FROM THE NTC:

Executing The Defensive Counterreconnaissance Fight

by Lieutenant Colonel (P) Chris Baggott

A successful defense depends on finding, targeting, destroying, or suppressing the enemy reconnaissance assets before they can report the unit's defensive positions.

FM 34-2-1

Security operations obtain information about the enemy and provide reaction time, maneuver space, and protection to the main body ... counterreconnaissance is an inherent task in all security operations.

FM 17-95

Counterreconnaissance is the sum of actions taken at all echelons to counter enemy reconnaissance and surveillance efforts through the depth of the area of operations. It is active and passive and includes combat action to destroy or repel enemy reconnaissance elements.

FM 17-95

Recent studies conducted by the Armor Center, TRADOC, and the RAND Corporation, as well as Combat Training Center (CTC) take-home packages, indicate that serious weaknesses exist in counterreconnaissance doctrine, organization, and training. There is a growing belief throughout the mechanized community that these weaknesses are solvable through a more focused reconnaissance and counterreconnaissance planning effort. Clearly, force-on-force results from the National Training Center (NTC) continue to be the catalyst behind these beliefs. This paper provides a conflicting opinion regarding procedures to resolve this perceived training shortfall. It emphasizes that security operations execution, discipline, and enforced standard operating procedures, vice increased planning or a revision of doctrine, will achieve required training standards.

A Typical NTC Battle and Synopsis:

Training Day (TD) 4, 1300 hours: 1st Brigade, 99th Division (BLUFOR) had just completed executing a movement to contact against the opposing force's (OPFOR) 32nd Guards Motorized Rifle Regiment (GMRR) in the NTC's central corridor. The brigade attack began at Hill 720 with movement oriented from east to west. Based on templated BLUFOR and OPFOR movement rates, it was anticipated that first contact would occur somewhere in the vicinity of Phase Line (PL) Red (vicinity Barstow Road). 1st Brigade reconnaissance forces identified the lead OPFOR motorized rifle brigade (MRB) formation approximately 20 kms west of PL Red (vicinity Crash Hill). The OPFOR's orientation focused at two predominant choke points (Brown and Debnum passes). The lead elements of both units gained contact at Hill 876. Although 1st Brigade fought tenaciously, the results were similar to many other NTC fights: a victorious OPFOR and a defeated 1st Brigade. Within minutes after the end of the battle, 1st Brigade was given a follow-on mission to conduct a defense in sector that included both the NTC's northern and central corridors. The 52nd Division (the NTC's notional higher headquarters) anticipated that the brigade would have approximately 36-40 hours to plan and prepare the defensive sector.

TD 4, 1700 hours: After a hasty mission and course-of-action analysis, a subsequent wargame, and leader's reconnaissance, the 1st Brigade commander issued guidance to his subordinate commanders. TF 1-2 (AR) would defend the central corridor while TF 3-4 (IN) (-) would defend the northern corridor. One armored team from TF 3-4 was designated the brigade reserve. Both task forces were responsible for counterreconnaissance operations in their designated sectors. Task force scout platoons were placed under the control of the brigade S2 and were positioned forward of the task forces with the mission of providing early warning of enemy reconnaissance forces prior to the maneuver battle, and to focus indirect fires during the battle.

TD 4, 2000 hours: TF 1-2 designated A Team (mech) as its counterreconnaissance force with a subsequent mission as the task force reserve. A Team established its counterreconnaissance positions along PL BLUE (Granite Pass to just west of Chod Hill). Fourteen combat systems were spread north to south along a frontage of approximately 10 kms (800-900 meters between vehicles). TF 3-4(-) also identified one mechanized infantry team (B Team) as its counterreconnaissance force, also with a subsequent task force reserve mission. The B Team (mech) commander positioned his forces along PL BLUE (vicinity Echo Valley from Granite Pass to Refrigerator Gap).

TD 6, 0600 hours: The 32 GMRR attacked. Both division and regimental reconnaissance forces had easily penetrated 1st Brigade's counterreconnaissance screen line during the previous two days. The OPFOR commander essentially had a 90-percent accurate read of the BLUFOR defenses. With limited forces to conduct the mission, the 1st Brigade had decided to economize his defensive preparation efforts along the north wall of the central corridor. Needless to say, the OPFOR commander fully understood the inherent weakness of the BLUFOR defense and attempted to exploit it. An MRB-size forward detachment (FD) was organized from available OPFOR assets and was given a terrain-oriented mission focused at Hills 876 and 780. Fundamental to this FD terrain objective was the implied task to fix (prevent BLUFOR maneuver against the regimental main body) BLUFOR forces in that proximity. Simultaneously, as the FD attacked in the south, the 32 GMRR main body attacked along the central corridor's north wall.

