

Chapter 10

Security for Maintenance Operations

Maintenance organizations must seek to become integrated into base defense plans for the MACOMs to which they belong. In order to do this, they must exert influence over its AO. They must also continue to maintain sufficient mass and combat power to ensure overall force protection. Future operations in non-contiguous AOs will leave voids between the brigade AOs. These voids will be outside the direct control of any of the division's combat power. In its most benign form, this situation leaves potential avenues of approach to what (on the traditional, linear battlefield) is known as the division rear area. At its worst, it routinely exposes the division's critical C2, CS, and CSS assets to threats they cannot defend against, much less defeat. This situation also restricts the flow of maintenance support to the brigades.

The division Rear Area Operations Center (RAOC) clusters vulnerable C2, CS, and CSS assets for mutual protection and employs a suite of security measures to counter the negative effects of the porous nature of non-linear, non-contiguous operations. Reinforced by dedicated and/or on-call CS/combat arms security forces and supporting fires, these security measures, leveraged with Non-Line of Sight Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (NLOS C4ISR), enhanced SU, and the division's COP, mitigate the risk to the division's critical C2, CS, and CSS assets and allow the flow of maintenance support to the brigades. The type, number, and relationship to the Rear Operations Center (ROC) of CS or combat arms security forces and supporting fires are METT-TC dependent. If the threat to C2, CS, and CSS assets, and/or to the flow of sustainment to the brigades rises to unacceptable levels, the Division Commander can further mitigate the risks by reducing or eliminating the voids between the brigade AOs. Any success enjoyed by the division in protecting its C2, CS, and CSS assets and ensuring the flow of maintenance sustainment through the voids, is negated if EADs cannot regularly project sufficient maintenance into the division AO. Close coordination with EAD CSS providers and their security forces is necessary to keep maintenance support flowing to the division and to maintain a channel through which maintenance operations can be conducted. See FM 3-90, Appendix E for a detailed but generic discussion of rear area and base security.

THREAT EVALUATION AND INTEGRATION

10-1. Threat evaluation is a detailed study of the enemy forces. It considers threat organization, tactical doctrine, equipment, and support systems. Sustainment vehicle drivers and customers coming into the division area are valuable sources of information. This information is obtained through debriefings, spot reports, and procedures delineated in the units TOC SOP. Once the threat evaluation is complete, this information is integrated with weather and terrain factors. This determines how the threat is likely to operate in the sustainment area. Base Cluster Operations

Centers must ensure all Base Commanders understand the different threat levels and the associated actions. The following describes each level:

- Level I threats are those which can be defeated by base or base cluster self-defense measures. They normally involve the activities of agents, saboteurs, and terrorists.
- Level II threats are those beyond base or base cluster self-defense capabilities. Response forces, typically MPs with supporting fires, can defeat this threat. This threat normally involves sabotage, raid, ambush, and reconnaissance operations. Special purpose or unconventional forces and tactical reconnaissance units normally conduct these operations.
- A Tactical Combat Force (TCF) is required to defeat a Level III threat. Depending upon the situation, the TCF may be a maneuver unit or units designated for sustainment area security; all or a portion of the division's reserve; or a maneuver unit diverted from one of the brigades. If previously designated, the TCF would be immediately available to the RAOC, if not already under its C2; otherwise, the TCF would be directed to defeat the threat by the TAC CP. Level III threats normally involve:
 - Heliborne operations.
 - Airborne operations.
 - Penetration by enemy forces from the main battle area.
 - Ground force deliberate operations (for example, operational maneuver groups with a linkup of smaller airborne and assault units).
 - Infiltration operations.

10-2. Receiving early warning of pending enemy actions gives the Base or Base Cluster Commander time to react to threats. Security measures vary with enemy threat, forces available, and other factors. All-around security is also essential. In order to gauge the threat and apply the appropriate security measures, the Base/Base Cluster Commanders must achieve and maintain SU of the division's COP. Any of the following could also warn of pending threat actions:

- Outposts.
- Patrols.
- Military police.
- Ground surveillance and counter-fire radars.
- The local populace.
- HN intelligence.
- Military dogs.
- Air reconnaissance and surveillance.
- Civilian informants.
- Actions of indigenous personnel near the base.

- Transportation missions.
- LOGPAC deliveries.

