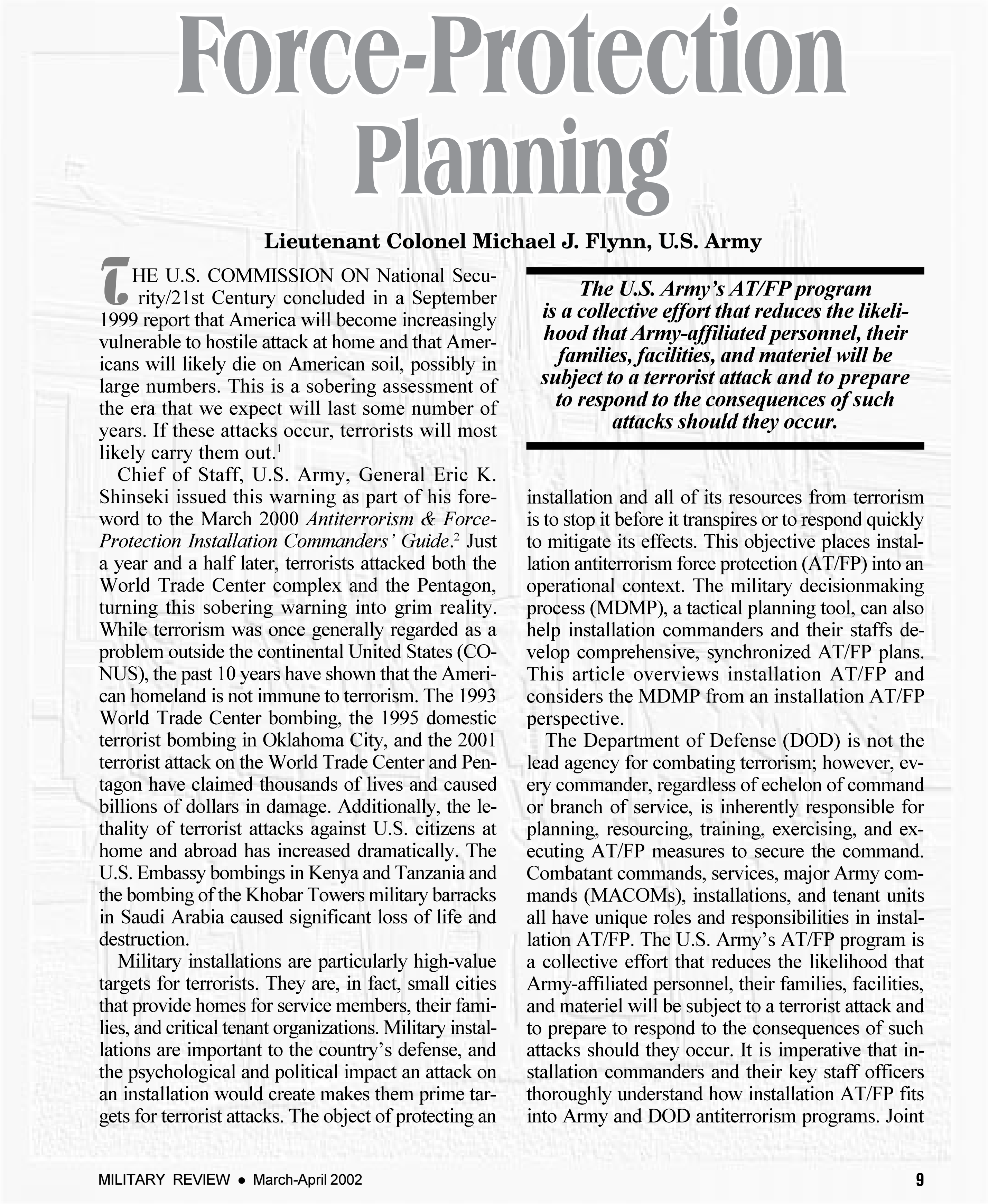
Installation Antiterrorism Force-Protection Planning

Lieutenant Colonel Michael J. Flynn, U.S. Army



THE U.S. COMMISSION ON National Security/21st Century concluded in a September 1999 report that America will become increasingly vulnerable to hostile attack at home and that Americans will likely die on American soil, possibly in large numbers. This is a sobering assessment of the era that we expect will last some number of years. If these attacks occur, terrorists will most likely carry them out.[1]

