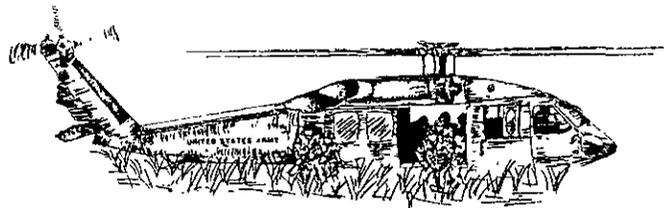
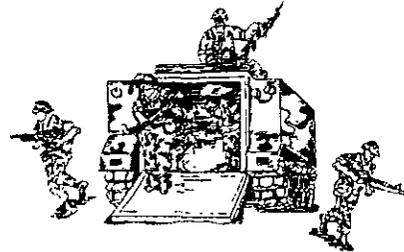


COUNTERING TERRORISM IN THE TRENCHES

Lieutenant Forrest L. Davis



Self-preservation is a certain, unchanging, inalienable right. Commanders demonstrate this right when they approve security plans.

And yet, too often today a U.S. battalion task force deployed alone to a terrorist environment continues to be a muscle-bound giant pitted against a much smaller and more agile enemy.

In planning for security against an unconventional threat, our task forces typically go with what they know—the *last war*. They build fighting positions, plan interlocking fields of fire, and design elaborate alert plans around 360-degree perimeters. In effect, the “Vietnam base camp” syndrome returns, and full alert contingency plans are developed, complete with wailing sirens.

If, however, at 0200 hours on any night, four unidentified personnel are detected within our perimeter, do we want our entire battalion’s soldiers running to fighting positions in partial uniform and without the facts? Do we want 20 minutes of chaos? Or do we simply want to contain and neutralize the threat?

The basic problem is that our current antiterrorism doctrine does not reach to the lowest levels in telling a task force commander how to organize, prepare, and employ his organic forces toward meeting every potential “special threat situation.” Publications such as FC 100-37-1, Unit Terrorism Counteraction, do include suggestions that help the infantry commander plan for specific operations—that is, convoy security, deployment, and the like. By themselves, these measures are excellent. But they are designed only to deter attack and, therefore, are defensive (or proactive) security

measures. If an infantry battalion commander is going to fully meet his security responsibility to his soldiers, he needs an offensive (or reactive) capability as well.

TC 19-16, Countering Terrorism on U.S. Army Installations, and FM 34-60, Counterintelligence, explain in some detail how an installation or post-level commander can organize his command to counter the full range of terrorist attack options. Thus, he can organize both a threat management force and a crisis management team and make them responsible for controlling and executing the antiterrorist plans. With imagination and special training, the guidance offered in those publications can be applied to an infantry battalion task force as well.

In 1986 the 2d Battalion, 504th Parachute Infantry, 82d Airborne Division, deployed to the Sinai Desert in the Middle East to continue the U.S. commitment to the Multinational Force and Observers (MFO) mission. This battalion task force decided to use the post-level guidance for its security planning.

The limitations under which the task force had to operate were similar to those any U.S. unit could expect to meet elsewhere.

First, the task force was the guest of a host country, in this case Egypt. Understandably, the worse public relations action the battalion could possibly take would be the inadvertent shooting of an innocent, or even criminal, local citizen. One accident or mistake and the task force could expect to be the target of popular, local criticism and, conceivably, of independent zealous action.