10-3. Collecting, collating, and disseminating reports, information, and data received from the above sources enhance SU within the sustainment area and larger battlespace, and add to the COP. Achieving SU of the COP by the application of analysis and judgment allows commanders at all levels to assume the appropriate protective posture and allocate scarce resources to countering threats.

BASES AND BASE CLUSTERS

10-4. A base is a unit or multi-unit position with a definite perimeter. The commander, through the operations officer, determines the position of the base in conjunction with the RAOC. The RAOC is collocated with the division sustainment CP under the overall supervision of the Assistant Division Commander (Support) (ADC(S)). The RAOC coordinates and manages the security of bases and base clusters in the division's sustainment area. If the sustainment CP is operating in the intermediate staging base (ISB), the RAOC collocates with the DISCOM CP and provides C2 for rear area security, fires, and terrain management in the DSA. When the sustainment CP operates outside the AO, a DISCOM Company constitutes a base. The Base Commander is normally the senior unit commander present. Selection of the Base Commander should take into consideration not only rank, but also branch and experience. Base clusters contain several bases grouped together to enhance security and mission accomplishment. A base cluster does not normally have a defined perimeter or established access point(s). Base clusters rely on mutual support among bases for protection. Mutual support is achieved through interlocking fires, integrated patrol and surveillance plans, and use of coordinated reaction forces.

10-5. The Base Cluster Commander must designate the personnel in the reaction force and ensure they have sufficient weapons, mobility, and communications. Failure of communications between Base/Unit Commanders can cause friendly fire casualties. They must also be trained to react quickly and appropriately. The base cluster will normally include units located in the support group area or DSA. EAD logistics units, such as maintenance/ammunition supply points, may be located at isolated locations within the sustainment area. These units either operate as separate bases or are assigned to a base cluster by the RAOC. In either case, EAD CSS units must come to the division with sufficient capability to ensure they do not become liabilities to the division's sustainment area defensive operations.

10-6. The Brigade Support Battalion Commander is normally the Base Cluster Commander for units in the BSA. The Base Cluster Commander establishes a Base Cluster Operations Center (BCOC) with assets primarily from the S2/3 section. The BCOC provides the command and control to plan, coordinate, and supervise base cluster operations. The BCOC interfaces with the RAOC on terrain management, movement requirements, and security operations. The BCOC positions units assigned to the cluster, into bases and it designates Base Commanders. The RAOC assigns divisional and non-divisional units in the sustainment area to base clusters or independent bases. The Base Cluster Commander is responsible for integrating Base Defense Plans into a Base Cluster Defense Plan.

SITE SELECTION

10-7. Placing CSS and maintenance units and operations usually requires the balancing of several competing criteria. Ideally, criteria relating to technical requirements (such as dimensions, internal and external routes, proximity to a water supply, availability of hardstand, and so on) will predominate, but frequently other criteria intrude. No matter how ideal the site may be for a particular unit or an operation's technical requirements, if it interferes with the overall scheme of maneuver, is inaccessible, or is indefensible, select another site. Some sites, because of their overall importance to the scheme of maneuver or area security must be occupied. This is to either ensure access by friendly forces or to deny them to hostile forces. This challenge is to select the best fit for the site and ensure it is tied into the overall scheme of bases and base clusters. However, some sites will be unusable for political, cultural, or religious reasons; or because of agreements with the HN and/or friendly forces. This challenge is to ensure these sites do not create gaps in the overall area security scheme or weaken the integrity of nearby bases and base clusters.

SITE SELECTION IN A MILITARY OPERATIONS IN URBAN TERRAIN ENVIRONMENT

10-8. The following are some factors which should be considered when selecting a maintenance operations site in urban terrain:

- **MSR Access.** Avoid sites with only one way to access the MSR(s), especially if the access way is congested or forms a good ambush site. Multiple access ways to the MSR(s) contribute to OPSEC and complicate threat attempts to interdict maintenance activities, whether by civil disturbance or ambush.
- **Space and Facilities.** Select sites with sufficient space for the efficient operation of the unit(s) occupying them. However, the space should not be any larger than necessary to avoid needlessly increasing the perimeter to be secured. Consider conducting intermittent activities outside of the perimeter. Compare the resources needed for occasional activity security against the need for additional full time point security for a larger site.
- **Features.** The following are features that enhance security and force protection:
 - Fences, hedges, walls, and buildings aid in crowd and access control. They can also provide concealment. However, do not assume that a fence or hedge will hold back a crowd or that a wall will stop any particular caliber fire or offer blast or fragmentation protection. Cover will stop a bullet, concealment will not. Imposing iron fencing may be entirely ornamental and flimsily attached to its supports. Many modern structures, particularly industrial shell buildings, are constructed of lightweight materials over a steel frame, offering little more than a weather-tight environment.

