedule, direct and coordinate response forces, and conduct incident management functions.

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

C-4. (U) Commanders consider several key questions when selecting training exercises. As shown in figure C-1, commanders refer to their training assessment before starting the exercise selection process to answer the following questions:

- (U) What are the specific antiterrorism training tasks?
- (U) What is the training audience for each specific antiterrorism training task?
- (U) What is the overall training objective?



Legend:

TADSS	training aids, devices, simulators, and simulations

Figure C-1. (U) Training exercise selection process assessment

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

- (U) What is the current proficiency level of the training audience?
- (U) What is the required level of training proficiency for this training audience on this particular task?
  - (U) Acquire new skills?
  - (U) Familiarize skills?
  - (U) Practice and sustain skills?
  - (U) Validate skills?

C-6. (U) 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. The crawl-walk-run technique is an objective, incremental, standards-based approach to training:

- (U) **Crawl.** 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.** 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.
- **Run.** The level of difficulty for training intensifies. Run stage training requires the resources that are needed to create the conditions expected in the projected operational environment. Progression from crawl to run for a particular task may occur during a 1-day training exercise or may require a succession of training periods.

C-8. (U) 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 help provide the variable conditions for supporting a crawl-walk-run training strategy. Some ways to change conditions are—

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

C-9. (U) 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.

TYPES (U)

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

- (U) Commander’s intent.
- (U) Mission orders.
- (U) Subordinates’ initiative.
- (U) Resource allocation.

C-11. (U) 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 a unity of purpose, where each succeeding echelon concept is nested in the other. Commanders who use nested concepts in training exercises provide an opportunity for subordinates to—

- (U) Practice decentralized decisionmaking and execution.
- (U) Exercise initiative within the commander’s intent.

C-12. (U) The nested concept method gives commanders—

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

C-13. (U) 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—

- (U) Underscore each subordinate's responsibility for the assigned mission in the context of the commander's mission, intent, and concept of operation.
- (U) 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. (U) Antiterrorism 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.) The types of exercises include the following:

- (U) **Tactical exercise without troops.** A tactical exercise without troops is an exercise conducted in the field on actual terrain that is suitable for training units for specific missions. It is used to train subordinate leaders and staffs in terrain analysis, unit and weapons emplacement, and in the planning and execution of the unit mission. This exercise would include the brigade combat team commander and staff, subordinate battalion commanders and staffs, and separate brigade combat team company commanders and senior noncommissioned officers.
- (U) **Communication exercise.** A communication exercise is done to ensure that all units can communicate with one another across various types of communication equipment. It identifies shortfalls in communication equipment, especially when working with host nation, multinational, and other partners who are not frequently assigned or attached to the higher headquarters. This exercise includes brigade combat team and battalion tactical command posts; main and rear command posts; brigade combat team separate company command posts; and host nation, multinational, and attached units.
- (U) **Command post exercises.** A command post exercise has simulated forces; it may be conducted from garrison locations or in between participating headquarters. This exercise includes brigade combat team and battalion tactical command posts, main and rear command posts, and brigade combat team separate company command posts. 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.
- (U) **Command field exercise.** A command field exercise is conducted with reduced troop and vehicle density, but with full mission command and support units. The brigade combat team executes antiterrorism measures developed during tactical exercises without troops and rehearsed during command post exercises. Participation includes the following:
  - (U) Battalion leaders, down to and including platoon sergeants.
  - (U) Battalion personnel.
  - (U) Criminal Investigation Division personnel (hostage negotiations, investigations).
  - (U) First responders (medical and fire).
  - (U) Quick-reaction forces.
  - (U) Military intelligence and signal companies.
- (U) **Tabletop exercise.** A tabletop exercise is known as a rock drill or sand table exercise. This exercise involves 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 antiterrorism appendix or the entire operation order. This exercise, depending on the scenario, can last for an hour or a full day. A tabletop exercise should be used when an antiterrorism appendix is new, as refresher training, or to familiarize new leaders with the antiterrorism appendix.

- (U) **Drill.** A drill is collective training event that focuses on selected functions, procedures, or portions of an antiterrorism appendix. For example, portions of an antiterrorism appendix that can be exercised to achieve limited objectives are command post exercises, notification drills, first-responder drills, and evacuation drills. A drill is a scenario-driven event and is usually limited to specific organizations or functions to test, assess, and validate specific portions of a plan. A drill can last from 1 to 8 hours or longer, if necessary.
- (U) **Full-scale exercise.** A full-scale exercise is the most complex antiterrorism 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 all or part of their antiterrorism measures. The exercise should be designed to test the elevation and reduction of FPCON measures and the planning and incorporation of random antiterrorism measures, 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 antiterrorism appendix and timelines, assess functional capabilities and skills, identify gaps in security, and test equipment. It can last several days.

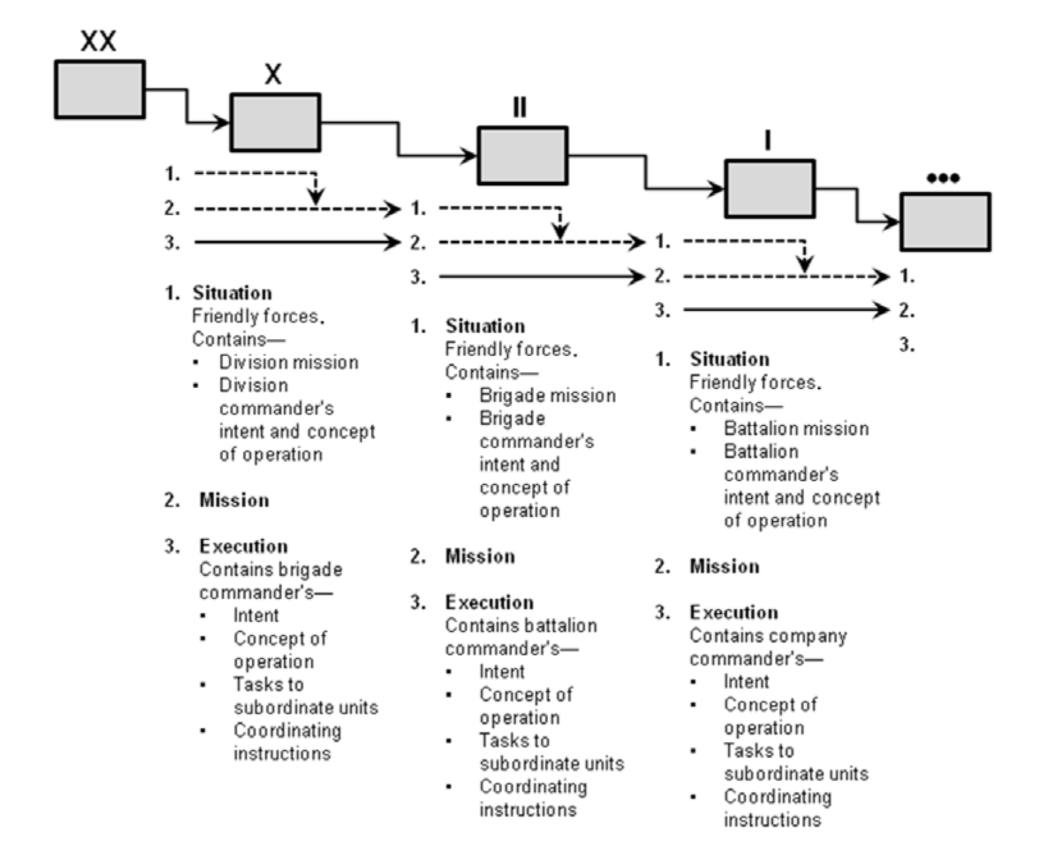
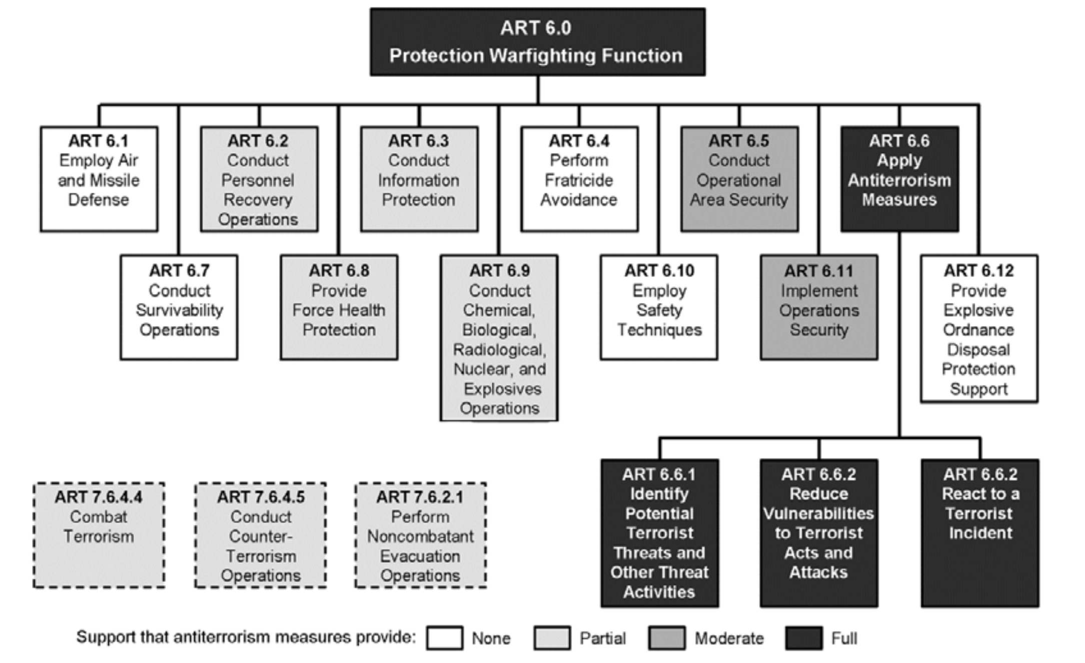

