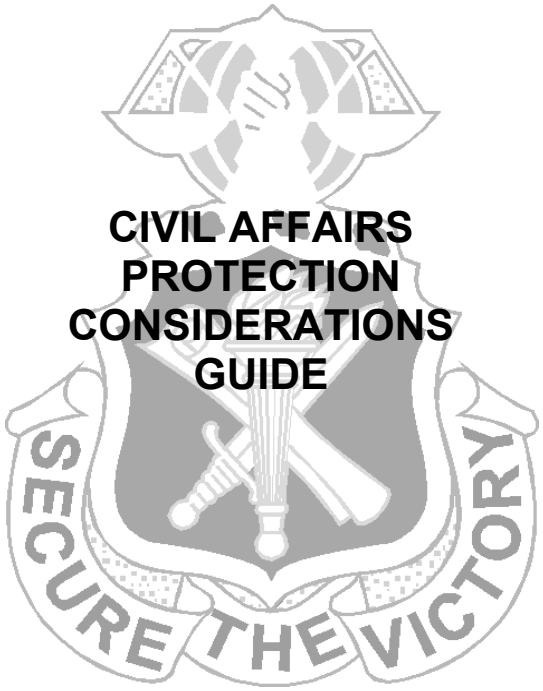
GTA 41-01-010



CIVIL AFFAIRS PROTECTION CONSIDERATIONS GUIDE

August 2010

HEADQUARTERS, DEPARTMENT OF THE ARMY

Contents

This page intentionally left blank.

INTRODUCTION

Protection is a paramount concern of all commanders. Every geographic combatant commander, every Army Service component commander, component subordinate commands, and component subordinate units have standing protection policies that require understanding and adherence by all personnel. Civil Affairs (CA) elements incorporate these requirements in planning to ensure compliance and mitigate risk.

Protection is the preservation of the effectiveness of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area (Field Manual [FM] 3-37, *Protection*).

The *protection warfighting function* is the related tasks and systems that preserve the force so the commander can apply maximum combat power. Preserving the force includes protecting personnel (combatants and noncombatants), physical assets, and information of the United States and multinational military, to include civilian partners (FM 3-0, *Operations*).

This graphic training aid (GTA) establishes the framework and context for CA Soldiers to apply protection measures throughout the conduct of Civil Affairs operations (CAO). It will identify measures to assist in planning and execution of missions as well as attempt to enhance the CA Soldiers' perception of how to directly influence the mitigation of threats by the application of CAO. CAO that are performed effectively by properly trained CA Soldiers will have a direct influence within the operational environment by establishing trust and rapport with the populace. A CA Soldier cannot accept a posture of complacency even when the outcome of CAO and civil-military operations is positive to the supported commander's goals and strategic objectives.

Many key items in this publication will require awareness and understanding throughout the ranks—from the largest command down to the individual Soldier. Individual threat awareness must be addressed throughout the planning, training, and conducting of the

missions. Planning protection can be very time-consuming, but when properly planned, the benefits pay an invaluable dividend. The situational awareness is greatly enhanced when every member of the team has an opportunity to provide input throughout the process. Following this procedure allows every Soldier to have a vested interest in being a sensor, especially since every member of the team has a unique perspective on the planning and developing of protection measures. Leaders of all levels who fail to adapt to this mode of thinking may be abandoning the opportunity for tapping the most valuable resources of information, a CA Soldier, as well as possibly presenting a weakness for the enemy to exploit. In the worst-case scenario, a Soldier's life may be at stake.

This GTA supersedes the subject of Force Protection Considerations originally published in Appendix E of FM 3-05.401, *Civil Affairs Tactics, Techniques, and Procedures*. It should be used in conjunction with the appropriate references that specialize in particular areas of protection.

The proponent of this GTA is the United States Army John F. Kennedy Special Warfare Center and School (USAJFKSWCS). Reviewers and users of this GTA should submit comments and recommended changes to Commander, USAJFKSWCS, ATTN: AOJK-DTD-CA, 2175 Reilly Road, Stop A, Fort Bragg, NC 28310-5000, or by e-mail to AOJK-DT-CA@soc.mil.

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

OVERVIEW

"*Commanders and leaders charged with providing or ensuring protection must begin with a thorough understanding of the operational environment, the risks and opportunities resident there, and the ways and means available for preserving combat power through protection.*"

FM 3-37, *Protection*, paragraph 1-9

As the Army continues to evolve and adapt to current and future threats, doctrinal publications are being developed to capture enduring concepts and best practices. This GTA will expand on many subjects related to protection and its correlation to CAO. In specific theater operations, it is best to conduct research with organizations that have explicit missions to mitigate certain common threats to the force, such as an Improvised Explosive Device Task Force. This section begins by providing the big picture of Army initiatives. These initiatives are the foundation on which all protection, to include CA protection, considerations should be built. For additional guidance, consider the References section of this publication which contains a list of Army and joint publications available for the reader to enhance his base of knowledge and expansion of operational awareness in relation to protection of the force.

Threats

Threats are nation-states, organizations, people, groups, conditions, or natural phenomena able to damage or destroy life, vital resources, or institutions. (See FM 3-0 for more information.) Commanders focus on threats to military operations that are generally coercive activities or information deliberately conducted or implemented by an adaptable enemy or a willful threat. Army doctrine describes threats through a range of four major categories or challenges—irregular, catastrophic, traditional, and disruptive (Figure 1, page 4). These categories can be used to begin threat identification and analysis; enhance situational understanding; and support plans, operations, and orders.

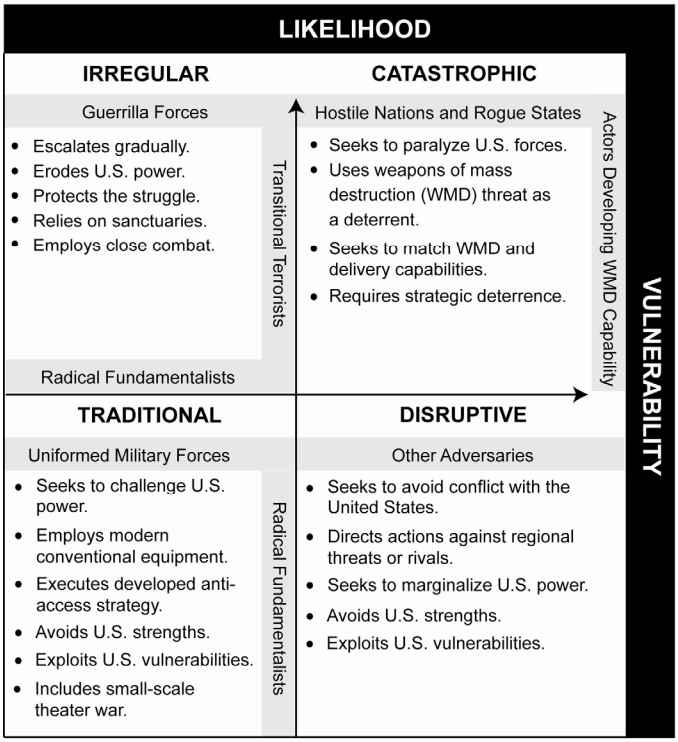


Figure 1. Security environment

Hazards

A h*azard* is a condition with the potential to cause injury, illness, or death to personnel; damage to or loss of equipment or property; or mission degradation (Joint Publication [JP] 3-33, *Joint Task Force Headquarters*). (See FM 5-19, *Composite Risk Management*, for more information.)

Both threats and hazards have the potential to decrease combat power and the operational effectiveness of the force. For this reason, their

overall assessment and mitigation is accomplished through the composite risk management (CRM) process and applied throughout the operations process. Commanders develop risk reduction measures and controls and threat mitigation strategies for all phases of military operations and activities. Army risk management doctrine provides six categories: (1) activity, (2) disrupters, (3) terrain and weather, (4) people, (5) time available, and (6) legal factors. CA, in analyzing the situation, advance the focus by applying the principles of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC) for hazard identification while being sure to consider the civil centers of gravity, civil decisive points, and civil lines of operation in their analysis. Accidental hazards are usually predictable and preventable and can be reduced through effective risk management efforts. Commanders **differentiate hazards from threats** and develop focused protection strategies and priorities that match protection capabilities with the corresponding threat or hazard while synchronizing those efforts in space, time, and purpose. (The purpose in this case is the mission.) However, hazards can be enabled by the tempo or friction or by the complacency that sometimes develops during extended military operations.

Forms of Protection

Military operations recognize five broad forms of protection (deterrence, prevention, active security, passive defense, and mitigation) to help organize the protection element of combat power (Figure 2, page 6). They are not sequential, reflect the continuous nature of protection, and may serve as a method to conceptualize protection capabilities for conducting operations.