- Parking lots, wide streets, and other open spaces provide separation from neighboring activity and increase the effectiveness of crew-served weapons, observation posts, and night observation devices.
- Absence of nearby tall trees, buildings, towers, and other structures that can be used as threat observation posts or firing positions into the site.
- Absence of sewers, storm drains, subways, and other subterranean passageways under the site. Where these features are unavoidable, steps commensurate with the threat and time available must be taken. At a minimum, the locations of manholes and other access ways to the surface must be located, observed, and covered by fires. To prevent infiltration into the site, manhole covers and other surface access ways should be welded shut or blocked. To prevent subterranean passageways under the site from being used for information gathering or to mine the site, they must be physically blocked before they penetrate the perimeter or they must be occupied and integrated into the Site Security and Defense Plan.

RISK ASSESSMENT AND MANAGEMENT

10-9. While threat evaluation and proper positioning of units and activities are key elements of force protection, they are part of a larger continuum, risk management. Conserving the austere CSS capability of the maintenance unit, particularly its maintenance capability, is critical to the division's capability to conduct sustained operations. Loss of personnel and equipment, whether they are caused by enemy action or accident, that are vital to the task of sustaining the brigade's and division's troops, threaten the division's capabilities. Threats to mission accomplishment that are layered on top of the actions of hostile forces and the local indigenous population include the following:

- Fatigue.
- Distraction.
- Inattention.
- Confusion.
- The failure to integrate new personnel into unit routines.

10-10. Failure to consider the totality of risk and take appropriate measures invites disaster. See FM 100-14 for guidance on the fundamentals, process, and implementation of risk management as an integral part of mission planning and execution.

REAR AREA SECURITY OPERATIONS

10-11. Sustainment (including maintenance) unit area defensive operations are actions taken by all units to secure and sustain the supported organization (primarily the division). These actions are taken in a concerted effort. They include those actions necessary to neutralize or defeat enemy operations in the division sustainment area (DSA). Perimeter security, active

intelligence gathering operations (such as interviewing convoy drivers and noise and light discipline) are necessary to neutralize or defeat enemy operations. The objectives are as follows:

- To secure the area.
- To prevent or reduce enemy interference with command, control, and communication.
- To provide unimpeded movement of friendly units throughout the sustainment area.
- To provide area damage control before, during, and after an attack or incident.

SECURITY

10-12. Viewed functionally, the three types of security requirements are point, route, and activity. Each of these are described below:

- Point security requirements are stationary, long term, or defensive in nature. They are related to actions in and around CS/CSS units and HQ that have a limited ability to secure them against Threat Levels I-III (these levels will be discussed later on in the chapter).
- Route security requirements are related to actions in and around the division's MSRs. They may be temporary or long term, and either offensive or defensive in nature.
- Activity security requirements are temporary in nature. They may occur anywhere within the supported unit's AO regardless of the nature of that AO contiguous or non-contiguous. They may also be either offensive or defensive in nature.

10-13. To enhance sustainment operations, DISCOM/maintenance elements, as well as C2, CS, and EAD CSS assets operating within the division AO, are often grouped together. Elements are grouped into bases for security and base clusters for mutual support. The RAOC, under the supervision of the officer in charge of the sustainment CP (normally the ADC(S)), is ultimately responsible for the composition of bases and base clusters in the division rear. A mix of weapon systems, planning and supervisory personnel, and varied communications assets are required to form a viable base. The DISCOM S2/3 sections coordinate with the RAOC on grouping of DISCOM units in the sustainment area. Similarly, the Brigade Support Battalion S2s/S3s coordinate with the brigades for planning security operations.