XX
X
II
I
•••
1.
2.
3.
1. Situation
Friendly forces.
Contains—
• Division mission
• Division commander's intent and concept of operation
2. Mission
3. Execution
Contains brigade commander's—
• Intent
• Concept of operation
• Tasks to subordinate units
• Coordinating instructions
1.
2.
3.
1. Situation
Friendly forces.
Contains—
• Brigade mission
• Brigade commander's intent and concept of operation
2. Mission
3. Execution
Contains battalion commander's—
• Intent
• Concept of operation
• Tasks to subordinate units
• Coordinating instructions
1.
2.
3.
1. Situation
Friendly forces.
Contains—
• Battalion mission
• Battalion commander's intent and concept of operation
2. Mission
3. Execution
Contains company commander's—
• Intent
• Concept of operation
• Tasks to subordinate units
• Coordinating instructions
1.
2.
3.

Figure C-2. (U) Nested concepts within mission command

MISSION-ESSENTIAL TASKS (U)

C-15. (U) The Army universal task list assists commanders in mission-essential task list development by providing 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 antiterrorism tasks from the mission-essential task list 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 when the current mission training plan is incomplete. (See figure C-3.)


ART 6.0 Protection Warfighting Function
ART 6.1 Employ Air and Missile Defense
ART 6.2 Conduct Personnel Recovery Operations
ART 6.3 Conduct Information Protection
ART 6.4 Perform Fratricide Avoidance
ART 6.5 Conduct Operational Area Security
ART 6.6 Apply Antiterrorism Measures
ART 6.7 Conduct Survivability Operations
ART 6.8 Provide Force Health Protection
ART 6.9 Conduct Chemical, Biological, Radiological, Nuclear, and Explosives Operations
ART 6.10 Employ Safety Techniques
ART 6.11 Implement Operations Security
ART 6.12 Provide Explosive Ordnance Disposal Protection Support
ART 7.6.4.4 Combat Terrorism
ART 7.6.4.5 Conduct Counter-Terrorism Operations
ART 7.6.2.1 Perform Noncombatant Evacuation Operations
ART 6.6.1 Identify Potential Terrorist Threats and Other Threat Activities
ART 6.6.2 Reduce Vulnerabilities to Terrorist Acts and Attacks
ART 6.6.2 React to a Terrorist Incident
Support that antiterrorism measures provide:
□ None
▨ Partial
▨ Moderate
■ Full

Legend:	
ART	Army tactical task

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

C-16. (U) Antiterrorism 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. Antiterrorism is a consideration for forces during military operations. To perform this function and mitigate risk and damage from terrorist attacks, the antiterrorism officer and commander implement antiterrorism 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 throughout the range of military operations.

C-17. (U) Doctrine and other sources can provide additional information relating to a mission. These sources include the following:

- (U) AR 350-1.
- (U) CJCSM 3500.04F.
- (U) FM 7-15.
- (U) Combined arms training strategies and proponent-developed collective tasks and drills.
- (U) Proponent-developed tasks approved by Headquarters, DA.

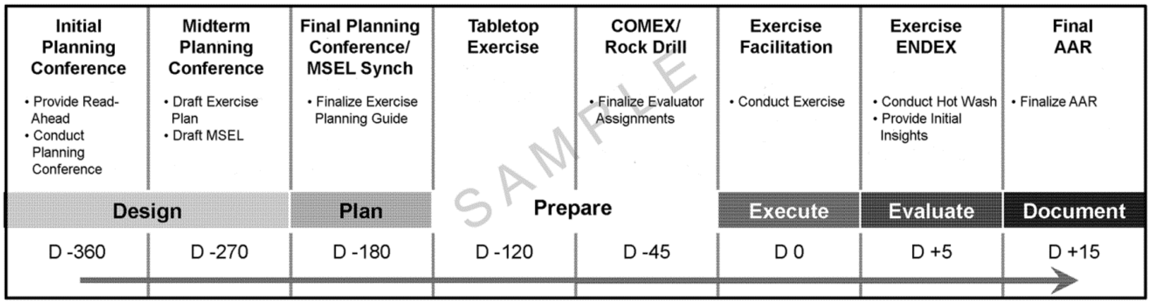
PREPARATION (U)

C-18. (U) A successful antiterrorism exercise, like any other exercise or training event, requires thorough planning. Commanders and staffs should use Service-specific doctrine to plan an antiterrorism 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 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 antiterrorism exercise include—

- (U) Antiterrorism exercises are threat scenario-driven, guided by exercise controllers, with commander involvement and support.
- (U) Drills may or may not have a threat scenario, depending on which function or portions of an antiterrorism appendix is being exercised. Commanders must examine which key functions or portions of an antiterrorism appendix are 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.
- (U) Observers/controllers are key players during exercises and should be identified and trained before the event. Observers/controllers 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, observers/controllers will be in an excellent position to capture lessons learned and facilitate the AAR process.

ANTITERRORISM EXERCISE DESIGN (U)

C-19. (U) To have a successful antiterrorism 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 are not participants in the actual exercise to maintain the level of surprise necessary for realistic training.



Initial Planning Conference	Midterm Planning Conference	Final Planning Conference/ MSEL Synch	Tabletop Exercise	COMEX/ Rock Drill	Exercise Facilitation	Exercise ENDEX	Final AAR
• Provide Read-Ahead • Conduct Planning Conference	• Draft Exercise Plan • Draft MSEL	• Finalize Exercise Planning Guide		• Finalize Evaluator Assignments	• Conduct Exercise	• Conduct Hot Wash • Provide Initial Insights	• Finalize AAR
Design		Plan	Prepare		Execute	Evaluate	Document
D -360	D -270	D -180	D -120	D -45	D 0	D +5	D +15

Legend:

AAR	after action review
COMEX	communication exercise
D	day
ENDEX	end of exercise
MSEL	master scenario event list
synch	synchronize

Figure C-4. (U) Sample timeline for exercise development

SCENARIO DEVELOPMENT (U)

C-20. (U) The operations officer, antiterrorism officer, and S-2 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 threat assessment. Host nation assistance can make significant contributions to scenario and threat development. Ensuring that valuable antiterrorism injections are developed is probably the most important task for action officers during the planning phase. This allows the training audience to experience a fluid operation that requires key antiterrorism staffing and decisions by leaders. The current threat assessment 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 include the following:

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

DANGER (U)

(U) 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. (U) 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 is produced in advance so that units can digest, plan, train, and ensure that the exercise is worthwhile.

C-22. (U) Once the scenario and directive have been developed, planners should create an exercise manual. It should contain the schedule, scope, objectives, injection 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. Injections 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 that are available only to key leaders, planners, and white hat observers/controllers.

THREAT RESOURCE (U)

C-23. (U) The Army Training and Doctrine Command G-2 Intelligence Support Activity produces a variety of products and series of terrorism handbooks for operational and installation/institutional Army mission support. (See *A Military Guide to Terrorism in the Twenty-First Century*.) The threat material is intended to help commanders—

- (U) Understand the operational environment, threat, and emerging techniques.
- (U) Understand the operational threat across the Army community (leaders, Soldiers, DA civilians, families, and contractors).
- (U) Use the products to support training and awareness for the operational Army forces and support activities.
- (U) Integrate realistic, current, and active threats into role-playing, training readiness, and institutional missions.

CONDUCT (U)

C-24. (U) Exercises will have many players. The exercise coordinator, other observers/controllers, player units, and role-players or red teams are key players. The exercise coordinator has the overall responsibility for running the exercise and monitors the pace of events according to the scenario. The observers/controllers 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 observers/controllers should also assist in tracking AARs.