Second, the host country considered itself respon-

XO

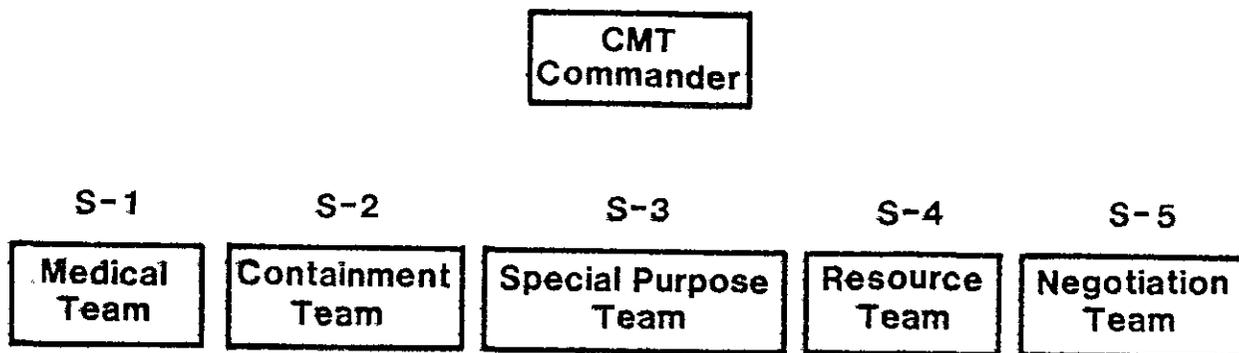


Figure 1. Organization of the crisis management team (CMT).

sible for the battalion's security because the battalion was on its soil. Although this was comforting, it in no way diminished the commander's security responsibility. In the event of a special situation that seriously threatened the lives of his men, was the commander to wait for the host country's response? Quite rationally, the commander had to plan as if the host country would be incapable of responding.

Third, the security mission against a potential terrorist threat, the only reasonable one, had to be planned using organic equipment and, most significant, conventional soldiers.

The crisis management team (CMT) concept was successfully applied, with each staff section being made responsible for special teams (see Figure 1). The application was consistent with normal operations and, in most cases, the sections merely had to reorient their perspectives and priorities.

The S-1 section assumed responsibility for the medical team. Deployed in anticipation of one casualty or multiple casualties, the team prepared for either event through mass casualty exercises. Since this team would have existed regardless of the commander's application of the CMT concept, its creation was essentially administrative.

The containment team, an S-2 section responsibility, was a platoon-size element responsible for sealing off or containing any area in which potentially hostile elements were known to be. In essence, the team would surround the enemy. This team was responsible for the inner security perimeter and cooperated closely with the task force Military Police element, which assumed responsibility for the outer perimeter. No one was permitted to pass through either perimeter without CMT approval. Together, these security rings allowed the task force to literally seize control of a designated area and with it, the tactical initiative.

The only tactical strike element within the CMT was the special purpose team (SPT). Employed by the S-3,

this team consisted of sniper and security elements that could mutually support each other in clearing buildings or conducting other military operations on urban terrain (MOU).

The resource team (S-4) was charged with providing any special supplies needed by other teams—anything from hot chow to 7.62 match ammunition. Special contingency items were set aside and held in reserve.

Interrogators serving as linguists, along with an attached civil affairs officer (S-5), made up the negotiation team. When used, the team had two basic objectives—to calm the threat and to gather information. (The concept of employment of all these teams is shown in Figure 2.)

PLANNING

In the Middle East, the typical terrorist target is not power stations and resupply lines. The target is people, often Americans. During the battalion's predeployment planning stage, therefore, the threat and the most likely methods of countering that threat were considered, and counteractions in the form of contingency plans were developed. For the most part, the proactive security measures that were adopted were deemed sufficient to prevent unnecessary vulnerability. For two unlikely yet potential scenarios, however, such measures were clearly not enough.

These two scenarios included, first, a terrorist breach of the base camp perimeter in order perhaps to plant satchel charges around the personnel billets. This was labeled the "detected intrusion" scenario. The second scenario was, of course, a hostage situation.

In both events, a reactive capability was needed. And in each, the special limitations requiring no mistakes, unilateral response, and the use of organic assets were considered.

Detected Intrusion. This contingency plan had as its

objective the containment (not engagement) of any suspicious elements located within the base camp, because, according to one qualified estimate, sapper teams could quickly place enough charges within the facility to kill 100-120 people. Modeled along the CMT concept, the plan envisioned the use of as many as four of the five crisis management teams.