10-14. Base Commanders are responsible for point security of their bases and for the direct fire area of influence surrounding their base. Targets identified and acquired outside that area are assigned to a maneuver or fire support unit. Base Cluster Commanders are responsible for coordinating the activities and fires of their constituent bases to enhance mutual security. Base/base clusters are capable of defeating Level I threats. However, they require additional forces to defeat Level II or III threats. Base Cluster Commanders are responsible for constituting and employing Quick Reaction Forces (QRFs) to delay Level II and III threats until CS or CA elements can be brought to bear to defeat the threat. Support units will typically use the

lowest possible protective posture (PP) in order to maximize available CSS capacity. The support units increase and adjust PP in accordance with the threat. The following are examples of protective postures:

- **PP1:** Crew-served weapons are emplaced and manned; hasty individual fighting position is prepared but not manned; QRF designated; checkpoints established at vehicular points of egress, no perimeter wire.
- **PP2:** Same as above with QRF assembled and ready to fight.
- **PP3:** Same as above with individual hasty fighting positions manned.

NOTE: Perimeter wire added to any protective posture in accordance with METT-TC, fighting positions improved as time permits.

10-15. As the threat pushes bases to higher PPs, the ability of their constituent units to provide CSS drops off sharply. If the threat level remains high for too long, external assistance in maintaining the appropriate PP will be required so logistics units can resume sustainment missions. Maintenance units conduct local security to help protect themselves from enemy actions. They use the physical security measures outlined in FM 3-19.30 to assist their local security efforts. These security measures include the following:

- Use security elements to the front, rear, and, when required, on flanks of convoys. Flank convoys would be required when missions could not be cancelled or altered, mission deemed necessary. Through command channels, the unit responsible for the convoy would request combat force protection or MP escort.
- Use listening and observation posts in bivouac areas.
- Identify probable avenues of approach and cover them with fields of fire.
- Employ obstacles to impede the enemy.
- Use challenge and passwords.
- Use early warning devices.

10-16. Positioning unit equipment and sections is the single most important factor in a unit's ability to provide adequate security while conducting maintenance for supported units. The point defense, with the fullest possible use of unit dispersion, has evolved as the most practical defense method. The concept is to disperse the unit and to emplace it by functional area. Only small areas are actively defended. Commanders at company level must place observation posts (Ops) and listening posts (LPs) on probable avenues of approach. Observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment are factors to be considered when placing Ops. By coordinating with adjacent units, commanders can implement an integrated warning plan that will lessen the impact on any one unit. Unattended ground sensors will further enhance OP and LP effectiveness. In areas where the populace is friendly, local law enforcement and government agencies can be valuable sources of information. Intelligence information can be evaluated for unit security.

SECURITY OF MAINTENANCE OPERATIONS

10-17. The porous nature of non-contiguous operations requires the use of heightened route and activity security measures to project maintenance operations (see Figure 10-1 for a comparison of contiguous and non-contiguous AOs). Faced with the combat power of the brigades and well secured bases in the sustainment area, an overmatched adversary will probably attempt to strike asymmetrically at a perceived weak link (sustainment operations traversing the voids between EAD, the sustainment area, and the brigades). To the extent possible, DISCOM and EAD CSS units exercising active force protection measures while conducting CSS operations contribute to route and activity security in the voids. However, there are practical limitations to their contributions due to lean unit designs and limited weapons systems and communications equipment. This is especially problematic where EAD CSS providers are concerned. EAD CSS units are generally designed for operations on a linear and contiguous battlefield where voids between the combat units are the exception rather than the rule. HN support equipment also tends to be commercial in nature and be operated by paramilitary personnel at best. These limitations notwithstanding, EAD must ensure sufficient security forces are present and employed to ensure the safe and timely delivery of maintenance operations into the division's AO. While ground convoys are less resource intensive, the threat level in the non-contiguous battlespace, OPTEMPO, and OPSEC considerations all contribute to the need for a capability of aerial distribution of sustainment into and throughout the division's AO. Regardless of their limitations, maintenance units can and must vigorously contribute to area and local security by employing all of the tools at their disposal. These tools include the COP; close coordination with all CSS providers, the supported units and any dedicated or on-call security forces; adherence to OPSEC; and the sound application of convoy and air delivery tactics, techniques, and procedures (TTPs).