TD 6, 1000 hours: Change of Mission. The 1st Brigade defensive sector has been penetrated and two MRBs are consolidating on the OPFOR objective. The AAR will begin in six hours.

BATTLE ANALYSIS

OPFOR:

The success or failure of the OPFOR's attack against a defending enemy is always predicated upon the success of the reconnaissance effort or, to use a non-doctrinal term, the success of the OPFOR's "reconnaissance pull." Reconnaissance pull emphasizes identifying and exploiting enemy weakness. This reconnaissance technique determines movement routes suitable for maneuver through an analysis of enemy disposition and composition and "pulls" the main OPFOR attacking force along the path of least resistance. Generally speaking, the OPFOR will never be able to mass sufficient combat power in accordance with doctrinal norms to attack a typical BLUFOR defense. At a minimum, the OPFOR commander would expect to have an overall 3:1 superiority when attacking a prepared BLUFOR defense. More importantly, and key to the focus of OPFOR reconnaissance efforts, is that, at the point of penetration, the OPFOR expects to achieve a positional 9:1 force ratio advantage. The reality of the NTC is that, at best, numerical parity between competing forces (BLUFOR defense to OPFOR offense) has become the standard. Thus, to gain situational numerical superiority at the point of penetration, the OPFOR commander is forced to attack on a narrow front. From the above discussion, it is obvious that OPFOR success is undeniably linked to its reconnaissance effort. When OPFOR reconnaissance fails, the OPFOR commander will be unable to identify the points or point of penetration and focus his combat power. Simply speaking, without adequate intelligence (a minimum read of 90 percent of the composition and disposition of the BLUFOR defense), the OPFOR commander is forced to fight the complexity of a deliberate defense using a combat formation similar to that he would employ during a regimental meeting battle.

Back to our example. Two nights prior to the OPFOR attack, divisional reconnaissance forces attempted to move through the BLUFOR defensive sector. Granted, continuous training and a thorough understanding of terrain is an undisputed OPFOR advantage.

Starting at dusk, division reconnaissance troops begin probing the BLUFOR defense, looking for possible holes along the counterreconnaissance line. The OPFOR effort is staggered over time (wave technique) and not all reconnaissance troops will begin moving at dusk. Some will begin at midnight and others in the early morning. This is done, simply, to provide a continuous reconnaissance push with the belief that some time during the night some or all of the counterreconnaissance troops will become less effective (sleep deprivation, loss of focus and situational awareness). In this case, by first light on TD 5, 50 percent of division reconnaissance were on their respective reconnaissance objectives and 50 percent were dead. Throughout TD 5, division reconnaissance accurately reported the disposition and composition of each BLUFOR defensive position.

Regimental reconnaissance initiated movement at dusk TD 5. As regimental reconnaissance moved into the BLUFOR defensive sector, remaining division reconnaissance moved through the BLUFOR rear area. No link-ups or exchange of information between reconnaissance forces occurred. Based upon the movement success of division reconnaissance the night before, regimental reconnaissance would use near-identical movement routes. Similar to the previous night, regimental reconnaissance was 50 percent effective in passing through the BLUFOR defense enroute to their assigned reconnaissance objectives. Since the OPFOR reconnaissance plan assumed less than 100 percent success, there were sufficient redundant personnel and systems to cope with a 75 percent attrition rate and still be capable of achieving the reconnaissance objectives.

The success of the reconnaissance effort set the conditions for the OPFOR commander to exploit inherent BLUFOR weaknesses. The knowledge gained from division reconnaissance enabled the OPFOR battle staff to identify the exact point of penetration. It also allowed the systematic and focused use of combat multipliers (artillery, close air support, EW, etc.) either to isolate or destroy enemy forces at the point of penetration. To see the enemy in order to maneuver effectively against him, and ultimately destroy him, is not solely linked to the reconnaissance effort. Prior to the mission, the OPFOR commander refined the enemy situational template and conducted a thorough leader's reconnaissance. These efforts enabled him to understand the nature of the terrain in his area of operation and gain an appreciation of the enemy that he would face. Not only did this allow him to develop an effective scheme of maneuver, it provided focus to his reconnaissance, security, and direct and indirect fire plans that supported the maneuver plan. Thus, through effective reconnaissance, the OPFOR commander methodically either refined or discarded potential operational plans, branches, and sequels.