> ***Note.*** (U) The Army Training and Doctrine Command G-2 Intelligence Support Activity provides a standardized orientation and lessons for actors and role-player training. The target audience is instructors and trainers of U.S. military forces and opposing forces and other applicable trainers for interagency, intergovernmental, civilian contractor, nongovernmental, private volunteer, and humanitarian-relief activities in training exercise design. The handbook (*A Military Guide to Terrorism in the Twenty-First Century*) 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. (U) 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 injections 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. (U) Once the briefings are accomplished, it is time to start the exercise. The injections 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 antiterrorism event would be extremely engaging, and the exercise should attempt to simulate those conditions. The antiterrorism exercise ends when all injections have occurred, player units have accomplished responses, and training objectives have been met.

EVALUATION (U)

C-27. (U) 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 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 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. (U) During their AAR, observers/controllers accurately record what they learn about events (by time sequence) to avoid losing valuable information and feedback. Observers/controllers use any recording system that is reliable (notebooks, laptops) and ensure that events are sufficiently detailed (identifying times, places, and names) and consistent. Observers/controllers and players should continually note and track AAR comments for later consideration. After the exercise, each echelon should conduct its own hot wash to capture lessons learned and AAR comments. If the exercise lasts more than 1 day, it is usually a good idea to have a hot wash at the end of each day.

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

C-30. (U) An AAR is the dynamic link between task performance and execution to standard. What actually occurred is placed against effective tactics, techniques, and procedures; doctrine; and unit standing operating procedures to correct deficiencies, sustain strengths, improve on weaknesses, and focus on the performance of specific mission-essential task list 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 performance of tasks (using measure of performance).

C-31. (U) The discussion of events helps Soldiers and leaders identify specific ways to improve unit proficiency. Units achieve the benefits of AARs by applying their results. Applications may include organizing observations, insights, and lessons; revising how the unit executes tactics, techniques, and procedures; and developing future training. AARs may reveal problems with unit standing operating procedures. 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 provide to assess performance, correct deficiencies, and sustain demonstrated task proficiency. These improvements will enhance unit performance in future operations. (See ADP 7-0, ADRP 7-0, and FM 6-01.1 for additional information on the AAR process.)

C-32. (U) Effective AARs require planning and preparation. During the 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 includes planning, preparation, execution, and follow-up (using AAR results).

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

- (U) **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.
- (U) **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 is 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 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 before the exercise and the tasks and goals that the unit had coming into 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 unit 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 antiterrorism appendix, and resource acquisitions. An antiterrorism exercise program for a unit conducting annual training, preparing for deployment, or participating in current operations can yield great benefits. Antiterrorism exercises improve the antiterrorism appendix, antiterrorism standing operating procedures, random antiterrorism measures execution, resource acquisition, and program review and increase awareness. Conducting an exercise is the best way to enhance base or organization antiterrorism programs and measures.

Appendix D

Antiterrorism Measures in Operational Contract Support (U)

(U) The incorporation of antiterrorism considerations into commercial relationships with U.S. and Foreign Service providers is essential to enhance the antiterrorism posture of operational forces in deployed environments. Contractors provide vital support and are part of the contingent for antiterrorism planning. Therefore, during the process to define contracted support requirements and during the contracting award, execution, and evaluation process, antiterrorism measures and actions should be considered, particularly when the contracted support could affect the security of DOD personnel.

REQUIREMENTS DEVELOPMENT PROCESS (U)

D-1. (U) Contracting for goods and services is a normal, ever-expanding function within DOD. Contracted support presents antiterrorism security challenges that, if not addressed, could create seams and gaps in the unit overall security profile. The federal acquisition regulations and associated supplements provide the legal guidance used to establish federal government contracts. They provide explicit directions for contract requirements, award, execution, and evaluation. AR 715-9, ATTP 4-10, and JP 4-10 contain current policy and detailed how-to guidance regarding operational contract support. U.S. forces are normally responsible for providing security and protection for contractor personnel when deployed. Unless specifically authorized by the terms of their contract, contractor employees are unarmed. At locations outside the continental United States, a status-of-forces agreement, memorandum of agreement, or other document prescribes guidance for the contracting process with regard to host nation service providers. It is the responsibility of the requiring activity (the command requesting commercially provided support) to incorporate antiterrorism security considerations into contract support requirement packages and local protection and base access plans. Unit antiterrorism officers should work closely with the higher-level unit antiterrorism officer, operational area security officer, and BDOC to ensure that antiterrorism-related security considerations are properly and legally incorporated into the operational area 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) antiterrorism clause in each applicable contract. Each ASCC should enforce antiterrorism security guidance specific to the combatant command AOR or joint operations area for the contract request process, based on individual threat concerns and agreements with host nations.

D-2. (U) The decision to use contractors in an area of operations requires an assessment of the vulnerabilities and risks posed to the contractor and its employees and the potential impacts on the operation. Commanders must also consider the difficulties facing contractors when hostile action against them is likely. If failure to provide the required support could jeopardize the overall success of the operation, contractor support may not be suitable.

D-3. (U) 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-4. (U) The requiring activity commanders are responsible for ensuring that antiterrorism security measures are considered in the requirements development process. Each commander should develop area-specific antiterrorism security guidance and incorporate it into the antiterrorism appendix. The commander’s guidance forms the core antiterrorism security criteria that are 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 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-5. (U) Requiring-activities need to closely consider special antiterrorism security considerations related to contract support during the development of the requirements package. This risk assessment process related to contract support will normally lead to one of the following results:

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

D-6. (U) 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 ATTP 4-10.

D-7. (U) It is recommended that commanders develop an informal antiterrorism contract coordination and review team similar to the ATWG to manage contract development. The step-by-step process for incorporating antiterrorism security into contracts is discussed below and outlined in table D-1.

Table D-1. (U) Antiterrorism security measures in the contract support process

Step	*Major Task*	*OPR*
Step 1. Determine contract requirements.	• Determine the contracting officer representative. • 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
Step 2. Perform AT risk analysis.	• Conduct an AT risk analysis. • Leverage local risk analysis information. • Determine the 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. Determine AT security measures.	• Develop specific AT security measures. • Leverage and 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
Step 4. Build the contract.	• Nominate a COR to the contracting office. • 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 appropriate contractor employee security and base access procedures. • Ensure that contracts are only awarded to vetted companies, as applicable, per local command policy.	Supporting contracting officer

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

Step	*Major Task*	*OPR*
Step 5. Award and execute the contract.	• Award the contract (contracting officer). • Incorporate contract security requirements into the unit AT plan (AT officer). • Notify the AT officer that the contract is awarded (COR). • Ensure that AT security measures are in place before execution (AT officer and COR). • Ensure that the contractor complies with AT measures in the contract (COR and contracting officer).	Supporting contracting officer, unit COR, and AT officer
Step 6. Review the contract.	• Periodically inspect AT security measures (AT officer and COR). • Review AT security measures if the local threat changes (AT officer). • Conduct an annual, formal review upon contract renewal (all).	Supporting contracting officer and unit COR

Legend:

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

STEP 1. DETERMINE CONTRACT REQUIREMENTS (U)

D-8. (U) The commander or 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 the scope of work are properly constructed in coordination with DOD, Service command, federal acquisition regulations, and local contracting authority guidance. At this step, the unit should determine how essential this contract service is to mission accomplishment. The following questions are asked:

- (U) Are there alternative means to providing the goods or service without assuming the increased risk of contracted support?
- (U) Which units will be affected by the scope of the contract, when will it be executed (timeframe), and where it will be executed?
- (U) Are there special areas or building access requirements where contractor employees require a common access card or an escort for access?
- (U) Are there any specific contract employee restrictions (security clearance requirements, restrictions on the use of non-U.S. citizen employees)?
- (U) Are current base access and security badging requirements sufficient to address the antiterrorism risks of this particular contract support request?
- (U) Is the requiring activity or designated supported unit prepared to provide contract oversight assistance in the form of contracting officer representatives and antiterrorism officer technical oversight?
- (U) Does the contract amount require the use of the antiterrorism/OPSEC coversheet for contracting?

D-9. (U) The concern during this step is to determine the relevant antiterrorism security considerations and the specific services being requested.

STEP 2. PERFORM ANTITERRORISM RISK ANALYSIS (U)

D-10. (U) The unit antiterrorism officer conducts an antiterrorism risk analysis of the proposed contract by using locally prepared antiterrorism assessments (threat, criticality, vulnerability, and risk). The use of these products helps the unit to assess and identify the potential antiterrorism vulnerabilities and risks associated with the contract and to incorporate specific antiterrorism security countermeasures into the contract. Part of this process is to consider alternative means of fulfilling the contract requirement as a way to mitigate or eliminate risks. The antiterrorism officer assists in the antiterrorism risk analysis process, ensuring that local security measures are leveraged or modified against risks and vulnerabilities associated with the contract.