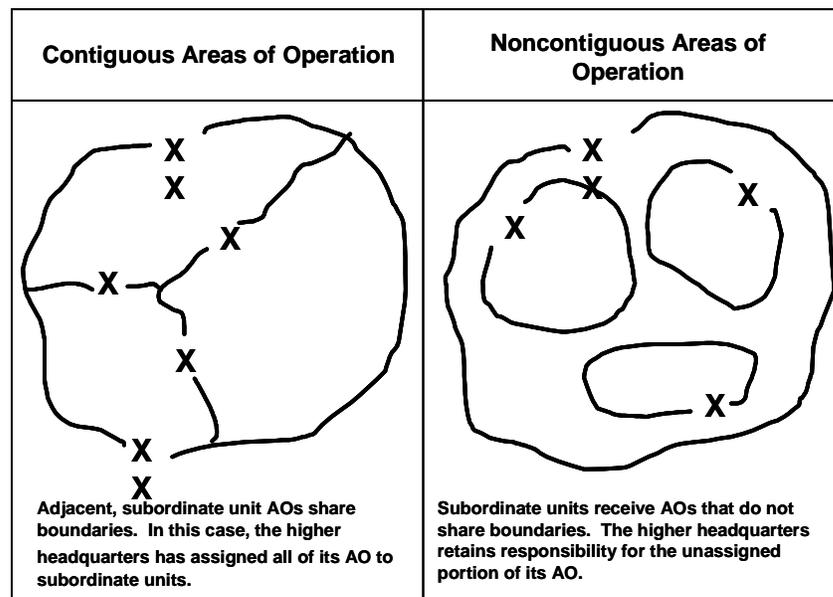


Figure 10-1. Areas of Operation

Using the Common Operational Picture

10-18. Information gathered from a host of sources (Ops, patrols, radars, manned and unmanned aerial sensors, informants, spot reports, and so on) feed the COP. The commander and his staff use the COP as the starting point of their analysis to select optimal times, routes, and methods for receiving and delivering maintenance support throughout their AO. They identify anticipated threats and plan countermeasures. Sharing the COP between the supported and supporting units is as important as sharing it within the supported unit.

Coordination

10-19. **With EAD CSS/Maintenance Providers.** Along with the supported organization's routes, times, and delivery methods are identified threat levels and security measures. Any dedicated and/or on-call security forces provided by the supported unit and all details of the hand-off of security responsibilities are also agreed upon.

10-20. **With the Brigades.** Routes, times, and delivery methods are identified and threat levels and security measures are identified. Any dedicated and/or on-call security support provided by the brigade and all details of the hand-off of security responsibilities are also agreed upon.

10-21. **With Dedicated/On-Call Security Forces.** The type and level of support is identified and link-up times and locations are agreed upon. Indirect fires are preplanned to cover probable ambush locations and air defense is coordinated as appropriate. All preplanned indirect fire points must be observable. Routes, times, and delivery methods are identified and threat levels and security measures are identified. All details of the hand-off of security responsibilities are also agreed upon, including the method of release or stand down of on-call support.

Operational Security

10-22. Avoid activities that signal upcoming events or, when unavoidable, reduce the threat's reaction time between the signal activity and the ensuing event. Vary convoy start times, routes, speeds, vehicle spacing, composition, and security hand-off locations. In other words, avoid patterns. Vary the frequency and order sustainment maintenance is pushed to the brigades. Keying resupply to actual consumption and planned OPTEMPO will aid with this. Vary the method used to push sustainment to the brigades. Inserting the occasional air delivery can mitigate the negative effect of a limited number of routes for convoy operations. Hide the nature of the cargo on vehicles. High pay-off cargos (ammunition, bulk fuel, and rations) are priority targets for destruction or hijacking and focus threat interest; anonymity diffuses it. Vary the locations requiring activity security (remote maintenance operations, ROM sites, FARPs, ATPs, landing zones, drop zones, and so on). Occupy them, as close to the time they are to be used as practicable; and, vacate them as soon afterwards as possible.

Convoy and Air Delivery TTPs

10-23. **Convoy Operations.** Coordinate the following with convoy participants:

- Start times.
- Routes.
- Speeds.
- Vehicle spacing.
- Security hand-off details with convoy participants.
- Dedicated and/or on-call security forces.
- Pre-planned and/or on-call indirect and air defense fires.
- Engineer counter-mine/obstacle support.
- Any elements whose AO will be crossed by the convoy.
- The element receiving the convoy.

