FM 34-25

CORPS INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS

SEPTEMBER 1987

HEADQUARTERS DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: Approved for public release: distribution is unlimited

FIELD MANUAL
NO 34-25

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, DC, 30 SEPTEMBER 1987

CORPS INTELLIGENCE and ELECTRONIC WARFARE OPERATIONS

Table of Contents

		Page
Preface		iii
Chapter 1	Challenges for Corps Intelligence and Electronic Warfare	1-1
	Corps Role	1-1
	Corps IEW Mission	1-2
	Identifying the Challenges	1-4
Chapter 2	Corps Intelligence in the AirLand Battle	2-0
	Structure of Modern Warfare	2-0
	Doctrinal Requirements for Intelligence	2-0
	Corps G2	2-11
	MI Brigade Commander	2-12
	MI Brigade	2-13
Chapter 3	Command and Control	3-0
	Operations	3-0
	Functions	3-5
	Command and Support	3-6
	Task Organization	3-7
Chapter 4	Intelligence in Combat Operations	4-0
	Operations	4-0
	Targeting Process	4-10
	Suppression of Enemy Air Defenses	4-17
Chapter 5	Special Operations and Enviromments	5-1
	Military Operations	5-1
	Low-Intensity Conflict	5-4
	Terrorism	5-9
	Rear Area Intelligence Operations	5-14

*This publication supersedes FM 34-20 (HTF), 6 May 1983; FM 34-21, 10 November 1982; FM 34-22, 19 March 1984; and FM 34-23, 21 January 1985.

		Page
Chapter 6	MI Battalion (Operations)	6-0
	Headquarters, Headquarters and Service Company	6-1
	Operations Company	6-2
	Communications Company	6-18
Chapter 7	MI Battalion (Tactical Exploitation)	7-0
	Active Component	7-0
	Reserve Component	7-10
	Airborne Corps (Active Component)	7-17
	Airborne Corps (Reserve Component)	7-20
	CI Support to Rear Operations	7-23
	CI Support to Terrorism Counteraction	7-24
Chapter 8	MI Battalion (Aerial Exploitation)	8-1
	Headquarters, Headquarters and Service Company	8-1
	Aerial Surveillance Company	8-3
	Aerial Electronic Warfare Company	8-4
	Operations and Sensor Systems	8-7
	Mission Requirements	8-11
	Mission Execution	8-15
Appendix	Military Intelligence Communications	A-1
Glossary		Glossary-1
References		References-1
Index		Index-1

PREFACE

This manual provides the Army's doctrine for corps intelligence and electronic warfare (IEW) operations. It describes how IEW elements organize and fight. It also presents corps-level tactics and techniques for accomplishing the four IEW tasks of situation development, target development, counterintelligence (CI), and electronic warfare (EW). It expands the IEW doctrine in FM 34-1, builds on the foundation provided by FM 34-80, and relates the IEW missions to FMs 100-5 and 100-15. It is based on the Army of Excellence (AOE) force structure, as configured at the time of publication. This doctrine is in concert with North Atlantic Treaty Organization (NATO) doctrine and strategy. It is also flexible and general enough to meet the needs of other forward-deployed corps and contingency corps in other theaters. Chapters one and two describe the IEW role at corps and in the AirLand Battle. The remaining chapters address information needed by military intelligence (MI) personnel at corps and within the MI brigade.

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

The proponent of this publication is HQ TRADOC. Submit changes for improving this publication on DA Form 2028 (Recommend Changes to Publications and Blank Forms) and forward it to Commander, US Army Intelligence Center and School, ATTN: ATSI-TD-PAL, Fort Huachuca, Arizona 85613-7000.

CHAPTER 1

CHALLENGES FOR CORPS INTELLIGENCE AND ELECTRONIC WARFARE

CORPS ROLE

Corps, the Army's largest tactical unit, is the instrument with which higher echelons of command conduct maneuver at the operational level. A corps is tailored for the theater and mission for which it is deployed. Once tailored, however, it contains all the organic combat, combat support, and combat service support (CSS) capabilities required to sustain operations for a considerable period.

Corps plans and conducts major operations and battles. It synchronizes tactical activities including the maneuver of its divisions, the fires of its artillery units and supporting aerial forces, and the actions of its combat support and CSS units. While corps normally fights as part of a larger land force--a field army or army group--it may also be employed alone, either as an independent ground force or as the land component of a joint task force. When employed alone, it exercises operational as well as tactical responsibilities.

Corps is assigned divisions of any type required by the theater and the mission. It possesses organic support commands and is assigned combat and combat support organizations based on its needs for a specific operation. Armored cavalry regiments (ACRs), field artillery (FA) brigades, engineer brigades, air defense artillery (ADA) brigades, and aviation brigades are the nondivisional units commonly available to the corps to weight its main effort and to perform special combat functions. Separate infantry or armor brigades may also be assigned to corps. Signal brigades, MI brigades, and military police (MP) groups are the usual combat support organizations present in a corps. Other units such as psychological operations (PSYOP) battalions, special operations forces (SOF), and civil affairs units are assigned to corps when required.

The success of a maneuver unit has never been so actively dependent upon timely IEW support to accomplish its mission. The corps mission in AirLand Battle and the mission of staffs and units are directly related. Maneuver commanders should understand the capabilities and limitations of IEW relative to their echelons and their areas of operations and interest.

OFFENSE AND INITIATIVE

This manual emphasizes flexibility and speed to underscore the basic tenets of AirLand Battle Doctrine--initiative, agility, depth, and synchronization. Senior intelligence staff officers and MI unit commanders at all echelons incorporate these tenets to the IEW tasks performed at corps. To execute the IEW tasks, commanders from the forward line of own troops (FLOT) to the national command authority (NCA) should understand the relationship of multidisciplined IEW support to mission execution.

DETERRENCE

The corps is deployed to act as a deterrent force, such as the forward-deployed corps in Europe or a contingency force in the Continental United States (CONUS). Missions assigned to the corps range from low-intensity conflicts (LICs) to general and nuclear war. Some corps missions allow for significant and detailed planning, such as the forward-deployed corps with a relatively stable threat and a consistent terrain base. Conversely, the contingency corps must be prepared to deploy against a variety of potential threats in various theaters with very short timelines. At the time of execution, commanders exhibit flexibility and initiative. The contingency corps serves strategic objectives while the forward-deployed corps achieves its objectives through synchronization of operations--rear, close, and deep--and through coordination with higher, lower, and adjacent echelons.

BATTLE

The challenges facing a corps commander as he fights on an integrated and extended battlefield are complex and highly demanding. While operations may receive varying degrees of emphasis, they are planned as a single, coordinate entity. The corps commander sees the battlefield in terms of space, time, an resources available. To win against a much larger enemy force, his battlefield management plan synchronizes intelligence operations with all elements of combat power and support.

CORPS IEW MISSION

The four primary IEW tasks the corps commander emphasizes are situation development, target development, EW, and CI. The combined application of these tasks gives him knowledge of the threat force. This knowledge allows him to disrupt threat operations and protect his own assets from exploitation.

Intelligence reduces uncertainties to known factors through study, analysis, and prediction. Operational guidance and the corps commander's concept of operation determine the focus of the MI staff effort.

Based upon the corps commander's concept of operations, the G2 analyzes the priority intelligence requirements (PIR) and information requirements (IR). Once approved by the commander, they form a base for collection operations. PIR and IR drive the tasking and execution of the four primary IEW tasks.

The IEW challenge requires flexibility, initiative, innovation, and understanding to provide IEW support for corps requirements. Every corps commander requires continuous, timely, and accurate intelligence to satisfy his intent.

SITUATION DEVELOPMENT

This IEW task is the basic process by which intelligence is developed. Information is collected, correlated, processed, and integrated into an all-source product to provide and keep current the intelligence estimate of the

situation. Enemy intentions are predicted in sufficient time for the corps commander to select the most effective action. Intelligence preparation of the battlefield (IPB) provides the analytical base for situation development. This is essential for battlefield planning and decision making.

TARGET DEVELOPMENT

This IEW task is based on situation development. It is the process of providing targets to commanders and fire support means. Target development provides the corps commander with timely and accurate locations of enemy weapons systems, units, and activities which may impact on his operations. Intelligence must be sufficiently accurate to support effective attack by fire, maneuver, and EW or to support deception operations.

ELECTRONIC WARFARE

The corps commander uses EW to his best advantage and attempts to deny its use to the enemy. The three basic EW tools available to the corps commander are electronic countermeasures (ECM), electronic counter-countermeasures (ECCM), and electronic support measures (ESM).

Electronic Countermeasures

ECM are the offensive arm of EW. ECM operations consist of jamming and electronic deception. Jamming signals are used to prevent or degrade threat reception by deliberate radiation or reradiation of electromagnetic energy. Electronic deception operations are normally conducted as a part of a larger deception operation and are seldom (if ever) conducted alone.

Electronic Counter-Countermeasures

Defense of the electronic spectrum is accomplished through the use of ECCM. ECCM are the responsibility of every soldier who either uses or supervises the use of radios or other electronic equipment.

Electronic Support Measures

ESM are essential for the collection of information leading to suppression, neutralization or destruction of enemy command, control, and communications (C^3) capabilities. ESM involve actions taken to search for, intercept, locate, identify, track, and monitor high payoff C^3 targets to ensure the desired effects are achieved.

In allocating his EW resources, the corps commander prioritizes available assets against battlefield targets. In most cases, the demands placed on EW assets exceed their ability to exploit or disrupt all high payoff targets (HPTs).

COUNTERINTELLIGENCE

Threat forces represent a constant, pervasive, and multidisciplined danger to the security of the US Army. Hostile intelligence services (HOIS) have the

ability to employ human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), and measurement and signature intelligence (MASINT) collection systems and organizations against the corps. CI activities conducted within the corps area of operations (AO) support operations security (OPSEC), battlefield deception, and rear operations.

IDENTIFYING THE CHALLENGES

HIGH- AND MID-INTENSITY CONFLICT

In any conflict, the MI staff synchronizes the functional intelligence effort within corps IEW elements. Division IEW activity, echelons above corps (EAC), other services, and Allied capabilities and efforts are also considered. Synchronization focuses efforts by sensor, discipline, echelon, and priority to provide intelligence information to the corps commander covering the breadth and depth of the battlefield. Tactically, orders and plans are based on intelligence. Operationally, intelligence anticipates needs and provides projected judgments which allow decisions on when and where to fight.

Intelligence activities are planned and conducted in support of rear, close, and deep operations. Through management and analysis techniques and a thorough knowledge of available resources and their capabilities, the G2 focuses the corps intelligence system to understand the threat in the corps area of interest.

The IEW system at corps is structured to best use the available resources to predict threat intentions. It identifies weaknesses and isolates times when the threat is most vulnerable and susceptible to friendly offensive action.

The IEW system also supports the selection of the most favorable terrain, predicts weather in the AO, and identifies the effects on enemy and friendly operations. With the same sense of initiative and synchronization, the G2 provides CI support. This action supports--

- Countersurveillance and counter-reconnaissance actions that protect the true status of friendly operations.
- Countermeasures that reduce or eliminate the radioelectronic combat (REC) threat.
- Deception that creates a false picture of friendly activities, preparations, and operations to support the commander's objectives.

LOW-INTENSITY CONFLICT

LIC pits intelligence against irregular and unconventional threat forces and terrorists. LIC poses a continuous threat and requires peacetime contingency actions. The commander requires intelligence resources to provide him intelligence for planning and execution similar to that in the higher

levels of conflict. The requirement for timeliness and accuracy of the intelligence product is constant. The intensity of the intelligence effort remains high. The difficulty of the tasks increases as the illusiveness of the encountered threat force increases. The emphasis on the intelligence disciplines may shift. Unique intelligence relationships with host nations may be required both in foreign internal defense (FID) and in peacekeeping operations.

At the low end of the threat spectrum are the independent, state-sponsored terrorists who serve as an instrument of government policy in peacetime and in both high- and mid-intensity conflicts. The intelligence investment in dedication, management, resources, and execution against these targets is costly. Prediction and appropriate counteraction are the challenges.

In LIC, corps operations and the supporting intelligence system fulfill strategic objectives and require corps intelligence to derive and design innovative arrangements.

CHAPTER 2

CORPS INTELLIGENCE IN THE AIRLAND BATTLE

STRUCTURE OF MODERN WARFARE

Our basic fighting doctrine is the AirLand Battle. Because war is a national undertaking, it must be coordinated from the highest to the most basic levels of execution. The IEW system is no different. Like the AirLand Battle Doctrine it supports, IEW exploits all available capabilities. The AirLand Battle is focused at the corps. Depending on the corps mission, corps IEW roles may be strategic, operational, or tactical. The very nature of modern warfare and national commitment directs that a corps IEW capacity be developed to fulfill one or all of these roles.

DOCTRINAL REQUIREMENTS FOR INTELLIGENCE

Corps intelligence is linked to theater, national, and Allied intelligence systems. At the operational level, intelligence must see deep enough to identify the enemy's center of gravity, his source of strength and balance. The direction of corps and higher intelligence capabilities strives to pinpoint the threat force and predict what he is most likely to do in time for the corps commander to concentrate enough combat power through fire and maneuver to defeat the threat force.

Intelligence gives the commander a decision-making edge. The G2 anticipates, coordinates, and executes intelligence missions well ahead to satisfy his commander's intent. Corps assets provide the commander and his G2 the greatest flexibility in accomplishing IEW tasks. The MI brigade commander, his staff, and subordinate commanders execute this singleness of purpose. Tactical engagements require more demanding responses from the IEW system. They require tighter cycles of performance to track enemy activities and systems with sufficient accuracy to direct fires on them.

Each of the four AirLand Battle tenets has an impact on IEW activities.

INITIATIVE

The offensive spirit thrives in initiative. Initiative forces the threat to conform to our operational purpose while we retain the capacity to act independently to defeat him. As individuals, we move within the framework of the commander's intent. In the offense, the IEW system seeks rapid solutions to problems regarding threat situation, intent, capabilities, and weaknesses. It also seeks rapid and accurate target development, with priority dissemination to EW, fire, and maneuver elements. Concurrently, it ensures OPSEC through CI and deception. In the defense, the IEW system seeks advance warning to turn the battle into an offensive advantage.

AGILITY

Friendly forces must act faster than the threat. To do this, intelligence focuses on reducing uncertainty. To "read" the battle the commander must "see" the battlefield. The G2 gives the commander the best available intelligence about the threat, focusing on what he will probably do, so that the commander can quickly decide and act to take advantage of every weakness. The corps intelligence system must be sufficiently agile and flexible to respond to changing situations.

DEPTH

Depth allows the commander time to plan, arrange, and execute operations; allows space to maneuver; and provides the ability to marshal and protect necessary resources. IEW provides situation and target intelligence throughout the depth of the battlefield. The G2 enables the commander to see beyond the requirements of the moment and aggressively gain information about the threat and the area.

SYNCHRONIZATION

The commander manages the battlefield in time and space to concentrate combat at decisive points. By coordinating the activities of corps forces with adjacent and higher commanders, the corps commander produces a synchronized operation. IEW activity is synchronized in a like manner. Synchronization achieves results, reduces overlap, and identifies gaps in continuity, time, and space. It also focuses the efficiency of the effort and its responsiveness and coverage to the full depth of the commander's AO.

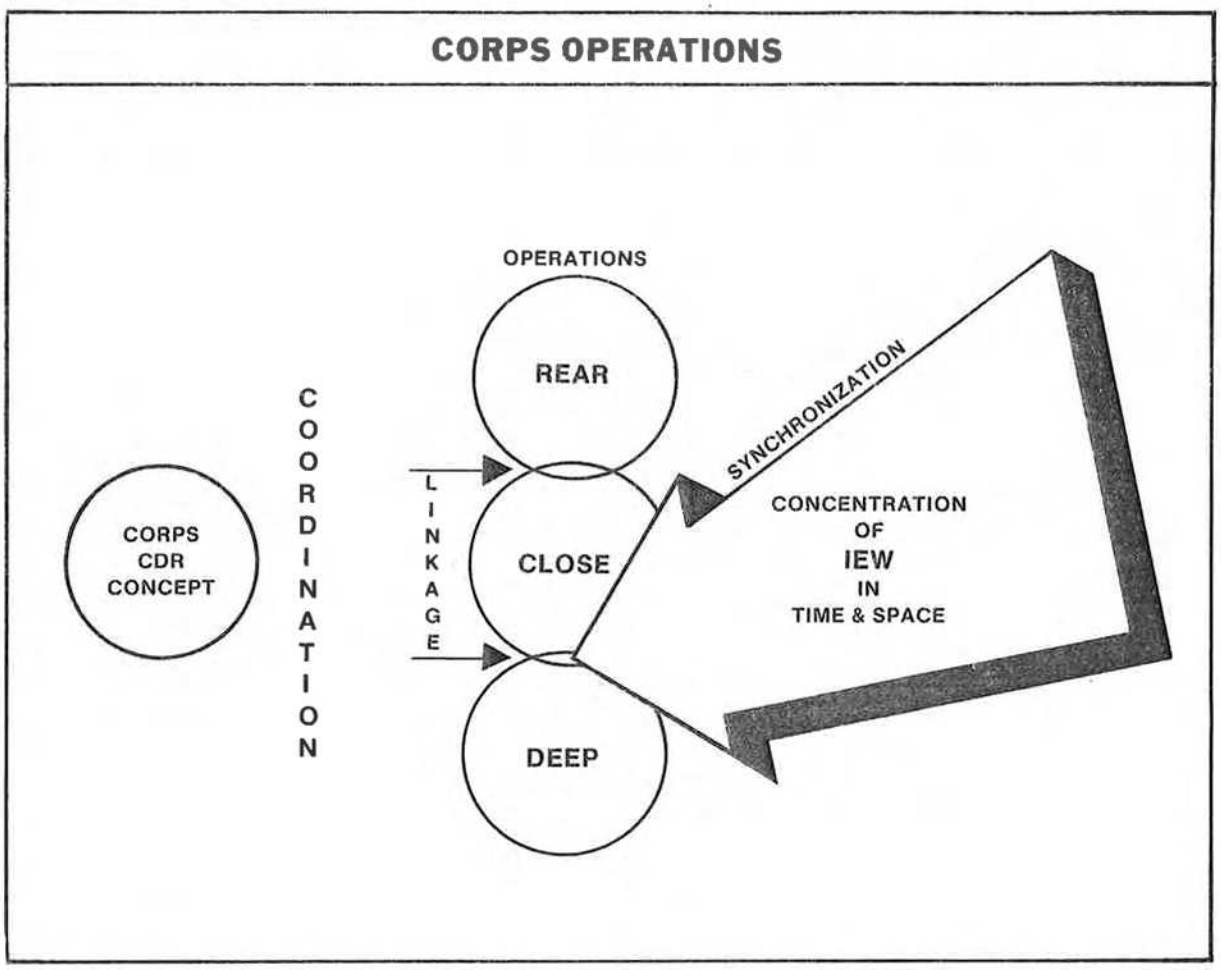
CLOSE, DEEP, AND REAR IEW

Close, deep, and rear corps operations (see following illustration) require continuous synchronization of IEW activities and deliberate planning for the use of IEW assets at all echelons. The G2 tasks corps assets, levies requirements on division assets, and requests support from EAC.

REAR OPERATIONS

The G2 and the corps IEW system have only limited capability to support the corps rear. CSS and reserve elements awaiting commitment provide intelligence assistance in support of rear operations. MI units respond to the fluid nature of the rear area as the dynamics affect the close operations at the FLOT. The rear area is ever changing in both geography and the units that occupy it.

CI elements of the corps and EAC monitor the rear for terrorists, saboteurs, and special action elements. They conduct extensive liaison with US and Allied forces and host-nation security organizations to fulfill collection requirements. When conventional forces penetrate the rear, the situation becomes more conventional and may require the diversion of other corps resources.



CLOSE OPERATIONS

In close operations, the corps G2 is concerned with the corps battle and the operations of the divisions. He seeks to ensure, through coordination and synchronization, the best use of corps and major subordinate command (MSC) organic assets. The MI brigade commander may be directed to deploy IEW assets to augment the division capability. In close operations, combat information flows from the ACR, air cavalry, artillery units, the committed divisions and brigades, air defense elements, and engineer units. The G2 speeds available intelligence to the committed maneuver and combat support units to assist in the conduct of combat operations.

DEEP OPERATIONS

FMs 100-5 and 100-15 express the doctrinal requirements for deep operations in the successful execution of the AirLand Battle. A corps is able to accomplish deep operations in both offensive and defensive situations. The corps commander accomplishes three critical tasks:

° Control the close fight.

° Deny the enemy the ability to concentrate his uncommitted forces.

° Attack enemy forces in-depth.

Two of these tasks are directly dependent upon successful deep operations. The accomplishment of the first task, control the close fight, is significantly enhanced by, and generally can, only be accomplished when aided by, appropriate deep operations.

Whether corps-level deep operations take the form of a deliberate attack, with multiple divisions keying on uncommitted enemy forces, or spring from other successful engagements leading to the exploitation and pursuit, the job for the corps G2 remains essentially the same: focus scarce collection assets and an overtaxed intelligence process to achieve maximum benefit.

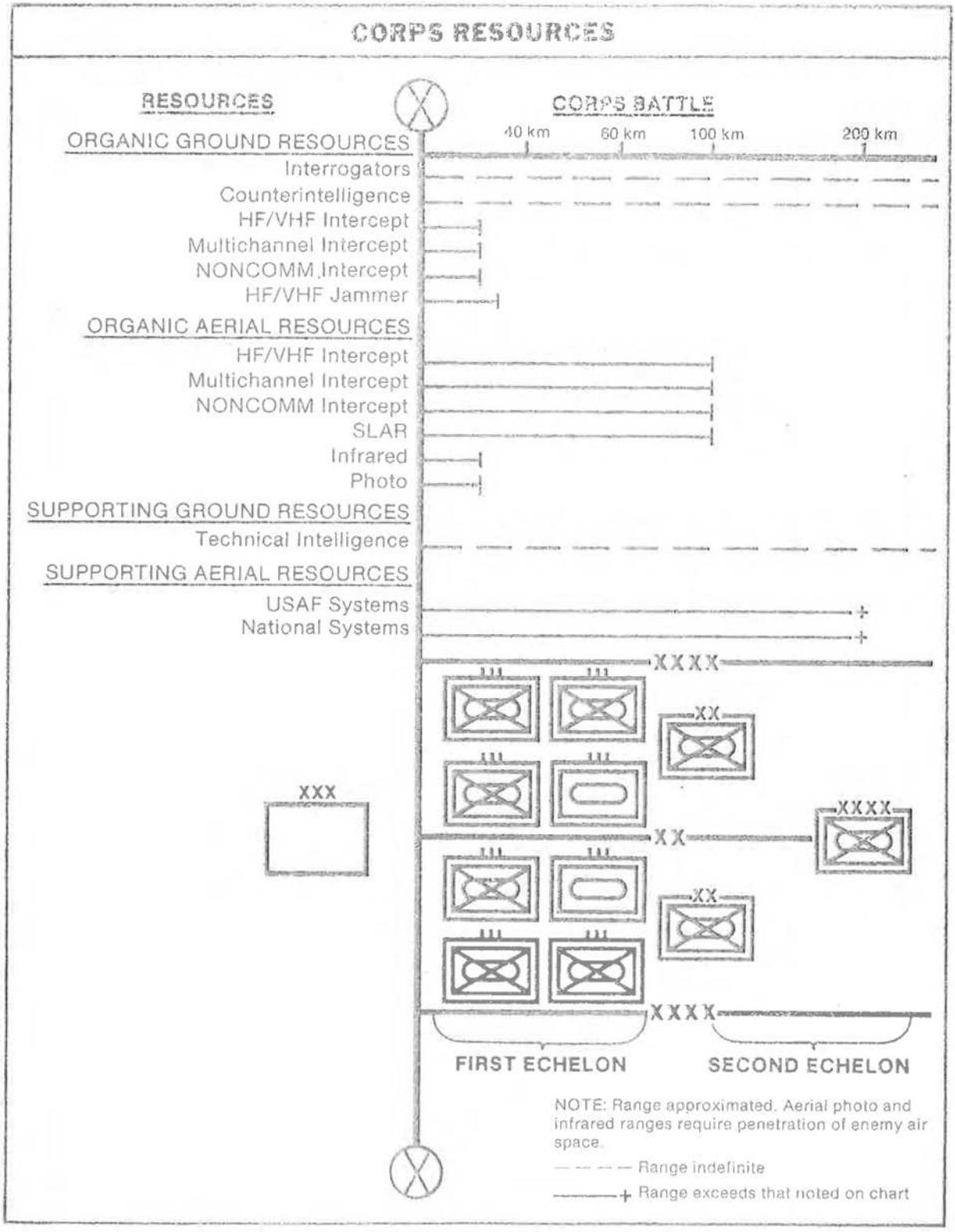
Deep operations place a heavy premium on knowing the scope, scale, and tempo of the threat's operations and where his main efforts will occur. To achieve decisive results, the G2 determines the threat strengths and weaknesses. A threat center of gravity is not generally exploitable by corps level operations, or any other level for that matter, unless a vulnerability can be isolated and attacked. Where vulnerabilities are not evident, the G2 shows where they can be made through the application of force or deception.

Corps intelligence functions are not organically structured or equipped to support deep maneuver operations. Collectors and processors have been designed with a stable, linear FLOT in mind. Doctrine originally called for the threat force to close on corps positions giving the intelligence process time to digest and distribute information to awaiting defensive forces. Thrusting corps forces deep across the FLOT places a severe strain on the intelligence response time. The G2 improvises in using existing assets for the much more demanding deep operations (see the following illustration on corps resources).

In ascending order of complexity, the corps G2 supports three distinct types of operations: first, the targeting process required to support deep missile attacks or attacks by high performance aircraft; second, a deep attack operation employing attack helicopters; the third and most complex, involves the use of ground maneuver forces.

TARGETING PROCESS

Deep missile and manned high performance aircraft are directed against threat follow-on forces or reserves at operational depths to disrupt the tempo of the threat offensive operations. To increase weapons effects and target vulnerability, attacks are generally launched against forces on the move. Concurrent attacks are launched against HPTs (such as command, control, communications, and intelligence (C3I) nodes) generating a more complete disruption of the movement. While this method of attack focuses more on disruption than on destruction, deep attacks can desynchronize enemy movement to achieve decisive results at the FLOT.


CORPS RESOURCES
RESOURCES
CORPS BATTLE
40 km
60 km
100 km
200 km
ORGANIC GROUND RESOURCES
Interrogators
Counterintelligence
HF/VHF Intercept
Multichannel Intercept
NONCOMM Intercept
HF/VHF Jammer
ORGANIC AERIAL RESOURCES
HF/VHF Intercept
Multichannel Intercept
NONCOMM Intercept
SLAR
Infrared
Photo
SUPPORTING GROUND RESOURCES
Technical Intelligence
SUPPORTING AERIAL RESOURCES
USAF Systems
National Systems
XXXX
XX
XXX
XX
XXXX
XX
XXXX
FIRST ECHELON
SECOND ECHELON
NOTE: Range approximated. Aerial photo and infrared ranges require penetration of enemy air space.
Range indefinite
Range exceeds that noted on chart

For deep missile and manned aircraft attacks the G2 senses where the enemy force is assembled, estimates its dwell time in that location, and senses the force as movement begins. The task, then, is to predict when critical elements of the enemy force pass a trigger point for subsequent attack by preplanned fire missions or air sorties. At the same time, high value targets (HVTs), such as critical enemy C^3I nodes, are monitored for potential attack or ECM operations. Because most targets can be rapidly reconstituted, attacks are timed to coincide with the most critical time window.