Chief of Staff, U.S. Army, General Eric K. Shinseki issued this warning as part of his foreword to the March 2000 *Antiterrorism & Force-Protection Installation Commanders' Guide*.[2] Just a year and a half later, terrorists attacked both the World Trade Center complex and the Pentagon, turning this sobering warning into grim reality. While terrorism was once generally regarded as a problem outside the continental United States (CONUS), the past 10 years have shown that the American homeland is not immune to terrorism. The 1993 World Trade Center bombing, the 1995 domestic terrorist bombing in Oklahoma City, and the 2001 terrorist attack on the World Trade Center and Pentagon have claimed thousands of lives and caused billions of dollars in damage. Additionally, the lethality of terrorist attacks against U.S. citizens at home and abroad has increased dramatically. The U.S. Embassy bombings in Kenya and Tanzania and the bombing of the Khobar Towers military barracks in Saudi Arabia caused significant loss of life and destruction.

Military installations are particularly high-value targets for terrorists. They are, in fact, small cities that provide homes for service members, their families, and critical tenant organizations. Military installations are important to the country's defense, and the psychological and political impact an attack on an installation would create makes them prime targets for terrorist attacks. The object of protecting an installation and all of its resources from terrorism is to stop it before it transpires or to respond quickly to mitigate its effects. This objective places installation antiterrorism force protection (AT/FP) into an operational context. The military decisionmaking process (MDMP), a tactical planning tool, can also help installation commanders and their staffs develop comprehensive, synchronized AT/FP plans. This article overviews installation AT/FP and considers the MDMP from an installation AT/FP perspective.

> ***The U.S. Army's AT/FP program is a collective effort that reduces the likelihood that Army-affiliated personnel, their families, facilities, and materiel will be subject to a terrorist attack and to prepare to respond to the consequences of such attacks should they occur.***

The Department of Defense (DOD) is not the lead agency for combating terrorism; however, every commander, regardless of echelon of command or branch of service, is inherently responsible for planning, resourcing, training, exercising, and executing AT/FP measures to secure the command. Combatant commands, services, major Army commands (MACOMs), installations, and tenant units all have unique roles and responsibilities in installation AT/FP. The U.S. Army's AT/FP program is a collective effort that reduces the likelihood that Army-affiliated personnel, their families, facilities, and materiel will be subject to a terrorist attack and to prepare to respond to the consequences of such attacks should they occur. It is imperative that installation commanders and their key staff officers thoroughly understand how installation AT/FP fits into Army and DOD antiterrorism programs. Joint