These actions are performed for both the outbound and return convoys. Disperse priority targets (high pay-off cargos) throughout the convoy. Carefully tailor passive and active defensive measures to METT-TC and ensure all convoy personnel are briefed. Emphasize any changes in rules of engagement and emergency actions. Convoys, whether they originate from within the division AO or come from EAD, must be provided with sufficient communications equipment (radios, MTS, and FBCB2). They must also be provided crew-served weapons (machine guns and grenade launchers), and external security support to ensure their safe transit of the voids between EAD, the sustainment area, and the brigades. MP will habitually provide the preponderance of convoy escort security details in both the divisional and corps rear area. For more information on convoy security refer to Appendix E of FM 3-90.

10-24. **Airdrop.** Depending upon space available at the receiving unit, activity security may be required for all, or a portion, of the drop zone. To support "replace forward, fix rear," outgoing mail, personnel evacuation, and the recovery of airdrop equipment, airdrop operations require at least occasional supplemental ground convoy, airland, and/or helicopter/slingload operations. Depending upon the threat, airdrop operations may require supporting Suppression of Enemy Air Defense (SEAD) fires.

10-25. **Airland Delivery.** Where suitable airports/airfields/landing strips exist, airland operations are possible. However, securing a given facility for fixed wing aircraft use requires considerably more resources than needed if the same facility is used for rotary wing aircraft. The frequency and duration of fixed wing airland operations and relative threat level will determine whether security of the approach and depart zones is a point or activity requirement. To reduce the amount of time aircraft are on the ground, retrograde shipments must be pre-assembled and ready for loading once the inbound cargo has been discharged.

10-26. **Slingload Operations.** Depending upon space available and the relative locations of the CSS and helicopter units, supporting route and/or activity security operations may be required to support the out-load portion of the slingload. At the receiving unit, activity security may be required for all, or a portion, of the landing zone. Depending upon the threat, helicopter

slingload operations may require supporting SEAD fires in the vicinity of the landing zone and/or at critical points along the flight path. To reduce the amount of time aircraft are on the ground or required to loiter in the vicinity of the landing zone, retrograde shipments must be pre-assembled and ready for loading/slingloading as soon as the inbound cargo has been discharged. For more information on Airdrop refer to FM 4-20.41, FM 55-450-2, FM 90-4, FM 90-26, and FM 100-10-1.

MOUT OPERATIONS

Focus Attacks on Service Support and Unprotected Soldiers. Threat forces may prey on soldiers poorly trained in basic infantry skills. Ambushes may focus on these soldiers while they are conducting resupply operations or moving in poorly guarded convoys. Urban operations are characterized by the isolation of small groups and navigational challenges, and the threat may use the separation this creates to inflict maximum casualties even when there is no other direct military benefit from the action.

FM 7-30, C1, Paragraph J-4. b. (7)

10-27. The above quote may well be applicable anywhere in a non-linear, non-contiguous battlespace. However, it has particular importance for the DISCOM and maintenance operations in urban terrain. Desert terrain is characterized by a scarcity of features. Urban terrain presents an overabundance of features and adds the dimensions of subterranean and vertical elements. A small patch of urban terrain can easily consume most, if not all, of a CSS unit's personnel in establishing and securing a perimeter. Security factors to consider in selecting an urban location for CSS operations include the following:

- Accessibility by streets, sidewalks, and parking lots.
- Sewers, storm drains, and subways.
- Through the interiors of adjacent buildings.
- Overlooked by surrounding structures.

10-28. Occupying and operating from fixed facilities (such as warehouses, factories, and other large buildings) provide CSS/maintenance units with a number of real benefits. Some of these benefits include increased efficiencies, protection from inclement weather, and enhanced OPSEC. The negative trade-offs are overly concentrating critical assets and ending up with a position that may not be able to be secured, much less defended.