Supporting stand-off attacks requires the G2 to rely on detailed IPB of the deep area and on sensors sharply focused on the area in question. The corps G2, generally, counts on electronic sensors like GUARDRAIL and QUICKLOOK to give the first indicator of movement and then follow up with side looking airborne radar (SLAR) to determine how closely the enemy force adheres to a predictive model. Having focused the correct sensors on the problem, the G2 ensures that a hot loop is established between the processor and the shooter and the corps fire support element (FSE) to reduce data delays to an absolute minimum. Long-range reconnaissance assets play a major role. Strategically placed near trigger points, long-range surveillance units (LRSUs) provide direct tip-offs of critical enemy movements and accurate target identification.

While corps intelligence collectors and processors are useful in the corps planning effort, that is, 72 hours or more into the future, they are of less utility supporting the minute-by-minute countdown to weapons launch. While EAC sensors are allocated to the corps deep attack mission, the processing delays are, generally, significant, and transmission times from the processor to the corps are prohibitively slow. EAC sensors' major contribution to the deep attack is to watch well beyond the engagement area for approaching forces and to help maintain the corps perspective of how the battle will unfold in the next 3 to 5 days.

DEEP ATTACK OPERATIONS

Deep attack helicopter operations executed by the corps attack helicopter regiment represent a quantum increase in complexity over stand-off attack methods for three principal reasons. First, the attacking aircraft move more slowly than missiles or high performance attack aircraft, increasing their exposure to enemy countermeasures and allowing the target greater opportunity to do the unexpected. Second, except in rare circumstances, the Air Force is not able to fly suppression missions or provide ECM support; therefore, the attack helicopter force carefully chooses FLOT crossing points and ingress and egress routes to avoid enemy interference. Third, communications links to deep penetrating aircraft are tenuous, often demanding jury-rigged arrangements such as using the GUARDRAIL AN/ARC-164 airborne radio to relay critical data in near real time. Offsetting these complexities requires an exceptionally close relationship between intelligence, fire support, and helicopter operations.

When a corps-level deep attack helicopter operation commences, most of the collection, processing, and dissemination assets are narrowly focused on the air operation. This by definition requires risks be taken elsewhere.

Approximately 2 hours before aircraft launch, the G2 makes a final assessment of enemy elements at the penetration point and updates the tactical fire direction system (TACFIRE) data base with known and suspected ADA sites. In close coordination with the FSE and attack helicopter operations staffs, suppression of enemy air defenses (SEAD) operations are planned. Provisions are made for the G2 to identify ADA elements remaining active after the suppression mission is fired. Selected suppression missions may be refired, or the air commander may elect to use an alternate ingress route. This real-time coordination demands near real-time exchange of data. The situation is best managed by collocating a G2, FSE, and helicopter team in a sensitive compartmented information facility (SCIF) area where they have instant access to critical information and where several alternate means of communications are available. Collocating a TACFIRE terminal in the SCIF is indispensable for moving target data rapidly around the battlefield.

With the helicopter force clear of the high-intensity ADA weapons zone near the FLOT, the G2 shifts assets to monitor activity along the ingress routes and in the target area. Targets for this force are nearly always moving threat forces for two reasons: First, the cleanest shots are available to attacking pilots. Second, local air defense systems are generally intermingled in the march column or focused on protecting key choke points. Accordingly, moving units are more vulnerable to attack than forces arrayed in a well protected assembly area.

Moving targets, however, represent a major challenge for the G2 who assesses rates of march and predicts arrival times at predesignated kill zones. Again, a close G2 attack helicopter unit coordination is required. Attacking aircraft must be synchronized with threat movement. Sensors and attacking aircraft must be redirected when the unexpected occurs.

Once the force is in the target area, the G2 has the responsibility to do near real-time damage assessment. He senses and reports enemy reactions to this attack. At the same time, the G2 focuses assets on the egress routes highlighting changes that have occurred since the attack was launched.

The G2 uses GUARDRAIL, QUICKLOOK, SLAR, and LRSUs much as he did for stand-off attack operations, with two exceptions: First, as previously discussed, the G2 causes all intelligence to be focused in an ad hoc operations cell, normally located at the corps main command post (CP) adjacent or integral to the corps tactical operations center (CTOC) support element. Second, each GUARDRAIL, QUICKLOOK, and SLAR operator involved in the mission is briefed in detail on the commander's intent and the schemes of his fire support and maneuver.

GROUND MANEUVER FORCES

Attacking deep, with mobile forces on single or multiple axes in concert with Air Force close support, battlefield air interdiction, air interdiction, and organic aircraft operations, a deception operation, a variety of ECM operations, and deep missile attacks, represents a most challenging environment for the corps G2. Intelligence collection and processing capabilities inevitably fall far short of the total need, requiring the corps commander to be deeply involved in assessing intelligence risks of the operation.

The commander's intent and PIR drive the intelligence process, but now because of the far ranging and varying types of operations, the G2 takes a phased approach to problem solving. Working closely with his analysts and his collection manager, the G2 shifts the focus of his intelligence efforts to meet emerging requirements.

Recognizing the severe limitations of the division's ground-based collection assets while on the move, the corps G2 uses SLAR, GUARDRAIL, and QUICKLOOK to feed near real-time critical intelligence to the division. Frequently, the division receives support from corps intelligence systems on targets well within its area of interest and within doctrinal range of divisional systems. This support is essential if the attacking division is to maintain its momentum in a fast-moving deep attack operation.

The division focuses on force-oriented objectives, attacking where least expected to exploit vulnerabilities of the enemy force. The corps G2, G3, and the FSE team have the responsibility of bringing friendly and threat forces together in time and space and achieving a decisive advantage over the threat. Threat force tracking and predicting are essential.

Division attack helicopter assets operate within the vacuum created by the attacking brigades as they eliminate air defense systems and disrupt enemy command and control (C2). Generally division attack helicopters operate forward of the point of contact to a limited depth in close concert with ground forces. Under these conditions, the corps G2 does not have to allocate additional assets to support the helicopter operations. Occasionally, the division commander may elect to strike at greater depths with his helicopter force. Planning for these deep operations involves the corps G2 from the onset to ensure adequate IEW assets are available.

Major operations, like a corps deep attack, have a series of branches to the plan and perhaps a sequel or two. The G2 has planned to support preplanned branches when executed and to respond to branches of opportunity that have not been preplanned.

Deep attack plans, like all other types of plans, have culminating points. Successful operations find the disruption of the enemy center of gravity occurring enroute to or near a culminating point so the mission is

accomplished before the force reaches its farthest extension. To determine the culminating point is extremely difficult for the corps commander and is a unique and exacting challenge for the G2.

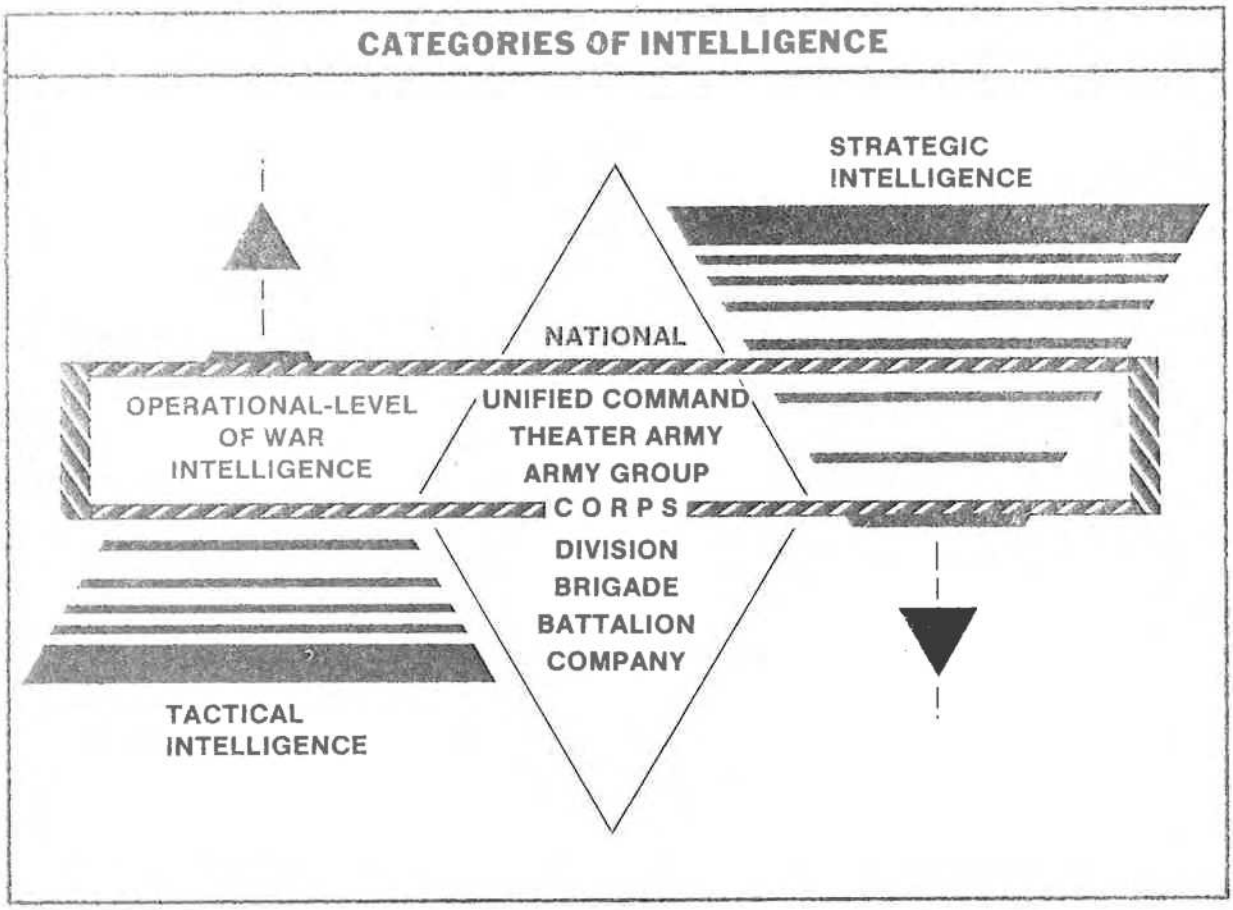
Deep operations place the heaviest burden upon and represent the greatest challenge to the corps IEW system. Support to the three types of deep operations is the most difficult corps IEW mission. The challenges include the identification of the threat's operational center of gravity and any associated vulnerabilities which would allow a feasible opportunity for the corps to strike at this center of gravity. Often the G2 recommends methods to create or expand these vulnerabilities as well as targeting in near real-time support to SEAD, breakthrough operations, meeting engagements, exploitation, and the pursuit. A major task is the prediction of threat reactions to our efforts to seize the initiative.

NATIONAL INTELLIGENCE

Intelligence is categorized as either strategic, operational, or tactical (see following illustration). The focus and definition of each are tailored to the echelon and type of decision maker to be supported. Strategic intelligence is defined as that intelligence required by national and Allied decision makers to formulate national, foreign, and defense policy. The intelligence requirements of the NCA are global, reflecting the complexities of a continuously evolving national interest and international context. The strategic intelligence community collects, analyzes, and disseminates intelligence which satisfies the constantly changing requirements of national-level decision makers. As the imperatives of American foreign and defense policy change, so too does the focus of strategic intelligence.

The establishment of theaters of war or unified commands (assigned distinct geographical AOs) reflects the imperatives of American foreign and defense policy. While the intelligence requirements of the NCA are global, the intelligence requirements of the theater or unified command reflect the peculiar peacetime and wartime responsibilities assigned to them in the joint strategic capabilities plan. The military strategy, force structure, and intelligence requirements of each theater of war are distinct. The nature of alliances, adversary military capabilities, and political and military objectives are different within each theater.

While a theater commander may require access to the assets of the strategic intelligence community to support peacetime or wartime campaign requirements, the immediate focus of the NCA may be towards political and military developments in another theater of war. Because of the demands on the strategic intelligence community and given the focus of tactical intelligence, an operational level intelligence perspective is necessary if the peacetime and wartime campaign planning objectives of the operational-level commander are to be realized. Operational level of war intelligence is defined as that intelligence required for the planning and conduct of campaigns within a theater of war. At the operational level of war,


CATEGORIES OF INTELLIGENCE
STRATEGIC
INTELLIGENCE
NATIONAL
OPERATIONAL-LEVEL
OF WAR
INTELLIGENCE
UNIFIED COMMAND
THEATER ARMY
ARMY GROUP
C O R P S
DIVISION
BRIGADE
BATTALION
COMPANY
TACTICAL
INTELLIGENCE

intelligence concentrates on the collection, identification, location, and analysis of strategic and operational centers of gravity that, if successfully attacked, will achieve friendly, political, and military-strategic objectives within a theater of war.

Operational level of war intelligence focuses on the intelligence requirements of theater, army group, field army, and corps commanders. The echelon focus at the operational level is situationally dependent, reflecting the nature of the theater of war itself, the political and military objectives of the combatants, and the types of military forces which can be employed. While the planning considerations of the tactical commander are principally military in nature, the campaign planning considerations of the national-level commander incorporate political, economic, psychological, geographical, and military factors.

Within a theater of war, joint and combined military forces achieve the political objectives set forth by the NCA. Realization of political objectives within a theater requires the defeat of those strategic and national centers of gravity which permit a threat alliance to maintain the momentum of a campaign effort and necessary political support. Identification, targeting, and defeat of these centers of gravity are contingent on an IEW perspective and system which takes into account the peacetime and wartime planning imperatives of an operational-level commander-in-chief. Certainly the demands on the strategic intelligence community at a time of war will limit the ability of theater staffs to access these systems. If the focus of operational responsibility is a theater command, the EAC MI brigade generally provides intelligence support to that command. Access to national-level systems is maintained by the EAC intelligence center (EACIC). However, the bulk of the all-source intelligence analysis and the performance of operational-level IPB functions to satisfy the requirements of theater staffs and commander are performed by the theater J2, with the support of the J2 staff and the EACIC. Because of the focus of intelligence at the tactical level of war, evolving battles and engagements, and the rapid dissemination and exploitation of combat information and tactical intelligence, intelligence produced at this level, if not properly screened, could well overwhelm theater and subordinate staffs and distract them from their necessary operational-level perspective.

Five, not four, IEW tasks are performed at the operational level of war: situation development, target development, electronic warfare, security and deception, and indications and warning. Situation development or IPB at the operational level of war involves four functions: theater area evaluation, analysis of the characteristics of the theater AO (geographical, political, economic, industrial, communications analysis of the entire theater of war to discern the operational impact of significant regional features will have on the conduct of both the friendly and adversary campaign effort), threat evaluation, and threat integration. Through the continuous development and refinement of situation, event, and decision support templates, the theater J2 determines the political and military designs of the threat, the specific threat objectives within theater, the time required to realize these

objectives, and target areas of interest (TAIs) keyed to strategic and operational centers of gravity. Target development at the operational level involves the identification of those HPTs as part of the theater command, control, and communications countermeasures (C^3CM) strategy--or operational engagement scenario--that if attacked lead to the defeat of centers of gravity. Electronic warfare or joint and combined EW at the operational level interfaces with other joint and combined destructive systems in the context of the theater C^3CM strategy. OPSEC measures and the theater deception strategy are incorporated in the theater campaign plan. Indications and warning involves the continuous development and refinement of regional or theater-based indicator lists which allow operational-level intelligence staffs to determine changes in the political, military, economic, and diplomatic behavior of a threat force, thereby, allowing the theater commander to better anticipate and understand NCA actions which may lead to the decision for military involvement. To avoid being caught by strategic surprise, it is essential that the theater commander and the NCA have theater-based all-source intelligence analysis (through the operation of the worldwide indications and monitoring system). High-intensity conflict in a theater of war is preceded by a failure on the part of the involved nations to adhere to long-standing rules of behavior. Once a theater J2 staff has discerned the adversary's political designs, the information gleaned during the performance of the second (analysis of the nature of the theater of war) and third (threat evaluation) functions of operational IPB yields a broad picture of how a threat alliance could be expected to fight and for what objectives.

CORPS G2

The G2 is the commander's expert on the enemy and provides critical intelligence for corps operations. The corps G2 directs the intelligence effort within the corps. He is responsible for the analysis of terrain, weather, and the enemy situation within the areas of interest and operation. Based on the commander's guidance and concept of the operation, the G2 develops and gains approval for the corps PIR and IR. Based on the corps commander's intent, he translates PIR and IR into taskings or requests for intelligence. He ensures the collection priorities are synchronized with the commander's intent and contributes to the development of target guidance. Under his supervision, national and tactical intelligence are fused into an integrated all-source product. He ensures rapid dissemination of needed intelligence and combat information.

ESM is a component of EW. While the G3 has overall responsibility for EW, ESM is a G2 function. ESM is the collection and reporting of combat information and targeting data obtained as a result of interception, identifying, locating, and monitoring the C-E activities of threat forces. It is used to support maneuver of corps combat units, fire support systems, and jamming. EW assets of the corps MI brigade conduct ESM activities in support of corps operations. The G2 exercises staff responsibility for planning, executing, and coordinating ESM operations throughout the corps area.

The G2 tasks the MI brigade as the principal agency for information and tasks all other corps elements with collection missions within their capabilities. He requests support and receives intelligence from EAC, other services, Allied nations, and national systems to meet corps requirements.

The G2 plans, directs, and coordinates CI operations throughout the corps area to--

- Determine friendly vulnerabilities to enemy reconnaissance, surveillance, and target acquisition (RSTA) activities.
- Identify enemy counter-C^3 capabilities.
- Predict deep operations conducted by enemy sympathizers, agents, saboteurs, and military forces.

The G2 recommends OPSEC measures to cover friendly operations and to protect essential elements of friendly information (EEFI). He coordinates countersurveillance and signal security (SIGSEC) measures with the G3 and other staff officers such as the communications-electronics (C-E) officer. He assists the G3 in planning deception operations. He identifies the deception target and the operational means to communicate the deception story to the target. He monitors enemy reactions to the deception story and provides feed-back information to the G3 and other staff officers for use in future operations. The G2 focuses on identifying and predicting the enemy threat to friendly rear operations. He recommends OPSEC, deception, and both lethal and nonlethal attack measures to counter enemy actions and to ensure friendly C^2 and sustainment operations in sensitive rear areas. The G2 supervises the CI analysis section of the CTOC support element. He coordinates with the corps G3, OPSEC, deception, C-E, and other staff elements to ensure CI support requirements are satisfied. He levies CI missions on the corps MI brigade, the only corps-level asset with a CI capability, and requests additional CI support from EAC, when needed.

The G2 establishes and enforces corps policy for information and document security. He also supervises the corps special security office (SSO) and ensures that corps policies and procedures follow Department of the Army (DA), Department of Defense (DOD), Director Central Intelligence (DCI), and National Security Agency (NSA) guidelines.

A major product useful to the G2 at all levels of conflict is IPB. IPB integrates enemy doctrinal information with the battlefield situation to create a dynamic picture of the battlefield. The analytic fit of forces to the battlefield is complex and time consuming and must be done before the battle begins. Continually updated, it is a powerful graphics tool used by the G2 to focus the intelligence effort.

MI BRIGADE COMMANDER

The MI brigade commander is responsible for the health, welfare, administration, training, and readiness of the MI troops under his command.

He deploys and directs elements of his brigade in the accomplishment of assigned missions and tasks. He manages missions and assets under his command in careful coordination with the corps G2 (see the illustration, Corps Resources, on page 2-4).

The MI brigade commander reports directly to the corps commander. He responds to the corps commander and advises on the employment of the brigade's resources.

Through his operations center, the brigade commander employs brigade resources in response to corps mission tasking.

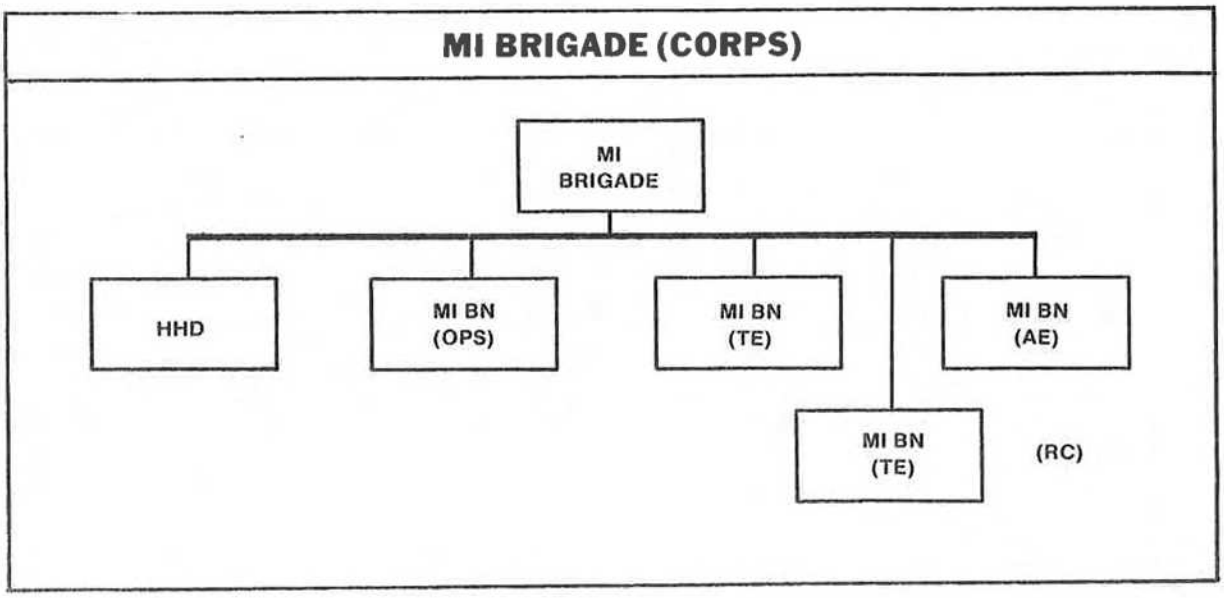
MI BRIGADE

The MI brigade (see the following illustration) is composed of a headquarters and headquarters detachment and three MI battalions:

° Operations.

° Tactical exploitation (TE).

° Aerial exploitation (AE).



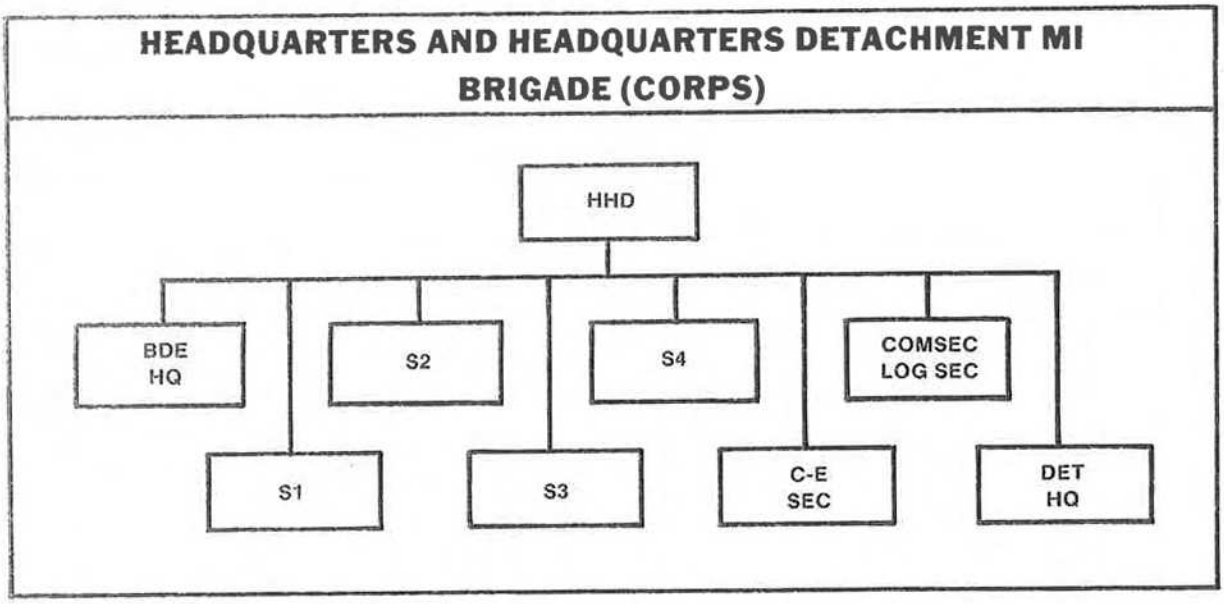
HEADQUARTERS AND HEADQUARTERS DETACHMENT

The organization of the headquarters and headquarters detachment (HHD) is shown in the following illustration. The mission of the HHD, MI Brigade at corps is to command and control all assigned and attached units. The HHD provides--

-- Command of subordinate elements conducting intelligence and EW operations.

-- Reinforcement of IEW support to division and below MI (CEWI) elements and other MI units or staffs.

-- Staff planning, control, and supervision of administration and operations of attached units.



MI BATTALION (OPERATIONS)

The MI battalion (operations) performs IEW functions in support of overall corps operations. It provides resources to assist the G3 in planning, coordinating, and evaluating the effectiveness of OPSEC measures and offensive EW operations.

The CTOC support element supports the G2 and G3 in the CTOC. It provides the collection management necessary to execute the four IEW tasks. It is a planning, coordinating, integrating, and directing element. It produces corps all-source intelligence. Elements of the CTOC support element provide OPSEC and deception for the G3 and EW and target development for the G3 and FSE. The technical control and analysis element (TCAE) is the corps focal point for SIGINT and EW execution under the brigade S3.

The signal company of the MI battalion (operations) provides communications links for tasking, reporting, and technical control.

MI BATTALION (TACTICAL EXPLOITATION)

The MI battalion (TE) provides CI, enemy prisoner of war interrogation (IPW), and ground based SIGINT and EW support to corps operations. The long-range surveillance company (LRSC) provides long-range surveillance support deep into the corps AO.

The CI interrogation company provides multidisciplined CI, OPSEC, interrogation, and document exploitation support to the corps. The company deploys throughout the corps rear and close operations areas. CI and interrogation personnel screen linecrossers and refugees, interrogate prisoners, and provide CI support to rear area operations.

The EW company has signal collection and communications jamming assets. Because of its range limitations, the company generally deploys well forward. It can be used to weight the battle in the same manner as maneuver units. EW capabilities include intercept of communications and noncommunications emissions and communications jamming. The corps LRSC organic to the active component (AC) MI battalion (TE) collects intelligence in the corps area and observes and reports enemy dispositions and movements.

MI BATTALION (AERIAL EXPLOITATION)

The MI battalion (AE) allows the corps commander to "see" the battlefield to the depth of the AO and beyond.

The MI battalion (AE) provides the corps commander with his deep-look capability through aerial reconnaissance, surveillance, and SIGINT collection. The reconnaissance and surveillance (R&S) assets of the MI battalion (AE) are in the aerial surveillance company. SIGINT assets are in the aerial EW company.

The aerial surveillance company provides R&S for the corps. The company plans and conducts aerial R&S of specific named areas of interest (NAIs) and avenues of approach into the corps AO.

The aerial EW company provides signal collection and processing for the corps. The company plans and conducts aerial SIGINT collection missions. It processes intercepted signals and reports combat information and intelligence data to the TCAE. Capabilities include communications intercept and direction finding (DF) (GUARDRAIL) and noncommunications emitter location and indentification (QUICKLOOK).

CHAPTER 3

COMMAND AND CONTROL

C^2 is the process of directing and controlling military forces. It is exercised by commanders. Staffs, operations centers, and communications and collection systems are all included in the C^2 system. Effective C^2 is critical to the attainment of any military objective.

The tangibles of C^2 are those elements which let the system work. Collection systems gather needed information. Staffs analyze, plan for what is to be done, and supervise the execution of the commander's orders. Operations centers are the focal point of any unit's operations. Communications systems provide the arteries through which information is reported, coordination is conducted, and tasks are distributed. They enable the commander to feel the pulse of his command at all times.