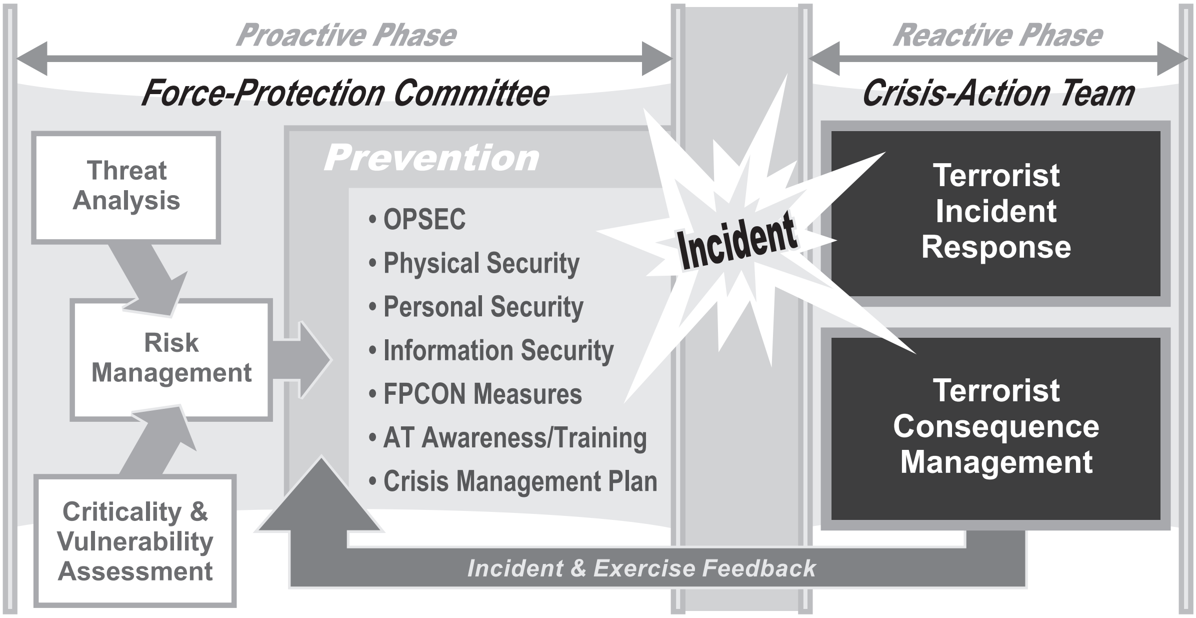


Figure 1. Antiterrorism Force Protection Concept

An installation AT/FP program's reactive phase involves those actions the installation takes to operationally increase FPCON protective measures in response to terrorists alerts, and the initial response and consequence-management actions it takes to contain and mitigate an actual terrorist incident.

Publication 3-07.2*, Joint Tactics, Techniques, and Procedures for Antiterrorism*, provides an excellent overview of the DOD antiterrorism program.[3]

Combating terrorism involves actions that include antiterrorism, counterterrorism, consequence management, and intelligence support taken to oppose terrorism throughout the entire threat spectrum. Where counterterrorism is offensive, antiterrorism is defensive. Antiterrorism focuses on defensive measures taken to reduce the vulnerability of individuals and property to terrorist acts.[4] The Army's AT/FP program is part of a broader national program of combating terrorism that is governed by Army Regulation (AR) 525-13, *Antiterrorism Force Protection: Security of Personnel, Information, and* Critical Resources.[5]

The Installation AT/FP Program

Each installation is a unique mix of threats, vulnerabilities, and acceptable levels of risk based on the factors mission, enemy, terrain, troops, time available, and civilians (METT-TC). An effective installation AT/FP program must synchronize intelligence, risk management, and existing security programs to ensure a holistic approach to countering the spectrum of security threats. While each installation's AT/FP program will vary, an underlying installation AT/FP program concept serves as a guide as depicted in Figure 1.[6]

The AT/FP program concept has two phases—a proactive phase and a reactive phase. The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness, and education and training that takes place before a terrorist incident. During this phase, consideration is given to information and intelligence gathering to develop a threat assessment. The threat assessment includes both threat analysis and the command's assessment of installation vulnerabilities ranked by criticality, or criticality and vulnerability assessment. Both elements together determine the risk and any steps necessary to correct or reduce identified vulnerabilities, or risk management.

The threat assessment is an integral part of the planning process and serves as the basis for developing a long-term AT/FP strategy. Because of limited resources, it takes time to achieve a fully prepared posture. The AT/FP strategy provides that long-term direction to guide the installation in a coordinated series of steps to realize that goal. The actual length of time the strategy considers is based on available resources and other installation missions. Generally, 5 years is a reasonable planning figure. Finally, the approved strategy must be translated into an effective AT/FP program and crisis-management plan for execution.

The prevention aspects of the proactive phase are based on synchronizing four separate but related security programs: operations security, personal security, physical security, and information security. Additionally, the DOD force-protection conditions (FPCON) system, formerly known as threat conditions, is also a prevention mechanism by which an installation operationally increases or decreases protective measures. The FPCON system consists of five conditions, ranging from normal through delta. Each FPCON describes progressive levels of security measures for implementing responses to threats to DOD personnel, information, and critical resources. Selecting the appropriate response to terrorist threats remains the responsibility of the commander having jurisdiction or control over the threatened facilities or personnel. Training and awareness are critical to an effective AT/FP program. Army and DOD instructions regulate individual, leader, and specialty training.[7]

An installation AT/FP program's reactive phase involves those actions the installation takes to operationally increase FPCON protective measures in response to terrorists alerts, and the initial response and consequence-management actions it takes to contain and mitigate an actual terrorist incident. Where the focus of the proactive phase is on planning and prevention, the reactive phase is centered on decisionmaking during execution. Key considerations during the AT/FP reactive phase include—

- Identifying first-response forces and the concept of their commitment.
- Performing command and control (C2), including authority and jurisdiction.
- Committing special response forces such as the Federal Bureau of Investigation (FBI), host nation security, and hazardous materials teams.
- Evacuating casualties.
- Conducting postincident procedures.

Postincident procedures consist of actions that protect evidence, handle captured personnel, identify and process hostages, document action to use during any prosecution, conduct public affairs operations, and identify changes required to the existing AT/FP plan.