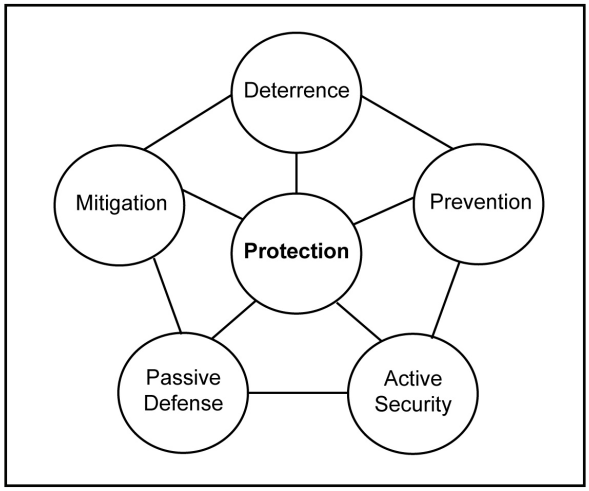


Figure 2. Forms of protection

Deterrence

The posture of an individual, formation, or structure can have a deterrent effect on threat decision making and result in protection. The presence of well-trained, equipped, and disciplined troops can often deter confrontation or conflict and protect the success of an individual, operation, or organization. Well-armed vehicles and fortifications may also deter enemy action and provide some level of protection for occupants and inhabitants. Random antiterrorism (AT) measures help deter terrorist attacks by disrupting routine patterns and presenting the appearance of greater security.

Prevention

Prevention involves the ability to neutralize, forestall, or reduce the likelihood of an imminent attack before it occurs; it can be achieved through deliberate action or as an effect. When linked to effective action, information sharing can increase situational awareness and increase protection. AT, operational security, and information security programs rely on situational awareness and individual

protective measures to reduce the likelihood of an accident or attack. Alert and warning systems can reduce the effectiveness of an attack or environmental event. Prevention does not typically represent an offensive, preemptive capability, but may employ other measures (information engagement, civil and public affairs, or preventive medicine).

Active Security

Dynamic activities with the organic ability to detect, interdict, avert, disrupt, neutralize, or destroy threats and hazards while maintaining the freedom of action can provide protection to the overall operation or force. Aggressive patrolling, route security, or local security measures in the vicinity of critical assets and bases provide protection. Some air missile defense assets represent active security measures.

Passive Defense

Protection can be achieved from survivability positions, fortifications, and physical barriers that are designed to protect forces and material from identified threats and hazards. Some level of protection can also be derived from the geographic positioning of a formation or critical asset; this may often be the most expedient method of providing protection for some assets or resources. Bases, base clusters, tactical command posts, refuel-on-the-move positions, forward logistics elements, and detainee holding areas are all positioned after considering the protection potential of a particular location. The proximity to threats and hazards, exploitable terrain, water features, and infrastructures can contribute to combat power potential by influencing the protection prospect of a specific area. The use of camouflage or smoke provides protection through passive means.

Mitigation

Mitigation is the activities and efforts that—

- Have the ability to minimize the effects or manage the consequence of attacks and designated emergencies on personnel, physical assets, or information.
- Preserve the potential, capacity, or utility of a force or capability.
- Have a protective quality.

Chemical, biological, radiological, and nuclear decontamination; personnel recovery; AT; and consequence management efforts may provide protection through mitigation and enable the restoration of essential capabilities.

Composite Risk Management

The CRM process (Figure 3, page 9) includes the following:

- Step 1 – Identify the hazard or threat.
- Step 2 – Assess to determine risks.
- Step 3 – Develop controls and make risk decisions.
- Step 4 – Implement controls.
- Step 5 – Supervise and evaluate.

The use of METT-TC provides a standardized methodology in identifying hazards and threats during a tactical or nontactical scenario. In the planning process, such as the military decision-making process or troop-leading procedures, METT-TC help shape the thought process as well as mitigate risks.

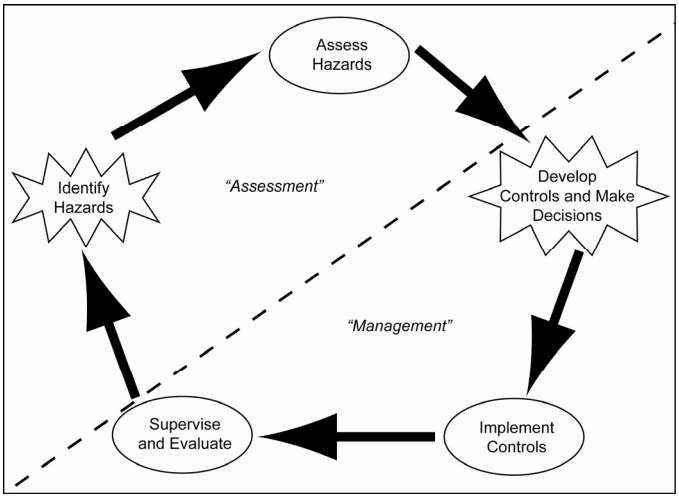


Figure 3. Composite risk management process

CIVIL AFFAIRS PROTECTION CONSIDERATIONS

CA Soldiers focus on protection at two distinct levels—the tactical level and support to the force. Figure 4, page 10, shows a typical CA element (the CA team) and its relation as part of the force at large in any given country.

At the tactical level, CA elements employ measures to counter threats and hazards to individual or team members while conducting CAO. Threats to CA Soldiers include enemy direct and indirect fire; a chemical, biological, radiological, and nuclear attack; an ambush; an improvised explosive device; enraged or disaffected civilians, thugs, or criminals; and theft of equipment. Hazards may include terrain and vehicle rollovers. CA Soldiers follow command guidance and unit standing operating procedures (SOPs), but also develop counter-measures on their own. This is especially true in a protracted environment where the operational situation is ever changing and,

therefore, reinforcing the importance of addressing threat awareness throughout the planning, training, and mission phases. When operating at the tactical level, protection of the force is imperative because, with even one casualty, morale may suffer and the team's mission capability can become substantially reduced.

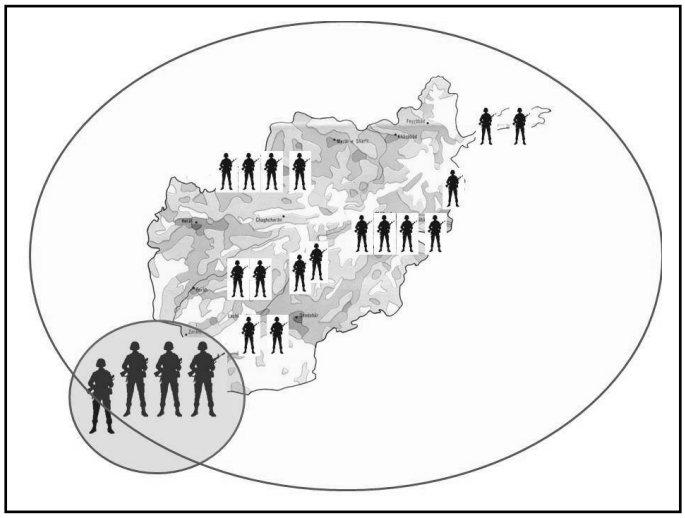


Figure 4. Civil Affairs in relation to the force

At the supported force level, conducting routine CAO can enhance protection of the supported force from threats and hazards within the civil component of the area of operations. This can be accomplished by confirming or denying assumptions and information, then integrating the information into the supported commander's common operational picture. Tactical CA elements have the advantage of operating within population areas, but the supported force may experience threats from dissidents, dislocated civilian populations, unfriendly political organizations, and terrorist activities, as well as theft of equipment. A perceptive CA element will observe many subtle and not-so-subtle indicators within the environment in which it operates. All observations should be noted and reported after each

mission. This after-action review will also provide the opportunity for the individual Soldier to contribute to the overall concept of protective measures in a given situation. This is an example of the force learning through practical application.

Antiterrorism

CA Soldiers should refer to the U.S. Army Antiterrorism Policy when developing measures for the protection of the force. All Department of the Army (DA) personnel, their families, installations, facilities, information, and other material resources will be protected from terrorist acts through a high-priority, comprehensive AT program. Commanders at all levels have the responsibility and authority to enforce appropriate security measures to ensure the protection of DA elements and personnel subject to their control. Commanders will ensure AT awareness and readiness of all DA elements and personnel (including dependent family members) assigned or attached. If the specific geographic combatant commander and DA AT standards or requirements conflict, the geographic combatant commander AT standard or requirement will take precedence. All military, DA civilians, and DA dependent family members will comply with theater, country, and special clearance requirements (Department of Defense Directive [DODD] 4500.54E, *DOD Foreign Clearance Program [FCP]*) before overseas travel. For additional information, Soldiers are encouraged to read Army Regulation (AR) 525-13, *Antiterrorism*.