When the information has been collected and analyzed and the staff work completed, the commander makes his decision. He combines the available information and the assessments of his staff with his knowledge, training, and experience to decide how his objective will be reached. The intangibles are the driving force of C^2.

The unique character of C^2 is that it must be effective under the extraordinary stress of battle. It must be effective in situations which are obscure, in compressed time, and under the stress of personnel and equipment losses. It must work quickly. The extent and variety of tasks confronting the commander require the cooperative efforts of a large group of people, the integration of complex systems, and a sensible division of work.

The C^2 of the MI brigade and its assets are essential to synchronize intelligence at the corps level. In essence, the resources under the brigade are the only dedicated intelligence assets organic to the corps commander. Effective command and management of these resources are crucial to resolve the close, deep, and rear intelligence picture. Upon this, the commander makes his decisions. Battlefield success relies on that intelligence picture.

OPERATIONS

The operations element of the MI brigade is the key to C^2. The MI brigade S3 supervises the operations center. He supervises the employment of brigade assets and directs and coordinates the efforts of the operations center staff.

When deployed, the operations center is made up of the S2 and S3 sections of the MI brigade and the TCAE that is organic to the operations battalion.

The TCAE exercises technical management of the SIGINT and EW assets of the brigade. It maintains an extensive technical data base and has a SIGINT processing and reporting capability.

The operations center deploys with the brigade CP and may be situated from 0 to 15 kilometers from the CTOC that is located in proximity to the corps main CP. The operations center is a tactical SCIF which will require appropriate security support and oversight and control by the corps SSO. Physical protection is provided by the SCIF security section provided by the operations company, operations battalion of the MI brigade.

MANAGEMENT

The brigade S3 is the brigade mission manager. Under his supervision, the operations center plans, directs, and controls the employment of the MI brigade. Many of the considerations governing the employment of assets directly affect both the mission and asset management functions. Close coordination with the operations center, the subordinate units, and the support elements at the CTOC is the essential part of the managment process.

Unit commanders carry out asset management in response to mission tasking received from the corps collection management and dissemination (CM&D) section.

In its collection management role, the CM&D section ensures that orders and requests are received and understood by the collection agency. It monitors the collection operation to ensure that the needed information is collected and reported in a timely manner. It modifies the collection plan as old requirements are satisfied, are no longer needed, or as new requirements are generated.

PLANNING AND TASKING ORGANIZATION

The planning and tasking organization ensures that assets are committed effectively to satisfy corps information requirements. Principles of employment are--

- MI resources are not in reserve, although they may support a unit held in reserve.
- Centralized control and decentralized execution allow subordinate elements maximum flexibility in executing the task.
- Rapid dissemination.
- Multidiscipline support.

MI assets always are placed where they can most effectively contribute to the destruction of the enemy.

In any employment profile, the means to rapidly disseminate time-sensitive information must be provided. Procedures are stated by field standing operating procedures, specified in tasking, or dictated by the tactical situation. In any event, procedures and communications are established to

provide information where and when it is needed. Every effort is made to use multidiscipline support to satisfy mission tasking. This ensures the most complete and accurate response possible.

The operations center directs the employment of brigade assets to meet the mission tasking formulated by the CM&D section, CTOC support element. Factors to be considered before tasking assets include--

° Mission priority.

° Asset availability.

° Asset capability.

° Tactical situation.

° Current and planned missions.

° Asset status.

° Flexibility.

° Economy of effort.

° Terrain.

° Weather.

° Asset security needs.

Mission requirements throughout the corps are likely to exceed the capabilities of available assets. Decisions on the relative importance and priority of tasks are based on the principle that each asset is engaged in the highest priority task it is capable of performing. Tasking priorities reflect the mission priorities established by the commander, the G2, and the G3. They must be flexible, subject to changes in the stated priority, and based on the corps commander's intent.

The operations center remains aware of the current status and location of all brigade assets. This includes knowledge of tasks being performed and their priority, as well as status reports received from the MI battalion operations centers. The brigade operations center reports asset status to the CM&D section for use in mission management and for advising the corps G2 and G3.

The current and projected tactical situation has a direct impact on all MI operations. It largely determines the mission tasking that will be received and the selection and deployment of the specific assets to accomplish the mission.

The operations center monitors task accomplishment throughout the brigade to ensure that priority requirements are met, and that MI assets are being employed to their maximum capability. The effectiveness of assets in meeting their tasked objectives are reviewed constantly and tasking adjusted as necessary.

ASSET TASKING

Through correlation and refinement, mission tasking is translated into asset tasking. Specific assets are identified to accomplish each mission. Instructions are prepared and communicated to the tasked elements.

Tasking directs one or more operating elements of the brigade to prepare for, or to carry out, specific operations. It also can assign or change mission support roles, depending upon mission requirements.

Tasking instructions must be clear and concise, yet convey all information necessary to accomplish the task. They must be keyed to the specific needs of the tasked asset. Tasking instructions include the following information, as a minimum:

- Task objective.
- Resources.
- Coordinating and reporting instructions.
- Time requirements and constraints, or when the operation is to be conducted.
- Background and supporting information.

Tasking is transmitted from the MI brigade operations center to the operations centers of the MI battalion (TE), MI battalion (AE), and the key elements of each company. The task is then passed to specific assets for accomplishment.

OPERATIONS CENTER AND CTOC SUPPORT ELEMENTS

The requirements levied by the CM&D section of the CTOC support element form the basis for all brigade operations. Through communications with the CM&D section and the ASPS, the operations center--

- Receives mission tasking based on the IEW needs of the corps commander.
- Coordinates tasking and priorities.
- Reports accomplishment of assigned missions.
- Has access to all-source intelligence products, to include order of battle information produced by the all-source production section (ASPS).

BRIGADE OPERATING ELEMENTS

The brigade operations center communicates with brigade elements to--

- Task assets to fulfill mission tasking levied on the brigade. This includes all technical, background, and associated information necessary to accomplish the task.
- Receive combat information and intelligence from SIGINT and EW collection elements for exploitation or further reporting.
- Receive operational status reports. Deployed SIGINT and EW assets report their status through their battalion operations center to the MI brigade operations center.
- Coordinate, as required.

OPERATIONS CENTER AND TCAE

The TCAE is the focal point for the exchange of SIGINT and EW combat information and intelligence in the corps area. To ensure that information is available when and where needed, the TCAE establishes technical data links with the following:

- EAC (to include TCAE and all-source analysis elements) and intelligence elements of other services.
- TCAE at the division and below.
- Adjacent corps TCAEs.
- Adjacent Allied EW units.

The TCAE is dependent upon EAC to provide communications for interface with the national SIGINT system. This requires the development of a data base.

The TCAE provides technical data to the TCAEs at the divisions, ACR, and separate brigade to support their current and planned operations. There is a dedicated link between the TCAE and CM&D to cue analytical efforts, to informally exchange information, and to coordinate intelligence production. Data received from these elements is added to the technical data base and integrated for further analysis and reporting. The TCAE is a tactical SCIF which requires OPSEC support and security oversight and control by the corps SSO. Communications support is provided by the communications company, MI battalion (operations).

Data is exchanged and operations are coordinated with adjacent corps by the TCAE. In some instances, the adjacent corps may be from an Allied nation. However, coordination is critical, regardless of the nationality of the unit.

Coordination is especially important for ECM operations near a common boundary. Communications may be established through the multichannel system, through EAC, or by using organic equipment.

FUNCTIONS

The operations center is deployed to provide the brigade commander with centralized control and coordination of current tactical operations of the brigade. Functions performed within the operations center are essentially the same as those of other operations centers on the battlefield. They differ only in the uniqueness of the brigade mission and the staff expertise required to manage it.

BRIGADE S3

The S3 supervises the operations center and has staff responsibility for directing the integrated management of brigade resources. He ensures that each mission tasking received is promptly acted on and given the multidiscipline support necessary to satisfy the requirement. Under his supervision, the management and tasking of assets are accomplished by the S3 section, assisted by the TCAE for SIGINT and EW assets.

S3 SECTION

The S3 section is staffed with a cross section of personnel having the MI aviation, tactical intelligence, and SIGINT expertise necessary to provide effective management of brigade resources. Each mission received from the CM&D section is carefully reviewed to develop specific tasks for each intelligence collector. Assets that can contribute to accomplishing these specific tasks are identified, and tasking instructions are prepared and transmitted. Tasking for CI, imagery collection, and interrogation assets is transmitted by the S3 section. Tasking for SIGINT and EW assets is passed to the TCAE for technical management, task development, and transmission.

The main functions performed by the S3 section in managing and controlling brigade assets include--

- Maintaining continuous coordination with the CM&D section.
- Keeping abreast of the current battlefield situation.
- Developing plans for the employment of assets based on projected corps operations.
- Keeping the CM&D section advised of the current capabilities and operational status of brigade assets.
- Formulating and transmitting mission tasking.
- Maintaining the current status of assets through operational status reports received from brigade elements.

° Monitoring task accomplishment and adjusting tasking when required.

° Maintaining the necessary management records and logs.

COMMAND AND SUPPORT

Command and support relationships guide how the MI brigade will be organized for combat and define the degree of control and responsiveness required to accomplish the IEW mission as derived from the corps mission.

COMMAND

C^2 synchronizes all battlefield efforts and provides direction to the fight. The command relationships which direct MI commanders are--

° Organic.

° Assigned.

° Attached.

° Operational control (OPCON).

Organic elements form an essential part of a unit. They are listed in the unit's tables of organization and equipment.

Assigned units are placed in an organization on a relatively permanent basis. They are controlled and administered for their primary function, or the greater part of their functions, by the organization to which assigned.

Attached units are placed under the temporary C^2 of another unit. The directive establishing this relationship specifies the terms of attachment such as the provision of CSS. The commander to which the unit is attached exercises the same degree of C^2 over the attached unit as over units organic to his command.

OPCON places one unit under the control of another for direction and employment. OPCON basically has the same intent as attachment but the controlling unit does not have responsibility for logistical and administrative support. OPCON does not permit the gaining commander to tailor the unit placed in OPCON to him.

SUPPORT

Support relationships are established through the assignment of IEW standard tactical missions. These missions define the specific relationship and responsibilities between supporting and supported units. They do not affect organizational structure or command relationships.

The use of standard tactical missions ensures responsive IEW support to the corps and supported commands. They afford the supported commander the degree of control appropriate to his mission. The four IEW standard tactical missions are--

° Direct support (DS).

° Reinforcing.

° General support (GS) reinforcing.

° GS.

MI brigade elements with a DS mission are immediately responsive to the IEW requirements of the supported unit. DS is the most decentralized of the four standard IEW missions. It is not commonly used for brigade elements.

MI brigade elements with a GS mission provide support to the corps as a whole and are immediately responsive to the IEW requirements of the corps commander. GS is the most centralized IEW mission. The MI battalion (AE) and certain elements of the MI battalion (TE) normally are held in GS of the corps.

The IEW capabilities of MI units or staff sections are extended by use of the reinforcing mission. Reinforcing MI elements remain under the command of the MI commander assigning the reinforcing mission. OPCON is exercised by the MI unit being reinforced. The reinforcing mission permits increased support to specific maneuver units without giving up complete control of brigade assets to the supported elements. Elements of the MI battalion (operations) routinely reinforce the corps G2 and G3 and the MI brigade S3. Task-organized elements of the MI battalion (TE) reinforce the IEW capabilities of the MI units at the divisions and major subordinate commands, as appropriate.

MI brigade elements assigned a GS reinforcing mission provide support to the corps as their first priority. They also support and reinforce another MI unit as a second priority. This mission provides additional flexibility to meet rapidly-changing tactical situations. It may be used to provide the ECB a degree of control over MI brigade assets operating in their areas.

There are eight responsibilities inherent to each standard mission. The following matrix illustrates these responsibilities as applied to the four IEW standard missions.

TASK ORGANIZATION

The MI brigade commander directs the task organization of the brigade to accomplish the IEW mission. This is derived from the corps commander's concept of operations and from tasking from the G3. Task organization ensures that the best possible use is made of the limited resources available to the brigade. In task-organizing for combat, the MI brigade commander primarily considers five principles of war. These are--

STANDARD MISSION RESPONSIBILITIES MATRIX

MI UNIT WITH A MISSION OF	DIRECT SUPPORT	REINFORCING	GENERAL SUPPORT REINFORCING	GENERAL SUPPORT
1. Responds to req of	* Supported unit ** MI bde ops cen	* Reinf MI unit ** MI bde ops cen	* MI bde ops cen ** Reinf MI unit	* MI bde ops cen
2. Receives tech control from:	* Supported Unit	* Reinf MI unit ** MI bde ops cen	* MI bde ops cen ** Reinf MI unit	* MI bde ops cen
3. Has for a zone of action:	* Supported unit area of operations/interest	* All reinforced MI unit areas	* Corps area of interest	* Corps areas of operations/ interest
4. Furnishes IEW spt elm:	* To supported unit	NA	NA	NA
5. Furnishes liaison officer/NCO:	NA	* To reinf MI unit	* To reinf MI unit	NA
6. Establishes comm with:	* Supported command ** MI bde ops cen	* Reinf MI unit and MI bde	* Reinf MI unit ** MI bde ops cen	* MI bde ops cen
7. Is positioned by:	* MI unit cdr in coord w/supported comd	* Reinf MI unit or as ordered by MI bde ops cen	* MI bde ops cen or reinf MI unit if approved by MI bde ops cen	* MI bde ops cen
8. Req tasking planned by:	* Supported Units	* Reinf MI unit	* MI bde ops cen	* MI bde ops cen

* First priority ** Second priority

° Objective.

° Economy of force.

° Unity of command.

° Simplicity.

° Security.

The MI brigade commander must understand clearly the mission of the corps and corps subordinate elements, as well as the brigade mission. The brigade is task-organized to support these mission objectives. Brigade elements are assigned objectives that directly and indirectly contribute to the corps mission.

Economy of force requires that the brigade commander organize the limited available resources with emphasis on the area where the corps main effort will take place. However, resources also must be allocated to adequately support secondary efforts.

Unity of command is ensured by coordinating the actions and organization of all brigade elements toward common goals through mission orders. When required by mission and deployment, company teams are formed. This provides a unified command structure for all brigade elements. Commanders control their subordinates but allow them freedom to exercise initiative in carrying out their mission.

Direct simple plans and clear concise orders are the key to simplicity. They reduce confusion and help eliminate misunderstandings. Simplicity generates flexibility and fosters initiative, resulting in responsive IEW support.

In organizing for combat, the MI brigade commander directs the task organization of the brigade to satisfy his requirements for--

° Flexibility. This provides the capability to quickly adjust to the unexpected.

° Control. The appropriate degree of control is achieved through assignment of IEW standard tactical missions as described previously.

° Mission. Sufficient support to accomplish the mission is allocated.

° Future operations. Since MI resources are not held in reserve, organization must accommodate rapid reorganization to meet planned mission requirements.

CHAPTER 4

INTELLIGENCE IN COMBAT OPERATIONS

OPERATIONS

Intelligence is the key to planning and executing corps combat operations. It is a dynamic process that continues throughout an operation. It is used by the corps commander to develop his concept of the operation and by the G3 for the initial task organization, deployment, and direction of resources to fight all phases of the AirLand Battle. It also provides the basis for redirecting the corps effort when needed.

The corps offense is coordinated by the corps G3. Surveillance operations locate threat forces in the corps areas of interest and operations. EW, long-range fires, and maneuver in-depth are used to attack threat forces in the AO whose delay or disruption is important to the success of current corps operations.

In offensive operations, the deep attack disrupts, isolates, immobilizes, and weakens defenders in-depth. As the deep attack continues, it prevents the reorganization of coherent defenses by blocking the movement of threat reserves and the escape of defending units. In defensive operations, the deep attack prevents the threat from concentrating combat power against the corps and alters combat ratios at the FLOT. Such actions create opportunities for offensive action by the corps.

Major corps defensive operations separate attacking echelons; protect maneuvers taken by the defender; and degrade threat C^3, combat, combat support, and CSS units. Once the means of attack have been determined, the IEW system provides the optimum time. Sections of the CTOC support element use sensors and other available sources to determine the best time of attack and monitors the effects of interdiction. Long-range weapons are scarce and targets need to be chosen carefully. C3, key logistics centers, units, or terrain targets are those which, if targeted, will most likely degrade the threat's capability.

The basic corps battle plan is to accomplish its missions through either defensive or offensive operations as prescribed by the theater--Army group--commander. In either case, the operational concept of the corps is based upon three principal requirements. First, the corps controls key engagements in the close arena. Second, the corps denies the threat the ability to concentrate combat power by attacking follow-on forces at operational depths. Third, the corps conducts successful rear operations to retain freedom of action.

The basic corps defensive plan is to determine where the threat attack will occur. The corps, then, takes actions to prevail in key engagements in the close arena. It denies the threat the ability to concentrate combat power

against forward divisions by disrupting the tempo of follow-on forces. The corps commits reserves, if available, to gain positional leverage through counterattacking in-depth.

Corps actions are developed to realize these ends. The unit uses either fires or maneuver or both with EW, deception, and other forms of combat power. Initial or covering force actions concern situation development.

Using organic surveillance assets, reports from covering force, and information provided from EAC, the corps staff determines the axis and strength of the threat main attack. These same IEW assets are used to locate and track the second-echelon divisions of the attacking army within the corps area of interest. From this information and knowledge of threat doctrine and behavior, projections are made.

The corps projects assembly area locations, occupation, and dwell times for follow-on forces. It also projects the time and place of second-echelon commitment and probable routes of march to join the close operations. As the attacking army's follow-on forces move toward the FLOT, search areas for RSTA assets are specified. These are based on projected threat locations and activity relative to the corps plan. The corps may seek intelligence on a specific target which has been predicted and designated for attack. It may confirm a specific phase of predicted enemy activity which is a key trigger for initiating friendly operations.

The relevance of specific targets is their ability to adversely influence the corps operations or to support or reinforce the corps concept. As targets for attack are acquired, they are matched against appropriate predesignated attack systems for engagement during predetermined times. Targets requiring attack by precoordinated air assets are supported by joint suppression of enemy air defenses (J-SEAD) operations.

As in defensive operations, counterattack operations provide the corps the opportunity to wrest the initiative from the threat. Corps focuses on deep operations and the second echelon and reserves. Deep operations require corps synchronization of intelligence, maneuver, and fire support to destroy enemy units in-depth or to seize key terrain.

Fires directed against follow-on forces or reserves at operational depth disrupt threat offensive operations. This forces the threat to alter his plan. Effective C^3CM are employed. Threat C^2 systems are monitored and, if required, destroyed. Given the corps commander's concept--to exploit the threat commander's decision-making process by deceptive and disruptive means--it may be more beneficial to protect the threat C^3 facilities. Deception measures and electronic jamming operations may create ambiguity and interrupt the threat commander's transmission of combat orders.

Also as in defensive operations, control of close operations is key to a successful corps offensive battle. The committed divisions of the corps accomplish this task by maneuvering to avoid threat strengths. The corps

commander structures close operations to entrap the threat through a series of battles all directed at supporting the broader theater campaign. Even more so than in defensive operations, offensive operations depend on the part played by the corps staff and supporting collection systems.

Tasks in a corps offensive are the same as those of a defensive operation. They locate threat follow-on forces and deny the threat commander's concentration of forces against the corps committed divisions. If the corps is committed to an offensive battle from a theater reserve posture, initial intelligence situational data is quickly provided by theater and other committed forces.

The corps staff develops probable enemy responses to the offensive. The corps, then, plans and executes effective joint fire packages. These deny the threat the ability to concentrate forces and interfere with friendly maneuver elements.

The IEW support of offensive operations supports the corps requirement to conduct the AirLand Battle. For offensive operations, intelligence is necessary to focus the corps commander's concept of the operation. It also helps to detect and attack key target sets in support of that operation. Intelligence is supported by IPB and key IPB products. These are event and decision support templates; the full range of available sensors; and national, theater, and corps assets. They provide battlefield, targeting, technical information, and the all-source estimate of the battlefield conducted by the corps G2. Given the picture of the battlefield produced by each of these efforts, the commander is in a position to project friendly operations.

Specific threat options are described by the corps G2 to allow the G3 and the FSE to identify specific threats and the times when they will interfere with friendly operations. Planning and coordination necessary to detect and attack these specific targets are accomplished early enough to cause required sensors, weapons, and C^2 systems to be set in motion at the appropriate time.

Sensors are capable of supporting target engagement and, concurrently, provide continuous battlefield situational updates. The corps interest in relevant targets is reinforced as the corps transitions from target planning to attack execution. Individual responsibilities within the CTOC are different. However, the NAI, TAI, and routes that must be updated to support the situation development and subsequent battlefield planning and decision making do not change. These same NAIs and TAIs are essential to facilitate target development and target attack.

Situation development supports target attack and, conversely, target attack supports situation development. These activities are not mutually exclusive and do not require discrete sensors. Situation development forecasts threat activities which will have a high probability of interfering with corps operations. It identifies the specific observable parameters to aid in their detection, focuses the collection management effort that tasks

specific sensors to detect them, and helps predict when such threat targets will be detectable.

Once the corps has determined what it must do to seize battlefield initiative, the what, when, where, and how details are described. These details project how the threat is expected to respond to the friendly operation. Accordingly, the most probable responses are examined to identify the time and space boundaries. Identifying these specifics further highlight those threat capabilities which must be attacked. This requires the G2 to have a thorough understanding of the threat doctrine and norms, so that given the factors of mission, enemy, terrain, troops, and time (METT-T) and the commander's concept, he can make a disciplined assessment of the threat's probable responses. This assessment is made using the backward planning sequence.

This sequence begins by describing the threat's response at the general level and works down to the detailed level. That is, after first describing general battlefield functional areas that the threat could be expected to use (for example, maneuver, close air support, artillery, air defense), these areas are further examined. Threat operational templates are used to determine the time and space parameters associated with them. This serves to limit the number of threat responses that need to be further considered in determining where on the battlefield they could occur and to establish the general time lines within each function.

Once probable threat battlefield functional responses have been examined, specific threat capabilities, weapons systems, and units are examined in more detail. This avoids having to conduct a detailed examination of every weapons system and unit.

This more detailed examination results in the identification of specific threat targets and target sets, as well as their observable characteristics. We determine which of these observables is detectable, what detection means are available, what means are available for attack, what payoffs are to be gained, and what costs are involved. The most threatening targets are dealt with first. Attack priorities are those targets which represent the greatest threat and which the corps can effectively attack. Thus, these attacks, provide the greatest payoff and leverage for the operation to succeed.

We, then, match the target's observable features with appropriate detecting sensor systems and the most appropriate attack means. Thus, we determine friendly capabilities to counter the threat's most probable efforts to interfere. Once we identify these sensors and attack means, tasking or warning orders are issued. This ensures that the means to detect and to attack the relevant threat capabilities are in position at the right time and place. This planning, focused by the projection of friendly operations, is predictive in nature.

Advanced planning and early coordination are initiated in detail only after specific threat capabilities have been converted to relevant targets

(units and weapons systems). These targets are, then, already described in terms of time and space parameters, prioritized in terms of their potential to interfere with friendly operations, examined for their detectable observables, and evaluated to determine the most appropriate ways of minimizing their interference. Coordination includes all the supporting functions that are required to successfully degrade a specific threat capability, but focuses primarily on ensuring that required sensor systems and attack means are in the right place at the right time, tasked to detect and attack specific relevant targets.

For the sensors, this requires the corps intelligence collection plan to be continuously updated and annotated. This, in turn, allows for more precise focusing of collection by the CM&D section. This is not difficult, since the use of threat operational templates, or any other listing of specific threat system observables, will indicate the nature of the observable behavior as well as identify the sensors that can be used to detect it.

Operational availability of sensors is also assessed since corps, theater, and national sensors contribute to the all-source estimate of the situation that enables the corps to project its operation in battle planning. This same battle planning enables the G2 to describe the threat's responses and identify specific enemy capabilities that could interfere with the friendly operation. (Specific sensors that can rapidly communicate the detection of threat activity are tasked to be in place to trigger the execution phase.) Organic sensors are tasked directly; while theater sensors are requested to be in the required location at the required time in order to detect specific observables. Whether organic or theater sensors are to be used, the corps G2 initiates such action through the corps collection management element. Specific request channels may differ slightly by area or command.

A similar process occurs in fire support planning. Once relevant targets are identified, organic and supporting deep attack assets are considered in constructing a plan for fires. Warning orders for organic weapons are dispatched to permit executing units to make initial computations and to determine weapons mixes, warheads, launch units, launch sites, and so on. Theater battlefield air interdiction assets, unconventional warfare, or SOF are requested through channels established for the particular theater. Identification of corps requirements, especially battlefield air interdiction, can, thus, be accomplished early enough to influence the daily air tasking order or to at least determine which theater battlefield air interdiction attack resources can be expected to be available. This also provides for the early exchange of required information.

At this point, some 12 to 36 hours before an attack is expected, the basic planning for deep attack is accomplished. However, this is a continuous process repeated every 12 hours or so. This projects, confirms, predicts, and freshens engagement opportunities 24 to 72 hours in advance.

During this same period, the corps deep attack elements are actively involved on a dynamic battlefield. Friendly projections are modified to

adjust to the changing battlefield situation. Friendly objectives and the operational availability of sensors and weapon systems are expected to have changed. And, of course, the corps is concurrently involved in detecting and attacking targets identified in previous targeting periods.

Because targets almost never appear precisely as anticipated, adjustments to account for threat behavior must be made. The need for such adjustments is anticipated, even though the specific details cannot be planned in advance. Experience in using deep attack targeting helps to predict areas which produce higher or lower confidence levels for planning. Future predictions are adjusted accordingly.

Uncertainty in planning is compensated for in that the actual attack is not based on the prediction. Rather, it takes place only when the forecasted threat occurs within projected engagement time frames. The specific threats become the trigger events for the attack when detected by the friendly sensors. They are attacked using the means determined by anticipated planning.

The key point here is that even though the target engagement may not be exactly as projected, the planning for target attack still bounds the problem in time and space and relates the targets to a friendly operation. Thus, the timely execution of an attack against any threat that can interfere with that operation has far greater flexibility and responsiveness than if no planning had been done.

If, during the execution phase of the deep attack, the forecasted threat behavior does not occur, no attack is initiated. If an unanticipated but more threatening enemy activity is detected and is determined to have greater potential for interfering with corps operations than the planned and detected threat behavior, then the new target is attacked by means already in motion. If a planned threat target has been detected and attacked but still continues to interfere with the corps operations, that target can be reattacked in minimum time.

During this time, any last minute coordination is completed with the higher headquarters, air space control, and Air Force support elements (through the battlefield coordination element at the tactical air control center (TACC)). When Air Force strike activity is jointly employed with corps attack systems, the TACC (or the TACC's ground attack control center in the future) controls the timing of the air attack. With close coordination between the CTOC and TACC, ground and air-launched strikes are synchronized.

At the corps deep attack delivery unit, final tactical fire control actions are completed. Firing units are deployed from hiding positions to firing positions, and final firing computations are completed at the firing site. Just before firing, the sensors again confirm activity and update on locations and directly notify the executing control element.

Depending upon the nature of the target, the type of sensor, and capability of the attack system, the specific activities at the corps firing unit during the final target update vary.

For moving targets, imagery collectors and sensors provide data to ground stations where the targets are under observation. When the launch computations are completed, and if the target continues to be observed, the launch is executed.

For sitting targets, where the targeted features are electromagnetic emitters, the sensor may confirm the latest location of a target just before launch. Once the attack is launched, the sensors may observe the target and provide information on the effects of the attack. If additional attacks are necessary, the CTOC will reinitiate the execution sequence, in priority with other activity.