C2. AR 525-13 requires that commanders establish committees and working groups to assist in developing, integrating, and managing the installation AT/FP program.[8] The force-protection committee (FPC) and its subordinate working groups consider the installation from the AT/FP perspective to assess the threat, integrate the installation's physical security features with its security capabilities, develop plans to compensate for weaknesses, and recommend enhancements to reduce installation vulnerabilities. The FPC meets at least semiannually—more frequently during increased threats—and is chaired by the installation commander or chief of staff. The FPC membership is based on the installation's size and staff structure. At a minimum, staff principals from the following staff sections form the FPC: provost marshal; security, plans, and operations; budget; staff judge advocate; information management; engineer; medical; public affairs; chemical; and criminal investigation. Other personnel to consider are supporting intelligence and counterintelligence commanders, tenant unit commanders, Reserve component forces, and other DOD and Department of the Army (DA) activities.[9]

The prevention aspects of the proactive phase are based on synchronizing four separate but related security programs: operations security, personal security, physical security, and information security. Additionally, the DOD force-protection conditions (FPCON) system, formerly known as threat conditions, is also a prevention mechanism by which an installation operationally increases or decreases protective measures.

The FPC has a broad range of duties and may establish subordinate working groups to address specialized aspects of the program. For instance, a threat working group, sometimes called an intelligence fusion cell, should be established to coordinate the production and dissemination of threat assessments and to ensure intelligence threat information and operational information are effectively and continuously integrated. Other working groups could include planning groups or vulnerability assessment teams. Ideally, the command's school-trained AT/FP officer supervises each group's operation.

Each installation must have a designated C2 center to plan and coordinate the command's AT/FP efforts during training and actual crises. Often referred to the emergency operations center (EOC), this C2 node must be readily available and functional on very short notice. The EOC functions by predetermined standing operating procedures (SOPs). As these SOPs dictate, predetermined and adequate communications systems must be made available at the location. The crisis-management team that operates from the EOC consists of staff officers from the FPC and other AT/FP working groups. Tenant unit commanders may also serve or have staff representation in the EOC. To be successful, crisis-management team members must be predesignated, train together, and be prepared to perform individual and collective C2 tasks under the installation commander's or his designated representative's control.

The FPC has a broad range of duties and may establish subordinate working groups to address specialized aspects of the program. For instance, a threat working group, sometimes called an intelligence fusion cell, should be established to coordinate the production and dissemination of threat assessments and to ensure intelligence threat information and operational information are effectively and continuously integrated.

Intelligence and counterintelligence. Intelligence and counterintelligence are the first line of defense in an AT/FP program. Commanders, however, must operate as laws and regulations require when conducting intelligence activities against domestic threats. Laws affecting intelligence-collection activities vary between CONUS-based and overseas installations. AR 381-10, *Intelligence Activities*, outlines the authorities and restrictions in intelligence activities.[10]

A variety of information sources are available to assist commanders in determining terrorist threats to installations. Defense Intelligence Agency threat assessments and State Department travel warnings provide useful information. The Army Antiterrorism Operations and Intelligence Cell publishes daily and weekly intelligence updates and products and distributes them worldwide to Army installations. MACOMs also frequently publish threat assessments and updates. Local threat information may also be available from local, state, federal, and host nation law enforcement and intelligence agencies.

Open-source information is publicly available and can be collected, retained, and stored without special authorization. News media, government hearings, and FBI and Central Intelligence Agency publications are examples of open-source information. Because terrorist acts are criminal acts, criminal records are a major source of terrorist intelligence. Commanders must work through established law enforcement liaison channels because collecting, retaining, and disseminating criminal records must be regulated. The installation's supporting U.S. Army Criminal Investigation Command detachment is an excellent source of assistance in determining the local terrorist and criminal threat.

Training and exercises. Key to an effective AT/FP program is elevating and sustaining terrorism awareness. Standards require that all personnel on an installation be trained to note and report suspicious activity. Individual awareness is especially important at installations with few security resources and high levels of risk. Response plans must also be exercised. A robust Random Antiterrorism Measures Program tests individual FPCON and other physical security measures, but it is equally important to regularly exercise the installation's ability to effectively transition between FPCONs. While there are no minimum time standards for FPCON transitions, commanders must know how long these transitions will take to establish a measure of confidence in any FPCON and threat environment. Lessons learned from training and exercises must be reflected in the annual review of the AT plan.[11]

AT/FP Planning

To develop an effective and comprehensive installation AT/FP plan, the commander and staff must conduct a thorough estimate of the situation and synchronize numerous agencies, functions, and resources to a common goal—protecting the installation from terrorism. Although designed for tactical planning, the MDMP provides the process to use to accomplish installation AT/FP planning. It is an established, proven analytical process that helps organize the thought processes of a commander and his staff to examine specific situations and reach logical conclusions. It helps them to apply thoroughness, clarity, sound judgment, logic, and professional knowledge in reaching decisions to develop effective plans.