10-29. A significant characteristic that differentiates urban terrain from other types is population density. Whether from fear of the unknown, the desire to protect possessions, a lack of transportation, or simply because there is nowhere else to go, substantial urban populations tend to remain in place during times of crisis. During past events, urban centers act as magnets for displaced persons from other areas. However, more recent events have proven that displaced civilians will seek refuge where they believe sanctuary can be found. However, this may not always be in an urban environment. Large populations can inhibit friendly forces ability to perform their missions, even during support operations aimed at aiding that same population. Crowds and civil disturbances, whether they occur spontaneously or are instigated by agitators, can delay or disrupt logistics

operations. During stability operations, instigating civil disturbances can be an effective method employed by one or more of the competing factions seeking an advantage over rivals or to strike asymmetrically at friendly forces. Criminal activity directed at the local population (both crimes of violence and property crimes) could spill over to affect friendly forces.

CONVOY OPERATIONS IN THE MOUT ENVIRONMENT

10-30. Convoy operations in urban terrain can be particularly challenging. Navigating an urban landscape with topographic maps can be difficult under peacetime conditions. Even with first-rate street maps, navigating can become increasingly more difficult when the effects of civil disturbances, rioting, and combat damage alter the landscape. The nature of urban terrain favors snipers and ambushes while offering the convoy only one small advantage. This advantage is the potential of many different routes to choose from for any given operation. However, this leads back to the problem of navigation. During stability and support operations in which the threat tends toward congestion, civil disturbances, criminal activity, and occasional sniping, the use of multiple routes may be the preferred approach. Having multiple routes and the freedom of when and how often to use them leverages the division's SU of a COP, secure communications, and the ability to maintain operational security to select routes that bypass congestion and confound active attempts to interdict convoys. However, in offensive or defensive operations, the intensity and type of threat (mines, ambushes, indirect fires, and so forth) may dictate confining convoy operations to a limited number of routes, which can be secured and maintained with available forces.

10-31. The following will place considerable stress on maintenance operations designed to sustain the brigade combat teams:

- Reduced trafficability.
- Interdiction of the MSRs.
- The fragmentation of units into small, isolated groups (all typical of urban combat operations).

10-32. EAD and divisional maintenance vehicles may prove too thin-skinned to survive the task of delivering maintenance support far enough forward. Even in less hostile environments, the limitations of commercial pattern trucks and/or political considerations may prevent HN vehicles from reaching the desired maintenance points. In either case, MHE- and soldier-intensive transloading operations will result.

DESERT OPERATIONS

Navigating the Urban Landscape

On the surface, the urban landscapes encountered by US troops in Mogadishu, Somalia (1992-1994) and Russian troops in Grozny, Chechnya (1994-1996 and 1999-2000) seem profoundly different. Mogadishu epitomized the lowest tier of third world cities – some places warrens of low, rambling structures crowding narrow, dusty streets and others long stretches of roads, mostly devoid of structures – while Grozny was the prototypical Soviet-style city – downtown, a mixture of older, elegant buildings and newer, drab office buildings; the suburbs, ranks of similar 10- to 12-story apartment blocks lining broad avenues. Mogadishu had a small seaport, an airport, a soccer stadium and only a handful of industrial facilities – all in disrepair, as were its limited utility systems. Grozny, at least prior to December 1994, was a reasonably intact, modern city. It had a wide variety of industrial and commercial installations and functioning, large-scale utilities systems. Like most Soviet-era cities, Grozny suffered from a lack of re-investment to maintain and upgrade its

systems, but, by and large, everything functioned.

Despite these differences, the remarkably similar feature these two cities shared, indeed the tie that binds all cities together for forces attempting military operations in them, is the tremendous difficulty they present to the task of getting from point “A” to point “B” (especially when the indigenous population or an opposing force is actively working to thwart that effort). Simply knowing where “A” and “B” are (no matter how precisely) and dispatching convoys along likely routes between them are not guarantees of success. Rather, getting and using real time knowledge and understanding of route conditions, threat/local populace activity and their likely intentions, and applying weapons, equipment, tactics, techniques and procedures appropriate to the situation are keys to success.