CA Soldiers operating at the tactical level are at a greater risk than Soldiers operating in support of missions by virtue of their assignment, vulnerabilities, location, or specific threat. Appropriate measures will be taken to provide enhanced protection. Personnel will be made aware of risks and trained in individual protective measures. Responsible commanders will ensure personnel have completed appropriate high-risk training (personal protection, evasive driving, AT awareness, and hostage survival) and are properly cleared for assignment to high-risk billets, facilities, or countries requiring such protection. AT training will be afforded the same emphasis as combat task training and executed with the intent to identify shortfalls affecting the protection of personnel and assets

against terrorist attack and subsequent terrorism consequence management efforts.

Leaders must ensure that AT training is included in mission rehearsals and predeployment training for all units (platoon level or above) prior to deployment. Multiechelon individual training using vignettes and AT scenarios is required. Leaders must also ensure that units deploying to or moving through **high-threat** areas conduct predeployment training that is supported by measurable standards, including standing rules of engagement (ROE); standing rules of force (ROF); area of responsibility; specific threat orientation; deterrence; specific tactics, techniques, and procedures exercises; lessons learned; and the operation and use of security equipment. Formal education should be provided that includes the Army's AT training program. These elements include Level I through Level IV training and area of responsibility-specific training. Commanders will ensure all assigned personnel complete appropriate formal training and education. Individual records will be updated to reflect completion of the AT training prescribed by AR 525-13. Commanders, at all levels, who receive individuals not properly trained will provide the required AT training as soon as feasible. Concurrently, they will report the deficiency through their chain of command to the losing unit's chain of command, which will institute appropriate corrective action to prevent the recurrence of the discrepancy. Personnel assigned or attached to an embassy on temporary duty under chief of mission authority must receive Level I AT awareness training from a qualified instructor. The completion of a Department of Defense (DOD)-sponsored and certified computer-based distance learning instruction for Level I AT awareness will not satisfy Department of State (DOS)/chief of mission requirements.

Area of responsibility-specific AT awareness training will be conducted to orient all Army personnel (including family members ages 14 and older) assigned permanently or temporarily transiting through, or performing exercises or training in, an area of responsibility. Geographic combatant commanders are responsible for the development of this area of responsibility-specific information. It is in addition to annual Level I AT awareness training.

Commanders will maintain a memorandum for record documenting an individual's training.

Individual Responsibility

In addition to AT requirements set forth by AR 525-13, CA Soldiers are responsible to their team and to themselves to maintain a high posture of protection. Like a link in a chain, each member of a team is a crucial link to mission success (Figure 5). In order to accurately portray the responsibilities of a CA Soldier throughout the mission cycle, the following sections will cover CA considerations at the individual and team/group levels, during tactical mission execution, and within facilities.

Figure 5. Individual responsibility

The following should be considered by individual CA Soldiers who are tasked with missions that contain tactical aspects. ***Note:*** Even CA Soldiers who are working in a staff or planning position may at some point participate in a patrol or movement within the context of their mission; therefore, these considerations will have universal application. Some of these considerations are actual requirements set forth by

various Army institutions and senior leadership. The list is not all-encompassing.

Survival, Evasion, Resistance, and Escape (SERE) 100

All personnel entering United States Southern Command (USSOUTHCOM), United States Pacific Command (USPACOM), United States Central Command (USCENTCOM), United States European Command (USEUCOM), and United States Africa Command (USAFRICOM) geographic combatant commands are required to complete SERE 100 Code of Conduct training to meet established theater-entry requirements. This course is preferably accomplished through Joint Knowledge Online, which is the established method to record joint course completion. Other servers throughout the DOD may provide access to SERE 100, but have no consolidating electronic database capability of completed courses as does Joint Knowledge Online. Individuals who have completed Level B SERE training (8-hour video presentation) or Level C SERE training (Service SERE schools) at any point in their career need not complete SERE 100 if proof of training exists. Accomplishing this requirement on a regular basis helps reinforce the conduct of Soldiers.

Combatives

The Chief of Staff of the Army stated during the 2004 Army Training and Leadership Development Conference that he wanted combatives training to be conducted in units. The Army Combatives Training Program recognizes that Soldiers who possess discipline, confidence, and personal courage enhance units' readiness. The dynamics of a full-spectrum combat environment demand that Soldiers have the courage, confidence, and competence to implement controlled aggression to use the minimum amount of force to control the situation. Commanders will implement a combatives training program that certifies safe and professional combatives training and competitions.

Composite Risk Assessments

At all levels, a CA Soldier must be proficient with the steps laid out in the risk assessment steps. Each person among the group has a

unique perspective to "identify the hazard or threat." This perspective can improve the determination of risk and the development and implementation of controls. The evaluation and supervision of these controls should transcend the rank structure and leadership when risks involve the safety of the force.

Shoot, Move, Communicate, and Treat

Each member of the group must practice and demonstrate proficiency in the use of their personal weapons, communication systems, modes of transportation, and the immediate treatment of wounded teammates.

While Soldier Training Publication (STP) 21-1-SMCT, *Soldier's Manual of Common Tasks, Skill Level 1*, clearly addresses individual combat survivability, it is incumbent upon mission planners to fuse warrior tasks into collective training that provides CA forces with realistic scenario-driven training. Combat survivability does not rest exclusively on the CA Soldiers' ability to engage targets, but also on the CA teams' ability to balance key warrior tasks with METT-TC.

Integrating contingency planning into premission training will offset operational risks and allow more flexibility in the execution phase of an operation. The nine-line medical evacuation (MEDEVAC) request, the evasion plan of action, AT plans, and force protection plans mitigate operational risks and hazards to either deter or respond to a hostile action. The evasion plan of action provides detailed instructions for CA forces in uncertain or hostile environments without direct support from friendly forces. CA mission planners should ensure that the evasion plan of action is tailored to meet specific mission requirements.

The simple acronym PACE (primary, alternate, contingency, and emergency) can assist the mission planner with identifying specific communication requirements and restrictions (Figure 6, page 16).

In addition to proficiency with standard communications systems, CA Soldiers who are operating in a nontactical environment (such as the support of the American Embassy) should be familiar with the

local telephone system and have readily available phone numbers to vital points of contact in the U.S. Consulate/American Embassy.

5. Command and Signal

a. Signal:

(1) Encryption system (primary and alternate).

(2) Communications security and cryptography security and control measures (to include destruction means).

(3) Existing communication nets within the joint special operations area.

(4) Code words.

(5) Frequency and call signs.

(6) Pyrotechnics and signals.

(7) External communications:

(i) **P**rimary.

(ii) **A**lternate.

(iii) **C**ontingency.

(iv) **E**mergency.

Figure 6. PACE plan nested in the 5th paragraph of a standard operations order

Protection Considerations During Civil Affairs Operations

It is difficult to prevent threat forces from attacking someone or something they want; however, there are ways that CA Soldiers can mitigate the effects and make themselves less desirable targets during the performance of CAO. When planning missions, if an operation order or operation plan is available, CA Soldiers should read Annex F (Protection) of the operation plan as a baseline to build from. CA Soldiers should not limit themselves to the following considerations when developing a sound protection plan. When planning a mission, they should establish priorities of protection by both unit and area.

They should also address the scheme of CAO area security, review routes, bases, and critical infrastructure. As with any planning sequence, CA Soldiers must understand all the civil considerations as they operate in support of the full spectrum of operations.

The following is a basic list of considerations that a CA team should incorporate into SOPs.

Maintain a low profile.

CA Soldiers should—

- Discourage very important person (VIP) treatment.
- Limit the use of staff cars or not use them at all. If they are used, the vehicle should blend in as much as possible with the vehicles used by the local population.
- Avoid using official or diplomatic license plates.
- Not permanently affix decals required by the base or embassy to the vehicle.
- Drive themselves, which allows them to control the routes, speed of travel, and pickup times.

Note: Personnel who have a driver or chauffeur are considered VIPs.

- If required to have a driver or escort, keep the number to a minimum and make sure he blends in with the local population.
- Downplay their importance when their jobs require them to be interviewed or photographed.
- Maintain awareness of operations security when in the presence of drivers.

Control the environment.

CA Soldiers should—

- Whenever possible, use on-base facilities. These generally offer better security and are probably better equipped to deal with hostile attacks.