STEP 3. DETERMINE ANTITERRORISM SECURITY MEASURES (U)

D-11. (U) During this step, the antiterrorism officer assists the unit in developing contractor support-related antiterrorism security measures. Antiterrorism security measures should be based on the outcome of the risk management process and reflect the commander’s overall antiterrorism risk management strategy. There should be a balance between effective security measures and costs and benefits. The unit and the antiterrorism officer should apply the commander’s antiterrorism security considerations during this step. In coordination with the appropriate protection and security staff, the antiterrorism officer should design antiterrorism 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 antiterrorism and security procedures to allow for random schedules, access and 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 areas 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, command protection section, or security section and the BDOC. The requiring activity must understand that these types of flexible antiterrorism measures may lead to increased costs, which may have to be justified to the approving official or may lead to degraded contractor performance at no fault of the contractors.

D-12. (U) Before submitting a requirements package for review and approval, commanders and their contract development team should—

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

Note. (U) 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 THE CONTRACT (U)

D-13. (U) This step involves combining the overall contract service requirements with antiterrorism security measures into an acquisition-ready requirements package, leading to the development of an actual contract. At a minimum, the requirements package should be staffed through the ATWG, legal officer, OPSEC officer, and commander. All Army requirements packages include a commander's formal antiterrorism review endorsement, which certifies that the antiterrorism security measures are satisfactory and that the commander has accepted the antiterrorism risk associated with the 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 antiterrorism 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. (U) Antiterrorism security measures for service contracts

AT Security Area	*AT Security Measures*
Contractor screening	• Vet companies through the joint forces command intelligence staff section of the mission (only applies to foreign contingencies). • Limit announcements for contractors to trusted sources based on mission sensitivity. • Conduct background checks (law enforcement, HN). • Screen company and prospective workers. • Define the process for replacing workers. • Establish a central contractor biometrics database that is accessible only to U.S. and non-HN security forces and contains contractor identification with pictures (normally only applicable in foreign contingencies). • Limit the work area. Clearly identify restricted or excluded areas where contractor personnel are not authorized without specific permission or an escort.
Access control	• Ensure that the access control roster (personnel and vehicles) is verified by the company. Ensure that personnel and vehicles receive background screening and/or HN certification. Ensure that substitutes receive the same vetting process. • Check badge systems and the exchange-badge system. • Check personal identification systems (work uniform, vehicle marking). • Check biometrics systems (fingerprint, iris, and facial feature reading devices). • Ensure that large vehicles (such as trash trucks) are empty when they enter the location. • Arrange vehicle loads to facilitate searching. • Verify the contents of large vehicles at distribution points 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.
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.

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

AT Security Area	*AT Security Measures*
Special security concerns	• Include contract services as part of the local risk analysis and management process. • Ensure that AT security measures which are already in place are leveraged and complemented. • Consider possible alternatives to fulfilling the required service, and determine if the service is required to accomplish the mission. • Consider time and space factors when determining hostile intent while planning 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 the acceptable level 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
FPCON	force protection condition
HN	host nation
U.S.	United States

D-14. (U) The contracting officer will ensure that the contract solicitation includes appropriate antiterrorism measures identified in the requirements package; this is normally done by referencing base or site access procedures. Contract- or site-specific antiterrorism 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 preapproved companies are considered for the contract award. Finally, the contracting officer will normally consider antiterrorism-related past performance as part of the contract 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 representative and the unit should notify the unit contracting officer before the start of contract services to ensure that all required antiterrorism security measures are in place.

STEP 5. AWARD AND EXECUTE THE CONTRACT (U)

D-15. (U) Contract oversight is a shared responsibility between the contracting officer and the requiring activity. The unit contracting officer representative should follow the quality assurance and surveillance plan, which should contain specific antiterrorism 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 antiterrorism security measures in place. Contract oversight includes reoccurring contracting officer representative inspections and evaluations of services rendered; periodic inspections 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 antiterrorism procedures. These change requests should be closely coordinated with the unit antiterrorism officer before sending them forward to the supporting contracting office for action. The requiring activity must understand that the requested contract modification may require additional funding, which may have to be justified to the approving official.

> ***Note.*** (U) Commanders, contracting officers, and antiterrorism 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.

STEP 6. REVIEW THE CONTRACT (U)

D-16. (U) Periodic review of the contract must be conducted. Where applicable, contracting officers will consider past performance, including antiterrorism performance, in awarding future contracts. Other service providers that are not under contracts governed by federal acquisition regulations (such as host nation port and airport personnel and some transportation providers) should be vetted where feasible.

CONTRACTOR PERSONNEL PROTECTION (U)

D-17. (U) Protection measures for contracted service personnel 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 commander’s responsibility, via the assistant chief of staff, operations staff.

D-18. (U) 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. Except for armed private security contracts, 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 when armed for personnel protection. (AR 715-9 covers contractor arming policy.) Commanders understand that contractors are subject to the same threat as Soldiers and must plan accordingly.

D-19. (U) 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 antiterrorism guidance directed by the Army and the combatant commander. Commanders may also be required to offer antiterrorism training to contractors authorized to accompany the force under the terms specified in the contract. It is also DOD and Army policy that 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 the benefits of measures undertaken to protect U.S. forces.

This page intentionally left blank.

Appendix E

Antiterrorism Assessments (U)

(U) Assessments form the foundation of every antiterrorism program and risk management approach which is used to defend against terrorist attacks that threaten infrastructure, personnel, and information. The information and examples in this appendix expand on the direction that is given in chapter 3 and provide guidance for commanders, leaders, and staffs to prepare assessments that weigh risk and defend against potential attacks.

THREAT ASSESSMENT (U)

E-1. (U) A terrorism threat assessment 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 antiterrorism 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. The DOD has developed four methodology factors to assist leaders and staffs with threat analyses (see table E-1) that are conducted country by country:

- (U) **Operational capabilities.** Operational capabilities are acquired, assessed, or demonstrated levels of the capability to conduct terrorist attacks.
- (U) **Operational** i**ntentions.** Operational intentions are stated purposes and/or actual attacks on U.S. interests.
- (U) **Operational** a**ctivities.** Terrorist group activities may not always be related to operational planning or present a threat to U.S. or host nation 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 activity by examining influential elements and by remembering that the situation is always fluid and subject to change.
- (U) **Operational environments.** The overall environment influences the ability and motivation of a terrorist group to conduct an attack.

Table E-1. (U) Methodology factors for threat analysis

Factors	***Considerations***
Operational Capabilities	
Terrorist group tactics	• What type of attack has the terrorist group conducted in the past? • Has the terrorist 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 terrorist 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 terrorist 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?

Table E-1. (U) Methodology factors for threat analysis (continued)

State sponsorships	• Does the terrorist 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 terrorist group indigenous, regional, or transnational? • Can indigenous groups operate regionally or internationally?
High-technology access	• Does the terrorist 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 method of operation? (A terrorist group will usually continue to use tactics, techniques, and procedures that have been successful in the past.)
Professional representations	• What is the overall level of competence? • Has the terrorist group consistently carried out successful, sophisticated attacks? • Has the group demonstrated a high or low degree of tradecraft?
Operational Intentions	
Recent attacks	• Has the terrorist 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 terrorist group have an anti-U.S. ideology? • Is the ideology stated publicly? • What are the group grievances against the United States? • What trigger events could entice the group to act?
Anti-host nation ideologies	• Does the terrorist group have an anti-host nation 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 terrorist group conducted an 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 terrorist 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?

Table E-1. (U) Methodology factors for threat analysis (continued)

Operational Activities	
Presence	• Is a terrorist group present but inactive?
Fundraisers and safe havens	• Does the terrorist group use the country for fundraising? If so, what type of fundraising? • How much money is generated? • What is its intended use? • Is 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 terrorist 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 terrorist 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 host nation security element disruptions	• Have U.S. or host nation security forces disrupted terrorist group activities? • Does the group perceive U.S. involvement? • What caused the disruption? • What was uncovered by security? • How does it affect group operational capability in the country?
Weapons caches	• Have weapons caches been uncovered? If so, what weapons were found? • Are the weapons consistent with group past weapons usage? • Who supplied the weapons?

Table E-1. (U) Methodology factors for threat analysis (continued)

Cell activities	• What type of activity does the terrorist group primarily conduct in country (operational, support, size of cells, number of cells)?
U.S.-targeted asset indicators	• Is there an indication that the terrorist 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	
Army presence	• What is 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 nation at war? • Could this influence a terrorist group to attack? • Is there active insurrection? • Is the terrorist group involved in the insurrection?
Host nation security and cooperation	• Can host nation 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 host nation cooperate with U.S. authorities? • Does the host nation share information?
Political influence	• (U) What political influences are affecting the motivation of the terrorist group to attack? • Did host nation strategies become more stringent after previous terrorist acts occurred?

Note. (U) Different tactics result in different degrees of threat. Groups that have conducted only property attacks present less threat than those who have conducted assassinations or attacks with large, vehicle-borne IEDs.