For many years, tactical commanders have used the MDMP to determine a plan of action for a particular situation. The MDMP's seven steps are the same for an installation protecting itself from a terrorist attack as for a tactical formation defending itself against an enemy offensive in combat. Using this principle with the same logical sequence and skillfully applied available information and experience will ensure an effective installation AT/FP plan:[12]

- Receive mission.
- Conduct mission analysis.
- Develop courses of action (COAs).

US Army

A 10th Mountain Division MP stands watch at a Bagram Airfield checkpoint.

Initially conceptualizing a COA may start by developing a concept to defend the installation's most critical vulnerabilities, then working out to the installation's perimeter security. A series of inner, middle, and outer security rings are matched against assets, programs, and functions to deter and prevent terrorist attacks.

- Analyze COAs.
- Compare COAs.
- Approve COAs.
- Produce operation order (OPORD).

The MDMP establishes procedures for analyzing a mission, developing and wargaming COAs against the threat, comparing friendly COAs against criteria and each other, selecting a COA, and preparing an operation plan or OPORD for execution. The MDMP steps allow the installation commander and his staff to organize their planning activities, share a common understanding of the mission and commander's intent, and develop effective plans and orders. Interactions among various planning steps allow a concurrent, coordinated effort that maintains flexibility, efficiently uses available time, and facilitates continuous information sharing. Field Manual (FM) 101-5, *Staff Organization and Operations*, provides a detailed discussion of the planning process and prescribes formats for staff estimates and orders.[13]

While the basic seven-step planning process is the same for all types of planning, there are unique considerations when developing installation AT/FP plans. FM 101-5 is written from a tactical staff's perspective. Some of the tactics, techniques, and procedures described in FM 101-5 may not apply to installation AT/FP planning. Targeting is one example. However, threat analysis, criticality, and vulnerability assessments, which are critical to AT/FP planning, are not addressed in FM 101-5. Additionally, there are some unusual challenges not often found in a tactical unit.

An installation is formed of units and functions that support the various administrative purposes of its residents and tenant units. It is not, as a rule, formed for combat operations. Installation staffs vary widely in size and capability. Some installations are assigned a staff officer for every conceivable function while others have only a few that cover multiple functions, among which is planning. Finally, installation planners are often less experienced

Threat Level Factors

Factor 1, Existence:
A terrorist group is present, assessed to be present, or able to gain access to a given locale.

Factor 2, Capability:
The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

Factor 3, Intentions:
Recent demonstrated anti-U.S. terrorist activity or stated and/or assessed intent to conduct such activity.

Factor 4, History:
Demonstrated terrorist activity over time.

Factor 5, Targeting:
Current credible information on activity indicative of preparations for specific terrorist operations and/or specific intelligence that show that an attack is imminent.

Factor 6, Security Environment:
The internal political and security considerations that impact on the capability of terrorist elements to carry out their operations.

Threat Levels

CRITICAL

Factors 1,2, and 5 are present.
Factors 3 or 4 may or may not be present.

HIGH

Factors 1,2, 3, and 4 are present.

MEDIUM

Factors 1,2, and 4 are present.
Factor 3 may or may not be present.

LOW

Factors 1 and 2 are present.
Factor 4 may or may not be present.

NEGLIGIBLE

Factors 1 and 2 may or may not be present.

Figure 2. Threat Level Guide

> ***The staff must examine the terrorist threat, including likely tactics, to determine what installation facilities, systems, and functions are vulnerable to attack. An elementary school, hospital, central mailroom, power-generation plant, commanding general's residence, water treatment facility, or the installation's information systems may all be vulnerable to terrorist attack.***

in the MDMP than officers in a tactical staff.[14]

The commander's role in planning. The commander is solely responsible for decisions, plans, and supervision, and his personal involvement in installation AT/FP planning is critical. The commander disciplines the planning process so that it is sensitive to time, planning horizons, simplicity, and level of detail. He also disciplines the product to ensure the output is relevant to the situation. To drive the planning process, commanders visualize, describe, and direct operations.[15]

Visualization begins in mission analysis as the commander understands the situation and develops how he wants the installation to move from its current state to the end state, which represents a concept of operations and mission accomplishment. Installation commanders visualize arranging activities simultaneously and sequentially to achieve desired effects. The commander begins to describe his visualization when participating in the MDMP. As he receives information during mission analysis, the commander focuses on developing COAs through the restated mission, his initial commander's intent, planning guidance, and the commander's critical information requirements (CCIR). The commander's intent, planning guidance, and CCIR all guide and focus the staff throughout the planning process.