Three active security elements operated within the base camp—an interior guard force, the Military Police, and the containment team. These three elements worked together to execute what were called “emergency actions.” For example, when a suspicious activity was recognized by any of the three elements, the other elements were notified immediately on an emergency radio frequency, and all of them essentially “stood on their toes.”

Thus, the guard force recalled enough men to post additional guards around the billet areas. The containment team prepared for deployment, and the Military Police dispatched a patrol to investigate.

When he arrived at the scene, the Military Policeman was asked to make an assessment. Is there activity? Is it criminal (burglary) or terrorist (are there personnel with weapons or has there been an explosion)? And finally, are the people responsible still in the vicinity? If so, the MP would fix their location and transmit this information to the containment team.

The containment team consisted of one platoon of two squads, and through rehearsals it was found that a single squad was enough to contain any major area within the base camp. When the signal to execute was given by the officer in charge of the tactical operations center (who was also on the emergency net), the team deployed, contained the identified area, and relieved the MP element. In moving into place, they allowed themselves to be seen, but their movement was quick

and always covered by overwatch fires. During numerous alerts, the containment team was on the scene within four or five minutes of the MP request for support.

Following the containment of an actual threat, the security posture of the base area would be improved. Movement would be kept to an absolute minimum and, through the linguist personnel or negotiation team, the host country would be invited to assume control over the situation. Assuming no unique need existed that would necessitate the employment of the medical, resource, or special purpose teams, the detected intrusion scenario and the security of U.S. forces would be complete.

Hostage Scenario. In the development stages, the hostage scenario was virtually identical to the detected intrusion scenario. An identified terrorist element would be contained in a specific structure or location, and freedom of movement within the area would now be a U.S. prerogative. The difference, of course, was that the terrorists would be holding U.S. personnel as hostages.

After identifying the terrorist element and confirming the presence of U.S. hostages, higher headquarters would be immediately notified and the negotiation team would be deployed to collect information and calm the situation. Assuming there was no imminent threat to the hostages, the activities of the crisis management teams would still be defensive. If the threat should change, however, and if relief by higher headquarters teams could not be expected, the special purpose teams would be deployed to assault and neutralize the situation.

A special purpose team was organized consistent with the battalion’s sniper team concept. Thus, since two snipers were normally supported by a security