E-2. (U) Counterintelligence support to the conduct of antiterrorism and protection vulnerability assessments consists of producing a threat assessment and making countermeasure recommendations in the final vulnerability assessment report concerning specific areas related to countering or negating known or suspected collection targeting of the supported command. *Threat assessment* is, in antiterrorism, examining the capabilities, intentions, and activities, past and present, of terrorist organizations as well as the security environment within which friendly forces operate to determine the level of threat (JP 3-07.2). A threat assessment is a stand-alone document that is produced from existing intelligence analysis and information that is developed through counterintelligence functions and liaisons with security, intelligence, and law enforcement agencies.

E-3. (U) The Office of the Under Secretary of Defense, Counterintelligence, and Security developed a standardized threat assessment that could be used to define the threat and inform the force of terrorist capabilities. The threat assessment provides a series of executive summaries and detailed discussions to inform units of the terrorist threat within a particular area of operations. The threat assessment 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.

E-4. The threat assessment should include—

- (U) Terrorist threats.
    - (U) Operational capabilities.
    - (U) Operational intentions.
    - (U) Operational activities.
    - (U) Operational environments.
- (U) Foreign intelligence and security service threats.
- (U) Crimes.
- (U) Civil disturbances.
- (U) Medical and safety threats.
- (U) Weapons of mass destruction.
- (U) Security environments.
- (U) Incident reporting and feedback points of contact.

THREAT CHARACTERISTICS (U)

E-5. (U) Intelligence plays a critical role in the antiterrorism program. Another approach that is available to the commander and antiterrorism officer for compiling a threat assessment is to use 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 analyzes the command 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 additional information.) Using this methodology, terrorists are evaluated on—

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

THREAT MATRIX (U)

E-6. (U) 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 threat assessment, 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-7. (U) 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 antiterrorism officers evaluate the threat, shift resources, and implement random antiterrorism measures. Threat modeling may also help commanders determine organizational tools (local support, recruitment capabilities, ideology) and operational tools (funding, training, CBRN capabilities, small arms).

E-8. (U) Table E-2 is a sample terrorist threat assessment 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 (weapon column) to the airfield; therefore, the scale is 1 to 10, with 10 being the most probable or most severe.

Table E-2. (U) Sample threat matrix

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	3
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	8
Suicide bomber	25 lb	Personal	6	4	24	2	4
MANPADS	SA7, SA16	Attack against aircraft during arrival or departure	3	6	18	NA	5
Active shooter	Pistol/ Rifle	Random shooting	2	8	16	4	6
CBRN	WMD	Weapon dispersed upwind of an event or train derailment	1	9	9	6	8

Table E-2. (U) Sample threat matrix (continued)

Legend:	
cal	caliber
CBRN	chemical, biological, radiological, and nuclear
lb	pound
MANPADS	man portable air-defense system
mm	millimeter
NA	not applicable
RPG	rocket-propelled grenade
WMD	weapons of mass destruction

CRITICALITY ASSESSMENT (U)

E-9. (U) A *criticality assessment* is an assessment that identifies key assets and infrastructure that support Department of Defense missions, units, or activities and are deemed mission critical by military commanders or civilian agency managers. It addresses the impact of temporary or permanent loss of key assets or infrastructures to the installation or unit ability to perform its mission. It examines costs of recovery and reconstitution including time, dollars, capability, and infrastructure support. (JP 3-07.2) The following criteria assists in standardizing the process of determining asset criticality:

- (U) **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.
- (U) **Effect of loss.** Effect measures the ramification of a terrorist incident in the area. Considerations include psychological, economic, sociological, and military impacts.
- (U) **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.
- (U) **Mission functionality.** Mission functionality measures key positions, special facilities, and specialized equipment used to fulfill assigned missions.
- (U) **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?
- (U) **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 (U)

E-10. (U) 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 prioritized for the commander's consideration. 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. Table E-3, page E-8, shows an example of a criticality assessment matrix.

Table E-3. (U) Sample criticality assessment matrix

Asset	*Importance*	*Effect*	*Recoverability*	*Mission Functionality*	*Substitute/ Repair*	*Other*	*Total*
Base exchange	8	7	5	3	5	0	28
Corps headquarters	9	10	9	7	7	0	42
Soldier barracks	10	10	9	10	10	0	49

Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity Tool (U)

E-11. (U) 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-12. (U) The purpose of the MSHARPP tool is to analyze likely terrorist targets and assess their vulnerabilities from the inside out, with focus on the U.S. military mission. Consideration is given to local threats, the 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 enemy known capabilities.

E-13. (U) The MSHARPP targeting 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 listed in the critical asset list. To complete the matrix, antiterrorism officers—

- (U) Identify and reevaluate key structures, capabilities, organizations, and individuals in the area of operations that terrorists may target.
- (U) 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. After prioritization is complete and the commander determines the assets that will be resourced, the defended asset list is updated.
- (U) Evaluate the potential target using the sample MSHARPP evaluation tool. (See table E-4.)
- (U) 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.

Table E-4. (U) Sample MSHARPP criteria tool

<table>
<tr><td colspan="3"><b>Mission Criteria.</b> 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—
• <b>Importance.</b> Measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value.
• <b>Effect of loss.</b> Measures the ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.
• <b>Recuperability.</b> 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.</td></tr>
<tr><td colspan="2">The unit/base cannot continue to carry out its mission until the attacked asset is restored.</td><td>9-10</td></tr>
<tr><td colspan="2">The ability to carry out the primary mission of the unit/base would be significantly impaired if this asset were successfully attacked.</td><td>7-8</td></tr>
<tr><td colspan="2">Half of the mission capability remains if the asset was successfully attacked.</td><td>5-6</td></tr>
<tr><td colspan="2">The unit/base could continue to carry out its mission if this asset was attacked, albeit with some degradation in effectiveness.</td><td>3-4</td></tr>
<tr><td colspan="2">Destroying or disrupting this asset would have no effect on the ability of the unit/base to accomplish its mission.</td><td>1-2</td></tr>
<tr><td><b><i>Why and how</i></b></td><td><b><i>Value</i></b></td><td><b><i>Controls and mitigation</i></b></td></tr>
<tr><td colspan="3"><b>Symbolism Criteria.</b> 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, or authority). Assess points in this area are based on the symbolic value of the target to the enemy.</td></tr>
<tr><td colspan="2">The location is associated with personnel or organization leaders who are involved in actions to which the attacker is directly opposed.</td><td>9-10</td></tr>
<tr><td colspan="2">The target has historical, religious, or other symbolic significance to the defender.</td><td>7-8</td></tr>
<tr><td colspan="2">The target is regarded as an invulnerable strongpoint by the defender.</td><td>5-6</td></tr>
<tr><td colspan="2">The target is associated with the economic or production capability of the defender.</td><td>3-4</td></tr>
<tr><td colspan="2">The target is a popular social gathering area for the defender populace.</td><td>1-2</td></tr>
<tr><td><b><i>Why and how</i></b></td><td><b><i>Value</i></b></td><td><b><i>Controls and mitigation</i></b></td></tr>
<tr><td colspan="3"><b>History Criteria.</b> Do terrorist groups have a history of attacking this type of target? Consider terrorist trends worldwide, but focus on local targeting history and capabilities.</td></tr>
<tr><td colspan="2">Attacks against this type of target are conducted routinely by most known threats (majority of attacks).</td><td>9-10</td></tr>
<tr><td colspan="2">Attacks against this target are conducted routinely by the primary threat.</td><td>7-8</td></tr>
<tr><td colspan="2">Attacks against this type of target have occurred.</td><td>5-6</td></tr>
<tr><td colspan="2">Attacks against this type of target have been threatened.</td><td>3-4</td></tr>
<tr><td colspan="2">Attacks against this type of target fit the method of operation of the threat.</td><td>1-2</td></tr>
<tr><td><b><i>Why and how</i></b></td><td><b><i>Value</i></b></td><td><b><i>Controls and mitigation</i></b></td></tr>
<tr><td colspan="3"><b>Accessibility Criteria.</b> 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.</td></tr>
<tr><td colspan="2">Easily accessible, standoff weapons can be employed.</td><td>9-10</td></tr>
<tr><td colspan="2">The target is inside a perimeter, but outdoors.</td><td>7-8</td></tr>
<tr><td colspan="2">The target is inside a building, but on the ground floor.</td><td>5-6</td></tr>
<tr><td colspan="2">The target is inside a building, but on the second floor or in the basement.</td><td>3-4</td></tr>
<tr><td colspan="2">The target is not accessible or is only accessible with extreme difficulty.</td><td>1-2</td></tr>
</table>

Table E-4. (U) Sample MSHARPP criteria tool (continued)