BLUFOR:

Simply speaking, successful counterreconnaissance will enable BLUFOR units to gain and maintain both initiative and maneuver dominance. Without question, most BLUFOR commanders generally understand the linkage and importance of the counterreconnaissance effort in achieving operational success in any defensive battle. Historically, however, most BLUFOR planning efforts are focused on the close battle and, to a certain extent, the deep fight. Habitually, BLUFOR units will designate a counterreconnaissance force from available maneuver units. Yet, there may or may not be any linkage to the overall BLUFOR reconnaissance and surveillance plan. Task force and brigade assets may work independently from the counterreconnaissance force. During this specific NTC battle, the BLUFOR commander organized his defensive sector into three, almost mutually detached, specific components: reconnaissance and surveillance, counterreconnaissance, and the main battle area.

The brigade S2 conducted the intelligence preparation of the battlefield (IPB) analysis process and determined what specific intelligence had to be collected to answer the commander's critical information requirements (CCIR). This IPB analysis resulted in the reconnaissance and surveillance (R&S) plan, which attempted to integrate reconnaissance forces into the overall intelligence-collection effort. Further, the R&S plan assigned specific intelligence acquisition tasks to specific units for action. During this battle, the R&S plan clearly identified five named areas of interests (NAIs). The NAIs were designed to determine OPFOR avenues of approach through key maneuver choke points. Task force scouts, combat observation laser teams (COLTs), ADA scouts, and minimum maneuver forces were integrated into this effort.

The brigade plan specified that each task force was responsible for counterreconnaissance within its assigned sector. TF 1-2 (AR) was designated A Team, while TF 3-4 (IN) was designated B Team. Additionally, both teams were designated as their respective task force reserve. Both A and B Teams assumed the counterreconnaissance line just prior to dark, thus no coordination occurred with forward brigade reconnaissance forces. A and B Teams maintained a 50 percent sleep plan. The rest of the brigade behind A and B Teams prepared orders and waited for first light to place obstacles and prepare fighting positions.

In addition to infiltration, OPFOR reconnaissance will conduct route reconnaissance for the subsequent main regimental body as well. BLUFOR reconnaissance, however, rarely conducts route reconnaissance. Instead, their focus is strictly infiltration (avoiding contact at all cost, penetrating enemy defensive positions and movement to a predetermined observation point). Throughout both nights prior to battle, OPFOR reconnaissance forces attempted to move throughout the enemy defensive sector.

Though detected at times, the OPFOR effort was largely successful. Since the BLUFOR counterreconnaissance effort was linear, all that the OPFOR was required to do was to penetrate the thinly held counterreconnaissance screen lines. At night, most of the rest of the brigade was asleep. Additionally, since both A and B Teams were alert at night, they were required to rest during the day. They conducted limited planning and virtually no rehearsals as the brigade reserve force. The BLUFOR commander's OPFOR defeat mechanism, his reserve, was unprepared to conduct its mission. Needless to say, during the battle, the reserve was neither at the right place, nor available at the right time, to support the BLUFOR plan.

An isolated battle at the NTC? Not really. Unfortunately, more and more times this has become a training standard. It doesn't have to be. Simple adjustments of counterreconnaissance and reconnaissance tactics, techniques, and procedures could remedy this training shortcoming.

Doctrine

An analysis of division through company doctrinal publications shows that the term or the mission of counterreconnaissance is rarely found. The logic behind this is simple. Counterreconnaissance, in and of itself, is not a mission. Rather, it is a component of defensive security operations. *FM 71-3 (Armored and Mechanized Infantry Brigade), FM 71-2 (The Tank and Mechanized Infantry Battalion Task Force)*, and *FM 71-100 (Division Operations)* discuss the importance of countering enemy reconnaissance and surveillance efforts. It is a continuous process that is conducted throughout the depth of the assigned area of operations. Further, security operations consists of three distinct tactical operations: screen, cover and guard. The size and composition of the security force, and what type security operation is to be conducted, is always dependent on the commander's estimate, as influenced by the factors of METT-T. The concept of enemy information denial, or counterreconnaissance, is an integral aspect, or enabling task, in each of these missions. The type of security operation to be conducted is based upon the orders received, the commander's estimate, and how it is influenced by the factors of METT-T. Counterreconnaissance, in and of itself, is little more (though it may become a critical aspect in ultimate mission success) than a tactic or technique employed during security operations.