In most cases, lethal C^3CM and SEAD attacks accompany attacks of moving targets to support the protection of friendly aircraft and reinforce threat C^2 stress at the same time his combat assets are under attack.

Target information from LRSU, unconventional warfare, or SOF assets located in the threat rear area is used to identify either a moving or sitting target. Additionally, such information contributes significantly to the completeness of the all-source intelligence that supports battle planning. In cases where LRSU, unconventional warfare, or SOF assets are tasked, the corps has already informed these elements of the role they are to perform. The corps has described the target, identified the general location and time of the projected engagement opportunity, and predesignated appropriate quick fire channels. The SOF liaison element at the CTOC provides the means for planning, coordination, and control of the SOF team.

Deep attack opportunities are both highly critical and relatively infrequent. Their exploitation requires limited corps deep attack resources. Therefore, execution control and timing are critical if the desired effects of massing air and ground elements of sensors and attack means are to be achieved. Synchronization in planning is wasted if synchronization in execution does not also occur.

In general, the probability of engagement success is proportional to effort made within the CTOC. This effort is conditioned by the threat level the target represents to corps operations and depends on the corps resources required to accomplish the engagement and the level at which the confirmed event is assigned by the corps. In most cases, an engagement against a large threat moving force (regiment or above) is a highly threatening relevant target. It requires the use of critical corps deep attack resources (weapons and sensors).

The corps chief of staff at the main CTOC will most likely be required to confirm the detection as the planned trigger event. He would then ensure that

the planned engagement still fits within the needs of the ongoing corps operation. Requiring the chief of staff's approval takes additional time for confirmation, but this is minimized by his having been involved and conditionally approving the engagement in battle planning.

Confirmation of less threatening detection events which require fewer corps resources can be made at lower levels within the CTOC. For example engagements against threat RSTA, REC, close air support, air defense, artillery, CP C2, and SEAD are critical, but less threatening, relevant targets.

To be successful, deep attack targeting at corps requires specific and timely coordination between the corps and supporting tactical air forces in the battle planning and engagement phases. Such coordination involves elements within the corps staff, EAC, battlefield coordination elements, (BCEs), and the TACC. This targeting concept specifically facilitates such coordination at the 24 hour (+) planning time frame, at any time between the initial planning and final execution, at 30 minutes before launch, and at the last minute update before launch.

Synchronization in the deep attack starts with the availability of deep attack information. This information provides a common and coherent view of the battlefield within the corps and with the corps and higher and joint headquarters. When the successively greater detail being collected and used at lower levels remains focused on the perspective (needed by the commander to evaluate the realities of the battlefield and to project future corps operations to achieve corps objectives) information needs are coherent.

A coherent view of the battle situation is used by the commander to formulate a concept of operations and by his staff to identify and recommend tasks to coordinate the integration of the specific battlefield functions. These guide those who plan and control subordinate actions that implement these tasks by providing the necessary frame of reference to appropriately focus and sequence fire support. Further, this frame of reference shapes the intelligence collection and processing activity to acquire the technical information necessary to detect and identify relevant observed threat behavior and to trigger specific targeting execution.

The information that provides the common view of the battlefield is battlefield situation information (deciding), target information (detecting), and technical information (delivering). Relevant threat observable information is common among these categories, but each category will also have different functional needs for information in terms of timeliness, quality, and granularity of detail. The needs and the tasks for acting upon the information are different.

Using the general battlefield picture provided by battle situation information, the commander projects achievable future operations, identifies potential interfering targets, directs the collection of relevant technical information, and confirms potential targets within required time, accuracy,

and detail dimensions. The battlefield situation information provides successively more detail over time. The probability of knowledge increasingly permits sharper focusing of collection activity. The greater the degree of detail available for the battlefield situation, the greater the clarity and definition of the perception of the battlefield. In addition, decision makers can quickly identify target and technical information needs to further focus collection and analysis.

The G2 is the primary source for battlefield enemy situation and deep attack target information. The G2 and FSE interact on a continuous basis to--

- Identify and nominate potential targets.
- Expedite the collection of sensor detection data.
- Identify target execution trigger events.
- Establish quick fire channels.

Within the term "battle planning" all activities that contribute to the corps' successful accomplishment of assigned missions are included. These activities range from the commander's concept of the operation and intent and the detailed level of operational planning, through coordination and control, to execution. Battle planning in its broadest application includes logistical sustainment and personnel management which support deep operations. Battle planning, here, purposely highlights those command, functional staff, unit, and executing systems interoperabilities and technical connectivities immediately applicable to deep operation activity.

This focus is on the activities involved in planning for the decision and for the operation. In this chapter, battle planning does not include target engagement. The difference between battle planning and target engagement is that target engagement is the execution phase of a single-phased, coherent deep operation.

Distinctive treatment of battle planning and target engagement is necessary to emphasize the differences between them in functions, timelines, sensors, communications, decisions, and actions. More important, the use of separate phases (without separate systems and structures) provides a clear distinction between the planning phase (where intelligence and advanced planning are highly emphasized) and the engagement phase (where the observed enemy activity itself provides the triggering mechanism to transition into an attack mode, using sensors, quick fire communications channels, and weapons established and coordinated in the planning phase where time is less stressful).

This approach (the decide, detect, and deliver sequence) is necessary (rather than the detect, decide, and deliver process) because it is active rather than reactive. A reactive process results in defeat. To dominate the

opponent, the commander is supported by a process that is focused on his own objectives. Because of the time required to execute large scale and joint operations, future operations are projected.

Feasibility, availability, and affordability of means are equally important in the selection of projected options for deep operations. A wide range of systems is available today and several new capabilities are being fielded. It is likely that a combination of old and new (low and high technology) systems will always exist. These conditions always demand careful analysis and evaluation in developing options for deep operations. Additionally, this mix requires careful planning to launch different executing forces and functions at the approximate times so that they collectively produce their combined effects at the required time and space. This is synchronization--the process which results in the concentration of combat power at the required time and space.

Different targets have unique detectable observables and vulnerabilities to specific weapons effects. Multiple sensors and weapons systems frequently are combined for successful attack. This adds complexity in planning and execution which may constrain operational availability. Each sensor and weapon system, by necessity, has different time considerations. Joint systems also operate within service-unique procedures.

For example, the corps could not expect to receive a HUMINT report of a pending move by an enemy division from a tactical assembly area in deep operations, then, expect to arrange for airborne sensors to immediately assist in delivering effective long-range fire against that target. Similarly, the corps would not have a high probability of success in attacking moving columns if the fire support and quick fire channels to attack the target were not arranged in advance. Similar conditions would also exist for attacking sitting targets, C^2, and SEAD. Time is also an enemy. In deep operations, time is defeated by anticipatory planning and advanced coordination.

Combining multiple sensors and weapons (in accordance with "attack packaging") requires forward thinking and backward planning to provide the necessary time to accomplish coordination. Projecting future operations in some detail provides the required commander's guidance. This guidance enables all the elements of the command to have a coherent focus on the objective in both space and time. With specific guidance and adequate time and detail for coordination, the commander can concentrate combat power at the decisive time and place.

Deep operations are a joint arena. The available joint systems provide the corps the additional means for successful deep operations in support of operational objectives. Joint interoperability is essential.

Successful functional interoperabilities in deep operations require feasible operational concepts. Concepts of operation are feasible only when they ensure compatible operational interfaces, procedures, and technical connectivities of the units and systems to be employed. These procedures and

connectivities are frequently theater specific. The concepts outlined herein, therefore, must be adapted to the unique conditions of each theater.

The combination of functions most frequently and directly related to deep operations are intelligence (eyes), C^2 (brain), the appropriate forms of combat (fist), and communications (nerves). To ensure that deep operations are inherently linked to the rear and close operations of the corps battle activities, these functional areas must start with, converge at, and end with the commander. It is the commander who focuses and conditions the required functional interoperabilities with his operational concept. The commander's planning establishes the who, what, where, when, and how considerations that must be accomplished by executing elements to achieve the essential synchronization. Coordination, accomplished principally by the staff in its planning for the operation, creates linkage whereby the control of discrete functions is exercised and integrated with the other executing elements to establish the tasks and timing of combined systems efforts.

The scope of the command and coordination activities will change somewhat, depending upon the corps objectives and METT-T. In most cases, combined and joint objectives are translated into specific corps mission requirements, with combined and joint resources integrated with organic corps capabilities. Operational availability of such resources depends on the importance of the corps mission, as well as the efficiency with which the corps identifies its specific needs--early enough to initiate the advanced coordination required.

Such coordination is especially critical where executing elements that do not habitually interoperate must combine to achieve the required effect. For example, integrating US reconnaissance and strike activities with organic, joint or combined, operational level fires or maneuver, packaging a sustaining logistics and a protective air defense capability to accompany a maneuver beyond the FLOT.

At the operational level of warfare, units seek to win battles and campaigns. As such, there is an overlap at the tactical and operational level of war in fighting battles. Battles are often the province of divisions and, normally, of corps and may extend for days or weeks. They are multidimensional, incorporating both land and air forces throughout the width and depth of the battlefield.

At corps, the campaign is a sustained operation designed to defeat an enemy, given simultaneous and sequential battles. It's carried out as part of a campaign plan that prescribes the general conduct of operations in a theater.

TARGETING PROCESS

PREPLANNING

Combat success is the product of careful planning and violent efficient execution. The targeting process is one which concentrates on planning. This planning ranges from a multicorps contingency dealing with a potential

conflict on a continent half a world away, to a brigade-sized operation planned in a matter of hours during the conduct of fierce combat activity.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD AND TARGET VALUE ANALYSIS

IPB and target value analysis (TVA) are tools used to prioritize potential targets. Using the IPB process, analysis projects the threat's strength, organization, equipment, and expected courses of action. TVA tools are then used to identify those threats which are most critical to the successful completion of an operation.

STAGES OF THE TARGETING PROCESS

Targeting is accomplished primarily by the G3 or S3, the G2 or S2, and the FSE. They are referred to as the "targeting triad." Other agencies that have major input are United States Air Force (USAF) representatives, engineers, the airspace management element, and chemical liaison officers.

Targeting is a continuous process and has five phases: focus, sensor tasking, information processing, attack, and assessment (see the following illustration). These phases are based upon a distributive data base where each staff agency collects and stores the data applicable to its own area but has access to the information stored by any other agency. The proper conduct of the targeting process depends on this sharing of information.

Focus

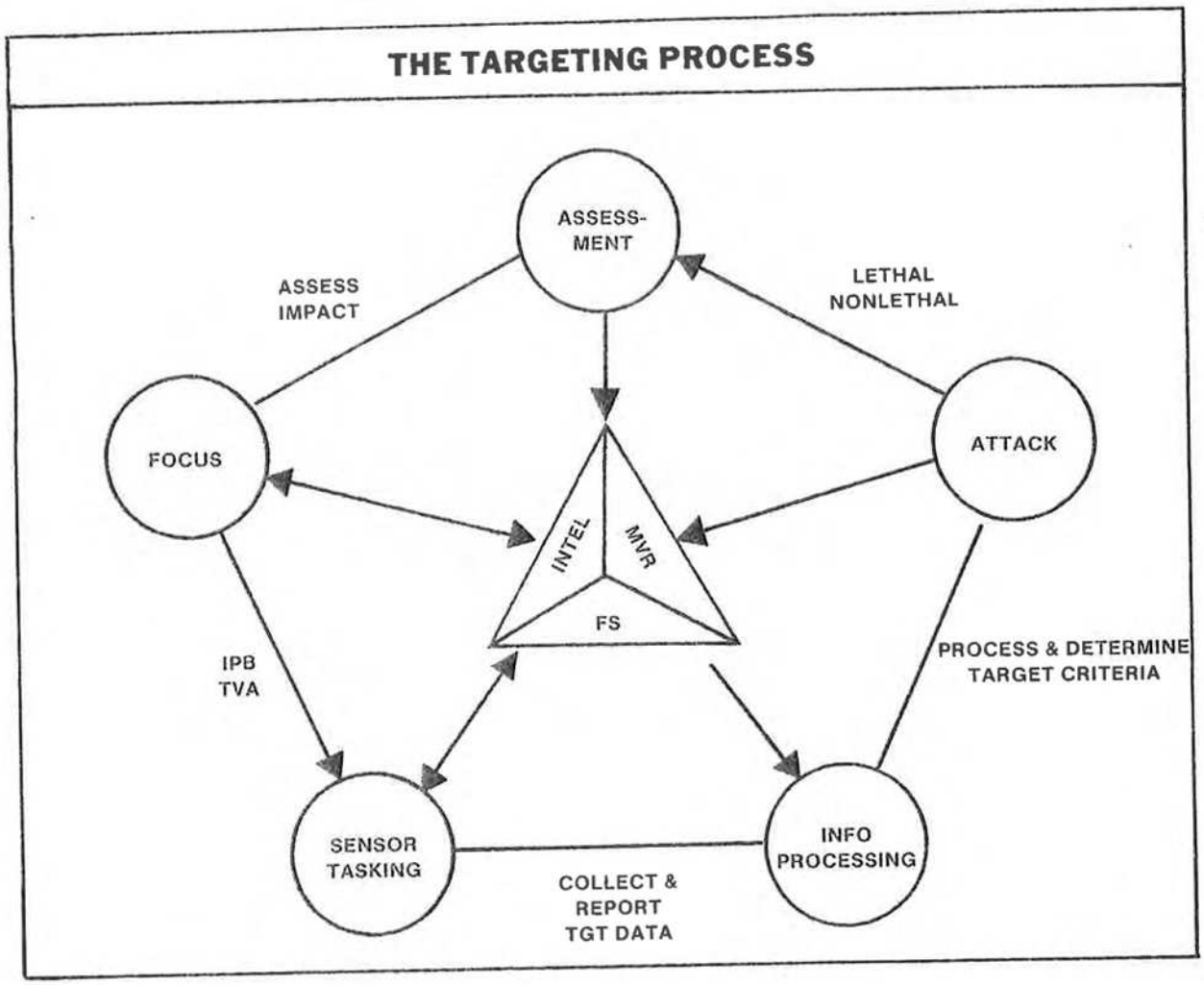
Focus is the initial phase in the targeting process. It reflects the mission planning cycle that a unit staff goes through to plan an operation. It is accomplished by the intelligence staff. To the greatest extent possible, this function should begin in a prehostility, predeployment environment.

After receipt of a mission statement from the commander, the intelligence staff conducts an analysis of the AO and starts the IPB process. This will most likely require tasking collection assets or agencies to provide the best information possible on the AO.

Based on the analysis of the AO and the flow of information developed by the IPB process, the intelligence staff predicts probable enemy courses of action and indicates the most likely course of action.

Based on the enemy courses of action, the targeting triad uses TVA tools to determine what elements of the enemy's force are keys to his success. A list of these elements become the HVT list.

The predicted enemy course of action and the HVT list are weighed by the commander and the G3 to determine the friendly concept of operations. Employing TVA with the friendly concept of the operation, the potential HPTs are identified, prioritized, and listed. This list is presented to the commander



as part of the concept of operation. An HPT list, once approved by the commander, identifies those HPTs upon which the force's collection effort and attack planning are focused. The G2 will designate certain targets for the communications intelligence (COMINT) assets. If approved by the commander, these targets must be coordinated with the intelligence staff before attack. Given the dynamics of the AirLand Battle, the priorities on the HVT list are subject to change.

Sensor Tasking

Sensor tasking is next in the targeting process. Clear and concise taskings must be given to each sensor system. The G2 is the principal figure in collection management. Proper collection planning and management aid situation and target development.

Each collection effort begins by processing IR. These requirements are generated by the commander's PIR, IR, targeting needs, taskings from higher echelons, and requests for information from subordinate and adjacent commands. At corps, many of these requirements are based on information needs associated with NAI and TAI developed through the IPB process. Regardless of their origin, the collection manager transforms them into specific collection requirements. Collection managers consider all assets available to their echelon (MI, maneuver, fire support, and so forth), and they must consider the assets available to subordinate, higher, and adjacent units. At each echelon, the managers of the various target acquisition and intelligence systems ensure that there are no gaps in the coverage of the battlefield.

As the sensors collect information, they report it as specified by the tasking agency and SOP. Some information generated by these sensors will be of no benefit to the targeting process, but it may be valuable to the overall situation development process. This information is forwarded to intelligence analysts to be used in developing other targets.

Close coordination among the G2, the collection manager, and the FSE is required. At battalion and brigade, this is accomplished through direct personal contact between staff officers. Coordination between staff elements at division and corps requires SOPs to ensure efficiency during operations. Precise commander's guidance, attack criteria, and HPT lists must be disseminated and implemented concurrently within the staffs.

Information Processing

Information processing is third in the targeting process. Successful targeting relies on the ability to process information and pass it to an attack means in a timely manner. The interface between IEW and fire support must be a viable and functioning system because target information is processed in both staff elements.

Target selection standards (TSS) are criteria by which personnel can determine which targets are valid and should, therefore, be considered for attack. Targets fall into two categories: targets and suspect targets. A target is defined as a geographical area, a complex, or an installation planned for capture or destruction by military forces. Suspect targets are potential targets which require further correlation or additional information before they can be attacked.

TSS are dynamic. They are approved by sensor managers, in coordination with the attack systems managers. TSS are keyed to the tactical situation and are dependent upon the urgency of the situation and other factors. The availability, lethality, and accuracy requirements of attack assets; the enemy's ability to stage deception activities; and the reliability of the source or agency that is generating the reports are some of these factors. TSS are designed to allow targeting personnel to distinguish between targets and suspect targets.

TSS must be developed because threat deception varies in scope and intensity throughout the battle. Elements of deception are--

° Dummy positions.

° Corner reflectors.

° Camouflage.

° Deceptive and imitative communications.

° Sound and flash simulators.

° Roving and offset guns.

° Feints and ruses.

° Loudspeaker broadcasts.

° False data plans (operational-tactical misinformation).

Some sensors have the capability to provide targets. Other systems provide only suspect targets because they have insufficient acquisition capabilities for the specific and accurate locations required for lethal attack. Data collected by these systems must be correlated with other data or used to cue other sensors to refine attack locations. When it is suspected or determined that the threat is using deception, his effectiveness must be evaluated to determine whether TSS should be changed. TSS are established to streamline and speed the efforts of targeting personnel and analysts. Indicators are tested and retested. When the information about the suspect location satisfies the TSS, it is considered a target.

An additional element of information processing is the establishment of attack criteria. These criteria answer the question: What do you wish to do to a target once it has been developed? The key elements of attack criteria require a rank order prioritization of the 13 target sets outlined in the TVA study, required effects of fire, when to attack, and restrictions, if any. Other information can be added or deleted as required, depending on the local situation and unit SOP. An attack guidance matrix (shown in the following illustration) is useful here.

Actual matrixes will be developed by the G3 or S3 and the FSE based on tactical situation. An explanation of possible columns in such a matrix follows:

° CAT indicates the order in which targets are presented in the relative worth matrix of the TVA spread sheet. These should not be reordered every time the matrix is produced. If certain categories are especially high payoff, these may be noted by a color code or an asterisk.

EXAMPLE ATTACK GUIDANCE MATRIX

CAT		HPT	HOW	WHEN	RESTRICTIONS
(C^3)	1	46, 48	N/EW	1	COORD ATTK W/EW
(FS)	2	1, 2, 7	N	A	DNE MLR OLDER THAN 10 MIN.
(MVR)	3	25, 28	25%	A	LAST VOLLEY RAAMS/ADAM
(ADA)	4	58	SIG 2	P	SEAD PROGRAM 120800A
(ENGR)	5		N	P	COUNTERMOBILITY PROGRAM %
(RSTA)	6	85	EW	P	
(REC)	7	103, 105	N	P	
(AMMO)	8		D	A	
(MAINT)	9		N	P	NOT HIGH VALUE/PAYOFF
(LOC)	10		N/G3	P	NOT HIGH VALUE/PAYOFF

° HPT indicates those targets, by target sheet number, that have been designated on the HPT list. To determine the urgency of response, fire support personnel can refer to the priority listing on the attack guidance matrix when the target comes in.

° HOW refers to the desired effects or the nature of the attack on the target. Fire support and operations personnel should specify these effects within the constraints of the division and the division artillery commander's general guidance. Desired effects can be specified by subjective terms such as suppress (S), neutralize (N), or destroy (D), jamming or other offensive means (EW), percentage of casualties or destroyed elements (X%), or noted as a number of battery or battalion volleys (X%). A coordinated attack is one that requires coordination with another agency (G2, G3, or USAF) before attacking with either lethal or nonlethal means (G2). This may be required to allow intelligence to be gathered or to preclude conflicts.

° WHEN a target should be attacked is indicated by the next column. The letter "P" indicates that targets should not be engaged now, but they should be planned for future fire (an anticipated preparation, SEAD program, counter-mobility program, and so forth) or simply put on file. The letter "A" indicates as acquired. Such targets should be engaged in the sequence that they are received in the headquarters, according to

the priority noted on the HPT list. The letter "I" indicates an immediate attack and is a special case. Such targets should be limited to a very small percentage of targets and only for the most critical types. Too many immediate targets will be disruptive and will lower the efficiency of attack systems.

Immediate attacks are those that take precedence over all others and must be conducted even if fire support means have to be diverted from attacks already under way. Some examples of very important targets include nuclear-capable missile systems, division headquarters, and nuclear weapons storage and support facilities. The force artillery S3 must establish procedures that allow for immediate attack of critical targets, but which do not seriously degrade the efficiency of the attack system.

° RESTRICTIONS are any constraints or special modifications of attacks. Such constraints note accuracy, time since acquisition, required coordination, or munitions restrictions by amount or type. This column should note which target categories are not high value and which targets should not be attacked during certain tactical situations. For example, it lists targets not to be attacked if the enemy is withdrawing. It is important that the operations and FSE work closely together to convert the commander's desires into specific requirements for the fire support system. The attack guidance should be clear and unambiguous to ensure rapid positive responses to targets. Other notes such as "target damage assessment required" or "missile target only" could be included.

In summary, data is received and compared to applicable TSS to ensure data validity. Once validated as a target, it is cross-checked against the attack guidance criteria. These stipulate the types of action to be initiated for a target in a particular target category. Examples include fire support and maneuver. A report number is then assigned and the report passed to the appropriate attack agency for action.

Attack

Fourth in the targeting process is attack, which is execution. When a target meets the TSS, it is passed to the appropriate attack agency (G3 or FSE). The target is added at an appropriate place on the list of prioritized HPT. Target attack includes--

° Select attack system. The attack agency determines the most appropriate attack option based on the attack guidance developed in the focus phase of the process.

° Task attack system. The attack agency then tasks the appropriate means (FA, USAF, EW, naval, and so forth) and that agency tasks a specific attack system to execute the mission. The tasking of a specific system is based on both system capability and availability.

° Execute mission. The tasked attack system conducts the necessary tactical and technical control to execute the assigned mission.

° End or reexecute mission, based on assessment. Based on the target attack assessment or other guidance, the target is either attacked again to obtain sufficient results or an end-of-mission report is generated. The unit's operational data base is updated to reflect the results.

ASSESSMENT

Assessment (fifth in the targeting process) is important because the commander must be certain that his force is successfully attacking the intended targets and that it is achieving the desired effects. Assessment, therefore, is actively planned, coordinated, and (when possible) executed concurrently with the attack. Assessment includes--

° Determining sensor availability.

° Tasking sensors.

° Collecting and reporting.

° Determining attack results.

° Determining refined data for target update.

Certain targets do not require active assessment. If an FA battery or battalion CP were to be attacked, the appropriate measures of a successful attack might be the termination of firing from the battery or suspension of communications from that headquarters. Because of limited collection assets, commands may have to accept these as examples of success for assessment on many targets.

Other targets will require active assessment. The destruction of an ammunition transfer point 15 kilometers beyond the FLOT might be considered so important it would require active collection efforts. The priority for assessment is based on the focus phase and modified by the G3 as the operation proceeds. Assessment is handled by the collection manager in the same manner as initial sensor tasking. When assessment is reported, it is checked against the attack criteria for desired results. If desired results were not achieved, it is determined whether the target still meets TSS. If the target still meets these criteria, it is entered back into the attack system.

Data from all targets which have been attacked, whether they are actively assessed or not, is provided to the intelligence elements.

For additional and specific information concerning fire support targeting and fire planning techniques, see FM 6-20.

SUPPRESSION OF ENEMY AIR DEFENSES

The corps is the focal point for Army SEAD operations. It assesses the situation, determines requirements, assigns priorities, and allocates resources. Additionally, the corps ensures that Army SEAD operations are integrated into the scheme of maneuver. In the CTOC, the G3 has overall staff

responsibility for combat operations. However, the fire support coordinator (FSCOORD) manages the SEAD effort through the corps FSE. This requires the integration and coordination of fire support means, aviation assets, intelligence gathering, and EW capabilities in consonance with maneuver force operations. The G2, in conjunction with the CTOC support element and ASPS, provides information and projected movement of the enemy air defense threat to the G3 and FSE. This data, as well as data on air space use, is integrated into the SEAD plan by the FSE. He also coordinates and tasks appropriate attack means. When Air Force assets are supporting Army operations (as in close air support) the air support operations center (ASOC) works closely with the corps G3 and FSE to coordinate suppression operations. The integration of all these staff elements reduces redundancy, ensures unity of effort, and maximizes the synergistic effect.

Intelligence and target acquisition play important roles in SEAD. Intelligence assets, using IPB data and guidance from the corps G2, seek to locate and identify the threat air defense order of battle. They seek those critical nodes which, if interdicted, will significantly degrade the threat capability. Army units at all echelons are tasked to report enemy sightings and activities for use in the intelligence-gathering process. Additionally, the EW sections at corps and division work closely with the FSE to coordinate intelligence activity and ECM attack requirements with the SEAD priorities. Accurate detection and location of enemy air defense systems is a high-priority Army intelligence task.

Targets are also identified by returning pilots, electronic intelligence (ELINT), COMINT, and HUMINT. Location and target description are transmitted through the intelligence system to the FSE at each echelon. The FSE uses this information to confirm the location of preplanned targets and to determine the attack means for targets of opportunity.

Army communications jammers, including QUICKFIX, TACJAM, and EXJAM, are employed to disrupt the C^2 function. Threat air defense systems identified by the intelligence system are targeted for jamming according to their potential impact on a specific operation. Jamming the threat air defense system C^2 nodes has two objectives: First, it can force the subordinate fire units to activate their radar to acquire targets, rather than relying on the C^2 system to report targets. Threat units, thus, expose themselves to acquisition and lethal attack. (This is useful, however, only if lethal systems are poised to attack when the threat fire unit radars are activated.) Second, jamming will also degrade the threat C^2 system during friendly air operations. This type of suppression requires close coordination of flight and jamming schedules. When Army aviation assets conduct cross-FLOT operations, the EWS coordinates the employment of escort and stand-off jammers. Additionally, the Air Force has jamming capabilities that complement and expand the impact of this technique. Jamming of threat air defense C^2 facilities is a part of a coordinated SEAD effort. It is normally done as part of a planned localized operation. It is rarely undertaken as part of complementary SEAD activities.

CHAPTER 5

SPECIAL OPERATIONS AND ENVIRONMENTS

MILITARY OPERATIONS

The environments encountered in areas of strategic concern to the United States are varied, and each exercises a unique influence on the conduct of military operations. The environments and special operations described in this chapter are of special concern because of their impact on corps IEW operations.

MILITARY OPERATIONS ON URBANIZED TERRAIN

Corps commanders recognize the importance of urban centers as strategic objectives, but the engagement of enemy forces in towns and cities is difficult. Buildings and other structures limit line of sight (LOS) and create a vertical dimension to the battlefield. This causes the battle to be fought at close range. These factors, as well as blockage of streets and other pathways by building rubble, create an environment that favors the defender. Reaction time is reduced for both the defender and the attacker.