- Choose locations that employ security measures; for example, guards, cameras, visitor sign-in rosters, and so on.
- Avoid street-level rooms.
- Be alert for anyone loitering or carrying objects that could conceal weapons.
- Be familiar with the uniforms of local police, military, fire department, emergency services, and hotel security. Also know the proper procedures for obtaining their services.
- Know routes and alternate routes and locations to safe houses or the primary U.S.-controlled area in the area of operations.

Select a working or meeting place.

CA Soldiers should ensure that—

- They choose locations that balance operational capabilities and protection measures.
- The area has reliable police, fire, and rescue services.
- The area does not have a high crime rate or any late-night establishments.
- The area has multiple routes to and from the working or meeting place and is not located on narrow or one-way streets.
- The building selected has high walls and fences.
- There is more than one gate to offer alternative ways in and out of the compound.
- The trees and shrubs serve as a screen to anyone trying to observe the grounds. Shrubbery within the perimeter and near the building should be trimmed or removed to prevent them from being used by intruders for concealment.
- When possible, dogs monitor the building and surrounding area.

- Security guards and night watchmen monitor the building and surrounding area.
- Doors and windows are strong. Existing locks are changed upon taking control of the building.
- When possible, doors and windows have bars.
- Employees are hired from approved embassy lists.
- During a meeting, participants do not sit in direct line with the windows.

Meeting outside of the workplace, CA Soldiers should ensure that—

- The meeting place has at least two exits.
- Whenever possible, a premeeting visit to the location is conducted to allow them to become familiar with the layout of the building and routes.
- Appointments are not made in advance.
- The interior is well lit.

Establishing Facilities and Conducting Operations as a Civil-Military Operations Center (CMOC)

A predeployment site survey is recommended when CA units are preparing for deployment. However, when that is not an option for mission planning, the CA unit should attempt to contact the unit that they may be replacing. If CA units do not have these two options available, then the leadership must identify appropriate sites in the area of operations that have an appropriate balance of protection and mission capability. A strong consideration to protection should be one of the assessments made prior to beginning the execution of the mission. Prior to any mission, leaders should establish standard protection criteria for their likely deployments. FM 3-05.230, *Special Forces Tactical Facilities*, can provide additional guidance.

A CA element identifies an acceptable location for the CMOC by analyzing the following criteria:

- Will the CMOC be located on or adjacent to—
  - Prisons, internment camps, dislocated civilian camps?

  - Hazardous or hostile areas?
  - Mass transit systems?
  - Pedestrian traffic?
- Host nation (HN) emergency service capabilities:
  - Locations.
  - Organizations.
  - Equipment.
  - Training.
  - Effectiveness.
- Organizations:
  - Terrorist organizations.
  - HN police/fire/medical services.
  - Loyalty to the HN government.
  - Relationship with the local populace.
- People:
  - Criminal activity.
  - Blackouts and curfews.
  - General health and well-being.
  - Infant mortality rate.
- What is the attitude of the local populace—
  - Toward the HN government?
  - Toward U.S. presence?
  - Toward enemy activities within the area of operations?
- Events:
  - Cultural events calendar.
  - Planned hostile demonstrations.

METT-TC

CA leaders develop force protection SOPs based on METT-TC. To standardize their SOP, leaders should consider the following:

- Ability to integrate with supported unit's security operations.
- Workspace for all of the CA element sections.

- Assessment of existing local, national, or international coordination mechanisms for existing civil-military interfaces, best methods for integration, and supplemental activities.
- Identification of assets to be protected and shortcomings, and evaluation against threat type and level.
- Noise, light, and litter discipline (burn barrels for all documents).
- Theater ROE or ROF.
- Public Affairs Office guidance.
- Current casualty evacuation plan, U.S. medical assets, and local national medical assets.
- Evacuation routes, after-action reviews, and lessons learned from outgoing forces.
- Cultural events calendar.
- Stay-behind theater assets.
- Communications requirements.

The location of the CMOC must be approved by the commander if the location is not predetermined. The following are additional considerations:

- Establish a separate CAO/civil-military operations planning area that is secure and screened from unauthorized access and public access areas. CMOC personnel conduct civil-military operations tracking information in support of the mission requirements and consider operational security.
- Establish plans for a mobile operations center or split operations, as required, in order to provide access points to nonmilitary elements, such as indigenous populations and institutions, intergovernmental organizations, other government agencies, and nongovernmental organizations outside the secured perimeter.
- Sections establish operations in accordance with the CMOC's SOPs, access rosters, duty roster, tasking information exchange procedures, emergency operations procedures, and health and welfare procedures.

- Sections establish journals, workbooks, status boards, map boards, charts, continuity books, and graphs required to manage CAO/civil-military operations as per the CMOC SOP and mission requirements.
- The CA element identifies other agencies that require workspace within the CMOC, including nongovernmental organizations, intergovernmental organizations, indigenous populations and institutions, other government agencies, and the private sector.
- Clearly define protection procedures based on likely scenarios ranging from infiltration or methods of attack for the protection or destruction of personnel, information, or equipment that may be sensitive. Assign personnel with primary and alternate responsibilities to each task once identified, ensuring that all personnel know the overall requirements.
- Develop a training plan for local nationals and interpreters that will support protection efforts by providing valuable insight to local customs and events, and work to prevent any social faux pas.
- Identify if there is a response force and consider their response time when making appropriate detailed plans and drawings. Their response time will be an important factor when designing the security posture and response of the CMOC.

Supplemental measures for protection are defined throughout FM 3-19.30, *Physical Security*.

During Transit

CA Soldiers can greatly enhance their personal security when conducting official and unofficial travel by following these general practices:

- Vary daily patterns, such as leaving and returning at different times.
- Consider escorts to and from work or travel with a neighbor.

- Establish a simple oral or visual duress procedure between team members and drivers (for example, a phrase or movement used by the team members or driver only if something is amiss).
- Vary taxi companies. Ensure that the identification photo on the license matches the driver. If uneasy for any reason, take another taxi.
- Do not attend social functions by yourselves. Attend with others, if possible.
- Examine the car before entering to see if there has been any interference. A small mirror on a rod is a cheap and effective method to inspect underneath cars. Do not touch the vehicle until it has been thoroughly checked (inside, around, and under).
- Avoid leaving items exposed in the car that identify affiliation to the U.S. Government or military (uniform items, Service-issued maps, official briefcases, and so on).

Security Practices While Driving

CA Soldiers can take the following measures to enhance security while driving:

- Keep car doors locked. Do not open windows more than a few inches.
- Develop load plans.
- When required to have a driver or escort, maintain operational security.
- Vary routes, speed of travel, and pickup times.
- Avoid using official vehicles, plates, or identifying features.
- Know locations and alternate routes to U.S.-controlled areas.
- Avoid overloading a vehicle and wear seat belts.
- Park vehicles in parking areas that are either locked or monitored.
- Keep the trunk locked.
- Drive in the inner lanes to keep from being forced to the curb.

- Use defensive and evasive driving techniques.
- Avoid driving close behind other vehicles (especially service trucks), and be aware of activities and road conditions two to three blocks ahead.
- Maintain freedom of movement. Beware of minor accidents that could block traffic in suspect areas such as crossroads. (Crossroads are preferred areas for terrorist or criminal activities because they offer escape advantages.)

If a terrorist roadblock is encountered, use the shoulder or curb (hit at a 30- to 45-degree angle) of the road to go around it or ram the terrorist's blocking vehicle. Blocking vehicles should be rammed in a nonengine area, at a 45-degree angle, in low gear, and at a constant moderate speed. The goal is to knock the blocking vehicle out of the way. In all cases, do not stop and never allow the primary vehicle to be boxed in with a loss of maneuverability. Whenever a target vehicle veers away from the terrorist vehicle, it gives adverse maneuvering room and presents a better target to gunfire.

Interurban, National, and International Travel Security Practices and Procedures

To enhance security in interurban, national, and international circumstances, CA Soldiers should—

- Restrict the use of ranks or titles.
- Avoid allowing unknown visitors in the hotel room or suite.
- Keep commanders and family members advised of the itinerary and subsequent changes. Clearly and emphatically restrict this information to those having a need to know.
- Refrain from wearing or carrying anything that identifies an association with the U.S. Government or U.S. military.
- Continually assess their environment. Look for exits, emergency services, and local security assets.

Travel to Potential Physical-Threat Risk Areas

Personnel en route to potential physical-threat risk areas (as identified by the Office of the Assistant Secretary of Defense for Stability

Operations and Low-Intensity Conflict) should attend one of the following courses:

- The Dynamics of International Terrorism Course conducted at the U.S. Air Force Special Operations School at Hurlburt Air Force Base, Florida. During this one-week course, personnel will receive lectures on threats by region (Europe, Middle East, Latin America, Asia/Pacific, and Africa), the history and psychology of terrorism, personnel combating terrorism measures (vehicle, personal, airline, and physical security), and hostage survival.
- A Regional Orientation Course (Middle East, Latin America, Asia/Pacific, and Africa) at the U.S. Air Force Special Operations School at Hurlburt Air Force Base, Florida. This one-week course offers personnel instruction in cultural, political/military, and individual security factors associated with the region.