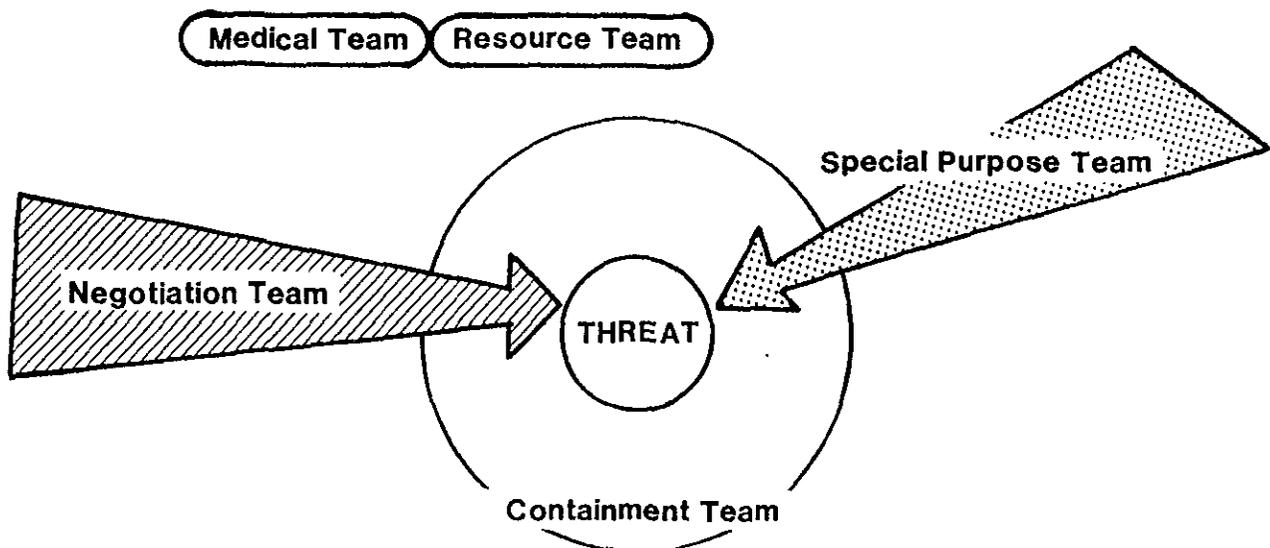


Figure 2. Concept of employment.

team of three, the five-man team was left intact but, instead of the security team supporting a sniper team, the two-man sniper team supported a three-man "building clearing team." We found we could organize two, or as many as four, special purpose teams from a pool of selected personnel from the battalion's scout platoon.

It must be emphasized that the employment of a special purpose team was to be considered the last of possible last resorts. The soldiers who made up the team were not special operation candidates, nor had they received intensive, antiterrorism training under uniquely developed conditions. They were, however, the products of a discriminating, inter-battalion selection process. They were snipers and scouts, and were well rehearsed in MOUT tactics—the best the battalion had to offer.

EFFECTIVE COUNTER

With the exception of the hostage scenario, the organization and system used by the Sinai task force proved an effective and potent counter to all terrorist threats. The counterterrorism organization allowed the unit to isolate any recognized elements within its area of operations for subsequent transfer to local national authorities. The system also achieved a balance between the task force's security needs and the political requirements of its non-combat mission. But it could have been better. Indeed, with additional specialized training, the task force could conceivably have countered all terrorist threats.

If we are going to be serious about securing ourselves from terrorism in every aspect, making it better means, first, considering this or a similar organization as a single component within the entire framework of the counterterrorism structure. Ideally, any organization adopted for use by an infantry battalion should complement the unit's existing structure. Second, clear doctrine should be developed and disseminated that outlines the crucial training tasks in developing a battalion-level CMT. This is no simple task, but considering the possibility of increased U.S. involvement in low-level instead of mid- or high-intensity operations, the doctrinal focus is warranted.

Developed in accordance with TC 19-16, a battalion level counterterrorism force could complement other crisis management systems and contribute to a smooth transition in jurisdiction from one headquarters to another. For example, if a deployed task force should find itself in the midst of a special threat situation, a relief in place by a higher headquarters would be simplified because each echelon would consist of common organizations employing similar terms. In effect, the establishment of like organizations as an Army-wide standard would simplify communication, coordination, and (in situations in which time was critical) unity of action.

The Sinai task force demonstrated that an infantry combat-oriented unit can be trained to respond appropriately in politically sensitive environments, but not without certain trials in training.

Two training concepts dominated the preparedness of our CMT. The first was containment, which required reorienting our soldiers' perspectives. The second was the training of the negotiation and special purpose teams.

Clearly, infantry soldiers are geared toward moving, shooting, and communicating, with particular emphasis on shooting. They are not sensitized to giving a potential perpetrator every benefit of the doubt, such as would be necessary in the establishment of a containment perimeter.

During our early training exercises, for example, the task force's training scenario described "two individuals, possibly armed, seen moving in the shadows near the storage building." In one instance, the containment team squad leader simply ordered his squad to assume battle formation, conducted an assault, and accomplished the "5-S's" (search, silence, segregate, safeguard, and speed to rear) on the two individuals.

On another occasion, the MP reaction team reported that the containment team should "secure" a particular area within the motor pool. The containment team did—by establishing *defensive* instead of *containment* positions around the location of the threat. In other words, their weapons were pointing in the wrong direction. The problem was terminology: The message said "secure," not "contain."