The genesis of BLUFOR security problems in either the offense or defense can be linked directly to poor planning, development, and execution of the security area. Frequently, BLUFOR units will task one or two companies/teams as the counterreconnaissance force, perhaps task-organize scouts, engineers, and COLTS with them, and assume that they have solved the enemy reconnaissance problem. In reality, what has actually occurred is the development of a linear "counterreconnaissance screen line" and the implied belief by the remainder of the brigade that they are relieved of any security or force protection operations. The OPFOR has simply to penetrate this screen line (a relatively easy task when you echelon the OPFOR reconnaissance effort over time) since the remainder of the BLUFOR is normally fast asleep.

When the situation is reversed, the success of the OPFOR counterreconnaissance effort rests with the universal clear understanding that security operations are everyone's responsibility, are continuous, and are fought throughout the depth of the defensive sector. Woe be it to an OPFOR leader, soldier, or unit who permits a BLUFOR reconnaissance force to penetrate any defensive position. Additionally, OPFOR counterreconnaissance tactics are not isolated to limited visibility operations. During daylight, there is a incessant effort by the organization to identify, isolate, and eliminate any reconnaissance forces that happened to infiltrate the defensive sector. EW assets focus on identifying enemy reconnaissance radio transmissions. Heliborne forces, in concert with the ground maneuver commander, will patrol potential key terrain observation points in order to identify and ultimately destroy enemy units. Active dismounted patrolling occurs throughout the defensive sector. The OPFOR tactical operations center, under the direction of the chief of operations (OPFOR S3), manages the entire effort while planning and preparation for the next battle is conducted simultaneously. The synergistic effect of this combined effort will normally lead to one of two potential outcomes: the elimination of any BLUFOR reconnaissance threat or rendering the BLUFOR reconnaissance effort ineffective.

If a BLUFOR unit loses the counterreconnaissance battle with the OPFOR, the loss begins almost immediately after the conclusion of the last fight. The BLUFOR is most vulnerable to OPFOR infiltration and reconnaissance during the period immediately after change of mission (COM). BLUFOR units are guaranteed that, immediately after COM from the last fight, they must reconstitute (unit or individual), attend an after-action review (AAR), and prepare for a follow-on mission. Preparation for the follow-on mission includes both the planning for the maneuver fight and the counterreconnaissance battle, as well. Yet, there are techniques available to satisfactorily complete planning for the subsequent operation, reconstitute, and execute security operations simultaneously.

Planning the Securlty Fight

The normal counterreconnaissance technique employed (evident in the example given) by a rotational brigade conducting a defense at the NTC is to identify either a tank or infantry team as the security force. The team may be reinforced with additional combat, combat service, and combat service support assets. Normally, this team is also tasked as the brigade reserve. The brigade commander's final OPFOR defeat mechanism conducts security operations at night and is expected to rehearse as the brigade reserve during the day. Obviously, from a time management perspective, to satisfactorily complete one of these two tasks to standard is difficult, but to expect that both can be mastered is absurd. Yet, we continuously relearn the same lessons. Perhaps the most telling systems failure is what this process tells the rest of the command indirectly: "A Team is solely responsible for counterreconnaissance." What this translates to are an unrehearsed reserve and a strong but shallow security crust. Once you are through, everyone else is fast asleep. What will further exasperate the problem is that the team identified as the counterreconnaissance force may or may not have conducted home station training in this capacity. OJT (on the job training) is normally not a good training technique at any of the three CTCs.

A technique to get through this security dilemma is not to identify a counterreconnaissance force in the first place and to attempt to ingrain the attitude within the command that security and force protection is continuous and everyone's responsibility. Consider that the execution of security operations is inherent in any defensive operation and the supporting task of counterreconnaissance will follow logically the exploitation, pursuit and consolidation phases of an offensive operation, or counterattack or consolidation in the defense. Planning for counterreconnaissance thus becomes a follow-on phase of an ongoing operation.