Installation security personnel may also receive the above training if they have completed the Antiterrorism Instructor Qualification Course at Fort Bragg, North Carolina.

Deployment and Redeployment

Deployments and redeployment phases of each mission are commonly the times when an element is most vulnerable. Commanders need to place a deliberate emphasis on protection.

Outbound CA forces can mitigate risks during transitions by—

- Maintaining situational awareness throughout redeployment operations.
- Providing after-action reports, a cultural events calendar, and enemy TTP to incoming forces.
- Reevaluating effectiveness of countermeasures.

Inbound CA forces can mitigate risks associated with transitions by—

- Conducting a predeployment site survey.
- Exercising increased alertness during transition operations while the unit acclimatizes to the new operational environment.

- Employing CRM.
- Posturing to deter possible hostile intentions.
- Ensuring ROE and/or ROF.
- Ensuring all assigned personnel have an updated Isolated Personnel Report.

Force Level

CA Soldiers enhance protection in any operation by conducting normal CAO and civil-military operations. This means they—

- Circulate among the populace.
- Establish rapport with ordinary citizens, key leaders, and representatives of intergovernmental organizations and non-governmental organizations.
- Conduct continuous deliberate assessments.
- Conduct civil reconnaissance.
- Provide input to all-source analysis centers on conditions, attitudes, and intentions of the populace.
- Determine the attitude of the local populace—
  - Toward the HN government.
  - Toward U.S. presence.
  - Toward enemy activities within the area of operations.
  - Toward general health and well-being.
- Determine the socioeconomic profile:
  - Ratio of private, public, and commercial properties.
  - Infant mortality rate.
- Monitor local news, radio, and other media.
- Develop emergency plan of action (evasion plan of action).
- Establish theater-specific significant activities and map accordingly.
- Maintain cultural events calendar.

Considerations during CAO include the following:

- Send situational reports regularly.
- Monitor weather conditions.

- Whenever possible, use U.S.-controlled facilities.
- Develop and implement primary, alternate, contingency, and emergency plans.
- Monitor weather conditions:
  - Moon charts.
  - Tide charts.
  - Weather patterns.

A training regimen for local national interpreters includes the following:

- Discourage VIP treatment.
- Vet all employees.
- Maintain situational awareness.
- Know the operational environment.
- Conduct deliberate civil reconnaissance.
- Maintain cultural events calendar.

Protection can be significantly improved with the proper mix of intelligence and information-gathering. Because civil information management is a core task of CAO, CA Soldiers must be sure to share their observations with the intelligence community. It is critical, however, that CA Soldiers do not misrepresent themselves as gatherers of intelligence.

INTEGRATING PROTECTION IN PLANNING USING RISK MANAGEMENT

This section focuses on integrating protection in the planning process by deliberately using risk management. The Army prescribes the use of the CRM process as the primary decision-making tool for identifying hazards and controlling risks across the full spectrum of Army missions, functions, and activities (Figure 7, page 28).

The CRM process should be applied to all forms of planning (Figure 8, page 28). Creating a habitual pattern within the planning process will only serve to improve the mission capability of both the force and equipment.

RISK ASSESSMENT MATRIX						
		Probability				
Severity		Frequent A	Likely B	Occasional C	Seldom D	Unlikely E
Catastrophic	I	E	E	H	H	M
Critical	II	E	H	H	M	L
Marginal	III	H	M	M	L	L
Negligible	IV	M	L	L	L	L
E = Extremely High		H = High		M =Moderate		L = Low

Figure 7. Composite Risk Management matrix

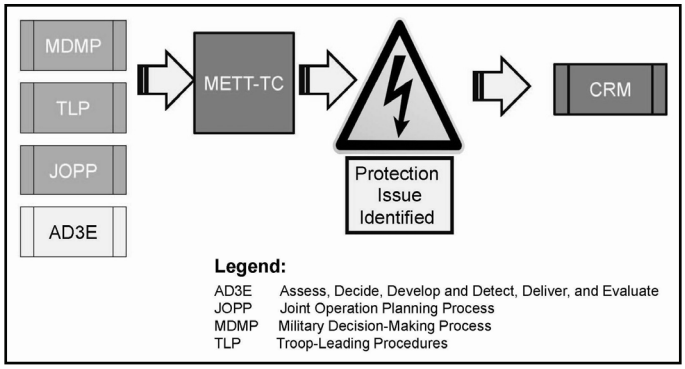


Figure 8. When to apply Composite Risk Management

CRM is a decision-making process used to mitigate risks associated with all hazards that have the potential to injure or kill personnel, damage or destroy equipment, or otherwise impact mission effectiveness. This tool assists the commander, leader, or individual in identifying, assessing, and controlling risks in order to make informed decisions that balance risk costs (losses) against mission benefits (potential gains). In the past, the Army separated risks into two categories: tactical risk and accident risk. While these two areas

of concern remain, the primary premise of CRM is that it does not matter where or how the loss occurs, the result is the same—decreased combat power or mission effectiveness. The guiding principles of CRM are as follows:

- *Integrate CRM into all phases of missions and operations*. Effective CRM requires that the process be integrated into all phases of mission or operational planning, preparation, execution, and recovery.
- *Make risk decisions at the appropriate level*. As a decision-making tool, CRM is only effective when the information is passed to the appropriate level of command for decision. Commanders are required to establish and publish approval authority for decision making. This may be a separate policy, specifically addressed in regulatory guidance, or addressed in the commander's training guidance. Approval authority for risk decision making is usually based on guidance from higher headquarters.
- *Accept no unnecessary risk*. Accept no level of risk unless the potential gain or benefit outweighs the potential loss.
- *Apply the process cyclically and continuously*. CRM is a continuous process applied across the full spectrum of Army training and operations, individual and collective day-to-day activities and events, and base operations functions. It is a cyclic process that is used to continuously identify and assess hazards, develop and implement controls, and evaluate outcomes.
- *Do not be risk-averse*. Identify and control the hazards; complete the mission.

Assess and Understand the Environment

The nature of the operational environment will have an obvious impact in planning to mitigate risks. The operational environment can be characterized by the degree of control the HN forces have to support and assist the operation. Regardless of the operational environment, protection of the force will remain of paramount importance. Figure 9, page 30, depicts the operational environment.

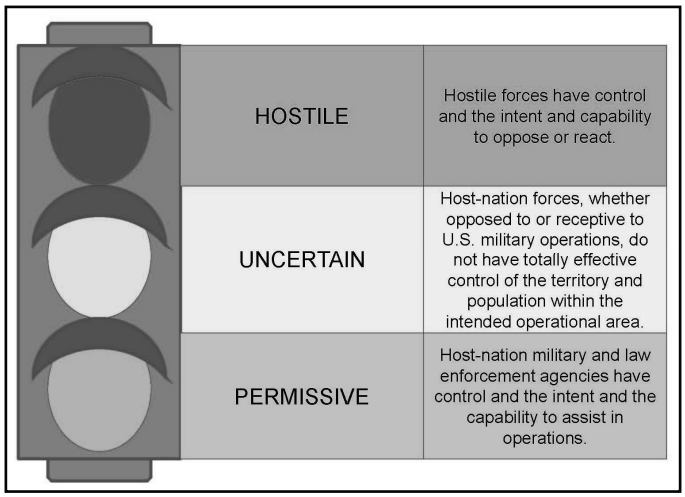


Figure 9. The operational environment

Identify Hazards and Threats to Determine Vulnerabilities

Threats are nation-states, organizations, people, groups, conditions, or natural phenomena able to damage or destroy life, vital resources, or institutions. Hazards are conditions with the potential to cause injury, illness, or death to personnel; damage to or loss of equipment or property; or mission degradation. Both threats and hazards have the potential to decrease combat power and the operational effectiveness of the force. Determining vulnerability will assist in the CRM process.

Determine Threat Types and Factors

This determination continues to assist and fuel the CRM process with information needed to develop countermeasures. A comprehensive picture of the threats will begin to take shape as the planner looks at the five forms of protection.

Develop Countermeasures

At this point in the CRM process, countermeasures begin to take shape. Countermeasures are those measures taken by a unit or individual to counter a specific threat at a specific time and place. Taking many forms, countermeasures mitigate threat-based risks and hazard-based risks. They include specialized procedures, personal equipment, unit or team equipment, facilities, and training. They may require reorganization of land use, reorientation of roadways, security improvements to installation entries, and improvements to existing structures and the surrounding site area. They may also require the creation of specialized elements that are task-organized to mitigate threats, respond to threats, and recover from the aftermath of threats.