Receiving the mission. The MDMP begins with receiving or anticipating a new mission. A directive from a higher headquarters, a change in FPCON, or a scheduled annual AT/FP plan review may initiate planning. Timely notification of an impending planning session facilitates the planning staff's preparedness. Critical activities outside of the installation staff, such as local, state, federal, and host nation organizations, should also be notified and invited to participate in the planning process. Upon notification of an impending planning session, staff officers prepare by updating estimates and other critical information relating to installation AT/FP. Planners must gather the necessary planning tools that will be used during mission analysis and COA development. These tools include—

- Copies of higher headquarters order and plans.
- Current and supporting installation plans such

as mass casualty evacuation plans and physical security plans.

- Installation maps and other available terrain products.
- Higher headquarters regulations, including applicable DA and DOD regulations and instructions.
- Installation SOPs.
- Appropriate FMs, pamphlets, and guides.
- Current staff estimates.

Mission analysis. Mission analysis is the crucial step in determining the mission and developing situational understanding. It consists of 17 tasks, not necessarily sequential, and results in a restated mission, commander's intent, and planning guidance to the staff for COA development. A thorough mission analysis enables the commander to better understand friendly forces and capabilities, the threat, and the environment. The intelligence preparation of the battlefield (IPB) begins during mission analysis. It integrates terrorist tactics, facts, assumptions, terrain, and weather to determine likely threat COAs. Installation staff officers should review FM 34-130, *Intelligence Preparation of the Battlefield*, for intelligence products that can be modified for installation AT/FP planning.[16] One of the results of IPB is the initial threat analysis. A threat analysis should be written according to the factors in Figure 2.

The threat analysis combined with the vulnerability assessment form the threat assessment. The threat assessment is not discussed in FM 101-5 and is unique to AT/FP planning. The staff must examine the terrorist threat, including likely tactics, to determine what installation facilities, systems, and functions are vulnerable to attack. An elementary school, hospital, central mailroom, power-generation plant, commanding general's residence, water treatment facility, or the installation's information systems may all be vulnerable to terrorist attack. The staff then ranks each vulnerability according to its criticality to the installation's mission.

For example, if force projection were a primary installation mission, the installation's airfield would rank high as a critical vulnerability. Because installations protect people, schools, commissaries, and housing areas may rank high on the criticality list. The prioritized list of facilities, systems, and functions, with their vulnerabilities, allows the commander to focus on each critical vulnerability in priority order. Finally, the staff must identify actions or tasks to mitigate each vulnerability. This analysis will identify required resources—money, troops, and special equipment—and resource shortfalls and will serve as a basis for COA development.

Mission analysis includes determining specified tasks, mostly from higher authorities, and implied tasks the installation planners determine. The mission-essential tasks are derived from the list of specified and implied tasks that form the basis of the mission statement. Most specified tasks for installation AT/FP are found in AR 525-13.[17] An analysis of those specified tasks will result in implied tasks. Implied tasks will primarily result from the installation's unique circumstances such as its location, associated tenant units, or its possible role as a force-projection platform.

News media, government hearings, and FBI and Central Intelligence Agency publications are examples of open-source information. Because terrorist acts are criminal acts, criminal records are a major source of terrorist intelligence. Commanders must work through established law enforcement liaison channels because collecting, retaining, and disseminating criminal records must be regulated.

Another part of mission analysis is determining limitations and assumptions. AR 525-13 and various legal documents provide many of the limitations imposed upon an installation regarding intelligence collection and the authority and jurisdiction of a terrorist incident. Commanders must operate as bound by law and regulations when executing AT/FP programs. Often things related to the installation and the adjacent community might impose a limitation on how the installation can operate in an AT/FP environment, including restricting mutual aid agreements. Limitations are important to the process because they prescribe boundaries that the command must anticipate.