The fragmented and compartmented nature of urban combat necessitates decentralization of operations. When passageways are blocked, man-packed systems must replace vehicle-mounted systems. This limits the effectiveness of electronic communications systems for C^2 and may force the commander to rely on wire communications. Important too, is the need to rely on intent and to act and exercise initiative without additional orders or guidance.

The IPB efforts, prior to urban combat, include the collection and analysis of city plans. Of special interest are sewer and subway systems, buildings and structures, and enemy fortifications. A thorough knowledge of these factors by the commander and his staff is essential if the tactical situation is to be exploited to its fullest potential.

The HUMINT effort is aimed at the collection of information from indigenous sources. These sources may be able to provide information based on direct observation of threat forces that may be difficult or impossible to obtain elsewhere. The information gained from the interrogation of these sources is also valuable in the planning and execution of CI efforts.

A threat defender enjoys several advantages by occupying urban terrain. Urban terrain provides the threat with excellent concealment and cover and provides protected elevated platforms for the collectors of intelligence. Because key installations are well concealed, they are much more difficult to identify and attack. The proximity of threat forces and reduced effectiveness of communications necessitate diligent OPSEC measures.

RIVER CROSSING OPERATIONS

The objective of any river crossing operation is to project combat power across a water obstacle while maintaining the integrity and momentum of the corps.

River crossing operations require detailed planning. Each one is unique. When operating in an environment, such as Europe, where there are frequent river crossings, each crossing requires consideration of its unique operational requirements. River crossings are normally conducted by divisions. MI support of river crossings is a key element in IPB. This requires a long lead time for preparation and includes an assessment of the enemy capability to resist the crossing. CI support to OPSEC also seeks to deny the enemy knowledge of the time and place of the crossing and other security measures required by the crossing. MI also works to provide early warning of threat counterattack. MI units normally support from the entry side of the crossing site, but some assets may accompany the assault force to continue support. The use of infiltrating MI assets of LRSUs to the exit side for R&S purposes should be considered.

DESERT OPERATIONS

The desert is an area of contrasts. The extreme heat of the day is replaced by cold temperatures at night. Extreme winds replace calm conditions very quickly. Just as quickly, unlimited visibility is replaced by blowing sand and dust. Caused by rainfall several miles away, flash floods occur without warning.

Military operations in the desert are characterized by rapid movement. Because of the good visibility and open spaces, units are widely dispersed. Units make maximum use of deceptive techniques such as camouflage and OPSEC.

The desert is well suited for the operation of IEW systems because it provides open space and unobstructed LOS. Because of thermal heating and dead spots, there is some degradation of amplitude modulated (AM) and frequency modulated (FM) radio communication.

Dust, sand, and heat place heavy requirements on unit maintenance assets. This causes an increased need for repair parts. Also, care must be taken to prevent contamination of petroleum, oils, and lubricants (POL). Water needs increase, especially when soldiers are not acclimated to the desert environment. Training for this environment is necessary to acclimatize soldiers as quickly as possible.

JUNGLE OPERATIONS

The jungle regions of Asia, Africa, and the Western Hemisphere are potential battlefields. The jungle has thick vegetation, high temperatures, high humidity, and heavy rainfall. Military operations are adversely affected, which takes its toll on both personnel and equipment.

Tactical operations tend to be decentralized, with a heavy reliance on helicopters for mobility. Because units are operating with less centralized control, more IEW systems are attached or placed in support.

The climate, vegetation, and reduced LOS reduce the effectiveness of AM and FM communications. Because of the corrosive effect of the humid climate, all equipment requires increased maintenance. Aerial observation and imagery collection efforts are also degraded by the heavy tree canopy that may be present and may require a greater reliance on HUMINT resources, especially CI and interrogation assets.

WINTER OPERATIONS

The effects of winter conditions have a significant impact on military operations. Because of the darkness, extreme cold, and deep snow, increased time is required even for simple tasks. The deep snow affects mobility, although hard frozen terrain may aid cross-country mobility. Mobility of forces is improved by the use of helicopters. Some IEW systems require movement by helicopter, although small loads may be man-packed.

HUMINT and IMINT are very good intelligence sources during winter operations. However, both are dependent on weather conditions. Since aerial operations are dependent on weather conditions, a heavy reliance may have to be placed on the use of patrols to gather battlefield intelligence. Patrols can also be denied movement during whiteout conditions.

The major impact of winter operations is caused by the effect of snow and extreme cold on equipment and personnel. Metal may become brittle and break easily. Vehicles and other pieces of equipment are often left running for extended periods of time. This results in a higher consumption rate of POL products. Blowing snow can clog air intake valves and cause engines to shut down. Training of personnel to operate in a winter environment is essential. While heavily dressed and working in deep snow, soldiers will encounter fatigue faster. Commanders must prevent overexertion by ensuring that troops are physically fit and by providing frequent rest breaks.

MOUNTAIN OPERATIONS

Mountainous terrain exists throughout the world and can have a significant impact on military operations. Rugged high terrain limits the useful range of many weapon systems and causes a heavy reliance on indirect fire systems. Movement of forces is also limited.

The compartmented nature of the terrain requires more decentralized operations with more IEW support. HUMINT is very useful for intelligence in mountainous terrain. Weather intelligence in the mountains becomes critical. Rapid changes in weather conditions, cloud cover, and wind chill factors have a strong influence on the tactical situation and are considered in operational planning.

The rugged terrain degrades electronic transmissions by reducing LOS and causing strong reflections of signals. This reduces the effectiveness of communications and IEW systems and places heavy use on relays and retransmission of electronic signals.

LOW-INTENSITY CONFLICT

Because of the political-military nature of LIC, its varied missions, and the unlikelihood that an entire corps would be employed in support of any single LIC contingency, LIC offers a significant challenge to the corps commander. Due to the critical need for timely, detailed, and often unique intelligence support inherent in each of the LIC missions, corps IEW planners, managers, and operators do share the large burden of this challenge.

The corps' pivotal location, with respect to general intelligence roles and requirements for LIC, also serves to focus much of the burden at this echelon. To meet mission requirements, doctrinally defined IEW tasks, existing IEW structures, and operational capabilities require modification, ad hoc tailoring, and possible limit-stretching. Specialized training is required for corps and subordinate-level assets involved in LIC.

LIC MISSION

The overall complexity and uniqueness of the US Army LIC mission is reflected in the definition of LIC: LIC is a limited political-military struggle to achieve political, social, economic, psychological, or military objectives. It is often protracted and ranges from diplomatic, economic, and psychosocial pressures through terrorism and insurgency. LIC is generally confined to a geographic area and is often characterized by constraints on weaponry, tactics, and levels of violence. LIC involves the actual or contemplated use of military capabilities up to, but not including, combat between regular forces.

The Army's LIC mission is divided into four general categories: FID, terrorism counteraction, peacekeeping operations, and peacetime contingency operations. These categories are not mutually exclusive and often overlap. FC 100-20 provides specific definitions of the four categories of the LIC mission.

As is apparent in the LIC definition and in the broad range of LIC mission categories, the corps must be able to respond rapidly to LIC contingencies in which overall objectives are not solely military. Such responses may be constrained by legal, social, and political constraints. They may be tied directly to US foreign policy goals. Due to its protracted nature, varying intensities of violence, and the need for extensive interface with host nations, US commands, and national-level authorities, FID offers the most complex mission within LIC.

LIC ENVIRONMENT--OPERATIONAL PLANNING CONSIDERATIONS

Austere Theater

LIC often occurs in far-flung austere regions where there are few or no communications or logistics infrastructures in place. Corps IEW assets employed piecemeal may, therefore, require augmentation to existing tables of organization and equipment logistics and communciations capabilities. The US combat forces' commitment generally cannot depend on adequate host-nation support. Consideration is given to developing a combat support and CSS support base before commitment of US combat forces. This provides the capability to conduct sustained operations.

Fragile Political Structures

Developing nations confronted with insurgent or terrorist threats are often plagued by weak political, economic, and military organizations. These weaknesses must be understood by IEW planners, managers, analysts, and operators. Intelligence products, collection assets, and methods used must be effectively tailored to meet host-nation political constraints or overall capabilities. Intelligence support is country-dependent. Thus, advance planning, when possible, is critical to successful IEW operations.

The Threat

The threat in LIC is invariably ambiguous, complex, and mainly HUMINT in nature. Insurgents and terrorists blend easily into the general population. They work hard to avoid patterns and place a high priority on security and intelligence functions. All of these factors provide difficult challenges to corps intelligence and CI assets.

Legal Constraints

LICs are seldom declared wars and, therefore, military forces lack the freedom of action generally associated with conventional war. Rules of engagement are much more detailed and constraining. Such constraints, related to IEW operations or supported combat operations, are well documented and understood.

Varying Levels of Violence

Levels of violence within LIC situations may vary in intensity. They may include nonviolent actions (organizing, recruiting, propaganda, and agitation), terrorist and guerrilla actions directed against the host-nation population or economic infrastructure, and conventional tactical operations. These actions may tend to be cumulative in nature. For example, all types of activities may occur simultaneously in varying parts of the country. The predominant threat may distinctly take one form or another. Levels of violence are dependent on a number of factors. These include overall insurgent capabilities, population support, and the effectiveness of the

counterinsurgent strategy. IEW operations must be flexible enough to rapidly change support from combat operations to security operations.

Psychological Operations and Civil Affairs

PSYOP and civil affairs operations are combat multipliers in LIC. Concern for the host-nation civilian population and addressing real or perceived grievances in the economic, social, or political realms cut to the roots of an insurgency. This, in turn, assists in separating the population from the insurgent as its primary source of support. Corps IEW operations, therefore, identify potential objectives for PSYOP and civil affairs activities. They provide requisite IEW support to these operations.

Centralized Control and Decentralized Execution

The political and often sensitive nature of LIC operations requires overall control or direction centralized at higher levels of command (US command or national level). Actual execution is decentralized. As a result, IEW assets belonging to the corps, receive overall guidance directly from higher authorities. Decentralized and independent execution is performed by corps asset managers and operators within the LIC area or at remote sites.

General Intelligence Roles in LIC

There are three general intelligence roles unique to LIC. Within these, corps IEW assets and capabilities play a key role. These roles are--

° Strategic intelligence monitoring.

° Support to host-nation operations.

° Support to US operational forces and combat commanders.

Because of their pivotal location as a central processing and dissemination point for both strategic and tactical intelligence, corps echelon IEW elements are key players.

Strategic Intelligence Monitoring

To effectively guide policy making, national-level authorities require strategic intelligence. Tactical military commanders with potential LIC contingencies require similar and much more detailed strategic intelligence data than if they were in a conventional conflict.

Focusing National-Level Assets

Corps analytical elements, particularly the ASPS, ensure that--

° Corps and subordinate elements identify their specific intelligence requirements with respect to LIC contingencies.

REMOTING

Remoting of complex collection assets may be forced by political factors or host-nation infrastructure constraints. Remoting requirements often stretch corps IEW assets to the limits of their operational capabilities. Consideration may be given to the use of third-country support.

HOST-NATION TRAINING

Host-nation intelligence structures are often weak or nonexistent. Corps IEW assets may need to train host-nation military intelligence organizations in basic intelligence analysis and operational procedures. Particularly important, is the upgrading capabilities of S2s at the tactical battalion and brigade levels. These echelons carry the brunt of the counterguerrilla efforts.

SUPPORT TO US OPERATIONAL FORCES AND TACTICAL COMMANDERS

The introduction of US combat forces into a LIC environment creates intensive security problems based on the size and visibility of US presence. Corps IEW elements already in place and those deploying with combat elements must plan for extensive security precautions.

TACTICAL HUMINT CRITICAL SOURCES

US combat forces employed in LIC require extensive augmentation by trained HUMINT assets, to include CI, interrogators, and document exploiters. CI assets are not expected to provide quick results. They need time to develop the networks and liaison required for successful collection. This may need host-nation approval or assistance which may or may not be provided. Interrogation and document exploitation efforts, however, are immediately fruitful, due to the potentially large numbers of enemy prisoners of war (EPWs), suspected insurgents, civilian sources, captured documents, and insurgent propaganda. Once fully developed, HUMINT capabilities play a key role in filling in the details and confirming indications and warning and general trends developed by technical collection assets.

TACTICAL ALL-SOURCE ANALYSIS

All-source analysis or fusion is as critical in LIC as it is in conventional war. All-source centers are established at various operational echelons to support both host-nation and US operations. The most intensive all-source analysis in LIC will likely support brigade- and battalion-level tactical operations. LIC requires extensive and detailed data basing, files management, and trend analysis, as well as an increased need for photographic and terrain mapping, interpretation, and analysis. Therefore, ad hoc augmentation cells made up of corps imagery analysts, OB analysts, and terrain analysts are required to provide DS to S2s at lower echelons.

COMMUNICATIONS PLANNING

Communications demands are as high in LIC as in other levels of conflict. Corps IEW and C-E elements, theater, and US commands coordinate communication support needs or interface requirements. Tactical communications systems (signal gear, prime movers, and generators) are expected to be maintenance-intensive in LIC areas. Hence, spare parts and equipment should be planned for and stocked.

US TRAINING

Combat forces with LIC contingencies must have a high degree of readiness and are trained to identify and fight the type of threat encountered in LIC. Corps IEW assets, along with those at division, provide threat and associated population data related to the LIC contingency areas for effective insurgent threat forces and counterinsurgent training. Such training includes--

- General information gathering and reporting techniques.
- Personality recognition factors.
- Ambush and counterambush.
- Terrorist counteraction and antiterrorist methods.
- Troop behavior and discipline, with respect to the civilian population.
- Cross-cultural communications.
- Insurgent and guerrilla weapons and equipment, doctrine, training, and tactics.

Additional training for IEW assets is specific, such as language training for more intelligence military occupational specialties (MOSs) and overall maintenance of language proficiency.

LIC-unique training for LRSU assets includes--

- Extensive guerrilla and terrorist profile and recognition training.
- Close-in reconnaissance and static operations skills for rural or urban environments.

TERRORISM

Terrorism is the calculated use of violence or threat of violence to attain political, religious, or ideological goals through destruction, intimidation, and coercion. Terrorism involves a criminal act that is often symbolic

and is intended to influence an audience beyond the immediate victims. Terrorism counteraction consists of those actions taken to counter (neutralize or defeat) the terrorist threat.

Terrorism counteraction includes defensive measures to reduce friendly vulnerabilities and offensive operations to counter the terrorist incidents.

Antiterrorism includes those defensive measures taken to reduce the vulnerability of personnel (to include family members), facilities, and equipment to terrorist attack. These measures defend US or Allied personnel and facilities. Antiterrorist measures include intelligence, threat analysis, and preventive measures.

Counterterrorism includes offensive measures taken in response to terrorist acts. These measures involve the use of Army resources, which include armed forces, collection of intelligence information, and threat-oriented analysis of that information in support of counterterrorist operations. Counterterrorist operations apply to all environments and missions in both peace and war. These missions range from assistance to Allies and US civil authorities to offensive US military operations conducted against terrorist personnel and bases.

Because of the clandestine nature of terrorism, the small size of terrorist operational cells, and the fanatical tendency of the terrorist leaders for security, intelligence is a critical factor in all terrorism counteraction operations.

TERRORISM COUNTERACTION

The "lead agency concept" is the heart of the US terrorism counteraction program concept. Within the US, the Department of Justice (DOJ) is the lead US agency responsible for countering terrorism, including collecting intelligence. Outside the US, the Department of State is the lead US agency. Overseas, intelligence collection is also regulated by current Status of Forces Agreements (SOFAs) and host-nation jurisdictions. The US Army Intelligence and Security Command (INSCOM), as the lead US Army agency controlling Army terrorism counteraction intelligence activities, coordinates with appropriate agencies when initiating intelligence activities.

RESPONSIBILITIES

Terrorist acts that occur within the US (including the District of Columbia, the Commonwealth of Puerto Rico, and US possessions and territories) are managed by the DOJ. Within the DOJ, the lead agency for investigations of and operational response to domestic terrorist incidents occuring in the US is the Federal Bureau of Investigation (FBI). The jurisdictional authority rests with the FBI, but if a major incident threatens US national objectives and security, the NCA may become the focal point. Involvement of MI in investigations of terrorist activities is governed by ARs 381-10 and 190-52.

The Department of State is the lead agency for countering terrorism against US personnel and facilities outside the US, its territories, and possessions and for handling the foreign relations aspects of domestic terrorism. The host nation has responsibilities according to international law and applicable SOFAs. Coordination between the host country and US intelligence agencies is accomplished through continuous liaison. SOFAs are supplemented by detailed memorandums of understanding.

The Deputy Chief of Staff for Intelligence (DCSINT), DA, develops policies, plans, and procedures for the collection, reporting, and dissemination of terrorist-related intelligence.

INSCOM provides overall direction and coordination for the Army CI effort at EAC.

The Criminal Investigation Division Command (CIDC) collects, evaluates, and disseminates terrorist-related criminal information to INSCOM to support intelligence collection systems and to installation commanders.

The G3 coordinates terrorism counteraction and makes security assessments for terrorism.

The G2 --

° Reports all actual or suspected terrorist incidents and activities to his immediate commander, supported activities, the provost marshal's office (PMO), and the local INSCOM office.

° Provides early warning of imminent terrorist attack to the commander.

° Initiates and maintains liaison, as a minimum, with the PMO, the local CIDC and INSCOM offices, security officers and managers, and host-nation intelligence and security agencies (as appropriate and authorized).

° Develops and presents terrorism threat awareness training and briefings to all personnel within the command.

Law enforcement staffs--

° Report all actual or suspected terrorist incidents and activities to their immediate commanders, supported activities, and to the local INSCOM office.

° Initiate and maintain liaison with local INSCOM office.

Installation activity security officers and managers--

° Report actual or suspected terrorist incidents and activities to their immediate commanders, supported activities, and local INSCOM and CIDC offices.

- Provide early warning of imminent terrorist attacks to their commander. Conduct regular liaison with their local PMO, INSCOM, and CIDC offices, and intelligence staffs.

- Ensure that terrorism threat awareness training and briefings are presented to their personnel.

INFORMATION

The collection and development of information on the terrorist threat to be included in the all-source data base are critical to terrorist counteraction. The categories of information are--

- Open source.

- Criminal.

- Intelligence sources.

- Internal sources.

Open Source

Open source information is publicly available and perhaps the most overlooked, yet valuable source of reliable information. Numerous publications cover terrorism and criminal activities and are available in libraries and on the commercial market. Leaflets, broadcasts, and other forms of communication by underground or dissident individuals and organizations may be of value.

Federal agencies also publish excellent materials on terrorism. Congressional hearings, the Central Intelligence Agency (CIA), the FBI, the Department of State's Office for Combating Terrorism, and the National Criminal Justice Reference Service offer quality terrorism material.

Criminal

Criminal information is developed by MP and other law enforcement sources or agencies. It is valuable, since terrorism involves criminal acts. CI special agents (SAs) coordinate with the provost marshal (PM), the military police investigator (MPI), and agents in the local office of the CIDC. These persons routinely work within the area defined as criminal information and are guided by ARs 190-30, 190-52, and 195-5, respectively. The local CIDC office should have current essential elements of criminal information on file. AR 190-52 requires the CIDC to collect, evaluate, and disseminate criminal information on terrorists to the local INSCOM representative and the intelligence threat analysis center (ITAC), and keep local commanders informed. The local CI office also must maintain liaison with the USAF Office of Special Investigations, the Naval Investigative Service, the FBI, local police, and outside continental United States (OCONUS) law enforcement and security agencies.

Intelligence Sources

Intelligence offices of both military and civilian investigative agencies maintain terrorist threat data that may be available to supplement the development of a well-planned, systematic, all-source data base. Collection of this information by US Army CI personnel is guided by ARs 381-10, 381-12, and 381-20. The ITAC disseminates specific threat warnings to applicable local commands and activities, to include PM and CIDC local offices. Periodic regional threat packets are provided by the local INSCOM representative to supported commands and activities. ITAC produces CI and threat summaries.

Internal Sources

Internal sources are a command's soldiers, dependents, and employees. When educated and aware of the potential terrorist threat, these may become valuable sources of information. The CI SA is responsible for stressing reporting of all terrorism-related indicators during periodic Subversion and Espionage Directed Against the US Army and Deliberate Security Violations (SAEDA) training (see AR 381-12)

OPERATIONS SECURITY

The success of terrorist acts or operations greatly depends on the information used in the operational planning. Though the objectives may differ, the means by which terrorists collect intelligence against potential US military targets, whether they are corps activities or personnel, are essentially the same as those used by traditional HOIS.

OPSEC, as it relates to terrorism counteraction, concerns controlling information and detectable activities which enable a terrorist to effectively exploit a target's weaknesses and neutralize or preempt a counterterrorist response. Terrorists gather information, reconnoiter potential targets (both primary and secondary), and select those targets which offer the maximum opportunity for success. Information passed on unknowingly by military and DOD personnel and family members is used by terrorists in their planning efforts.

OPSEC procedures used to deny the terrorist this information are--

- Protection of itineraries, travel plans, and personnel rosters.
- Elimination of established patterns.
- Protection of building and facility plans, billeting assignments, and very important person guest lists.
- Discussion of classified or sensitive information only on approved cryptographically secured telephone or radio circuits, such as automatic secure voice communications.

° Protection of personal or family information from nonacquaintances.

° Coordination of physical security measures to protect personnel and prevent unauthorized access to equipment, facilities, materiel, and documents.

REAR AREA INTELLIGENCE OPERATIONS

In any future conflict, intensive enemy activity in the rear area can be expected. Such activity is designed to create panic and disruption. In attacking our rear areas, the enemy's objectives are--

° Destroy headquarters, logistics installations, nuclear-capable delivery systems, and nuclear storage sites.

° Disrupt rear area C^3 centers.

° Kidnap or assassinate high-ranking military and political persons.

° Interrupt aviation operations, early warning, and air defense systems.

° Seize or destroy flood control systems and lines of communication (LOCs), such as highway junctions, key bridges, tunnels, and defiles.

° Harass supply lines and LOCs.

° Destroy or disrupt reserves.

SPECIAL WARFARE OPERATIONS

The Threat fully appreciates the important role that special warfare operations play in a main offensive. Special warfare operations directed at the rear area include co-opted and independent terrorist and sympathizer special purpose forces, air assault, airmobile, motorized rifle air combat troops, naval infantry forces, operational maneuver groups (OMGs), and REC. Threat special warfare operations are designed primarily to support a surprise attack. Clandestine operations in the target area commenced before the start of hostilities increase the probability of key target destruction in friendly rear areas before increased security measures are completed. Threat operations emphasize--

° Secrecy.

° Planning.

° Unity of command.

° Resupply.

° Detailed target lists with alternate objectives.

° Multiple destruction methods.

° Effective, secure communications.

Threat special operations may be divided into three categories of operations:

° Strategic.

° Operational.

° Tactical.

The differences are in the scope of the mission, types of forces used, and the level of C^2.

Strategic missions are conducted by the highest level of the Threat command and are expected to have a significant impact on a war or campaign. Threat forces typically involved in strategic missions are airborne, special, and naval infantry forces. Their targets are high priority targets, often deep behind the target nation's lines. They are always critical to the target nation's political, economic, social, and military survival. Strategic targets include national capitals, airports, or other important administrative, industrial, economic, or political centers. Strategic forces will try to undermine national resistance or attempt to establish a new theater of military operations.

Operational missions are typically conducted by squad- to division-sized units in support of Threat front and army operations. These forces are primarily concerned with the destruction of friendly forces' army and corps. Threat forces typically involved in operational missions are tank heavy forces, air assault brigades, and special forces teams. Mission objectives may be to secure bridgeheads, airfields, river-crossing sites, or key terrain. They may try to exploit postnuclear strikes, to encircle enemy troops, or to destroy C^3 ADA or nuclear delivery systems and facilities.

Tactical missions are controlled at division level. Tactical special warfare forces at division which threaten the rear area are deep reconnaissance troops and air-transportable combat forces. Tactical heliborne forces are normally elements from a division's motorized rifle battalion. However, air assault by airmobile troops allocated from front- or army-level may be used. Tactical missions are usually conducted by a reinforced company or by a battalion. Tactical heliborne objectives are usually 15 kilometers from the forward edge of the battle area (FEBA) within range of division artillery in daylight and link-up with an advancing friendly force is within hours. Tactical reconnaissance forces also perform limited sabotage missions. Tactical rear area missions seize key terrain, destroy key weapons and C3 facilities, conduct blocking maneuvers or ambushes, encirclement of enemy forces, or deception actions.

The threat to the rear area is time and situation dependent. Threat forces view operations against US rear areas as extensions of the overall battle. They attempt to direct their activities in the rear area to support the total battle. Particular US units, (for example, air defense, nuclear missile launchers and storage, and C^3) because of their time-dependent and situational missions, find increased rear area threat operations.

The levels of rear area threat described below are not to be directly correlated with a partiuclar threat special warfare mission. For instance, any three levels of the threat could be directed at strategic, operational, and tactical level. However, the Threat attempts to task the most appropriate force available to accomplish the mission. Also, friendly units could experience a Level I or Level III tactical, operational, or strategic threat simultaneously (for example, the terrorist threat and a threat by regular combat force units).

Threat Level I

Level I Threat activities, conducted by agents, sympathizers, and terrorist groups, may be happening outside of the Threat forces' control. This characteristic makes predictive analysis extremely difficult. While these groups may be trained and equipped by the Threat forces, they may be conducting operations autonomously with no further direct contact with the Threat force. They may operate according to Threat force principles, but not under direct Threat control. Their primary mission is, first and foremost, intelligence collection. As control is established and the situation crisis escalates, they may be directed to destroy HVTs themselves.

Agents, controlled directly or indirectly by HOIS, perform espionage, sabotage, and subversion as primary missions. These agents are active in peacetime, performing subversion and espionage. However, the majority of agents in peacetime are used in a passive role. When international tensions indicate armed conflict, the threat activates agents from the FLOT back through CONUS. Along with and to support their military unconventional warfare forces, HOIS use the following types of agents:

Agents in Place. Agents are recruited in vital areas of the target nation--in political circles, intelligence and security agencies, the military, industry and academic institutions, and in the mass media.

Confusion Agents. Confusion agents spread rumors which cause Allied CI and security services to expend great amounts of time, manpower, and effort confirming or disproving them. These agents spread fabricated information which is based on fact. They are controlled by hostile forces. To protect other active HOIS operations, the confusion agents' mission is to mislead Allied security services.

Provocation Agents. Similar to double agents, HOIS have trained persons to provoke friendly forces into self-damaging actions. For example, information is provided of an impending attack against a rear area logistics site, when in

actuality the attack is in another sector against a different target. The original report may cause a friendly commander to allocate reaction forces to the bogus target, leaving the real target unprotected.

Sleeper Agents. As a rule, these trained agents are inactive, sometimes for years. With the approach of hostilities, these agents are activated to engage in political agitation, espionage, and sabotage.

Mass-Recruited Agents. When hostilities begin and during the battle, the Threat infiltrates low-level agents into friendly areas as refugees. They report on overt military and nonmilitary activities, such as convoy routes and unit identifications. Their compromise constitutes no real operational loss for the threat and can tie up Allied CI and security assets, thereby, diverting attention from more significant HOIS operations.

Regardless of motivation or target selection, Level I activities consist of small groups directed against pinpoint targets. Attacks are of short duration. Unless intelligence provides indications and warning of potential targets, reaction forces are unlikely to arrive at a Level I activity in time to interdict the threat force.

Sympathizers are a threat to military personnel, facilities, and communications in rear areas through random acts of arson, sabotage, theft, and assassination. HOIS organizes these sympathizers to support threat operational forces in Levels II and III.

Terrorist organizations confronting friendly rear areas are dedicated to overthrow the established government or economic system. Threat doctrine stresses terrorist acts to prepare for and conduct offensive operations. The threat attempts to organize or influence host-nation terrorist group activities. The goal is to paralyze a target nation's will and ability to react effectively when open conflict occurs. Terrorist actions are directed against civilian populations, host-nation military and government organizations, commercial facilities, and US military and civilian personnel.