A tremendous guide to assist in the development and planning of the counterreconnaissance task is *FM 34-2-1 (Tactics, Techniques and Procedures (TTP) for Reconnaissance and Surveillance and Intelligence Support of Counterreconnaissance).* The title of the manual may be misleading. It does not, in fact, furnish counterreconnaissance TTP. Rather, it is a guide in the development of the R&S plan as a mechanism to focus security operations in general, and the conduct of counterreconnaissance specifically.

The key point is that the planning for security operations, and the enabling task of counterreconnaissance, logically flows at the conclusion of the immediate operation and its execution is, in fact, the operational linkage to any subsequent mission. Planning in this manner eliminates the concern or predicament that the unit will be forced to execute security operations without the benefit of either a mature or rehearsed plan. Granted, the battlefield conditions anticipated at the conclusion of the maneuver battle may not hold true, but the organization will have at least a 60 percent security plan ready for execution. A few adjustments to the plan may be all that is necessary to achieve a more acceptable 80 percent solution. Perhaps even more germane to this discussion, a security operations SOP, similar to that of the OPFOR, that follows the completion of any offense or defense, may rectify this potential battle dynamics dilemma.

As a unit transitions from the offense to the defense, the higher headquarters will normally provide defensive sector graphics. This may be little more than a forward and rear boundary and left and right limits. The brigade will assign task force sectors and the task force will assign company/team sectors or battle positions. This minimal information is more than enough to develop the unit's security plan. Within the various defensive sectors, a combination of security and defensive preparations should occur. Clearly, the unit must prepare its defensive positions skillfully, and must anticipate the threat of both day and night enemy reconnaissance movement.

Mounted and dismounted patrolling must be integrated into the entire effort. The task force and brigade command posts orchestrate the entire effort. Heliborne, EW, ADA, and indirect fires are integrated into the operation. Forward of the task force sector and well within the range of supporting indirect fire systems, scouts (to include COLTS, ADA, and engineers) are focused at potential infiltration movement routes. Care must be taken not to over-task these limited scouting resources.

Commanders must prioritize and curb their named area of interests (NAI) appetite. Specifically, a task force scout platoon cannot effectively monitor more than two or three NAIs. More often than not, there has been a tendency at the NTC to task a single scout platoon to observe in excess of five NAIs at any one time. The effect of this tasking is that none of these NAIs will be observed effectively. Additionally, to enhance effectiveness, NAIs must be developed and issued with a specific task and purpose.

Too often, BLUFOR scouts will go forward armed with little more guidance than to observe a piece of terrain. Terrain is important only in respect to what it could afford enemy or friendly forces. For example, when a scout is tasked to observe a critical maneuver choke point NAI, he must be able to identify and observe both TAIs (target area of interests) and triggers within the NAI. Additionally, the scout must have a redundant communications capability in order to work through any enemy jamming.

There are numerous other tactics and techniques that can be integrated into the overall security effort but the impact remains the same: an inherent awareness throughout the command of the importance of security operations, counterreconnaissance throughout the depth of the defensive sector, centralized command and control, and decentralized execution of the combined effort. In our example, the intricacies of security have been integrated as a logical concluding (phased) operation of an ongoing mission, and can yet be further refined to become little more than a task force or brigade SOP.

Training Implications

• **See the Battlefield —** *FM 100-5* (Final Draft, 5 August 1997) states that when conducting operations, Army forces must perform five fundamental actions when applying military power: see, shape, shield, strike, and move.[1]

Seeing is more than understanding your own capabilities and limitations, but it involves understanding those of the enemy as well. Unit commanders at all levels must understand basic enemy doctrine and tactics. This is not the sole responsibility of the military intelligence community. Commanders will often spend numerous hours developing ground maneuver courses of actions without a full appreciation of enemy capabilities or constraints. Tactical maneuver (OPFOR or BLUFOR) can be viewed as little more than the application of common sense to the terrain. Units should wargame against an uncooperative enemy. Too often during a war game, a course of action will be accepted without a full appreciation of the enemy. The brigade or battalion S2 (if he plays the enemy commander during the wargame) can be easily and often discounted by an energetic S3 or commander. The key point is that it is the responsibility of the unit commander to be well versed in enemy order of battle, doctrine, and potential tactics.