10-33. Desert operations, including unique force protection issues, present a host of operational challenges for CSS units. Because of the openness of desert terrain, site selection for CSS units must place concealment and disguise as high priorities when selecting a site. This is due to the openness of desert terrain and the potential ability for the threat to possess (or has access to the products of) aerial- or space-based observation platforms. CSS units must conform their operations to the local ground patterns. They must also avoid regular spacing, straight lines, right angles, and vertical stacks; all of which signal human activity and are visible for considerable distances. Whenever possible, select sites along and confine vehicle operations to existing trails or tracks to avoid telegraphing the existence of new or increased activity. The openness of desert terrain provides plenty of opportunities to employ crew-served weapons out to their maximum effective ranges and beyond. However, this can be a mixed blessing. Frequently, a base will find that most, if not all, of its perimeter is on a high-speed avenue of approach. This will give its limited crew-served weapons overly wide sectors to cover and diluting their effectiveness. Careful coordination between the bases in a base cluster and the preparation of multiple firing locations at each base can mitigate this and allow fires to be massed when and where necessary.

FRATRICIDE AVOIDANCE

Commanders seek to lower the probability of fratricide without discouraging boldness and audacity.

FM 3-0, Paragraph 4-27

10-34. Fratricide avoidance (a component of the element of combat power, protection) involves the application of measures to ensure the affects of friendly fires are not visited upon friendly forces. Fast-paced, round-the-clock operations involving long-range, high-lethality weapons systems on a non-linear, non-contiguous battlefield call for active measures such as:

- Positive weapons control.
- Disciplined operational procedures coupled with robust passive measures (for example, well-understood identification measures for friendly personnel and equipment).

Conditions that contribute to fratricide can vary with terrain as evidenced by the following discussion of the desert and MOUT environments, which occupy opposite extremes of the terrain spectrum.

Fratricide Avoidance in the Desert Environment

10-35. The ability to fire out to and beyond weapons maximum effective range increases the possibility of fratricide, both upon friendly elements approaching a base cluster and between bases in the same cluster. This situation arises because, unimpeded by terrain, vegetation, and man-made objects, weapons fire extends far beyond the distance at which positive identification of friend or foe can be made (especially at night and other periods of reduced visibility). The featureless terrain also contributes to disorientation and inability to gauge distance. Limiting access to base clusters to specified routes, positive identification measures, appropriate spacing of bases, and fire control measures (such as range cards and limit stakes) all contribute to avoiding fratricide.

Fratricide Avoidance in the MOUT Environment

10-36. Fratricide prevention is an important consideration in MOUT for quite the opposite reason than it is in dessert terrain. The density of urban terrain features, including tall structures and subterranean passages, contributes to a convoluted forward line of own troops (FLOT). This, in turn, leads to sudden, close meetings of friendly and threat forces, as well as potentially unexpected friendly-to-friendly encounters. Particular attention must be paid to the coordination of recognition signals, arrival times, and routes for DISCOM and EAD sustainment convoys entering and moving within the brigade areas. Since meeting engagements in urban terrain tend to occur at close quarters, survival dictates immediate and decisive action to carry the day.

10-37. This can lead to a “shoot first, ask questions later” mindset. This mindset must be countered by clear IFF procedures and techniques to identify and stop “blue-on-blue” engagements. Unintended adverse effects of fires contribute to fratricide and collateral damage. Lethal fires, CAS, and artillery, are difficult to place where needed in denser, built-up area. Grenade launchers and mortars are generally better suited for MOUT environments. This is due to the close proximity of combatants and many

vertical obstacles are problematic for systems that deliver munitions with a low-angle trajectory and have dispersion. Short range, high trajectory fires are useful for hitting targets in yards, narrow streets, alleyways, and the upper floors of multi-story buildings. Indirect fires of any type tend to be less effective against targets on the intermediate, lower, and below ground floors of buildings.

10-38. Against these targets, direct fires and/or assault are usually necessary to prevail, although indirect fires can be useful in obscuring threat observation of friendly operations or suppressing threat activity. Regardless of the type fires employed, the existence of hard, flat surfaces contributes to the production of secondary projectiles and ricochets, which can have undesired results. Engaging threat targets against a backdrop of urban landscape can also be disastrously counterproductive if friendly fire penetrates that backdrop and strikes friendly forces or non-combatants beyond. To mitigate these risks, the RAOC's and DISCOM's SU must include an appreciation of the effects of friendly and threat fires on surrounding urban landscape and the locations of nearby friendly forces and non-combatants so that fires can be employed to best counter the threat while reducing the risk of fratricide and collateral damage.