Threat Level II

In contrast to Level I operations, which may be outside of threat control, Level II operations are orchestrated by the threat. They support tactical, operational, and strategic objectives. Their use is dictated by army and front missions. Their operations, if detected, are an intelligence indicator of army or front potential. Nuclear weapon storage sites and launch systems, C^2 headquarters, key terrain, avenues of approach into rear areas, major logistics facilities, and reserve forces are the main objectives of these operations.

Threats to friendly rear areas at Level II are characterized by diversionary operations conducted by special-purpose troops. In addition, reconnaissance and sabotage operations are conducted by regular units of less than battalion size.

The threat maintains highly trained, special purpose troops for behind-the-lines operations. Manned by skilled officers and noncommissioned officers (NCOs), their training includes demolitions, communications, foreign weapons, and fluency in the languages of the target area. Before the first battle, these forces infiltrate international borders, possibly using commercial airlines.

Infiltration is also accomplished by airdrop, helicopter, vehicle, on foot, and by sea. Wearing Allied forces' uniforms or civilian clothes, they attempt to penetrate military facilities, march columns, and other targets of opportunity. They try to disrupt, destroy, or mislead friendly forces. Nuclear weapons storage sites and launch systems, C^2 headquarters, communications facilities, and reserve unit areas are primary targets for these forces. (See FM 100-2-2, Chapter 5, for a hypothetical scenario on the employment of special purpose troops.)

Threat motorized rifle and tank divisions have reconnaissance battalions which conduct reconnaissance of the enemy rear area and provide intelligence on enemy troop disposition out to 100 kilometers beyond the FLOT. The battalion normally employs itself in squad-sized elements. It may have six to eight separate armored reconnaissance squads. The battalion conducts reconnaissance probes on three or four axes.

Specially organized reconnaissance groups may be directed to raid installations or to conduct ambushes, although their primary mission is to collect intelligence information. They can also be directed to locate specific reserves and to identify boundaries between units. These groups may also conduct specific missions, such as the capture of prisoners or documents or the surveillance of unit positions or movements.

Threat Level III

Enemy highly-mobile, well-trained airborne, heliborne, and amphibious forces operate in conventional or nuclear environments. These specialized units, together with deliberate ground force operations, pose the Level III threat to friendly rear area operations.

As with US airborne or heliborne operations, Level III operations are complex. Aircraft are marshaled, equipment palletized, and troops concentrated. Air defense suppression missions, clearing of air defense corridors, and eventual linkup with ground forces is planned and executed.

Airborne Operations. Threat paratroopers are organized into elite parachute divisions. To allow flexibility in employment, Threat airborne forces are directly subordinate to a supreme high command, with operational control exercised by the general staff. In wartime, some airborne units are allocated to Threat theaters of military operations and fronts for strategic operations. Units are also temporarily allocated to fronts and combined arms and tank armies for specific operational depth missions.

Other airborne units are retained under the control of a supreme high command for contingencies. Airborne units may be air dropped or air landed with light armored vehicles, including BMDs and ASU 85s. Once committed, airborne units either await a linkup or fight their way back to their lines.

Heliborne Operations. The Threat has dedicated heliborne or air assault units and some motorized rifle units trained to perform heliborne operations. Heliborne operations are conducted by company- and battalion-sized forces. Their objectives are nuclear weapon storage sites and launch systems, command and control headquarters, key terrain or avenues of approach, and logistical facilities. These heliborne forces may be augmented with antitank, anti-aircraft, and artillery units. Some light armored and wheeled vehicles can be included in the force for use as missile carriers and reconnaissance vehicles. Weapons are light machine guns, antitank grenade launchers, antitank missiles, surface-to-air missiles, recoilless rifles, and mortars.

Amphibious Operations. Threat naval forces have initiated extensive training and development of their naval infantry. Recent developments indicate a definite seaborne threat against critical enemy rear area ports and facilities. The Threat naval infantry can conduct tactical landings with highly mobile forces, air-cushioned vehicles, and high-speed landing ships. The Threat amphibious operations are--

- Strategic landing. A multidivision landing with naval and air support to open or expand a military operation.
- Operational landing. A regiment- or division-sized landing to seize an island, a base, or coastal facility.
- Tactical landing. A battalion-sized or larger strike against an enemy coastline or facilities. This operation may support an inland ground force operation.
- Reconnaissance and sabotage landing. A landing conducted by a battalion, company, or platoon against coastal facilities.

In deliberate ground force operations, the Threat can employ a high-speed exploitation force to form a division- to an army-sized unit. This force, called the OMG, is tailored structurally for the mission and is designed to move deep into a rear area. It is to seize critical objectives, usually before the second-echelon Threat formations are committed to combat. The mission of the OMG is, if required, to help the first echelon penetrate the enemy defenses, and more important, to raid deep into the enemy rear as early in the offensive as possible. Typical OMG targets are nuclear weapons, C^3, air defenses, and airfields.

CI SUPPORT

In addition to knowing the threat capabilities in the rear area, CI personnel must know the scheme of maneuver for friendly units. They must know and understand the commander's rear area support plans. Failure to thoroughly understand these subjects can leave devastating gaps in countermeasure development and identification of critical targets.

OPSEC support is a crucial rear operations element. The multidiscipline threat posed by HOIS demonstrates a remarkable ability to identify gaps in our security that can be exploited. Due to the more static nature of rear area units, OPSEC must be a continual, day-to-day function. Only by denying Threat intelligence through OPSEC and portraying the false through deception, will we ensure that the Threat commander is sufficiently confused as to our real dispositions. Through constant vigilance, the Threat can be denied surprise. Without the element of surprise, a knowledge of the location and strength of our troops, and a suitable drop zone, the Threat is not likely to sacrifice their soldiers.

Upgrading intelligence holdings from reports submitted by all sources plays an important part in providing an accurate picture of Threat intentions for rear area operations. Because the rear area threat is dynamic, CI personnel must continually assess the threat level and develop and recommend appropriate countermeasures (see FM 34-60A (S/NOFORN).

The illustration on the next page demonstrates the wide range of CI responsibilities in support of rear operations. Many of these activities, such as Level I threat operations, are in progress long before the outbreak of declared hostilities.

REAR AREA IPB

Rear area IPB is a process used to reduce uncertainties concerning the rear area. Through IPB, HVTs for the threat may be predicted. Once predicted, HVTs may be guarded, surveilled, or should destruction occur, replaced. Rear area IPB supports both rear operations and area damage control (ADC). Although of slightly different focus than the traditional IPB process, terrain and weather analysis, coupled with the friendly mission, will identify HVTs. CI analysts assigned to the G2 section assist the ASPS, the corps support command (COSCOM) S2, and G3 or G4 planners in rear area IPB. These analysts, with full appreciation of the threat and providing CI analysis to the rear area IPB, play a major role in the command's efforts to reduce the uncertainties involving rear operations. In analyzing the rear area, CI analysts consider the following five steps.

Step 1--Threat Evaluation

Step 1 is a detailed study of threat forces, their composition and organization, tactical doctrine, and weapons and equipment. Available data on terrorist elements that may affect the rear area is included in the threat evaluation. Threat evaluation determines capabilities and how they operate

CI SUPPORT TO REAR OPERATIONS

	EAC		ECB	
	PEACE	WAR	PEACE	WAR
Rear area IPB	X	X	X	X
Liaison CONUS	X	X	X	X
Liaison OCONUS	X	X	X	X
RA threat collection/briefing	X	X	X	X
Threat awareness training/security advice and assistance	X	X	X	X
Defensive source operations	X	X	X	X
Incident investigations	X	X	X	X
Create/update white/black/gray list	X	X	X	X
Identify/capture teams/cells	X	X		X
Analysis of enemy SIGINT operations	X	X	X	X
Analysis of enemy IMINT operations	X	X	X	X
Analysis of ECM operations	X	X	X	X
Stay-behind operations	X	X		X
Terrorism counteraction	X	X	X	X
Screening and interrogation	X	X	X	X

relative to their doctrine and training. Analysts will not only determine Threat targets in our rear area, but will consider the quantity and quality of Threat forces detailed to conduct rear area operations.

Step 2--Area of Interest Evaluation

Step 2 is the evaluation of the rear area of interest. Analysts consider the friendly assigned mission, concept of operations, and anticipated threat to that mission. This mission analysis includes an extensive understanding of how the commander and staff anticipate the battle plan and how the COSCOM will logistically support the concept of operation. Given almost any scenario of conflict, the combat support and CSS units will have extended LOCs with limited assets. CI personnel must assist the planners to ensure integration of OPSEC planning, deception operations, and full integration with G2 collection management and analytical sections. Concerning the rear operations, CI personnel receive tasking from the CM&D section. As they collect on the taskings and report the information to the CI analysis section, this information is analyzed and developed into a usable product. It is then provided to the ASPS for inclusion into the all-source analysis process and to the CM&D section for further dissemination.

Bridges and overpasses are likely targets because they are easy to destroy and difficult to replace. Thus, all bridges and overpasses along the main supply route are likely targets. If the bridges are irreplaceable, then fording sites near the bridges are identified. If fording sites are not available, then simple bank reduction by engineer assets may reduce the magnitude of the loss of the bridge, or ADC could be asked to stockpile bridging material for field-expedient bridges.

Engineer personnel, either with the CP or within the rear operations, are made aware of these bridges and overpasses and their importance. Constant interaction with collection management provides surveillance of these targets during reconnaissance of more traditional targets.

Steep gradients and numerous S-turns also provide potential targets of logistical elements. Logistical vehicles, heavily loaded with supplies, slow to a crawl negotiating S-turns or steep grades. These are likely ambush points, since this is where the heavily loaded vehicles are most vulnerable. Overpasses, especially when used in a road network from one cut to another, are key targets for the Threat. Their destruction makes large stretches of the road useless, and they are difficult to replace. A detour route around the overpass, preplanned and made known to all drivers, may be necessary to ensure that the supplies arrive in time to affect the battle.

Increased patrolling by MPs in a rear operations mission and surveillance by ground surveillance radars or overhead platforms may provide indications and warning intelligence. CI operations in and around these areas, from liaison to defensive source operations, support the indications and warning effort against these target areas. Narrow railroad cuts may provide concealment and cover for semipermanent combat support and CSS assets.

Camouflage nets placed across the top of the cut will provide some overhead concealment, in addition to LOS concealment.

Threat imagery analysts will be concentrating on locating "traditional" logistical elements in wooded areas adjacent to likely main supply routes. IPB may identify tunnels which would provide excellent cover and concealment for supplies or activities. Security for tunnels is easy to implement.

Because of the concealment afforded Threat forces, roads that bisect heavily wooded areas are likely obstacles and ambush sites. During World War II, German forces routinely cleared trees away from such roads, which made partisan ambushes more difficult and less frequent. The cleared trees were used for barrier construction elsewhere. If not feasible, locating of such main supply routes away from these ambush sites may be possible.

Cleared areas near critical bridges, roads, and road junctions are likely heliborne or airborne insertion areas. Percent of slope calculations on these cleared areas may reveal that it is too steep for helicopter landings. Threat forces will usually use cleared areas which afford nearby concealment away from built-up areas. They are willing to trade time from target for security. Integration of these areas, with the overall collection plan, is a necessity.

Step 3--Terrain Analysis

Terrain analysis of the rear area offers a distinct advantage over analysis of Threat-held or denied areas, since rear area analysis may be verified by ground reconnaissance. The military aspects of terrain, once defined by the IPB, are surveilled to ensure accuracy. CI teams perform ground analysis, and surveillance assets are tasked to fill in gaps or critical areas, possibly along with the development of OPSEC profiles. Once the G3 and G4 planners have assigned the main supply routes from the corps and division support area to the combat trains, terrain analysis is applied to determine rear area HVTs that the Threat will attempt to interdict, disrupt, or destroy. A demographic analysis of the rear area assists in identifying possible terrorist sympathizers and support bases.

Step 4--Weather Analysis

The effects of weather, primarily precipitation, are analyzed when determining bridge and overpass priorities. Streams whose bottoms vary in composition are carefully analyzed when determining fording sites. The composition of the soil adjacent to the bridges and the effects of precipitation on that soil must be understood. An alternate fording site, with banks reduced and astride a gravel stream bottom, is of little use if the approaches become "gumbo" and are no longer of use without stabilization. Fog provides concealment of main supply routes which cross likely target areas. Since overlays make this predictable, fog may be used to prioritize our reconnaissance efforts in the rear area. Therefore, IPB must always be analyzed with the threat uppermost in the mind of the analyst.

Step 5--Threat Integration

The last step in the rear area IPB process integrates Threat doctrine with weather and terrain data. The objective of integration is to determine how the Threat will fight as influenced by weather and terrain. Threat integration is accomplished through the development of situation, event, and decision support templates. For example, Threat doctrine calls for company-sized airborne drop zones. (Company-size is 1-kilometer square and regimental-size is 3 kilometers x 4 kilometers.) These drop zones are normally 5 kilometers from the objective. They are screened from observation from the objective area by terrain or vegetation. Using weather and terrain threat criteria, a situational template is constructed which discriminates likely drop zones from those which do not fit the above criteria. Surveillance of these drop zones provide the only warning necessary to defeat the Threat attack.

From these likely drop zones, single and multiple routes to the objective are identified. Such routes are normally the most direct route to the objective. But they avoid built-up areas, if at all possible. Doctrine calls for these routes to be off-the-road as much as possible. IPB of these routes provides TAIs.

Situation templates are constructed showing likely rendezvous points. Threat doctrine calls for company-sized rendezvous points to be located on an easily found terrain feature approximately 1 kilometer from the opposite side of the objective from which the assault was launched.

Should the Threat use multiple airborne drops, such as a battalion drop with companies on multiple drop zones, threat doctrine calls for a battalion rendezvous point that is often as far away as 10 kilometers from an objective. Using the above doctrine, likely rendezvous points in a solution template are also likely TAIs.

Threat doctrine normally calls for a 1-hour consolidation on the initial drop zone before movement of the entire element to the objective. Reconnaissance elements, however, are dispatched as soon as possible to provide intelligence on the previously selected routes to the objective, as well as intelligence on the objective itself.

A decision support template is constructed of likely airborne operations against specific units or activities in the rear area. This decision support template uses NAIs for likely drop zones. It also uses TAIs for choke points along routes from the drop zones to friendly units and activities, and includes all likely rendezvous points. Such NAIs focus collection planning in the rear area and TAIs are incorporated into target plans. Should multiple drop zones be predicted through IPB, the resultant multiple routes to friendly units or activities may provide decision points where Threat routes may be predicted, if reported. Such decision points, incorporated into the collection plan, provide early warning to specific units. (See FM 34-3 for a thorough discussion of these templates.)

CHAPTER 6

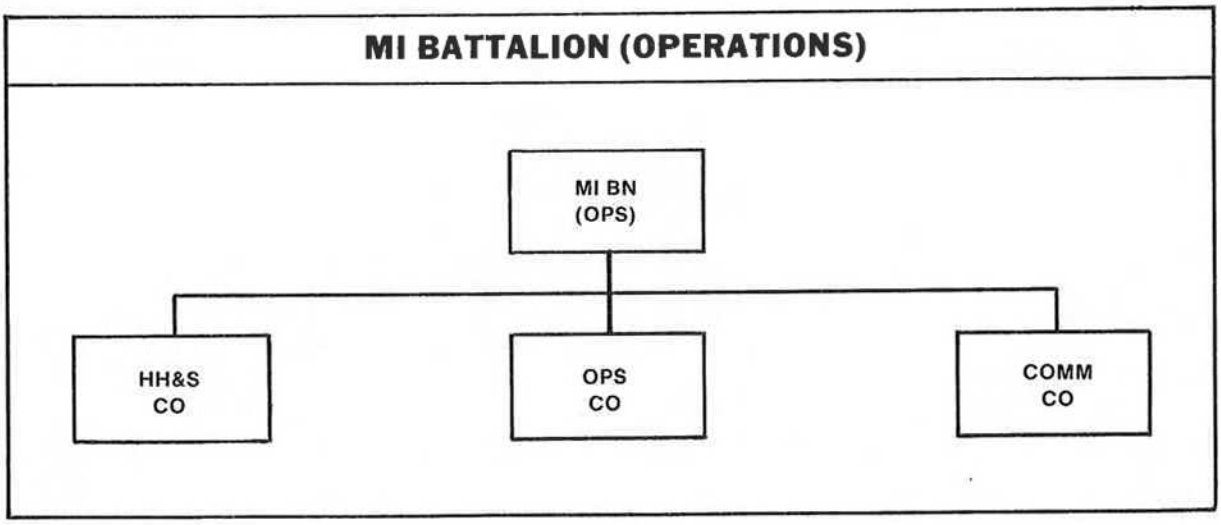
MI BATTALION (OPERATIONS)

The MI battalion (operations) is composed of operating elements which support corps IEW operations (organization is shown in the following illustration). The mission of the battalion is to--

- Support the corps G2 in performing requirements and mission management of situation and target development and CI.
- Support the corps G3 in performing requirements and mission management of OPSEC, deception, and ECM.
- Provide security to the SCIFs located within the corps.
- Support the MI brigade S3 in the management of brigade SIGINT and EW resources.
- Provide secure intelligence communications to the MI brigade and corps MSCs.

The CTOC support element assists the corps G2 and G3 in planning, coordinating, integrating, and directing IEW operations. It also provides all-source intelligence production and collection management for the G2.

The TCAE is the technical manager of corps SIGINT and EW operations. It coordinates and provides technical direction, control, and analysis for SIGINT and EW operations conducted by the MI brigade. The TCAE is normally located within the MI brigade operations center and reports directly to the brigade S3.

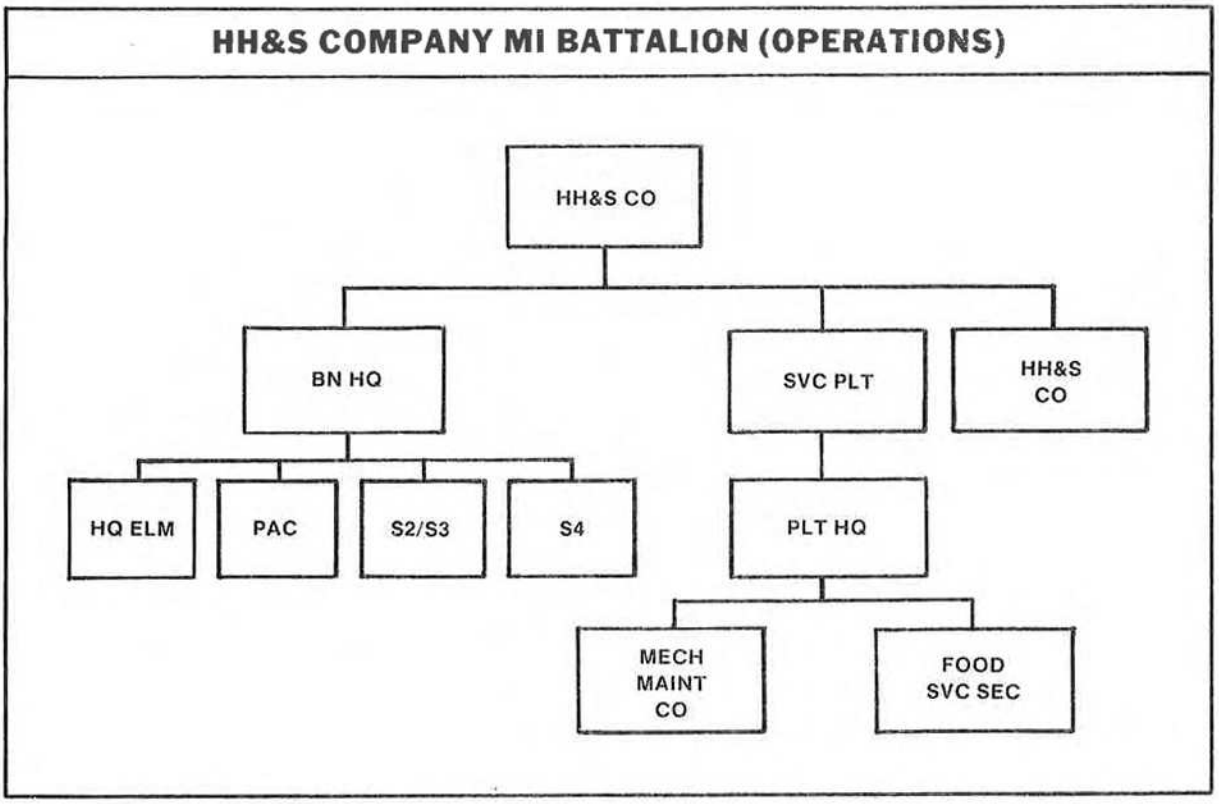


Communications are critical to successful IEW operations. MI brigade assets deploy throughout the corps area, from the FLOT to the corps rear boundary. The operations battalion provides the communications necessary for tasking, reporting, and technical control.

HEADQUARTERS, HEADQUARTERS AND SERVICE COMPANY

The company provides C^2 of assigned and attached units, consolidated food service, and mechanical maintenance for the battalion on organic equipment except C-E equipment.

Headquarters, headquarters and service (HH&S) company for the MI battalion (operations) is organized as shown in the following illustration.

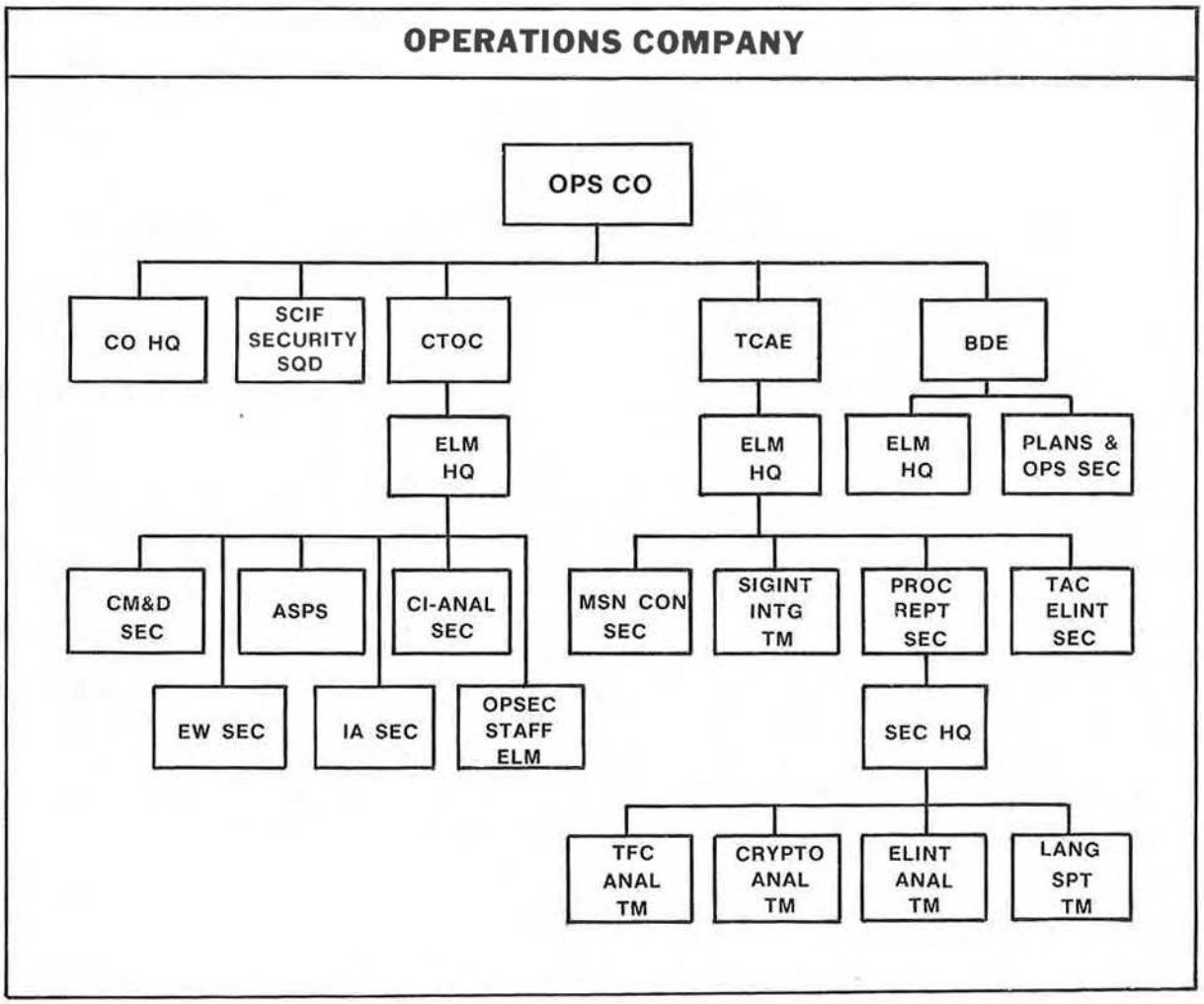


The battalion headquarters provides staffing and C^2 of assigned and attached elements. The battalion commander is responsible to the MI brigade commander for the performance of his unit. Two AN/VRC-46 radios are provided to the battalion commander to operate in the MI brigade command net and the MI battalion (operations) command net. He is assisted in his duties by the XO.

OPERATIONS COMPANY

The operations company provides the personnel with the appropriate expertise to manage and task the intelligence resources of the MI brigade, corps G2 and G3.

The operations company is organized with a company headquarters, which provides C^2, a SCIF security squad, a CTOC support element, and a TCAE (organization of the operations company is shown in the following illustration).



COMPANY HEADQUARTERS

Under the direction of the company commander, the company headquarters deploys the primary operating elements of the company and the normal day-to-day administrative and personnel support. The headquarters provides

discipline, administration, and training of personnel. The commander and company staff coordinate with the staff elements of the battalion to ensure that food service, maintenance, and communication support are provided. The company headquarters is located in the vicinity of the MI battalion CP.

SCIF SECURITY SQUAD

Under the supervision of the squad leader and the direction of the operations company commander, the SCIF security squad provides 24-hour physical security for up to three SCIFs. This squad consists of MP personnel assigned to the operations company. Each SCIF security team will provide 24-hour physical security and entry control for its facility. Minimum physical security requirements for field SCIFs are specified in DIAM 50-3, Chapter 7.

Special security officers review and update their unit field SOP to ensure that security standards are met. Some of these standards are described below.

When the SCIF area is located within the confines of the supported command's tactical operations center (TOC) or defensive perimeter, the SCIF is surrounded immediately with a minimum of single-strand concertina wire. SCIFs located in this environment for an extended period (that is 48 hours or more) increase their physical barrier to triple-strand concertina wire. In those instances in which the SCIF is outside the supported command's TOC or defensive perimeter, the SCIF is fenced with triple-strand concertina wire. However, if the SCIF moves frequently, single-strand concertina or a similar type of wire may be employed.

The perimeter of the controlled area is guarded by walking or fixed guards who observe the entire controlled area. The guards are armed with weapons and ammunition prescribed by the supported command. Guards need not be indoctrinated for sensitive compartmented information (SCI) providing they conduct roving patrols and control access outside the protective perimeter. Roving guards are required to observe the entire controlled area when observation is not possible from a fixed position. If additional guards are needed, the SSO coordinates such support with the MP unit commander.

Access to the SCIF area is restricted to a single gate or entrance. The gate or entrance is guarded on a 24-hour basis. A landline between the entrance point guard and the SSO administrative area facilitates the rapid and efficient entry of cleared personnel.

The SSO maintains a current access roster that includes SCI-indoctrinated personnel of the local command and other authorized personnel requiring access. Access is restricted to those on the access roster. Access by others (that is, maintenance personnel) may become necessary, but must be minimized.