• **Visualize, Plan and Prepare Security Operations Throughout the Depth of the Defensive Sector.** Commanders should avoid the operational pitfall of executing a linear security or counterreconnaissance plan. This falls into the category of "easy say, hard do." The framework of the defense includes deep operations forward of the FLOT, security operations throughout the area of operations, the main battle area, reserve and rear operations. Too often as an organization, we will become completely focused on defensive preparations in the main battle area and give limited guidance and time to security and force protection responsibilities. In terms of an effective defense, these tasks must be more in balance. Command posts must be able to battle-track not only the preparation of the defense, but security operations as well. Security is an operational requirement and not the sole domain of the unit S2. Additionally, the use of scouts as a counterreconnaissance force must be weighed carefully against the mission and available resources. Often, scouts involved in counterreconnaissance will not be alive during the deep or main battle area fight. If the commander's operational plan includes scouts focusing indirect fires deep, consideration must be given regarding any additional tasks scouts can be expected to complete to standard during the security fight.

- **Simplicity is a Combat Multiplier.** We, in the Army, have institutionalized a common belief that any complex problem can be solved through better and more focused planning. Some suggest that the method to resolve the issue of faulty security execution is through the identification of an additional staff officer (chief of reconnaissance) to manage the task and the development of a reconnaissance order (to be planned prior to the subsequent mission order). They look at the OPFOR's regimental chief of reconnaissance as an example of this process. Not only are they wrong about the OPFOR, they are wrong about the creation of another staff agency or agent to execute the task and, most importantly, they have added more complexity to the issue. The OPFOR's chief of reconnaissance is the BLUFOR's brigade S2 by another name. They forget that the OPFOR has had the opportunity to plan each battle's reconnaissance and surveillance prior to the start of the maneuver rotation. They forget that the OPFOR is not only familiar with the terrain but practices its trade constantly. Granted, in terms of planning or execution, many security lessons can be learned from the OPFOR. But, to suggest that the solution to poor security operations is to further increase our planning efforts and institute another staff planning layer is, frankly, absurd. The answer to the task of counterreconnaissance is an awareness that security operations should be planned as the final phase of any operation (understanding that the plan will not be perfect and will have to be adjusted to comply with battlefield realities), that the burden of counterreconnaissance belongs to the entire organization and must be conducted continuously throughout the depth of the battlefield, that it is managed by the unit commander and his battle staff (certainly not the domain of the S2), and that whenever possible it is conducted in accordance with established unit SOPs.

- **Rehearse, Sequence, and Resource the Security Effort.** The rehearsal is the most important part of the deliberate planning process, period. It is the last opportunity for the unit to deconflict, cross-check, and prepare. This statement will more likely than not cause an uproar with all clipboard-wielding OCs (observer/controllers) and planning zealots who have convinced themselves that if something tactical is broken, the key to its fix is more planning. I won't belabor the point. Unfortunately, the issue remains that we have a tendency to rehearse the battle through the task of offensive or defensive consolidation and reorganization and rarely expend any effort in follow-on security operations. Viewing security operations as the natural linkage that is sequenced between the last battle and next battle to be fought will ensure that you have at least a preliminary plan to execute, and if necessary adjust. Additionally, don't forget your combat multipliers. Orchestrate the effort with indirect fires, EW assets, ADA, logistics, etc. Have enough redundancy in the plan so that when a key unit or individual is not available (AARs, reconstitution) another can take his place.

- **Force Protection.** Don't ask your soldiers to do something in training that you wouldn't ask them to do in combat. CTC gamesmanship should be highly discouraged, and our leadership should always be on the lookout for it. Scouts positioned forward of the FLOT should be in range of friendly indirect fire systems. This includes not only those conducting ground infiltration, but also those conducting air insertions. Also, consider the duration of the mission assigned and the methodology to sustain and evacuate that force. More germane to this discussion is the fact that there is a direct correlation between force protection and how the unit conducts the task of counterreconnaissance that denies friendly information to the enemy. An effective security operation will take the initiative away from the opposing commander. The success or failure of the reconnaissance effort, regardless of the competitor, will normally predict the outcome of the imminent battle. Specifically, in this example, reconnaissance failures will force the OPFOR to attack under unfavorable conditions and will intensify overall BLUFOR survivability.