LESSONS LEARNED

In time the lessons learned were accumulated and the containment team showed an ability to deploy rapidly and contain a possible threat element with little exposure to potential fire. Indeed, there was a certain shock effect to its deployment when the soldiers jumped from their two-and-a-half-ton trucks and ran to establish the positions pointed out by their squad leader. Anyone who found himself a target of the team would have had to conclude that he was surrounded by a very professional and well organized force.

The steps we followed in training our soldiers in the defensive, yet non-combat, mission of containment should be studied by other units. The combined lessons learned should then be compiled with a view to filling a definite doctrinal need.

The training of the negotiation team and the special purpose team is an issue of paramount importance. Consistent with the available experience and equipment, we prepared these elements to handle potential hostage scenarios. The negotiation team's linguists were coupled with a mental health specialist and would have been employed primarily as interpreters. The special purpose team concentrated on coordinat-

ing sniper fire with building assaults by security teams. These elements were not what they could have been with more intensive training, and some argued that their actual employment would have been disastrous. But in the opinion of the command, they were better than no capability at all.

U.S. Army interrogators are taught how to penetrate human defenses and procure information. They know how to manipulate human emotions and, in peacetime, are quite often used as linguists. If these people can be trained to interrogate, is it unreasonable to assume that they can also be trained to negotiate? If not all interrogators, at least a representative number might receive additional training that would give a battalion task force this capability.

Finally, if the number of independent task forces presently being deployed does not justify the expenditure of funds for training large numbers of interrogator personnel, then selected individuals should be trained before the deployment of a designated task force. The training programs exist. We simply need to secure the school quotas.

As with the negotiation team, the special purpose team must have unique skills if it is to be of any real tactical value during a special threat situation. The team must be familiar with typical terrorist ruses and must be capable of entering a building quickly and neutralizing the threat. The members must be flexible, able to work under considerable stress, and expert with the .45 or 9mm pistol. They must be a real team, each member with intimate knowledge of the others' capabilities and weaknesses.

Attaining the skills needed to employ the techniques of neutralization is a demanding task and certainly not within every soldier's reach. But every infantry battalion has some special soldiers with the necessary mental and physical prerequisites. Training for these select people might begin at the Military Police School with a two-week introduction to special purpose team tactics. As with the training for the negotiators, we just

need to get the training slots.

To maintain these perishable skills, generic scenarios could be packaged for training use in a unit. During ARTEPs, for instance, terrorist situations could be included and certification by competent authority obtained.

The possibility of continued and even increased deployments of virtually independent task forces to terrorist threat areas is almost certain. With these deployments, the right of TF commanders to ensure the security of their personnel is also certain. But single-source doctrinal guidance has yet to be developed for the lone infantry battalion.

The Sinai task force, on the leading edge of this doctrinal need, demonstrated that the crisis management team concept employed by installation commanders could be tailored to meet its commander's needs. Working under restrictions—no mistakes, potential unilateral response, and the use of organic assets only—the task force was able to counter all but one threat scenario. And that one, the hostage threat, is also within the reach of an infantry battalion.

A clear, organizational model sanctioned by doctrine and training guidance detailing the steps toward preparation are two areas worthy of greater attention. Overall, developing a capability to respond will not be cheap and, to some, a "part-time" counterterrorism team may seem like the proverbial "bull in a china shop." But few situations are more damaging to unit esprit de corps, deployment effectiveness, and national prestige than one in which an inferior force holds an infinitely superior force at bay. An infantry battalion commander has a right to respond. He has a duty to respond.

First Lieutenant Forrest L. Davis, Military Intelligence, is a 1984 ROTC graduate of the University of Texas at El Paso. He is now S-2 of the 2d Battalion, 504th Parachute Infantry Regiment, 82d Airborne Division. Formerly an enlisted soldier, he has served with the 101st Airborne and 24th Infantry Divisions.