A minimum of two SCI-indoctrinated personnel are present in the SCIF at all times.

Emergency destruction and evacuation plans are maintained on a current basis and kept in the facility.

When not in use and during SCIF relocation, SCI material is stored in General Services Administration (GSA)-approved containers.

Communications, both wire and radio if possible, are established and maintained with the security guards. Use of field telephones is authorized if a filter or some other suitable means is used to preclude inadvertent disclosure of information over open lines or circuits. FM radios constitute a potential security hazard and are not to be used within the SCIF. An AN/VRC-46 is provided for each team for mobile patrol of the facility and an AN/PRC-77 for entry control or foot patrol of the facility. The SCIF squad will be located with the CTOC and TCAE.

CTOC SUPPORT ELEMENT

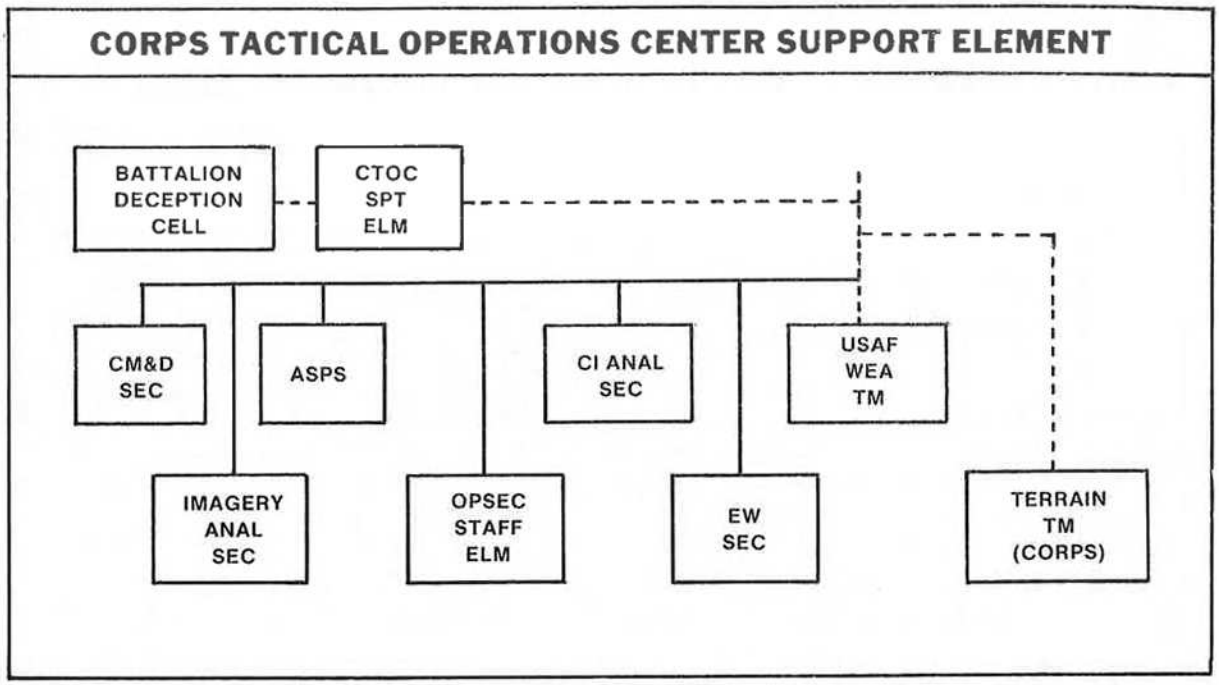
The CTOC support element operates under the staff supervision of the corps G2 and G3. It provides the corps G2 with intelligence and CI planning and intelligence collection management, production, and dissemination. It supports the G3 with EW, OPSEC, and deception planning. The support element is supported by a USAF weather team and a corps terrain team. To accommodate the additional workload caused by activation of the reserve component (RC) divisions, the element is augmented with personnel from the RC MI battalion (TE) when that unit is activated. The CTOC support element is organized as shown in the following illustration.

Collection Management and Dissemination Section

The CM&D section, under the staff supervision of the G2, is the major intelligence planning element for the corps. It provides identification of intelligence requirements management, mission management, and intelligence and combat information. Intelligence requirements are usually generated by the G2, outside agencies, the ASPS, and the CM&D itself. Based on the tactical situation, the CM&D section plans and develops collection missions and tasks the appropriate agencies.

Collection management makes the most effective use of available collection resources. The three steps of collection management are requirements, mission, and asset management. Requirements and mission management is accomplished by the CM&D section. Asset management is performed by the unit S3 or G3 or by the agency controlling the resources.

Collection management begins with the identification of requirements. In planning an operation, they usually support command and staff estimates. After the commander's decision and concept of the operation are announced, PIR recommendations are developed by the G2. Because of their criticality, PIR are approved by the commander.



IR are developed concurrently with PIR. These requirements reflect other capabilities, vulnerabilities, and characteristics of the AO which may affect mission accomplishment. IR generally are developed from command and staff requirements which do not qualify as PIR.

Requirements management translates general PIR and IR into specific, detailed, answerable questions. It enhances the focused, efficient employment of intelligence collection organizations. Converting requirements into meaningful, specific collection tasks begins with requests from subordinate divisions, ACRs, separate brigades, and adjacent corps. These requests are received over dedicated communications. Dissemination is normally through these same channels. The intelligence center and the CM&D section exchange requirements, intelligence, and other information over similar direct communications.

The CM&D section requirements manager--

° Logs incoming requirements or requests.

° Assigns an identification number and suspense.

° Ensures that all necessary information is included.

° Checks the ASPS data base to see if an immediate response can be sent.

° Consolidates new and existing requirements.

° Assigns priority (PIR are the highest priority).

° Interfaces with the corps SSO regarding availability of hard-copy and electrical SCI products.

° Submits requests for SCI processing to the corps SSO for validation.

° Develops indicators and SIR to fulfill the request.

° Determines who needs the information other than the requester.

Mission management identifies, selects, and tasks collection resources to satisfy SIR. The mission manager maintains extensive data on the capability and availability of organic resources as well as those of higher, lower, and adjacent echelons.

On receipt of SIR from the requirements manager, the mission manager determines supportability and the types of resources needed to satisfy each request. He selects specific units or agencies based on--

° Availability.

° Capability.

° Suitability.

° Balance.

° Cuing and redundancy.

The mission manager also consolidates new and existing tasking and prepares and transmits mission tasking.

Close coordination with the ASPS is required throughout mission management. The ASPS determines if the request can be answered from existing data. Analysts assist the requirements manager in developing indicators and SIR. IPB is particularly important to focus on key areas on the battlefield for collection.

Mission tasking normally specifies the collection agency, information required, reporting procedures, time requirements, and support relationships for MI resources. Tasking for the MI brigade is sent by dedicated

communications to the brigade operations center. Tasking of non-MI resources is through the G3. Requests and taskings for higher, adjacent, and lower echelons is sent through CM&D-to-CM&D channels.

Intelligence and combat information reporting by collection assets is as follows:

- Combat information derived from any source is immediately disseminated to the appropriate user by the quickest means available.
- SIGINT and EW assets report information back to the TCAE in the brigade operations center. Collected information is analyzed, correlated, and transmitted to the ASPS by the TCAE.
- Other MI assets, such as interrogation, CI, and aerial surveillance report information directly to the CM&D section and brigade tactical operations center.
- Reported information is then passed to the ASPS for analysis and integration into the all-source data base.

The ASPS determines the pertinence and accuracy of the collected information. Additional requirements are developed from identified gaps. The CM&D section monitors reporting and the completion of assigned missions. Collection planning and mission tasking are adjusted as necessary.

The CM&D section disseminates collaterally classified or unclassified intelligence and information to the G2 operations section which further disseminates it to appropriate commands, agencies, or staff sections. Combat information is forwarded to the corps G2, the staff section for dissemination to the appropriate G3 section. Intelligence is disseminated to--

- The corps commander and his staff.
- Commanders of units subordinate to the corps and their staffs.
- Adjacent and higher commanders.
- Other users.

How the intelligence is actually disseminated depends on several factors, such as importance and perishability. In all cases, the CM&D section is responsible for disseminating the required intelligence to the proper user as quickly and securely as possible.

Non-MI resources, including tactical units supported by MI resources, normally report collected information through intelligence channels.

Information that they report is based on at least three criteria:

° Corps PIR and IR. Those collection requirements which are disseminated and responded to as described earlier.

° Directed collection tasks. Those immediate to the corps requests which are tasked to subordinate elements.

° Impact on higher echelon operations. That information collected during normal operations which is estimated to have an impact on echelons other than the one that collected the information. Such information may be a compilation of reports received by subordinate units and reported to the corps through normal channels. The CM&D may, in turn, use this information to prepare reports for EAC and adjacent corps.

All-Source Production Section

The ASPS, under the staff supervision of the G2, supports the corps with all-source intelligence production. It develops and maintains the intelligence data base and identifies gaps in the intelligence effort. It forwards all-source intelligence products to the CM&D section for dissemination. The ASPS, assisted by the corps terrain team and the USAF weather team, accomplishes situation and target development functions using IPB and TVA methodologies.

All-source intelligence is the product derived from the processing of information collected from all available sources. Therefore, all personnel working within the ASPS must be indoctrinated for access to SCI. Information used to develop all-source intelligence is raw data, combat information, and finished intelligence products. Sources at corps level are--

° All corps collection agencies and subordinate commands.

° Adjacent corps.

° EAC or national collection agencies.

° Other services.

° Allied forces.

Whenever possible, all-source intelligence is the basis upon which commanders and their staffs plan and conduct tactical operations. The commander would prefer to base his combat decisions on all-source intelligence. However, the commander often does and certainly will make many decisions based on a single bit of unconfirmed information if from a reliable source.

Processing, the primary function of the ASPS, consists of recording, evaluating, and analyzing. It begins as soon as information is received from the CM&D section or through interface with other analytical elements and

agencies. The sequence depends on the nature and urgency of the information. Usually, recording is first. On urgent items, however, recording may occur simultaneously with evaluating and analyzing.

Data are stored in a manner that permits immediate retrieval. To record and control information, the ASPS uses several common aids. Data base files consist of all files necessary to maintain processed data and produce intelligence. The three most common files are target folders, situation maps (SITMAPs), and order of battle (OB) files. The target folder is essential to the target development and actions. OB records and files are used for the production of new intelligence. Other files are established as necessary.

Evaluation is a standardized method used to determine the pertinence, reliability, and accuracy of information in further processing, dissemination, and decision-making actions.

Analysts determine whether the information is directly related to the AO, and who is affected by the information. The source and reporting agency are assessed for their consistent dependability based on prior experience or by accepting the judgment of another headquarters. The information is then compared to similar information from the other sources in an attempt to confirm or deny it. When the analyst identifies gaps in intelligence which prevent a reasonable deduction, he generates a request for information and passes it to CM&D for action.

Another technique used by the ASPS to process and analyze information is IPB. IPB is the detailed analysis of the battlefield, weather, and terrain and continues into the combat environment. It develops data on specific enemy forces and potential conflict areas. This data, when reduced to graphic form, provides a ready means to determine and analyze changes in an AO or in the enemy force.

IPB is a cyclic process that begins with battlefield area analysis. This is followed by detailed weather and terrain analysis of the corps AO with the assistance of the USAF weather team and the corps terrain team. Analysis focuses on avenues of approach and mobility corridors. Analysis enables the commander to focus on those areas where the enemy can move, shoot, and communicate. Overlays and matrixes that graphically display weather and terrain effects are prepared to facilitate threat integration.

Templates are used to develop a detailed analysis of enemy capabilities and possible courses of action relative to existing and forecast effects of weather on the terrain. Templates graphically display to the commander how the enemy would like to fight on a specific piece of terrain, given a certain weather scenario. This technique also applies to friendly rear areas in support of OPSEC.

IPB is continuously updated. It supports planning and decision making by the corps staff and aids in directing intelligence, EW, and OPSEC planning and operations.

Through the processing and IPB functions, the ASPS develops a comprehensive data base. ASPS provides intelligence summaries and information satisfying specific staff requirements.

The ASPS also supports other CTOC support element sections. It supports the CM&D section in collection planning and monitors the collection plan to identify gaps. It passes OB information to the TCAE to facilitate SIGINT analysis. It supports the EW section with intelligence on the enemy REC threat and provides electronic order of battle (EOB) data. It cues the imagery analysis section by providing OB information. It also provides targeting data to the FSE of the deep attack cell.

The mission of the ASPS is continuous and demanding. Its primary product, all-source intelligence, is critical to the successful combat operations of the corps. It provides the most accurate, reliable product possible.

Imagery Analysis Section

The imagery analysis section exploits imagery for the corps. Intelligence gained from imagery is reported through the CM&D section. The imagery analysis section assists other CTOC support elements in determining imagery support requirements.

USAF Weather Team

The USAF weather team provides weather observation to the staff weather officer (SWO) and forecast support to the corps. The team works closely with the ASPS and the terrain team to integrate weather into IPB.

Corps Terrain Team

A terrain team is assigned to the corps. The team supports the ASPS in IPB and provides other terrain intelligence assistance.

Counterintelligence Analysis Section

The CI analysis section, under the staff supervision of the G2, assists in determining the risk the enemy intelligence threat poses to friendly operations. It plans and recommends mission tasking for corps CI assets and works closely with the OPSEC support element to meet the OPSEC responsibilities of the G3. The CI analysis section--

- Maintains the hostile intelligence collection threat data base and provides timely HUMINT to ASPS on a continuing basis.
- Analyzes threat collection capability and intentions.
- Identifies friendly force vulnerabilities to intelligence collection, sabotage, and terrorism.
- Supports G3 risk analysis.

° Assists in developing EEFI.

° Recommends OPSEC measures.

° Identifies deception opportunities.

° Assists in deception planning.

° Assists in preparing OPSEC plans and annexes.

° Develops OPSEC evaluation requirements.

° Supports rear operations planning and operations.

It manages the CI mission for the G2. This includes mission management of CI support to OPSEC, rear operations, deception, and terrorism counteraction. Source control and approval of CI specialized operations, such as defensive source operations and tactical agent operations are handled according to FM 34-60A (S/NOFORN). CI missions are passed to the CM&D section for tasking to the MI brigade. Requests for EAC support are also sent through CM&D channels.

OPSEC Staff Element

The OPSEC staff element assists the G3 in fulfilling OPSEC responsibilities. It prepares and implements the corps OPSEC plans and annexes, manages the OPSEC training and education programs, and develops OPSEC survey requirements and missions. Taskings for MI brigade support to the brigade operations center go through the CM&D section.

Electronic Warfare Section

The EW section assists the G3 in carrying out EW staff responsibilities. It plans EW operations and recommends task organization and allocation of EW resources.

The EW section--

° Supports the G3 with EW planning to include J-SEAD and C^3CM.

° Works in close coordination with the TCAE to identify opportunities for effective targeting using jamming, deception, or PSYOP.

° Coordinates EW operations between division, corps, and EAC to preclude disruption of the friendly use of the electromagnetic spectrum.

° Coordinates with FSE and BCE to ensure corps EW headquarters are supported and included on the air-tasking order when Air Force support is needed.

- Coordinates with the corps C-E officer to preclude jamming or interfering with friendly frequencies.
- Coordinates with corps collection manager to ensure protected frequencies are not jammed.

BATTLEFIELD DECEPTION ELEMENT

Battlefield deception elements (BDEs) are at both corps and division. Although both elements operate toward the same objective, that is, accomplishment of the deception plan, their functions vary greatly in the planning and execution of battlefield deception.

The corps BDE is responsible for augmenting the theater deception objective. As required, it ensures applicability to the division-level BDE, provides deception planning support, supports the execution of corps deception operations, and executes limited deception events with organic resources such as decoys, communications deception, and logistics or critical node replication. The corps BDE is, generally, collocated with and operates under the staff supervision of the CTOC G3.

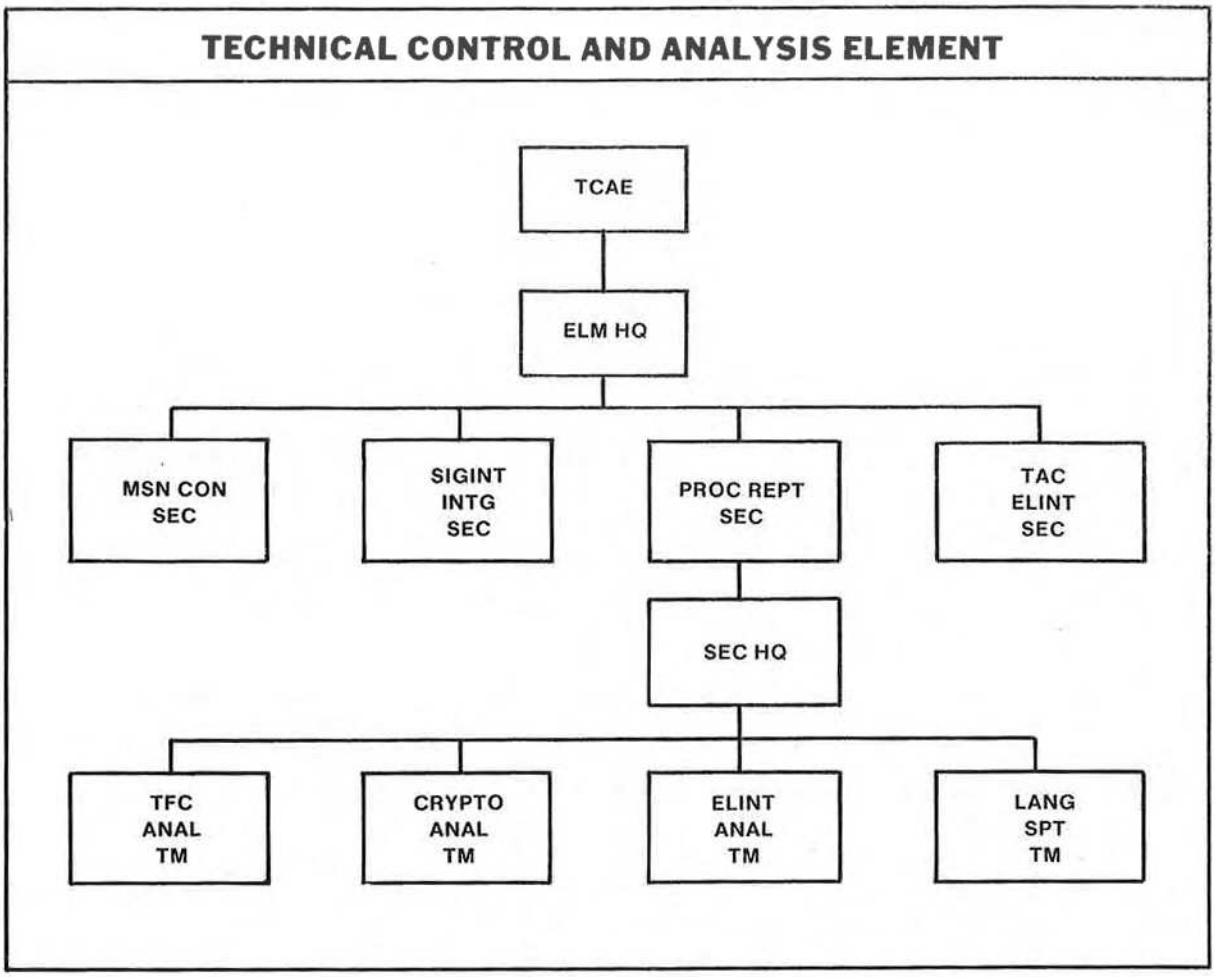
TECHNICAL CONTROL AND ANALYSIS ELEMENT

The TCAE assists the S3 in the technical management of the SIGINT and EW assets of the brigade as well as for the corps master control station (MCS) SIGINT and EW assets. It also levies specific tasking requirements. The TCAE is responsible for the mission planning and asset management of the jammers attached from the MI brigade EAC. Signal intercepts are analyzed and reported as required. The TCAE maintains an extensive technical data base to support SIGINT agencies at echelons corps and below (ECB) and EAC and serves as the interface between corps and EAC. Because the rapid flow of information is critical to SIGINT and EW operations, the TCAE is heavily dependent on reliable, secure communications. The TCAE is located within a SCIF and is an area of concern for the corps SSO. The TCAE organization is shown in the illustration on the following page.

Element Headquarters

The element headquarters is responsible to the operations battalion commander for supervising and directing efforts of the TCAE.

Mission Control Section. The mission control section is responsible for tasking and controlling the SIGINT and EW systems of the brigade. It serves as the liaison to SIGINT and EW units ECB and EAC, develops and issues specific tasking for all brigade SIGINT and EW assets, and acts as the coordinating agency for all SIGINT and EW activities within the corps area. Collection and jamming coordination prevents unnecessary duplication of effort and facilitates the handing off of enemy elements as they move across unit areas or enter a subordinate unit's AO.



Because of its tasking, coordinating, and controlling responsibilities, it must be fully aware of SIGINT and EW activities within the corps area. To ensure that this information is available, it receives, sorts, catalogs, and distributes all messages, data, and reports received at the TCAE.

The mission control section receives resource status reports (RSRs) on all SIGINT and EW systems within the corps, as well as information from sources such as--

° Organic brigade resources.

° The divisions, ACR, and separate brigade.

° EAC and national level.

Mission tasking, as received for collection operations, states only the information required, when it may be found, and when it is required. Mission tasking for ECM operations specifies the target or targets, time required, intended purpose, and any controls which have been established. In developing asset tasking, the mission control section--

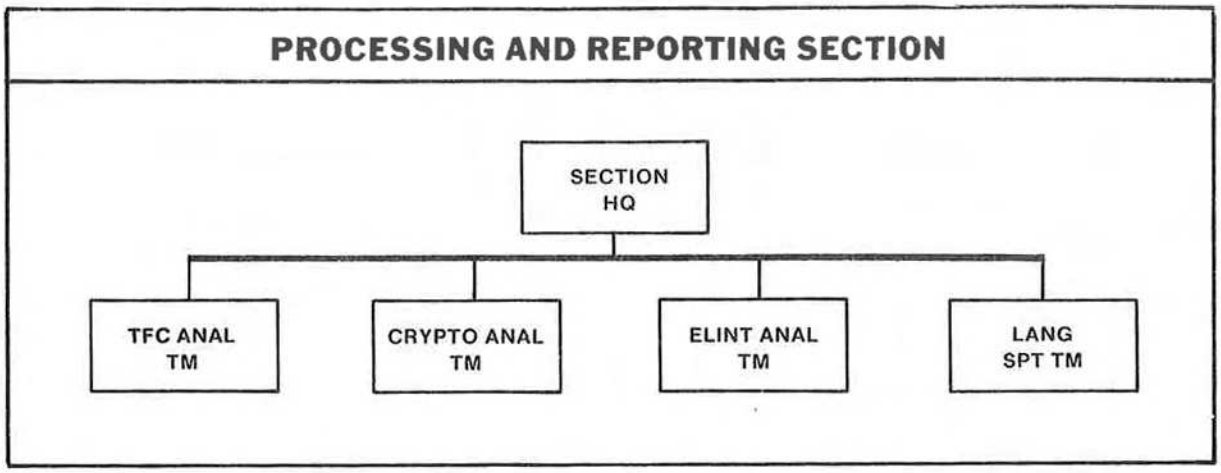
- Identifies specific enemy nets or emitters to be intercepted or jammed using available technical data.
- Identifies the specific assets to accomplish the task, based on capabilities and current status.
- Assembles the necessary technical control data.
- Formats and transmits asset tasking messages.

In meeting mission tasking requirements, it reviews combat information and intelligence reports to evaluate the effectiveness of current tasking. It improves the coverage of target nets and emitters. These reports are sent to the CTOC for further dissemination and inclusion in all-source intelligence products.

RSRs from assigned and attached assets are recorded, consolidated, and forwarded to the CM&D and EW sections. Technical control data is added to the TCAE data base and disseminated to higher, lower, and adjacent MI units to support their respective data base requirements and SIGINT and EW operations.

The mission control section also ensures that SIGINT and EW systems are mutually supporting and that collection and jamming missions are executed in a coherent manner. The availability of technical control data, to support ECM missions planned by the EW section, is communicated to the EW section via the CM&D section on a continual basis. Targeting data to support the lethal attack of HPT is communicated to the CTOC FSE via the CM&D section according to the field unit SOP.

Processing and Reporting Section. The processing and reporting section processes and analyzes the signal intercept data received from the collection elements. Processing is directed toward developing intelligence to meet corps needs and to add to the technical control data base. Normally, data received has been partially processed by the collection element for intelligence that is to be exploited immediately. When such information is developed during processing, it is passed to the integration and reporting section for immediate dissemination to the CM&D section. The processing and reporting section is organized as shown in the following illustration.



The headquarters, processing and reporting section, directs and coordinates the efforts of its four teams to ensure that all aspects of intercepted traffic are fully exploited. It has primary responsibility for the technical control data base. It--

- Receives material from the collection elements and logs and routes it through the appropriate teams for processing.
- Consolidates and forwards the results of analysis to the SIGINT integration and reporting section for dissemination.
- Establishes and maintains the technical data base.
- Ensures that all technical data recovered through analysis is entered into the data base.
- Maintains the necessary management logs and registers to control the production of intelligence and to facilitate interaction among the four teams.

The traffic analysis team processes intercepted Threat communications to extract intelligence and to add to the technical data base. It constructs the communications portion of the Threat EOB. The team--

- Maintains historical data on communications, including net structures.
- Examines intercepted traffic for exploitable information.
- Develops net diagrams.
- Isolates the work of individual transmitters.

° Correlates DF results to locate transmitters.

° Exploits captured threat Signal Operation Instructions.

The cryptanalysis team exploits operational codes and ciphers to produce intelligence, assists the other teams, and adds to the technical data base. The team--

° Maintains data on known cipher code systems, to include jargon and brevity codes.

° Receives copies of all enciphered traffic.

° Performs cryptologic diagnostic tests to determine code systems in use.

° Assists in deciphering intercepted traffic.

The ELINT analysis team processes noncommunications signal intercept to construct the noncommunications portion of the threat EOB and to add to the technical data base. Primary functions are--

° Maintaining technical and OB information on noncommunications emitters.

° Comparing and correlating intercept recordings with technical and collateral information to identify emitters by type and function.

° Processing DF results.

° Locating and identifying Threat emitters.

The language support team transcribes, translates, and analyzes Threat voice communications from tape recordings made by the collection elements. The team--

° Maintains reference data on Threat language, customs, and local geography.

° Maintains historical data on Threat voice communication net structures.

° Receives recordings of selected voice traffic, to include any reports issued.

° Translates traffic deciphered by the cryptanalysis team.

SIGINT Integration Section. The SIGINT integration section produces detailed intelligence and technical reports to meet the SIGINT needs of the corps. Information from all SIGINT sources is combined, correlated, and analyzed to develop a complete picture of all enemy signal activity within the corps area. Primarily it receives information from the TCAEs of the divisions, the ACR, and the separate brigade; the processing and analysis section; and the SIGINT collection elements of the brigade. When available, information from adjacent

corps, EAC, and other services is included. It integrates and analyzes all material to detect major changes in Threat signal status, recover additional technical information, and combine fragmented reports of Threat activity.

Its specific functions are--

- Receiving, cataloging, and integrating all tactical reports (TACREPs), SIGINT hard copy, and technical reports pertaining to the corps area.
- Consolidating and correlating DF results to locate emitters and develop Threat force movements or relocations.
- Correlating the SIGINT-derived OB with that produced by the ASPS to associated emitters with identified Threat units.
- Responding to requests for technical support from SIGINT and EW elements of the brigade with data developed through integrated analysis.
- Formatting and releasing TACREPs and other reports produced by the processing and reporting section.
- Analyzing this integrated data and producing the necessary reports.