<table>
<tr><th><em>Why and how</em></th><th><em>Value</em></th><th><em>Controls and mitigation</em></th></tr>
<tr><td colspan="3"><b>Recognizability Criteria.</b> The recognizability of a target 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 technical sophistication and training of the enemy.</td></tr>
<tr><td colspan="2">The target is clearly recognizable under all conditions and from a distance. or it requires little or no training.</td><td>9-10</td></tr>
<tr><td colspan="2">The target is easily recognizable at small arms range or requires a small amount of training for recognition.</td><td>7-8</td></tr>
<tr><td colspan="2">The target is difficult to recognize at night or in bad weather, it might be confused with other targets or target components, or it requires some training for recognition.</td><td>5-6</td></tr>
<tr><td colspan="2">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, or it requires extensive training for recognition.</td><td>3-4</td></tr>
<tr><td colspan="2">The target cannot be recognized under any conditions except by experts.</td><td>1-2</td></tr>
<tr><th><em>Why and how</em></th><th><em>Value</em></th><th><em>Controls and mitigation</em></th></tr>
<tr><td colspan="3"><b>Population Criteria.</b> Population addresses two factors: the 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 a group has a history of targeting, or is predicted to target military personnel, family members (U.S. citizens in general), civilian employees of the U.S. government (including local nationals), senior officers, high-risk personnel, or members of an ethnicity (racial, religious, or regionally defined).</td></tr>
<tr><td colspan="2">Extremely large population center; attack causes mass casualties (1,000+). There is a significant impact on international policy with the highest level of stress on infrastructure.</td><td>9-10</td></tr>
<tr><td colspan="2">Large number of people; attack causes mass casualties (500+). A known target group is present. There is a significant impact on international policy or significant stress on infrastructure.</td><td>7-8</td></tr>
<tr><td colspan="2">Moderate number of people; attack causes extensive casualties (100+), known target group may be present. Significant impact on national policy or major stress on infrastructure.</td><td>5-6</td></tr>
<tr><td colspan="2">Sparsely populated; attack causes few casualties (10+), prone to having small groups or individuals, or little target value based on demographics of occupants.</td><td>3-4</td></tr>
<tr><td colspan="2">No or very few people present; attack causes very few casualties (1-10) or contains people that the terrorist group considers desirable to avoid harming.</td><td>1-2</td></tr>
<tr><th><em>Why and how</em></th><th><em>Value</em></th><th><em>Controls and mitigation</em></th></tr>
<tr><td colspan="3"><b>Proximity Criteria.</b> Is the potential target located near other personnel, facilities, or resources that afford it some form of protection (intrinsic value, protected status, fear of collateral damage)? 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 an attack.</td></tr>
<tr><td colspan="2">The target is in close proximity; serious injury, damage or death, or total destruction of protected personnel and facilities is likely.</td><td>9-10</td></tr>
<tr><td colspan="2">The target is in close proximity; serious injury, damage or death, or partial destruction of protected personnel and facilities is likely.</td><td>7-8</td></tr>
<tr><td colspan="2">The target is in close enough proximity to protected personnel and facilities that injury or damage is likely, but destruction is not likely.</td><td>5-6</td></tr>
</table>

Table E-4. (U) Sample MSHARPP criteria tool (continued)

Population criteria (continued).		
The target is partially isolated; unwanted collateral damage to protected symbols or personnel is likely.	3-4	
The target is isolated; no chance of unwanted collateral damage to protected symbols or personnel is possible.	1-2	
Why and how	***Value***	***Controls and mitigation***

Legend:

U.S. United States

E-14. (U) Another way to reflect the results of the criticality assessment is by filling out an MSHARPP matrix. (See table E-5.) The values (1 to 10) are assigned to each factor based on the associated data for each target taken from the MSHARPP tool. The number 10 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 and has numerical data to assist in making risk decisions during the risk management process.

Table E-5. (U) Sample MSHARPP matrix

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

CRITICALITY, ACCESSIBILITY, RECUPERABILITY, VULNERABILITY, EFFECT, AND RECOGNIZABILITY MATRIX (U)

E-15. (U) The CARVER targeting matrix is a valuable tool in determining criticality. The CARVER targeting matrix 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). The CARVER targeting matrix assesses a potential target from a terrorist perspective to identify what the enemy might perceive as a good (soft or valuable) target. Commanders and antiterrorism officers may address—

- (U) **Criticality.**
  - How rapidly will the impact of asset destruction affect unit 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?
- (U) **Accessibility.** How easily can an enemy gain access to weapons?

- (U) **Recuperability.** How long will it take to repair or replace the asset?
- (U) **Vulnerability.** Is the asset hardened or guarded? Are measures in place to mitigate the threat?
- (U) **Effect.**
  - Will reprisals against allies result?
  - Will national MISO 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?
- (U) **Recognizability.** Can the enemy recognize the target and its importance?

E-16. (U) 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—

- (U) Listing systems and subsystems for strategic analysis.
- (U) Listing complexes or components of subsystems and complexes.

Note. (U) The scale can be adjusted for tactical analysis.

E-17. (U) The CARVER targeting 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-18. (U) To complete the matrix, antiterrorism officers identify and reevaluate key structures, capabilities, organizations, and individuals in the area of operations that terrorists may target. They—

- (U) Evaluate the potential target by using a criteria evaluation tool. (See table E-6.)
- (U) 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.
- (U) Record the information into the sample CARVER matrix for each asset.

Table E-6. (U) Sample CARVER criteria tool

<table>
<tr><td colspan="3"><b>Criticality Criteria.</b> 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 ability to make war or perform essential functions.</td></tr>
<tr><td colspan="2">Immediate halt in output, production, or service; target cannot function without it.</td><td>9-10</td></tr>
<tr><td colspan="2">Halt within 1 day or 66% curtailment in output, production, or service.</td><td>7-8</td></tr>
<tr><td colspan="2">Halt within 1 week or 33% curtailment in output, production, or service.</td><td>5-6</td></tr>
<tr><td colspan="2">Halt within 10 days or 10% curtailment in output, production, or service.</td><td>3-4</td></tr>
<tr><td colspan="2">No significant effect on output, production, or service.</td><td>1-2</td></tr>
<tr><td>Why and how</td><td>Value</td><td>Controls and mitigation</td></tr>
<tr><td colspan="3"><b>Accessibility Criteria.</b> A target is accessible when an operational element can reach the target 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 be able to reach the target and remain there for an extended period.</td></tr>
<tr><td colspan="2">Easily accessible; standoff weapons can be employed.</td><td>9-10</td></tr>
<tr><td colspan="2">Inside a perimeter, but outdoors.</td><td>7-8</td></tr>
<tr><td colspan="2">Inside a building, but on the ground floor.</td><td>5-6</td></tr>
</table>

Table E-6. (U) Sample CARVER criteria tool (continued)

Accessibility Criteria (continued).		
Inside a building, but on the second floor or in a basement.		3-4
Not accessible or only accessible with extreme difficulty.		1-2
Why and how	Value	Controls and mitigation
Recuperability 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 that requires 1 month or more.		9-10
Replacement, repair, or substitution that requires 1 week to 1 month.		7-8
Replacement, repair, or substitution that requires 72 hours to 1 week.		5-6
Replacement, repair, or substitution that requires 24 to 72 hours.		3-4
Same-day replacement, repair, or substitution.		1-2
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.		9-10
Vulnerable to light antiarmor weapons fire or charges of 5 to 10 pounds.		7-8
Vulnerable to medium antiarmor weapons fire, bulk charges of 10 to 30 pounds, or very careful placement of smaller charges.		5-6
Vulnerable to heavy antiarmor weapons fire, bulk charges of 30 to 50 pounds, or special weapons.		3-4
Invulnerable to all but the most extreme targeting measures.		1-2
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 location of the public near the target, but also considers the domestic and international reaction as well.		
Overwhelming positive effects for the terrorist; no significant negative effects.		9-10
Moderately positive effects for the terrorist; few significant negative effects.		7-8
No significant effects; neutral.		5-6
Moderately negative effects for the terrorist; few significant positive effects.		3-4
Overwhelming negative effects for the terrorist; no significant positive effects.		1-2
Why and how	Value	Controls and mitigation
Recognizability Criteria. The recognizability of the target 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.		9-10
The target is easily recognizable at small arms range and requires a small amount of training for recognition.		7-8
The target is difficult to recognize at night or in bad weather, it might be confused with other targets or target components, or it requires some training for recognition.		5-6
The target is difficult to recognize at night or in bad weather (even within small arms range), it is easily confused with other targets or components, or it requires extensive training for recognition.		3-4
The target cannot be recognized under any conditions except by experts.		1-2
Why and how	Value	Controls and mitigation

E-19. (U) The CARVER matrix is a decision tool for rating the relative desirability of potential targets and for allocating attack resources. (See table E-7.) It reflects the results of the evaluation tool above, compared to the criticality of other assets within unit responsibility.