- **SOPs, Battle Command and Battle Tracking.** *FM 25-100* states that all activities within an organization should be conducted within a "band of excellence." Essentially, this performance band dictates that a unit should strive for the consistent "80 percent" product rather than attaining only a few 100 percent and many failures. Clearly, time is the limiting factor that prevents consistent excellence in all areas. Despite what is in our training doctrine, the environment of the CTCs have invariably placed units in the position of performance peaking only during the maneuver battle. At COM, key leaders are expected to participate in AARs from platoon level on up, conduct unit and individual reconstitution, decontaminate if necessary, and prepare for the next fight that will undoubtedly come within the next 48 hours. This period of time, from COM to the time that a unit is prepared to execute a follow-on mission, will often approach 12 or more hours. This cycle is also the time that a BLUFOR unit is most susceptible to OPFOR reconnaissance and infiltration. To solve this training problem is not necessarily easy, but it can be fixed. First, it must be universally accepted in the unit that the S2 can certainly facilitate conducting the task of counterreconnaissance, but security operations is everyone's responsibility. In the OPFOR, security is a command function. Battle-tracking of the security mission is conducted on the chief of operations (unit S3) situation map. There is a continuous dialogue throughout the security fight between the OPFOR commander and his subordinates. The entire unit is aware of its counterreconnaissance responsibilities, and with religious fervor comply with the unit security SOP. Enemy reconnaissance forces are tenaciously tracked, hunted down, and killed. While the leadership of the OPFOR is conducting AARs and other tasks, battle captains monitor and manage the security effort. The key to successful security operations resides in disciplined forces, focused battle command, simple but achievable plans, and battlefield awareness.

Concluding Thoughts:

Care must be taken not to take CTC battle results and assume that they are

Continued on Page 47

COUNTERRECONNAISSANCE

from Page 11

predictive and will provide an absolute representation of actual combat. No one will dispute that the CTCs, in general, and the NTC, specifically, have enhanced our training effectiveness and our combat readiness. Yet, we must be cautious in any training assessment conducted at the CTCs that forecast categorical battle facts. Bluntly speaking, the CTCs are little more than a higher magnitude form of “laser tag.” Despite the most serious efforts, the CTCs cannot replicate nor adequately simulate the moral domain of conflict. History has shown that battlefield performance may be enhanced by improved physical and C3I systems, but the moral domain of conflict continues to remain predominant. This moral domain embodies the true spiritual and human aspects of combat.[2] Failure at the CTC results in a flashing CVKI (combat vehicle kill indicator) light and a painful exercise in reconstitution. Failure on the battlefield results in dead soldiers and a failed mission. The CTCs cannot replicate the moral impact and paralyzing consequence of effective enemy indirect fire concentrations. Further, it is doubtful that our Army’s leadership would allow any combat unit to disintegrate to less than 5 percent combat strength before being pulled or relieved from the battlefield. It is highly questionable that any brigade-size maneuver unit would receive such a large variety of time-sensitive combat missions that we demand at the CTCs. I do not suggest, however, that the CTC training methodology is incorrect. Training efficiency demands that we continue on this course. Yet, we must be cautious in our interpretation of training results. Specifically, when discussing security operations, we may have missed the mark when we conclude that NTC failures reflect deficient doctrine, tactics, and mediocre planning.

Although we must continue to focus on all phases of security operations, particular emphasis on preparation and execution is warranted. Incessant planning is not the answer. Not all answers to battle training failures can be directly linked to faulty planning. Focused and relatively simple security operations SOPs, coupled with disciplined execution throughout the organization, will resolve the mystery of conducting the task of counterreconnaissance. This article has attempted to provide a methodology to do just that. Through the use of simple but flexible SOPs, a shared responsibility for security operations throughout the command, and planning for security as a sequential or concluding phase of any mission may alleviate some of these training challenges.

Notes

[1] *FM 100-5* (Final Draft, 5 Aug 97), p. 5-1.

[2] *FM 100-5,* p. 2-10.

LTC (P) Chris Baggott, currently in the second year of a War College SAMS Fellowship, is the command designee of 3d Armored Cavalry Regiment (June, 98). He has commanded two armored cavalry troops, served as a brigade S4, and as S3 of a tank battalion and three cavalry squadrons. Additionally, he served as aide de camp to the 3rd Armored Division Commander; G3 Plans, III Corps; brigade XO, 3d Bde, 1st Cav; and commander, 1-11 ACR (OPFOR). His military education includes AOAC, Airborne and Ranger Courses, CGSC, SAMS, and Defense Strategy Course.