Implement Countermeasures

Implementation of countermeasures must occur as soon as possible after identification of a threat. The least costly, and often the most effective, protection measures are those incorporated during the planning phase. Implementing appropriate protection measures at the planning stage can preclude the need for piecemeal and costly security enhancements later.

CA Soldiers must remember that countermeasures are most effective when—

- Endorsed by the commander.
- Understood by all participants.
- War-gamed.
- Written into operational and contingency plans.
- Resourced.
- Exercised or rehearsed.

Note: Failure to achieve any of these reduces the chance a countermeasure will succeed.

Evaluate Effectiveness of the Countermeasures

Over time, threats change as situations change. Countermeasures that may have been effective one day may no longer be effective the next

day. As CA Soldiers conduct continuous assessments, they reevaluate the threat and the countermeasures arrayed against the threat. They develop new countermeasures as old ones are determined to be no longer effective. As before, CA Soldiers should follow the six points mentioned above to ensure the new countermeasure is effective. See Figure 10 to follow the process identified above.

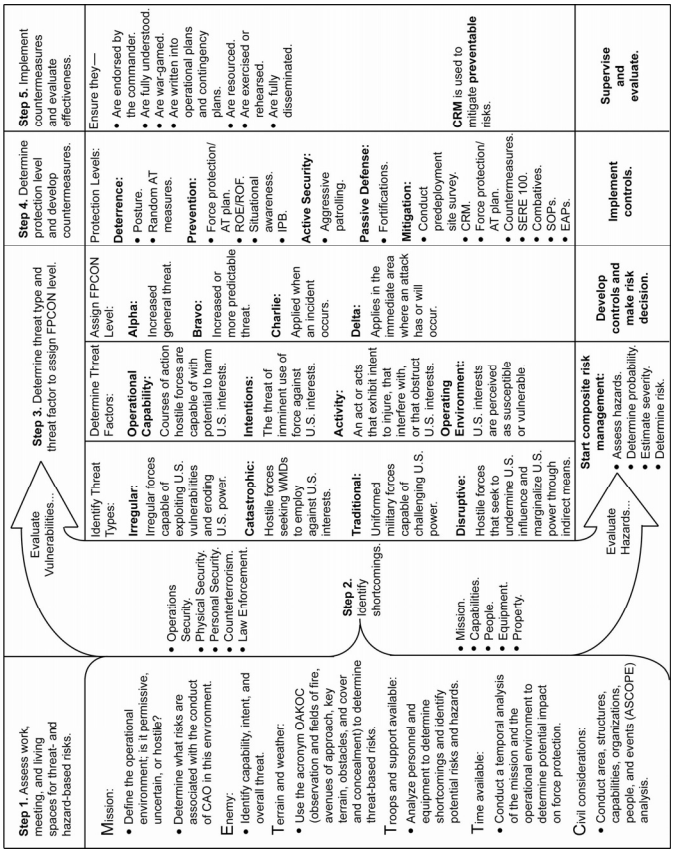


Figure 10. Planning and the CRM process

FORCE PROTECTION CONDITIONS AND THREAT LEVELS

Threat levels are developed by intelligence staff officers and should be used as one source of information in determining the appropriate force protection condition (FPCON) for a command, installation, facility, area, or unit. Such assessments will be based on the standardized Joint Service Criteria promulgated by DOD and Joint Service Criteria. The following sections are tailored to protection considerations for CA elements; Appendix B of Army Regulation 525-13 provides an overview that has recommendations for the entire DOD.

The Force Protection Conditions System

The FPCON system discussed here is mandated in DODD 2000.12, *DOD Antiterrorism Program*, and Department of Defense Instruction (DODI) 2000.16, *DOD Antiterrorism (AT) Standards*. They describe progressive levels of security measures for implementation in response to threats to U.S. Army personnel, information, and critical resources. The FPCON system is the foundation of all AT plans and orders. AT plans and orders must be constructed to address the threat assessment and implement the measures described in this section. The measures listed below are based on the DOD measures located in DODI 2000.16, with additional Army-common implementing guidance. When producing plans, local commanders must further refine this guidance into more specific instructions in order to meet the unique requirements of the specific location. The FPCON system may have limited application to Army elements that are tenants on installations, facilities, or buildings that are not controlled by U.S. military commanders or DOD civilians exercising equivalent authority. Still, Army commanders of such tenant elements should execute the FPCON measures that do not involve installation-level actions, at least to a limited degree.

There are five FPCONs that prescribe the minimum countermeasures an installation, unit, or facility will conduct in order to address the threats identified. It may be necessary to implement certain measures from higher FPCON levels resulting from intelligence received or as

a deterrent. At FPCON Alpha through Charlie, commanders will implement selected measures from higher FPCONs as a part of random AT measures. At any FPCON, commanders may implement any measures they deem appropriate from any higher FPCON.

An AT plan, with a complete listing of site-specific AT security measures linked to a FPCON, will be classified at a minimum as Confidential. When separated from the AT plan, site-specific AT security measures and FPCONs should be handled as For Official Use Only (FOUO). Figure 11 outlines the general guidelines of each FPCON level.

Normal	Alpha	Bravo	Charlie	Delta
• General global threat. • Routine security posture. • Access control at all DOD installations and facilities. • Minimum FPCON for U.S. Army commands.	• Increased general threat. • Nature and extent are unpredictable. • Must be capable of being maintained indefinitely.	• Increased or more predictable threat. • Prolonged periods at this level may affect operational capability and civil-military relationships .	• Applies when an incident occurs, **or** • Intelligence received indicating some form of terrorist action, **or** • Targeted personnel or facilities likely. • Prolonged periods at this level may create hardship and affect activities of the unit and personnel.	• Applies in the immediate area where an attack has occurred, **or** • When intelligence has been received that terrorist action is imminent. • Usually declared as a localized condition. • Not intended to be sustained for an extended duration.

Figure 11. Force protection condition descriptions

Note: There are different levels (steps) of implementation within each FPCON. The specific nature of implementation for each FPCON will not be discussed in this GTA because the classification is FOUO. However it can be obtained in AR 525-13, Appendix B. Area of responsibility-specific guidance is available from the staff of the combatant commander. This information is usually considered FOUO and is accessible through the Secret Internet Protocol Router Network (SIPRNET).

Threat levels

The decision to implement a particular FPCON is a command decision that should be based on an assessment of the threat, vulnerability of personnel or facilities, criticality of personnel or facilities, availability of security resources, impact on operations and morale, damage control considerations, international relations, and the potential for U.S. Government actions to trigger a threat response. Frequently, information concerning threat groups is limited to general descriptions of their capabilities and intentions. Often, specific tactics and targets are not identified until it is too late to implement deterrent measures or until after an attack has taken place. For this reason, the absence of specific information concerning the immediate threat should not preclude implementing a higher FPCON and/or additional security measures when general information indicates an increased vulnerability or heightened risk to personnel or facilities.

Threat levels are developed by intelligence staff officers and should be used as one source of information in determining the appropriate FPCON for a command, installation, facility, area, or unit. Such assessments will be based on the standardized Joint Service Criteria promulgated by DOD and Joint Service Criteria.

Threat levels are determined by assessing the situation using the following four threat factors (Figure 12, page 36):

- *Operational capability*. The acquired, assessed, or demonstrated level of capability of a terrorist group to conduct terrorist attacks.
- *Intentions*. The stated desire or history of terrorist attacks against U.S. interests by a terrorist group.
- *Activity*. The actions a terrorist group is conducting and whether that activity is focused on serious preparations for an attack.
- *Operating environment*. The overall environment and how it influences the ability, opportunity, and motivation of a terrorist group to attack DOD interests in a given location.

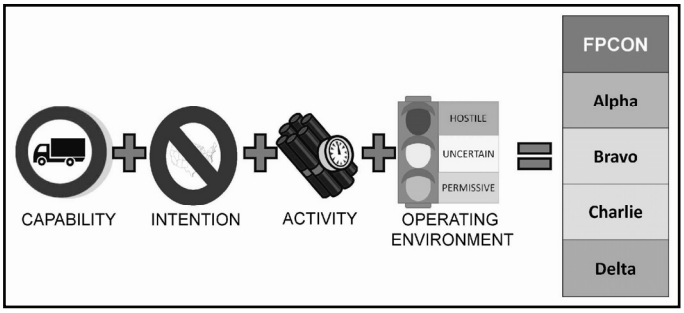


Figure 12. The four factors of a threat assessment

The following terminology will be used to describe the various threat levels to ensure uniformity throughout DOD:

- *High.* Anti-U.S. terrorists are operationally active and use large casualty-producing attacks as their preferred method of operation. The operating environment favors the terrorist.
- *Significant.* Anti-U.S. terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty-producing attacks as their preferred method but has limited operational activity. The operating environment is neutral.
- *Moderate.* Terrorists are present but there are no indications of anti-U.S. activity. The operating environment favors the HN/U.S.
- *Low.* No group is detected or the group activity is nonthreatening.