Installation staffs work hard to gather every relevant fact to AT/FP. Unfortunately, it is nearly impossible to begin an operation with all desired information. Assumptions fill in the gaps where certain information is not available and provide the necessary details to continue the planning process. They must be constantly reviewed for validity. There is always a danger of assuming away problems, particularly threat potential. Because of the dynamic and opportunistic nature of the threat, it is best to include all terrorist possibilities. The greater the time between planning and execution, the greater the probability that facts will replace most assumptions.

Central to the MDMP, and particularly important for installation AT/FP, are CCIR and essential elements of friendly information (EEFI). The commander needs accurate, timely information to conduct his visualization, to make decisions, and to direct action. CCIR drive and prioritize the information-collection plan, subsequent allocations of collection resources, and analysis efforts. The two elements of CCIR are priority intelligence requirements (PIR) and friendly force information requirements (FFIR). Although not part of CCIR, EEFI are disseminated with CCIR and reflect things the command wants to protect. During mission analysis, the staff develops and nominates information requirements to the commander for his consideration as CCIR and EEFI.

The MDMP's seven steps are the same for an installation protecting itself from a terrorist attack as for a tactical formation defending itself against an enemy offensive in combat. Using this principle with the same logical sequence and skillfully applied available information and experience will ensure an effective installation AT/FP plan.

Most CCIR are directly linked to decision points. Thus, answers to CCIR enable the commander to anticipate required decisions and make them quickly. Commanders and their staffs continuously review CCIR throughout the planning process and as the situation changes during execution, particularly when the threat is ill defined, hidden, and changes drastically.

PIR focus on information about the enemy, terrain, and weather. During planning, installation AT/FP PIR focuses on building the threat assessment. During times of normal activity, they are broadly stated and address a variety of possible threats. Collection against PIR for installation AT/FP relies much more on civilian agencies and less on organic assets than does collection during combat. There are numerous restrictions on Army forces collecting information on domestic threats, thus the restrictions severely hamper collection against PIR for installation AT/FP. The commander must focus on a cooperative relationship with domestic security organizations to be able to fully understand the threat. The results will forecast terrorist operations and then determine a working estimate of potential terrorist target values.

Realistic PIR for installation AT/FP focus on understanding what the enemy is attempting to do and reverse engineer that into determining what friendly forces can do about it. Some PIR are also developed to support decisionmaking during execution. For example, examining the indicators that terrorists will use wheeled vehicles as weapons of mass destruction against the installation could lead to a decision to increase vehicle inspection criteria at installation access points or to restrict the route of all heavy commercial vehicles on the installation.

FFIR are those critical information requirements the commander and staff need to know about friendly forces and their capabilities as they relate to the mission. An example FFIR could read, "Inability to secure a stated mission-essential vulnerable area (MEVA)." If an AT/FP plan relies on a tenant infantry brigade to secure installation MEVAs during FPCON Charlie, deploying the infantry brigade would significantly impact mission accomplishment. The answer to this FFIR may lead the installation commander to several decisions, including requesting support from higher headquarters.

EEFI are critical aspects of friendly forces that if known by the enemy would compromise, lead to failure, or limit friendly forces' success. Operations security is the process commanders follow to protect EEFI. The location and accessibility of selected critical infrastructure, such as a cable communication hub, or installation security vulnerabilities are examples of AT/FP EEFI.

COA development. COA development is the next step in the MDMP. After receiving the commander's planning guidance, the staff develops COAs to analyze and compare. For installation AT/FP, COA development is organizing installation assets to reduce friendly vulnerabilities from a terrorist threat. In tactical planning, planners begin COA development by analyzing friendly and enemy forces' combat power. They use historical minimum-planning ratios to gain insight on possible missions. In installation AT/FP planning, this step should consist of a troop-to-task analysis to enable planners to determine resource requirements and shortfalls. For example, matching generic units, functions, and assets against FPCON Charlie's 40 preventive measures will produce the installation's resource requirements. The troop-to-task analysis will help planners develop multiple COAs that are suitable, feasible, acceptable, distinguishable, and complete.

Initially conceptualizing a COA may start by developing a concept to defend the installation's most critical vulnerabilities, then working out to the installation's perimeter security. A series of inner, middle, and outer security rings are matched against assets, programs, and functions to deter and prevent terrorist attacks. Another way to begin conceptualizing may be to start with a worst-case scenario such as a high-explosive vehicle bomb detonated at a unit headquarters. In this instance, the planner first develops the COA from the reactive perspective, then develops a concept of prevention.

COAs are presented to the commander for his consideration in the form of a concept statement and sketch. The concept may be phased—preincident, incident, and postincident—or proactive, reactive. It should describe the objective and the main effort of each phase. The main effort could be by unit or, more likely, by function.