Table E-7. (U) Sample CARVER matrix

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

E-20. (U) After completing the matrix, total the scores. Rank the totals in the priority column to prioritize vulnerabilities and 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:

- (U) **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 fallback site for conducting the same mission from another location.
- (U) **Reduce accessibility.** Control pedestrian and vehicle movements. Employ barriers, barricades, fences, remote motion sensors, and remote video surveillance equipment.
- (U) **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 access sufficiently away from personnel massing facilities.
- (U) **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 (U)

E-21. (U) A vulnerability assessment is used by the commander to determine the susceptibility of assets to attack from prioritized threats identified by the threat assessment, intelligence preparation of the battlefield, and war games against their prioritized critical assets. A vulnerability assessment 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 vulnerability assessment helps address resource needs and the physical security focus. Even with a successful antiterrorism appendix, vulnerabilities can be discovered, especially during AARs of large-scale exercises; during war games within the MDMP; and after enemy contact. The vulnerability assessment is usually conducted after a threat assessment and criticality assessment. Commanders can use vulnerability assessment methodology for combat patrols and mission planning.

VULNERABILITY MATRIX (U)

E-22. (U) A vulnerability assessment 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 of 1 to 10. The number 10 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-23. (U) The antiterrorism officer uses the matrix in table E-8 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.

Table E-8. (U) Sample vulnerability matrix

Asset	*Recognizability*	*Accessibility*	*Vulnerability*	*Recoverability*	*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

WAR-GAMING VULNERABILITY ASSESSMENT METHODOLOGY (U)

E-24. (U) The MDMP provides an established and effective methodology to conduct vulnerability analyses through war games. 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-9 are not intended to be definitive; they are suggested techniques for identifying vulnerabilities during COA analysis or war games. Unit personnel should supplement these questions and discussions as appropriate.

Table E-9. (U) 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 and evacuate the casualties) • Abort or continue the mission	• Follow-on attack targeting first responders • Information operation exploitation of attack
• 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 was 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, and target pairing? • What is the impact on the unit mission?	NA

Table E-9. (U) War-gaming vulnerability analysis (continued)

Event	***Action***	***Reaction***	***Counteraction***
Course-of-Action, War-Gaming, and Antiterrorism Vulnerability Analysis			
• When did the terrorist event occur?	• When was the attack initiated? • Why was the attack initiated at this time? • How long does the attack take?	• How long until the unit recovers from the attack and aborts or continues the mission? • How long until needed assistance arrives on site?	NA
• Where did the terrorist event occur?	• Where was the attack initiated? • Why was 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?	NA
• What was the purpose or intent of the terrorist event?	• Why was the attack initiated? • What are the intended/desired effects of the attack?	• Did the attack achieve the desired results?	NA
• Discuss the planning and execution of the terrorist event.	• How was attack the initiated? • What has to happen for the attack to occur?	• Was the attack self-initiated?	NA
Legend: NA not applicable			

TACTICAL-UNIT VULNERABILITY ASSESSMENT METHODOLOGY (U)

E-25. (U) 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 area of operations, 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. Leaders can use the following METT-TC framework to assist in conducting unit vulnerability assessment:

- (U) **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.
- (U) **Enemy.** Leaders assess the most likely and most dangerous COA based on the unit intelligence preparation of the battlefield and updated threat assessment. 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 enemy-desired attack results, they can concentrate the unit response on preventing the intended effects. (How was the attack initiated? What had to happen for the attack to occur?).

- (U) **Terrain and weather.** Leaders assess the 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 the engineer staff officer can develop geospatial products to assist commanders in identifying terrain that supports the enemy use of IEDs and other common terrorist tactics.
- (U) **Troops and support available.** Leaders determine the organic equipment that the unit needs 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?)
- (U) **Time Available.** Available leaders assess when the enemy is most likely to attack and when the unit is most vulnerable. The vulnerability assessment 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-, time-, 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?)
- (U) **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 (U)

E-26. (U) The risk analysis combines threat, criticality, and vulnerability ratings for each asset and develops a quantifiable assessment level of risk. (See table E-10.) The risk assessment equation follows:

$$\text{Risk} = \text{Criticality} \times \text{Vulnerability} \times \text{Threat Probability}$$

Table E-10. (U) Risk analysis table

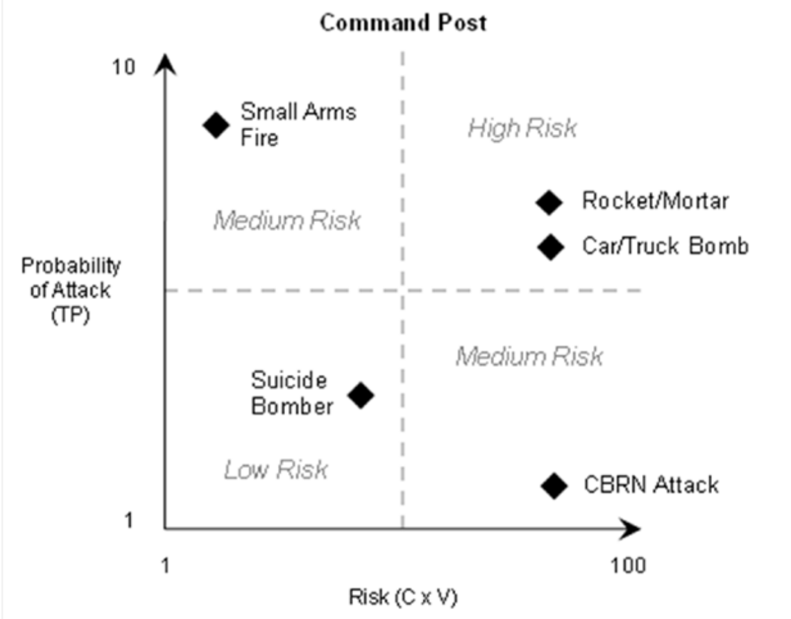
Asset	***Attack Means***	***C (1–10)***	***V (1–10)***	***C x V***	***TP (TP) (1–10)***	***Risk Analysis Total C x V x TP***
Command post	Car/truck bomb	9	8	72	6	432
	Suicide bomber	9	4	36	3	108
	Rocket/mortar	9	8	72	7	504
	Small arms fire	9	1	9	9	81
	CBRN attack	9	8	72	1	72

Legend:

C	criticality
CBRN	chemical, biological, radiological, and nuclear
TP	threat probability
V	vulnerability

E-27. (U) 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.

E-28. (U) The risk analysis should quantify existing risks and make recommendations to reduce risk levels to mitigate damage. (See figure E-1.) Risk mitigation lessens the impact of loss from a successful terrorist attack and develops a COA to plan for incident management.



Legend:

C	criticality
CBRN	chemical, biological, radiological, and nuclear
TP	threat probability
V	vulnerability

Figure E-1. (U) Risk analysis graph

E-29. (U) During the risk analysis, the commander at the appropriate level must consider the preceding elements and make well-informed decisions when planning FPCON measure implementation and terrorist incident response measures. The risk analysis 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 prioritized threats and critical assets and identified vulnerabilities and deficiencies can be entered into the risk management process as outlined in chapter 5.

Glossary

The glossary lists acronyms and terms with Army or joint definitions.

SECTION I – ACRONYMS AND ABBREVIATIONS

AAR	after action review
ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AOR	area of responsibility
AR	Army regulation
ASCC	Army Service component command
AT	antiterrorism
ATP	Army techniques publication
attn	attention
ATTP	Army tactics, techniques, and procedures
ATWG	antiterrorism working group
BDOC	base defense operations center
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and explosives
CIA	Central Intelligence Agency
CJCS	Chairman of the Joint Chiefs of Staff
CJCSM	Chairman of the Joint Chiefs of Staff manual
COA	course of action
CoC	code of conduct
DA	Department of the Army
DD	Department of Defense
DC	District of Columbia
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
fed	federal
FM	field manual
FOB	forward operating base
FORSCOM	U.S. Army Forces Command
FOUO	for official use only
FPCON	force protection condition
G-2	assistant chief of staff, intelligence

GPW	Geneva Convention III *Relative to the Treatment of Prisoners of War*
HRP	high-risk personnel
HSPD	Homeland Security Presidential Directive
IED	improvised explosive device
IOS	Impacting the World of Science
JP	joint publication
MDMP	military decisionmaking process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MISO	military information support operations
MO	Missouri
MSCoE	Maneuver Support Center of Excellence
MSHARPP	mission, symbolism, history, accessibility, recognizability, population, and proximity
No.	number
OPSEC	operations security
PA	public affairs
pam	pamphlet
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
std	standard
TNT	trinitrotoluene
TRADOC	United States Army Training and Doctrine Command
U	unclassified
UFC	united facilities criteria
U.S.	United States
USC	United States code
USS	United States ship

SECTION II – TERMS

None.

References

REQUIRED PUBLICATIONS

These documents must be available to the intended users of this publication.