There is no automatic link between a threat level and a FPCON, although implementation of FPCON Delta suggests receipt of targeting information (intelligence that terrorist action against a specific location is likely). However, commanders should consider the threat level as a key element in determining the appropriate FPCON for their organizations.

DOD analytic agencies often differ in assigning threat levels to the same countries or areas. This occurs because analysts occasionally disagree concerning conclusions that could be drawn from available intelligence. Different threat levels may also be possible due to differing perspectives among organizations. For example, the Navy is concerned about ships, port areas, and areas frequented by their personnel. These areas may be quite different from areas of concern to Army commanders, even in the same country.

Explanation of Differences Between DOD and DOS Threat-Level Classification Systems

The DOD and DOS threat systems are two entirely different systems. They differ in purpose and use different methodologies to determine threat levels (Figure 13, page 38). The DOD analysis focuses strictly on the terrorism threat level, whereas the DOS analysis covers a larger array of four broad threat categories, only one of which—political violence—deals with the terrorism threat.

The DOD terrorism threat-level assessment considers only those indicators and warnings pertaining to terrorism threats. The DOD terrorism threat-level assessment is intended to declare a terrorism threat level for a particular country or area. DOD terrorism threat-level assessments are event driven and include information regarding the terrorist threat to DOD personnel, facilities, and materiel. The DOD terrorism threat-level assessment is used to inform DOD personnel and dependents under the AT program of a combatant commander, through the combatant commander's information channels.

The DOS threat assessment process evaluates all-source information relative to four broad threat categories and then develops the CTL for all active foreign service posts staffed by direct-hire U.S. personnel and DOD elements (either permanent or temporary-duty personnel), to include accompanying dependents and facilities that operate under the authority of a chief of mission. One of the primary purposes of the CTL is to aid in prioritizing posts for receipt of security resources; that is, equipment, temporary duty personnel, funding, and so on. The higher the threat level, the higher the priority for the

implementation of a standard set of security enhancements. A higher threat level immediately justifies the use of additional resources to attain the assigned standards for protection at that particular level of threat.

DOD	DOS
• Uses all-source analysis. • Is flexible (revised as indicators, warnings, and activities occur or change). • Uses four factors in analysis. • Has a four-step scale. • Issues threat-level assessments through the Defense Intelligence Agency (DIA) and combatant commanders. • Is not used to indicate the potential of a specific attack. DIA, the Services, or the combatant commanders issue formal specific warnings.	• Uses four composite threat list (CTL) threat categories. • Assigns a threat level to each category for a specific post (only one dealing with terrorism). • Disseminates its post-specific threat categories and levels in the CTL (semi-annually). • CTL is designed to aid DOS and diplomatic security in prioritizing overseas security programs. • Reflects an evaluation of a specific time period. • Has the capability to immediately warn of a specific threat . • Threat levels are the result of post inputs and coordination within the agencies at the national level.

Figure 13. How DOD and DOS classify threats

All commanders will ensure the DOD assessment is addressed as "DOD Terrorism Threat Assessment." The DOS assessment is addressed as "DOS Composite Threat List." Per DOD policy, when the combatant commander declares or changes a terrorism threat-level assessment for a particular country, the combatant commander will ensure that all DOD personnel and their dependents in the country for which he has AT responsibility are informed of this assessment. This includes informing the U.S. Defense Representative.

In locations where combatant commander forces are present in significant numbers, and there is a difference between the DOD terrorism threat-level assessment and the DOS CTL threat level (for the political violence category), DOD has directed that the following

procedure be used to provide clarification: DOD, through the Defense Intelligence Agency (DIA), will publish a message in coordination with DOS diplomatic security, noting the difference and providing an explanation for the difference. The message will be disseminated to the Services, combatant commanders, and to the appropriate U.S. Defense Representative. The combatant commander, through the U.S. Defense Representative, will have the responsibility to inform all DOD personnel, under chief of mission authority, of the information contained in the message. A higher DOD threat assessment will not require action by DOS to increase AT measures but is intended only to inform DOD personnel, under chief of mission authority, of DOD's assessment of the threat.

There is also a possibility of differences in terrorism threat-level assessments between DOD (DIA) and the combatant commanders for a particular country. The DIA, as the DOD lead agent, is responsible to clarify or resolve the differences. If there is a valid reason for the difference, the DIA will inform the DOS.

EXAMPLES OF MITIGATION AND COUNTERMEASURES

Figure 14, pages 40 through 44, outlines examples of CA mitigation.

Threat Identifi-cation	Threat Definition	Threat Level	Countermeasures
Areas			
Criminal Enclave	History of criminal violence against passers-through	High	**Mitigation:** Travel according to supported element's protection guidelines (2-man rule, 2-vehicle rule). Maintain situational awareness, weapons security, and radio contact with base unit. Identify patterns and methods of attack.
			Response: Follow mission ROE. Notify base unit. Identify characteristics, personalities, and methods used by hostiles.
			Recovery: Return to base. Report any compromised information or equipment. Debrief. Refine procedures immediately.
Structures			
Vulnerable Living Space	Living space adjacent to unsecured compound (hostile environment)	High	**Mitigation:** Negotiate for base security to regularly check the unsecured area with the owner of the adjacent compound. Maintain situational awareness and be alert. Plan to eventually move living space or secure the adjacent compound.
			Response: Follow mission ROE. Notify base unit. Defend until quick-reaction force arrives and threat is defeated. Treat wounded.
			Recovery: Treat wounded and MEDEVAC if necessary. Report any compromised information or equipment. Debrief. Refine procedures immediately. Upgrade defensive posture immediately.

Figure 14. Civil Affairs mitigation examples

Threat Identifi-cation	Threat Definition	Threat Level	Countermeasures
Capabilities			
Local Militia	Capability to organize and mobilize rapidly when provoked	Low	**Mitigation:** Identify what provokes the community to become hostile or to mobilize the militia. Train the force in how not to provoke the community. Establish positive relationship with militia, political, law enforcement, and other leaders. Engage the populace with normal CAO. Establish a plan that includes assistance from local authorities.
			Response: Follow approved response plans. Perform as liaison between supported unit and local authorities to help diffuse the situation. Maintain awareness of personal security situation. Report all information to base unit.
			Recovery: Conduct projects or other activities to reestablish or enhance a positive relationship between the force and the community if legitimizing this organization supports the overall mission. Refine response plans, as necessary.

Figure 14. Civil Affairs mitigation examples (continued)

Threat Identifi-cation	Threat Definition	Threat Level	Countermeasures
Organizations			
Terrorist Organization	History of improvised explosive device bombings against U.S. targets in region	Critical	**Mitigation:** Engage the populace with normal CAO. Travel according to supported unit force protection guidelines (2-man rule, 2-vehicle rule). Maintain situational awareness, weapons security, and radio contact with base unit. Observe indicators among populace, such as excessive interest in military activities, unexplained or suspicious cancellation of civilian activities, and unusual movement of vehicles, materials, or people. Report observations to appropriate channels.
			Response: Take a protective posture according to unit SOP. Notify base unit. Identify characteristics, personalities, and methods used by aggressors.
			Recovery: Assist investigators as liaison between supported unit and local authorities. Refine SOP, as necessary.

Figure 14. Civil Affairs mitigation examples (continued)

Threat Identifi-cation	Threat Definition	Threat Level	Countermeasures
People			
Thieves	Penetration of military facilities, vehicles, or personal space for equipment or information	Medium	**Mitigation:** Employ strict physical security, operations security, and personal security measures. Maintain situational awareness. Keep civilians no closer than one arm's distance from Soldiers.
			Response: Review law enforcement and higher headquarters' reporting SOP. Review ROE regarding apprehension use of force.
			Recovery: Prosecute thieves according to appropriate law. Publicize incident through information assets. Hold meeting with local authorities or public forum to discuss the implications of stealing equipment or information from military forces. Get commitment from local authorities to prevent future incidents.