COA analysis, comparison, and decision. Steps four, five, and six of the MDMP are similar between tactical and installation AT/FP planning. The detailed COA analysis allows the staff to refine and synchronize each COA. The procedures for conducting a wargame are found in FM 101-5 and can be modified to fit AT/FP planning.[18] COA comparison begins with each staff officer analyzing and evaluating the advantages and disadvantages of each COA. The staff then collectively compares each COA to identify the one that has the highest probability of success.

There are several techniques that help the staff determine the best recommendation. The most common technique is the decision matrix, which uses evaluation criteria to assess each COA's effectiveness and efficiency. After completing its analysis and comparison, the staff identifies the preferred COA and recommends it to the commander. After the COA decision brief, the commander selects the COA he believes will best accomplish the mission and issues any additional guidance on priorities, preparing orders, rehearsing, and preparing for mission execution.

A thorough mission analysis enables the commander to better understand friendly forces and capabilities, the threat, and the environment. The IPB begins during mission analysis. It integrates terrorist tactics, facts, assumptions, terrain, and weather to determine likely threat COAs. Installation staff officers should review FM 34-130,* Intelligence Preparation of the Battlefield, *for intelligence products that can be modified for installation AT/FP planning.

Producing orders. The final step in the MDMP is to complete the plan and publish the order. The AT/FP plan follows the same five-paragraph OPORD format described in FM 101-5.[19] There are some specific annotated AT/FP plan formats available to planners. The Joint Staff J34 section, for example, publishes an installation planning template.[20] Additionally, the J34's June 2001 publication of *The Guardian*, a quarterly AT/FP newsletter, provides an example of an annotated AT/FP plan.[21] ***MR***

NOTES

[1] Department of the Army (DA), *Antiterrorism & Force Protection Installation Commanders' Guide* (Washington, DC: U.S. Government Printing Office [GPO], March 2000), 3.
[2] Ibid.
[3] Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism* (Washington, DC: GPO, 17 March 1996).
[4] Department of Defense Instruction 2000.16, "DOD Antiterrorism Standards" (Washington, DC: GPO, 14 June 2001), 6.
[5] U.S. Army Regulation (AR) 525-13*, Antiterrorism Force Protection: Security of Personnel, Information, and Critical Resources* (Washington, DC: GPO, 10 September 1998), prescribes four levels of antiterrorism training.
[6] JP 3-07.2, IV-2. Chart modified by author.
[7] AR 525-13.
[8] Ibid.
[9] Captain Jeffery A. Hutchison, USN, "Elements of an AT Program," *The Guardian* (March 2001), 6.
[10] AR 381-10, *U.S. Army Intelligence Activities* (Washington, DC: GPO, 1 July 1984).
[11] Hutchison, 8.
[12] DA, "Installation Preparedness for Weapons of Mass Destruction: Installation Commanders' Blueprint," (Washington, DC: Headquarters, DA, May 2001), 27.
[13] U.S. Army Field Manual (FM) 101-5, *Staff Organization and Operations* (Washington, DC: GPO, 31 May 1997).
[14] Ibid., 28.
[15] For a full discussion on commander's visualization, see FM 3-0, *Operations* (Washington, DC: GPO, June 2001).
[16] FM 34-130, *Intelligence Preparation of the Battlefield* (Washington, DC: GPO, 8 July 1994).
[17] AR 525-13.
[18] FM 101-5.
[19] Ibid.
[20] Chairman of the Joint Chiefs of Staff, Combating Terrorism Section (J34), Installation Planning Template.
[21] Chairman of the Joint Chiefs of Staff, Combating Terrorism Section (J34), *The Guardian* (June 2001).

Lieutenant Colonel Michael J. Flynn, U.S. Army, is a doctrine author with the Combined Arms Doctrine Directorate, Fort Leavenworth, Kansas. He received a B.A. from Eckerd College and an M.A. from the U.S. Army Command and General Staff College (CGSC) while attending the School for Advanced Military Studies. He is a graduate of CGSC. He has served in various command and staff positions, including executive officer, 3d Battalion, 22d Infantry, Fort Drum, New York; deputy G3 and chief of plans, 10th Mountain Division, Fort Drum; and G1 plans and operations officer, 1st Armored Division, Bad Kreuznach, Germany. He is currently writing U.S. Army Field Manual 5-0, Army Planning and Orders Production.