ADRP 1-02. *Terms and Military Symbols*. 24 September 2013.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 8 November 2010.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

ARMY

Most Army doctrinal publications are available online at <www.apd.army.mil>.

ADP 2-0. *Intelligence*. 31 August 2012.

ADP 3-0. *Unified Land Operations.* 10 October 2011.

ADP 3-07. *Stability*. 31 August 2012.

ADP 3-37. *Protection.* 31 August 2012.

ADP 5-0. *The Operations Process.* 17 May 2012.

ADP 7-0. *Training Units and Developing Leaders.* 23 August 2012.

ADRP 2-0. *Intelligence*. 31 August 2012.

ADRP 3-0. *Unified Land Operations.* 16 May 2012.

ADRP 3-07. *Stability*. 31 August 2012.

ADRP 3-28. *Defense Support of Civil Authorities.* 14 June 2013.

ADRP 3-37. *Protection.* 31 August 2012.

ADRP 5-0. *The Operations Process.* 17 May 2012.

ADRP 6-0. *Mission Command.* 17 May 2012.

ADRP 7-0. *Training Units and Developing Leaders.* 23 August 2012.

AR 25-30. *The Army Publishing Program.* 27 March 2006.

AR 190-14. *Carrying of Firearms and Use of Force for Law Enforcement and Security Duties.* 12 March 1993.

AR 190-58. *Personal Security.* 22 March 1989.

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. *Operational Contract Support Planning and Management*. 20 June 2011.

ATP 3-39.32. *Physical Security.* 3 August 2010.

ATP 3-39.35. *Protective Services.* 31 May 2013.

ATTP 3-39.10. *Law and Order Operations.* 20 June 2011.

ATTP 4-10. *Operational Contract Support Tactics, Techniques, and Procedures*. 20 June 2011

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 3-24. *Counterinsurgency*. 15 December 2006.

FM 3-35. *Army Deployment and Redeployment*. 21 April 2010.

FM 3-50.1. *Army Personnel Recovery*. 21 November 2011.

FM 3-57. *Civil Affairs Operations.* 31 October 2011.

FM 6-01.1. *Knowledge Management Operations.* 16 July 2012.

FM 7-15. *The Army Universal Task List*. 27 February 2009.

FM 27-10. *The Law of Land Warfare.* 18 July 1956.

DEPARTMENT OF DEFENSE

DODD 1300.7. *Training and Education to Support the Code of Conduct (CoC)*. 8 December 2000.

DODI 2000.16. *DOD Antiterrorism (AT) Standards*. 2 October 2006.

DODI O-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.

UFC 4-010-01. *DOD Minimum Antiterrorism Standards for Buildings*. 9 February 2012. <http://www.wbdg.org/ccb/DOD/UFC/ufc_4_010_01.pdf>, accessed on 10 April 2014.

UFC 4-020-01. *DOD Security Engineering Facilities Planning Manual*. 11 September 2008. <http://www.wbdg.org/ccb/DOD/UFC/ufc_4_020_01.pdf>, accessed on 10 April 2014.

JOINT

Most joint publications are available online at <www.dtic.mil/doctrine/new_pubs/jointpub.htm>.

CJCS Guide 5260. *A Self-Help Guide to Antiterrorism.* 10 June 2013. <http://www.dtic.mil/doctrine/training/cjcsm3500_04e.pdf>, accessed on 10 April 2014.

CJCSM 3500.04F. *Universal Joint Task Manual*. 1 June 2011. <http://www.dtic.mil/cjcs_directives/cdata/unlimit/g5260.pdf>, accessed on 10 April 2014.

JP 1. *Doctrine for the Armed Forces of the United States.* 25 March 2013.

JP 3-0. *Joint Operations.* 11 August 2011.

JP 3-01. *Countering Air and Missile Threats*. 23 March 2012.

JP 3-05.1. *Joint Special Operations Task Force Operations.* 26 April 2007.

JP 3-07.2. *Antiterrorism*. 14 March 2014.

JP 3-13.3. *Operations Security*. 4 January 2012.

JP 3-24. *Counterinsurgency*. 22 November 2013.

JP 3-26. *Counterterrorism*. 13 November 2009.

JP 3-28. *Defense Support of Civil Authorities.* 31 July 2013.

JP 3-50. *Personnel Recovery*. 20 December 2011.

JP 3-57. *Civil-Military Operations.* 11 September 2013.

JP 3-61. *Public Affairs.* 25 August 2010.

JP 4-0. *Joint Logistics.* 16 October 2013.

JP 4-10. *Operational Contract Support.* 17 October 2008.

JP 5-0. *Joint Operation Planning*. 11 August 2011.

Other Sources

10 USC. *Armed Forces*. <http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-front&num=0&edition=prelim>, accessed on 10 April 2014.

32 USC. *National Guard*. <http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title32-front&num=0&edition=prelim>, accessed on 1 April 2014.

EO 13224. *Blocking Property and Prohibiting Transactions With Persons Who Commit, Threat to Commit, or Support Terrorism*. 23 September 2001.

Fed-Std-376B. *Preferred Metric Units for Use by the Federal Government.* 5 May 1983. <http://www.nist.gov/pml/wmd/metric/upload/fs376-b.pdf>, accessed on 10 April 2014.

Geneva Conventions, Convention I, *Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field,* Common Article 3. 12 August 1949.

Geneva Conventions, Convention III. *Relative to the Treatment of Prisoners of War (GPW)*, Geneva. 12 August 1949.

Hague Conventions, *Protection of Cultural Property in the Event of Armed Conflict.* 14 May 1954.

HSPD 5. *Management of Domestic Incidents*. 28 February 2003.

Law of Armed Conflict Deskbook 2012, <http://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2012.pdf>, accessed on 10 April 2014.

National Support Framework, May 2013. <http://www.fema.gov/library/viewRecord.do?id=7371>, accessed on 10 April 2014.

Public Law 106-523. Military Extraterritorial Jurisdiction Act of 2000. 22 November 2000. <http://www.pubklaw.com/hi/pl106-523.pdf>, accessed on 10 April 2014.

Uniform Code of Military Justice, <http://www.ucmj.us/>, accessed on 10 April 2014.

U.S. Army TRADOC G2 Handbook No. 1. *A Military Guide to Terrorism in the Twenty-First Century*. 15 March 2008.

PRESCRIBED FORMS

None.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate web site (www.apd.army.mil). DD forms are available on the Office of the Secretary of Defense (OSD) web site at www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm.

DA Form 2028. *Recommended Changes to Publications and Blank Forms.*

DD Form 254. *Department of Defense Contract Security Classification Specification*.

WEB SITES

Army Knowledge Online, Doctrine and Training Publications Web site, <https://armypubs.us.army.mil/doctrine/index.html>, accessed on 10 April 2014.

Army Publishing Directorate, Army Publishing Updates Web site, <http://www.apd.army.mil/AdminPubs/new_subscribe.asp>, accessed on 10 April 2014.

RECOMMENDED READINGS

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.

ADP 1. *The Army*. 17 September 2012

ADP 6-22. *Army Leadership*. 1 August 2012.

ATP 5-19. *Risk Management*. 14 April 2014.

Brachman, Jarret M. *Global Jihadism: Theory and Practice.* London: Routledge, 2009.

DA Pam 385-30. *Mishap Risk Management*. 10 October 2007.

DODI 5400.13. *Public Affairs (PA) Operations*. 15 October 2008.

Juergensmeyer, Mark. *Terror in the Mind of God: The Global Rise of Religious Violence.* Berkeley: University of California Press. 2003.

FM 3-11.21. *Multiservice Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Consequence Management Operations.* 1 April 2008.

FM 3-13. *Inform and Influence Activities.* 25 January 2013.

FM 3-28. *Civil Support Operations*. 31 July 2013.

FM 4-02.7. *Multiservice Tactics, Techniques, and Procedures for Health Service Support in a Chemical, Biological, Radiological, and Nuclear Environment.* 15 July 2009.

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 Jeffrey R. Victoroff (Ed.) *Tangled Roots: Social and Psychological Factors in the Genesis of Terrorism.* Netherlands, IOS Press. 2006.

UFC 4-010-02. *DOD Minimum Antiterrorism Standoff Distances for Buildings*. 9 February 2012. <http://www.wbdg.org/ccb/DOD/UFC/ufc_4_010_02.pdf>, accessed on 10 April 2014.

Venzke, Ben, and Aimee Ibrahim. *The al-Qaeda Threat: An Analytical Guide to al-Qaeda’s Tactics & Targets.* Tempest Publishing. 2003.

Index

Entries are by page number.

ATP 3-37.2
3 JUNE 2014

By order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

Gerald B O'Keefe

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1412901

DISTRIBUTION:

Active Army, Army National Guard, and United States Army Reserve: Distributed in electronic media only (EMO).

This page intentionally left blank.

PIN: 104247-000