Figure 14. Civil Affairs mitigation examples (continued)

Threat Identification	Threat Definition	Threat Level	Countermeasures
Events			
Planned Hostile Demonstrations	History of violence against U.S. or coalition personnel and facilities	Medium	**Mitigation:** Engage the populace with normal CAO. Travel according to supported unit force protection guidelines. Maintain situational awareness, weapons security, and radio contact with base unit. Observe indicators among populace. Report observations to appropriate channels.
			Response: Follow approved response plans. Perform as liaison between supported unit and local authorities to help diffuse the situation. Maintain awareness of personal security situation. Report all information to base unit.
			Recovery: Conduct projects or other activities to reestablish or enhance a positive relationship between the force and the community. Refine response plans, as necessary.

Figure 14. Civil Affairs mitigation examples (continued)

CA Soldiers must remember that countermeasures are most effective when—

- Endorsed by the commander.
- Understood by all participants.

- War-gamed.
- Written into operational and contingency plans.
- Resourced.
- Exercised or rehearsed.

Note: Failure to achieve any of these reduces the chance a countermeasure will succeed.

Implement Countermeasures

Implementation of countermeasures must occur as soon as possible after identification of a threat. The least costly, and often the most effective, protection measures are those incorporated during the planning phase. Implementing appropriate protection measures at the planning stage can preclude the need for piecemeal and costly security enhancements later.

Evaluate Effectiveness of the Countermeasures

Over time, threats change as situations change. Countermeasures that may have been effective one day may no longer be effective the next day. As CA Soldiers conduct continuous assessments, they reevaluate the threat and the countermeasures arrayed against the threat. They develop new countermeasures as old ones are determined to be no longer effective.

EVASION PLAN OF ACTION

The evasion plan of action example (Figure 15, pages 46 through 48) outlines the most common format. Information should be tailored to meet specific mission requirements.

EVASION PLAN OF ACTION

1. Situation:

a. Enemy situation:
   (1) Enemy disposition in probable evasion areas.
   (2) Enemy population control measures.
   (3) Enemy capabilities in response to elements in evasion.
   (4) Paramilitary security and police forces.
   (5) Analysis of indigenous population.

b. Friendly situation:
   (1) Joint special operations task force recovery assets available.
   (2) Allied forces in vicinity of probable evasion.
   (3) Sympathetic indigenous populations in vicinity of probable evasion.

c. Conditions for CA element to initiate evasion.

d. Conditions for the joint reception coordination center (JRCC) operational staff to launch recovery assets or drop resupply bundles:
   (1) Capabilities.
   (2) Limitations.

Example:

JRCC capabilities and procedures. After the JRCC has determined a need for recovery, the aircrews will launch in the next predetermined available window of darkness (most likely). The JRCC and the liaison officer/Air Force Special Tactics (AST) coordinate this mission for every 24-hour period (air tasking order cycle) generically in support of the joint special operations area, and the mission is cancelled daily if not needed. Example: Aircraft will service pickup zones (PZs)/designated areas for recovery (DARs) between 0230 and 0300 and service two sites (PZs) per night. The first attempt will be Pri and Alt PZ, night 2 will be Alt PZ and PZ 1, night 3 will be PZ 1 and PZ 2, and so on. This needs to be walked through in a rehearsal over a map with the AST.

Figure 15. Evasion plan of action example

2. Mission.

3. Execution:

a. Concept of the operation:

(1) Ingress or infiltration:

(a) Actions prior to and after the Military Demarcation Line (MDL).

(b) Actions during the first 48 hours.

(c) Actions after the first 48 hours.

(2) Egress or exfiltration:

(a) Actions prior to and after the egress decision line (EDL).

(b) Actions during the first 48 hours.

(c) Actions after the first 48 hours.

(3) Planned initial evasion point.

(4) Actions prior to the initial evasion point:

(a) Detachment complete.

(b) Split team/separated members.

(5) Actions after the initial evasion point:

(a) Detachment complete.

(b) Split team/separated members.

(6) Actions at planned recovery points.

(7) Selected areas for evasion and DARs, if applicable. Selected areas for evasion are normally designed by the DIA/Joint Personnel Recovery Agency. DARs are designated by the combatant commanders.

(8) Emergency resupply drop zones:

(a) Actions.

(b) Locations.

(c) Drop times.

(9) Planned routes or corridors.

(10) Final evasion destination.

(11) Border crossings:

(a) Locations and descriptions.

(b) Procedures.

Figure 15. Evasion plan of action example (continued)

(12) Actions upon capture or detainment (DIA/Joint Personnel Recovery Agency recommended resistance techniques for the specific region).
(13) Cover for status and cover for action.

b. Contact procedures and special instructions (SPINS):
(1) Unit code word.
(2) SPINS (all information below comes from the published SPINS in the air tasking order):
(a) Letter (as per SPINS, determined by day of insertion).
(b) Color (as per SPINS, determined by day of insertion).
(c) Word (as per SPINS, determined by day of insertion).
(d) Number (as per SPINS, determined by day of insertion).
(e) Duress word (as per SPINS, determined by day of insertion).
(f) Search and rescue dot (SARDOT).
(g) Recovery activation signal (RAS).
(h) Code word for mirror.
(i) Code word for strobe.
(j) Code word for pen-gun flares.
(k) Code word for smoke.
(l) Number/code word combination.
(m) Search and rescue numerical encoding grid (SARNEG).
(3) Evasion notification procedure from task force.

4. Service support:

a. Survival equipment and signaling devices accompanying the element.
b. Emergency resupply bundle location and drop times.

5. Command and signal:

a. Detachment chain of command.

Figure 15. Evasion plan of action example (continued)

ACRONYMS

AR	Army regulation
AT	antiterrorism
CA	Civil Affairs
CAO	Civil Affairs operations
CMOC	civil-military operations center
CRM	composite risk management
CTL	composite threat list
DA	Department of Army
DAR	designated area for recovery
DIA	Defense Intelligence Agency
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOS	Department of State
EAP	emergency action plan
FM	field manual
FOUO	For Official Use Only
FPCON	force protection condition
GTA	graphic training aid
HN	host nation
IPB	intelligence preparation of the battlefield
JP	joint publication
JRCC	joint reception coordination center
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
PZ	pickup zone

ROE	rules of engagement
ROF	rules of force
SERE	survival, evasion, resistance, and escape
SOP	standing operating procedure
SPINS	special instructions
USAJFKSWCS	United States Army John F. Kennedy Special Warfare Center and School
VIP	very important person
WMD	weapons of mass destruction

RECOMMENDED SOURCES

Army Publications

AR 25-55, *Department of the Army Freedom of Information Act Program*, 1 November 1997

AR 525-13, *Antiterrorism*, 11 September 2008

FM 2-0, *Intelligence*, 23 March 2010

FM 2-19.4, *Brigade Combat Team Intelligence Operations*, 25 November 2008

FM 2-22.2, *Counterintelligence*, 21 October 2009

FM 2-22.3, *Human Intelligence Collector Operations*, 6 September 2006

FM 2-91.4, *Intelligence Support to Urban Operations*, 20 March 2008

FM 2-91.6, *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection*, 10 October 2007

FM 3-0, *Operations*, 27 February 2008

FM 3-05.230, *Special Forces Tactical Facilities*, 8 February 2009

FM 3-05.401, *Civil Affairs Tactics, Techniques, and Procedures*, 5 July 2007

FM 3-19.30, *Physical Security*, 8 January 2001

FM 3-25.150, *Combatives*, 1 April 2009

FM 3-37, *Protection*, 30 September 2009

FM 5-0, *The Operations Process*, 26 March 2010

FM 5-19, *Composite Risk Management*, 21 August 2006

FMI 2-01, *Intelligence, Surveillance, and Reconnaissance (ISR) Synchronization*, 11 November 2008

FMI 2-01.301, *Specific Tactics, Techniques, and Procedures and Applications for Intelligence Preparation of the Battlefield*, 31 March 2009

FMI 2-22.9, *Open Source Intelligence*, 5 December 2006

FMI 3-35, *Army Deployment and Redeployment*, 21 April 2010

GTA 31-01-003, *Detachment Mission Planning Guide*, 1 March 2006

STP 21-1-SMCT, *Soldier's Manual of Common Tasks, Skill Level 1*, 18 June 2009

Department of Defense Publications

DODD 2000.12, *DOD Antiterrorism Program*, 18 August 2003

DODD 4500.54E, *DOD Foreign Clearance Program (FCP)*, 28 December 2009

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

Joint Publications

JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, 16 June 2009

JP 2-03, *Geospatial Intelligence Support to Joint Operations*, 22 March 2007

JP 3-0, *Joint Operations*, 17 September 2006

JP 3-06, *Joint Urban Operations*, 8 November 2009

JP 3-07.2, *Antiterrorism*, 14 April 2006

JP 3-08, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations*, 17 March 2006

JP 3-33, *Joint Task Force Headquarters*, 16 February 2007

JP 5-0, *Joint Operation Planning*, 26 December 2006

GTA 41-01-010