The TACREP is the primary means of disseminating SIGINT on the battlefield. The TACREP is prepared in two parts, separated by a detach line. The first part of the report includes the technical information on which the report is based. It is marked with the appropriate special intelligence (SI) classification and caveats.

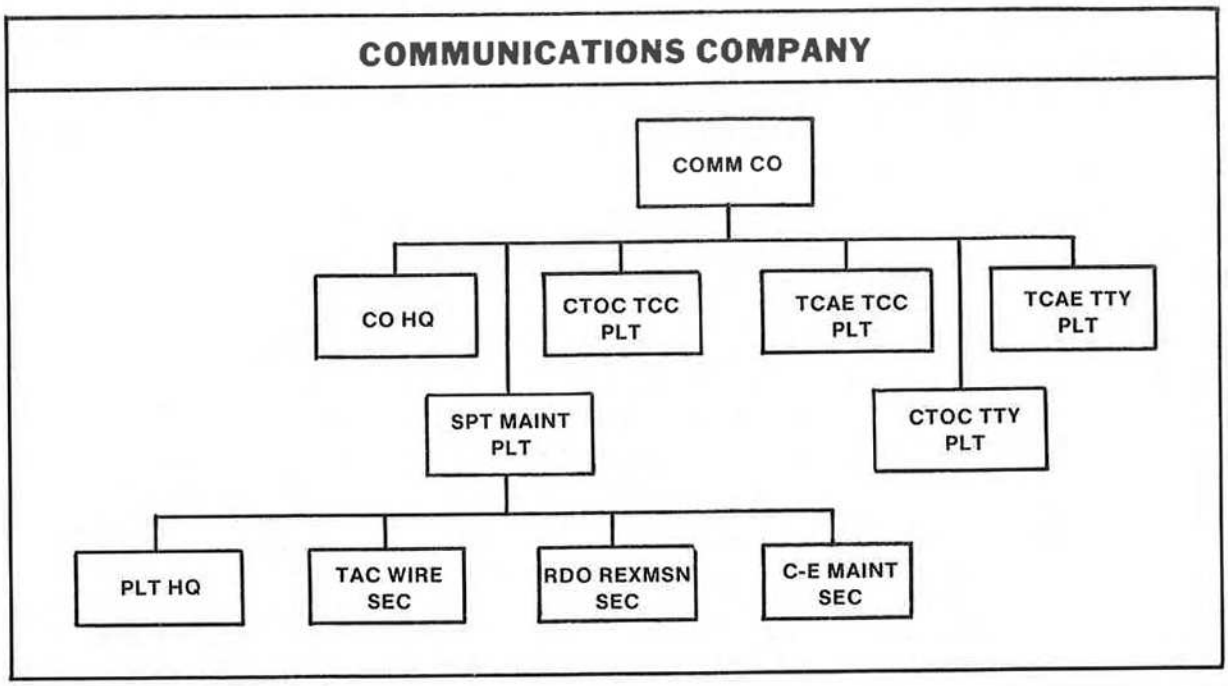
Part two is generally in the spot report format or as directed by the corps G2. It includes the intelligence being conveyed, but it is sanitized to avoid all direct reference to the source. The TACREP recipient can detach this portion of the TACREP generated at the TCAE.

TACREPs are directed toward satisfying the SIGINT needs of the corps. They are sent to the ASPS for inclusion in the all-source intelligence product. Other distribution may include all TCAEs within and adjacent to the corps, commanders and higher echelons, or as directed by tasking.

Tactical ELINT Section. The tactical electronic intelligence (TACELINT) section receives and processes ELINT data from aerial platforms and national systems. It maintains an extensive data base on the corps area.

COMMUNICATIONS COMPANY

The communications company is organized as shown in the following illustration.



The communications company commander ensures that responsive, reliable, and secure communications are provided to the MI brigade. The headquarters oversees the day-to-day operations of company personnel and administrative functions. The company commander also has C^2 of company assets. The company headquarters coordinates with the corps SSO, MI brigade, and MI battalion C-E staff officers to ensure mutual support and minimum signal or security problems. It is usually located in the vicinity of the battalion CP.

SUPPORT AND MAINTENANCE PLATOON

The support and maintenance platoon has a platoon headquarters, a C-E maintenance section, a tactical wire section, and a radio retransmission section. It--

- Provides C-E and communications security (COMSEC) maintenance support for the battalion and the brigade headquarters, headquarters detachment.

° Provides tactical wire communications support for the brigade CP and the IEW sections of the CTOC.

° Operates radio retransmission stations for critical brigade FM nets.

A COMSEC custodian is assigned to assist in the management of cryptographic material issue, storage, and accountability. The platoon, less the tactical wire section and two radio retransmission teams, will be located in the vicinity of the battalion CP. The tactical wire section will be located in the vicinity of the battalion TOC.

CTOC TCC PLATOON

Under the supervision of the platoon leader and platoon sergeant, the CTOC telecommunications center (TCC) provides four AN/TSC-58 communications systems and one AN/GSQ-80. These provide communications with the MI brigade, divisions, ACR, and heavy separate brigade.

CTOC TELETYPEWRITER PLATOON

Under the supervision of the platoon leader and platoon sergeant, the CTOC teletypewriter platoon provides 12 AN/GRC-122 radio teletypewriter (RATT) systems. Four systems are centrally located for CTOC support and termination of the eight deployed AN/GRC-122s. The eight deployed elements support each of the four divisions, one ACR, one heavy separate brigade, the MI battalion (TE), and the MI battalion (AE). The platoon, less eight deployed AN/GRC-122s, will be deployed in the vicinity of the CTOC TCC platoon.

TCAE TELETYPEWRITER PLATOON

Under the supervision of the platoon leader and platoon sergeant, the TCAE teletypewriter platoon provides 14 AN/GRC-122 RATT systems. Six are centrally located for TCAE support and termination of the eight deployed AN/GRC-122s. The eight deployed elements support each of the four divisions, one ACR, one heavy separate brigade, MI battalion (TE), and MI battalion (AE). The platoon, less five deployed AN/GRC-122s, will be located in the vicinity of the TCAE TCC platoon.

TCAE TCC PLATOON

Under the supervision of the platoon leader and platoon sergeant, the TCAE TCC platoon operates two AN/TSC-58 and one AN/MSC-32 communications systems. One AN/GSQ-80 message center is provided for centralized control of all traffic to division and corps TCAE elements. All operators must be SI cleared.

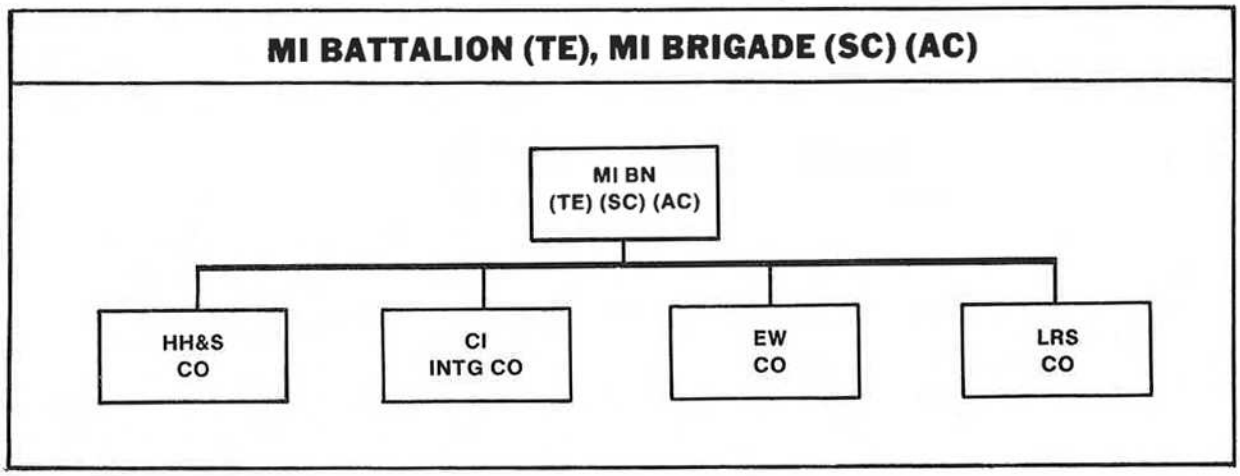
CHAPTER 7

MI BATTALION (TACTICAL EXPLOITATION)

The MI battalion (TE) provides C-E, IPW and ground-based EW support to corps operations. The MI brigade has the MI battalion (TE) (AC) and the MI battalion (TE) (RC). Both have the same mission, to support the corps IEW misssion. The structure of the AC and RC differs but the mission remains the same.

ACTIVE COMPONENT

The MI battalion (TE) standard corps (SC) (AC) is organized with an HH&S company, a CI interrogation company, an EW company, and an LRSC (shown in the following illustration). The MI battalion (TE) (AC) of the MI brigade organic to SC provides corps and its subordinate units with CI, IPW, ground-based SIGINT collection, long-range surveillance, and EW or communications jamming (COMJAM).



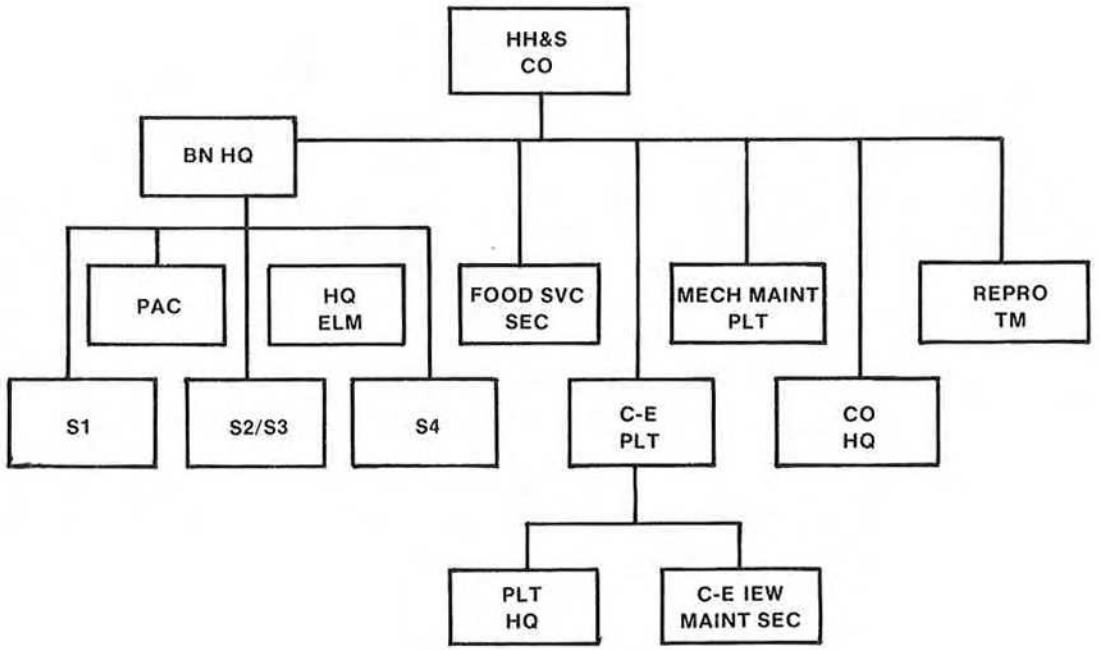
HEADQUARTERS, HEADQUARTERS AND SERVICE COMPANY

The HH&S company is organized as shown in the following illustration.

The HH&S company commander commands and controls battalion operations and assigned and attached elements. The HH&S company is normally located near the MI brigade headquarters and provides consolidated logistic support for the battalion. The battalion headquarters consists of the battalion commander and the supporting staff sections. The HH&S company commander--

- Ensures that food service and maintenance elements deploy as directed and provide the support required by the MI battalion (TE).
- Coordinates with the battalion executive officer to select battalion CP sites.
- Plans and directs the setup of the MI battalion (TE) CP at the new site.
- Coordinates and supervises local security efforts at the headquarters CP.

HH&S COMPANY, MI BN (TE), MI BRIGADE (STANDARD OR LIGHT CORPS) (AC)



Food Service Section

The food service section is staffed to operate two field dining facilities--one at the battalion CP and one at the CI interrogation company.

C-E Platoon

The C-E platoon headquarters provides personnel and equipment to operate the battalion TCC. It provides consolidated C-E maintenance support and limited reproduction facilities. It is organized with a C-E maintenance section, TCC section, and a reproduction team.

The C-E IEW maintenance section performs organizational maintenance on all MI battalion (TE) organic and attached equipment. C-E IEW maintenance personnel may be attached to MI maintenance facilities supporting units.

The TCC section provides personnel and equipment to staff and operate the battalion TCC. A COMSEC custodian is assigned to the battalion and assists in the management of cryptographic material issue, storage, and accountability. The TCC section establishes battalion wire communications.

The reproduction team provides film processing facilities to support the LRSC and the CI interrogation company hand-held photography requirements.

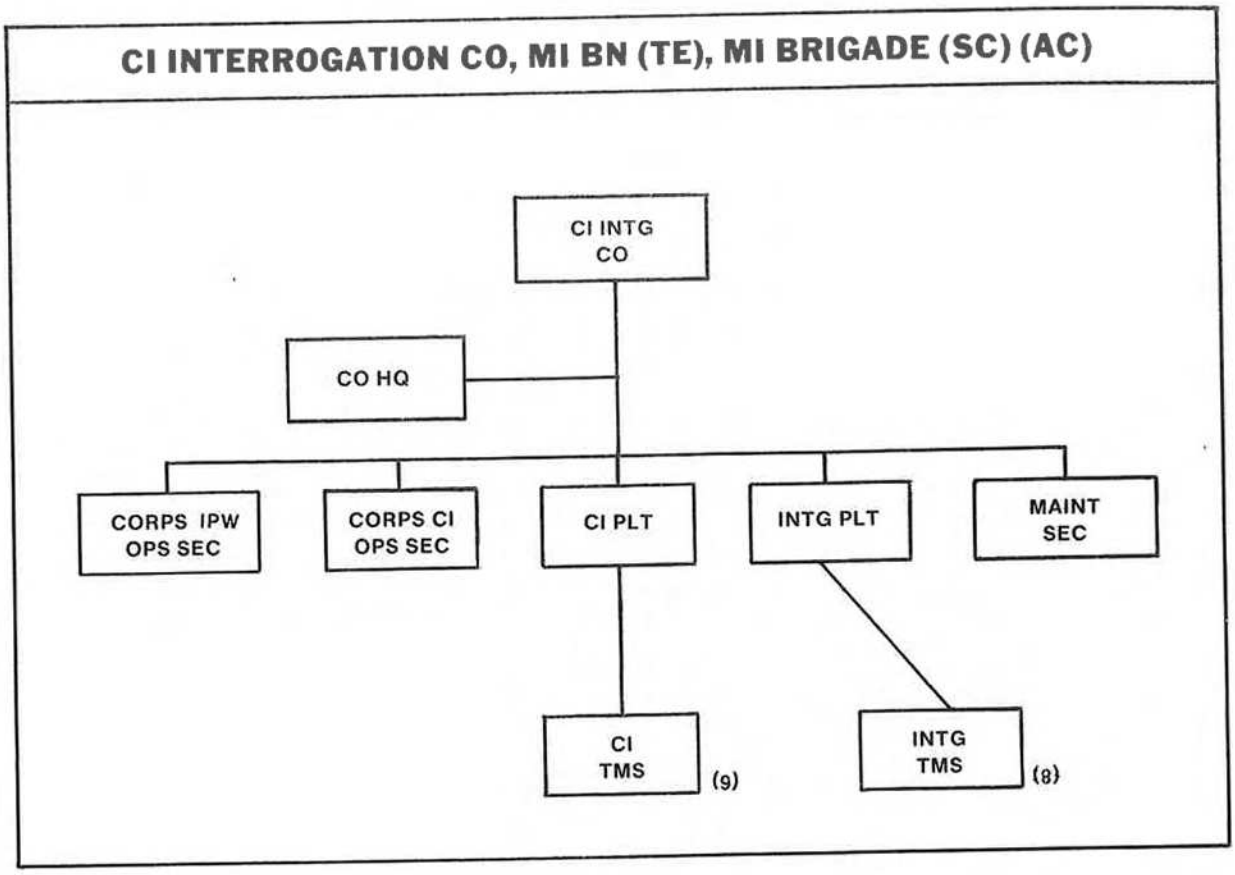
Mechanical Maintenance Platoon

The mechanical maintenance platoon provides consolidated unit maintenance and recovery support for battalion equipment, except C-E and COMSEC. Platoon personnel may be attached to forward units to assist in maintaining MI battalion (TE) equipment. The maintenance platoon leader is also the battalion motor officer and reports to the battalion executive officer on matters of vehicle and generator maintenance.

CI INTERROGATION COMPANY

The CI interrogation company provides multidiscipline CI and OPSEC support, interrogation support, and document exploitation.

The CI interrogation company consists of a company headquarters, a corps IPW operations section, a corps CI operations section, a CI platoon, an interrogation platoon, and a maintenance section (see following illustration).



Company Headquarters

The company headquarters has C2 of assigned or attached elements.

Corps IPW Operations Section

In response to taskings from the brigade operations center, the corps IPW operations section provides planning, supervision, and coordination for corps IPW assets.

Corps CI Operations Section

In response to taskings from the brigade operations center, the corps CI operations section provides planning, supervision, and coordination for corps CI assets.

CI Platoon

The CI platoon protects corps activities from the hostile multidisciplined intelligence collection threat, subversion, sabotage, and terrorism. The platoon provides CI support to OPSEC, rear operations, terrorism counteraction and deception. The CI platoon is organized with a platoon headquarters and nine CI teams. These teams are placed in GS, or if the situation warrants DS, of units within the corps AO. The CI platoon provides--

- CI support to OPSEC (described in FMs 34-60 and 34-60A (S/NOFORN)) identifies the hostile threat, recommends OPSEC measures, and monitors the effectiveness of applied OPSEC measures. CI teams conduct OPSEC evaluations to provide accurate and complete information on how effectively units are using OPSEC measures and identifies shortfalls that need correction.

- CI support to rear operations (described in FMs 34-60 and 34-60A (S/NOFORN)). For rear operations responsibilities, see page 7-23.

- CI support to terrorism counteraction (described in FMs 34-60 and 34-60A (S/NOFORN)). For terrorism counteraction responsibilities, see page 7-24.

- Deception (described in FMs 34-60 and 34-60A (S/NOFORN)) includes all actions to mislead the enemy into actions which are counter to their interests.

The interrogation platoon performs tactical IPW and interviews refugees and line crossers. It exploits threat documents and provides limited translation and interpreter support.

The interrogation platoon has a platoon headquarters and eight interrogation teams.

IPWs and exploitation of captured enemy documents (CEDs) are excellent sources of information. They provide the commander information on future intentions and plans of the enemy threat. They reveal enemy morale, troop strength, medical status, logistics, and other information that can only be obtained from the threat itself.

Corps IPW assets may be employed in GS of the corps, in a reinforcing role to corps units, or in a combination of the two.

When employed in a GS role, IPW assets are normally located at the corps EPW compound or located forward at division EPW holding areas. They collect against corps intelligence requirements tasked by the corps CM&D sections. Transportation requirements are handled by tasking the division transportation officer or the COSCOM assistant chief of staff, transportation, to provide support.

When employed in a reinforcing role, corps IPW assets are placed under the direct supervision of the supported unit's organic MI organization. They are located at the division EPW holding areas or the forward EPW collection points in the brigade trains areas. They are tasked to collect on the intelligence requirements of the supported unit by the supported unit's CM&D section or S2. Direct IPW support from corps to subordinate units is not certain nor can it be considered permanent. Corps IPW assets are distributed, according to the situation, to support the corps commander's concept of operations. They may have to be redistributed as the situation changes.

IPW assets are assigned standard tactical missions. They screen and interrogate EPWs or detainees and exploit CEDs. Document exploitation can presently be performed in the MI battalion (TE) (RC). Through these functions, they attempt to satisfy the requirements levied on them.

EPWs or detainees are screened to select those to be interrogated and to determine the order in which they will be interrogated. The screener assigns a two-character code to each EPW he screens. This code indicates the willingness of the EPW or detainee to answer questions pertinent to the requirements of the supported command and the amount of pertinent knowledge the EPW or detainee possesses.

Interrogations of EPWs or detainees produce reports that answer the requirements of the supported command. Following interrogation, each EPW or detainee interrogated is assigned to a category according to his intelligence value. This assists interrogation operations at higher levels. These categories are not the same as those used in screening, and they may be changed at higher echelons.

The degree to which CEDs are exploited depends on the time and personnel available. Each echelon exploits CEDs for information that answers its requirements, but they may not delay the evacuation of the documents. Exploiting CEDs involves accounting, screening, and categorizing them according to their intelligence value; extracting and reporting information contained in them; and forwarding them through evacuation channels to higher echelons.

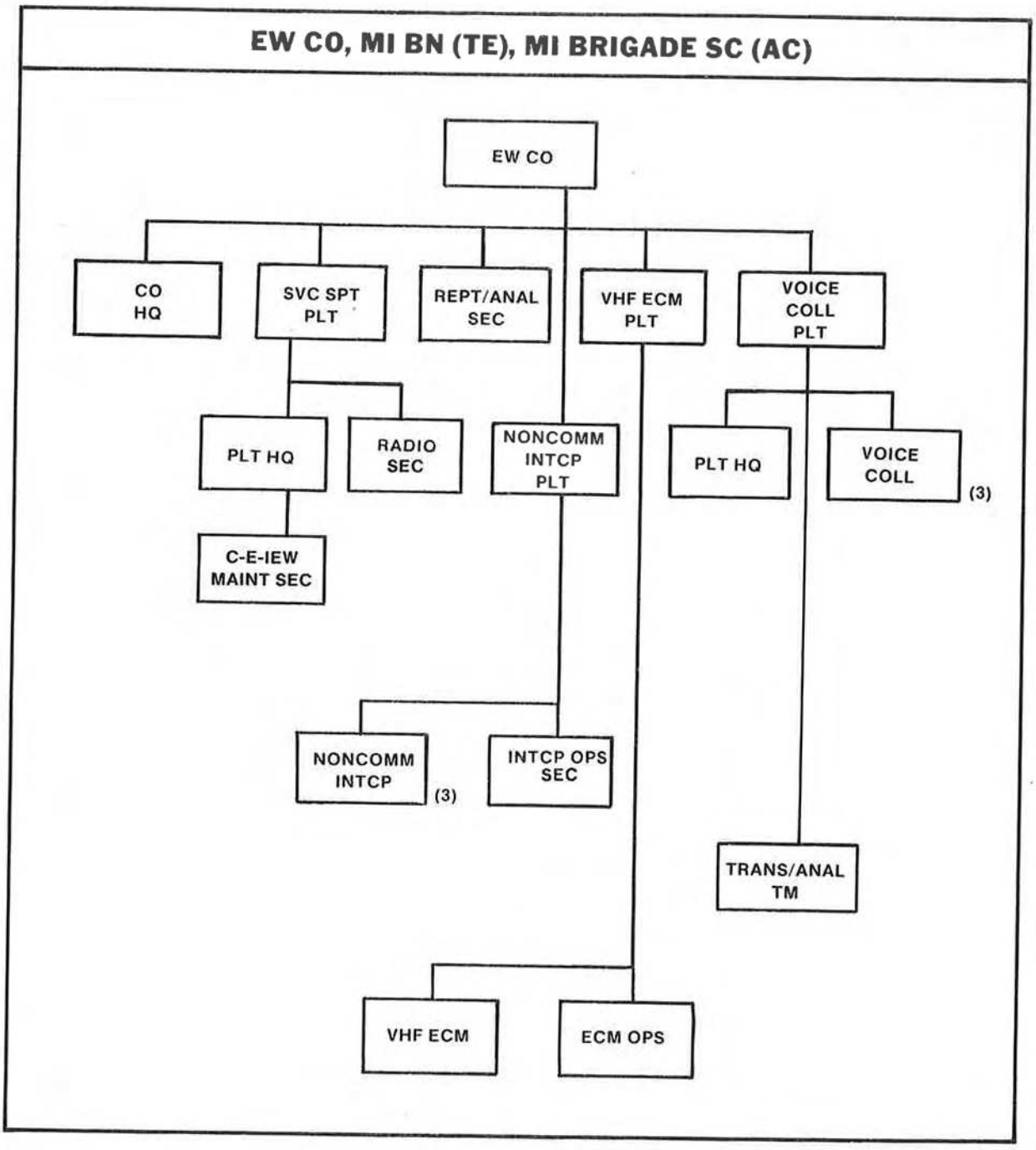
Interrogators must know about the current tactical and strategic situation, the commander's plans, the threat, and the intelligence requirements of the command. They must be allowed access to files and reports which will provide this information. They must also be provided access to EPWs, detainees, and CEDs.

Maintenance Section

The maintenance section provides organization maintenance on all organic vehicles, power generators, and tactical communications equipment.

ELECTRONIC WARFARE COMPANY

The EW company has a company headquarters, a service support platoon, a reports and analysis section, a noncommunications intercept platoon, a very high frequency (VHF) ECM platoon, and a voice collection platoon. (See the following illustration.)



Company Headquarters

The company headquarters has C^2 of company elements, internal supply, and support services. The unit depends on the HH&S company for food service support. The appropriate corps units provide medical, financial, legal, and personnel administrative services and MP support.

The EW company commander is responsible for operations conducted by each element assigned or attached to his command. He also--

- Ensures that actions prescribed in the EW and intelligence annexes to the corps operations plan are carried out.
- Ensures that taskings received from the TCAE at the MI brigade operations center are completed.
- Oversees deployment of company assets to sites that minimize the possibility of detection by enemy forces and where the mission can best be accomplished.
- Inspects deployed elements to ensure effective operations and that adequate support is provided, either from the supported units or from the brigade operations center.

Service Support Platoon

Service Support Platoon Headquarters. The service support platoon headquarters has C^2 of the C-E IEW maintenance section and the radio section.

CE-IEW Maintenance Section. The CE-IEW maintenance section provides organizational maintenance for both tracked and wheeled vehicles and repair service for power generator equipment, teletypewriters, and IEW tactical systems.

Radio Section. The radio section, under the service support platoon, provides RATT equipment and operators to support the EW company.

Reports and Analysis Section

The reports and analysis section receives tasking from the TCAE of the brigade operations center. It maintains a technical data base and routes the mission requirements to the appropriate operational team. It receives data from the collection positions and analyzes it for combat information and reportable items. It then forwards the analysis, together with any operator's comments, work sheets, and tapes, to the TCAE for further processing.

Noncommunications Intercept Platoon

The noncommunications intercept platoon headquarters supervises platoon operations. The platoon leader--

- Ensures effective task execution.
- Redeploys personnel and equipment as directed by specific tasking or when deployment is necessary for successful mission execution.
- Ensures that personnel are adequately trained, equipped, and supported to complete the tactical mission.

Noncommunications Intercept Operations Section. The noncommunications intercept operations section is organic to the noncommunications intercept platoon headquarters. It coordinates and monitors the noncommunications intercept teams' operations. The noncommunications intercept teams intercept noncommunications emissions, report information, and provide lines of bearing on enemy noncommunications systems.

VHF ECM Platoon

The VHF ECM platoon headquarters has C^2 of the ECM operations section and the three VHF ECM teams. The platoon leader--

- Ensures prompt execution of the operational mission.
- Redeploys personnel and equipment in response to mission tasking.
- Ensures that personnel are adequately trained, equipped, and supported to complete the tactical mission.

The ECM operations section, organic to the VHF ECM platoon headquarters, coordinates and monitors the VHF ECM team operations.

The VHF ECM teams jam threat radio communication systems in the VHF frequency spectrum. When tasked, they conduct electronic deception operations.

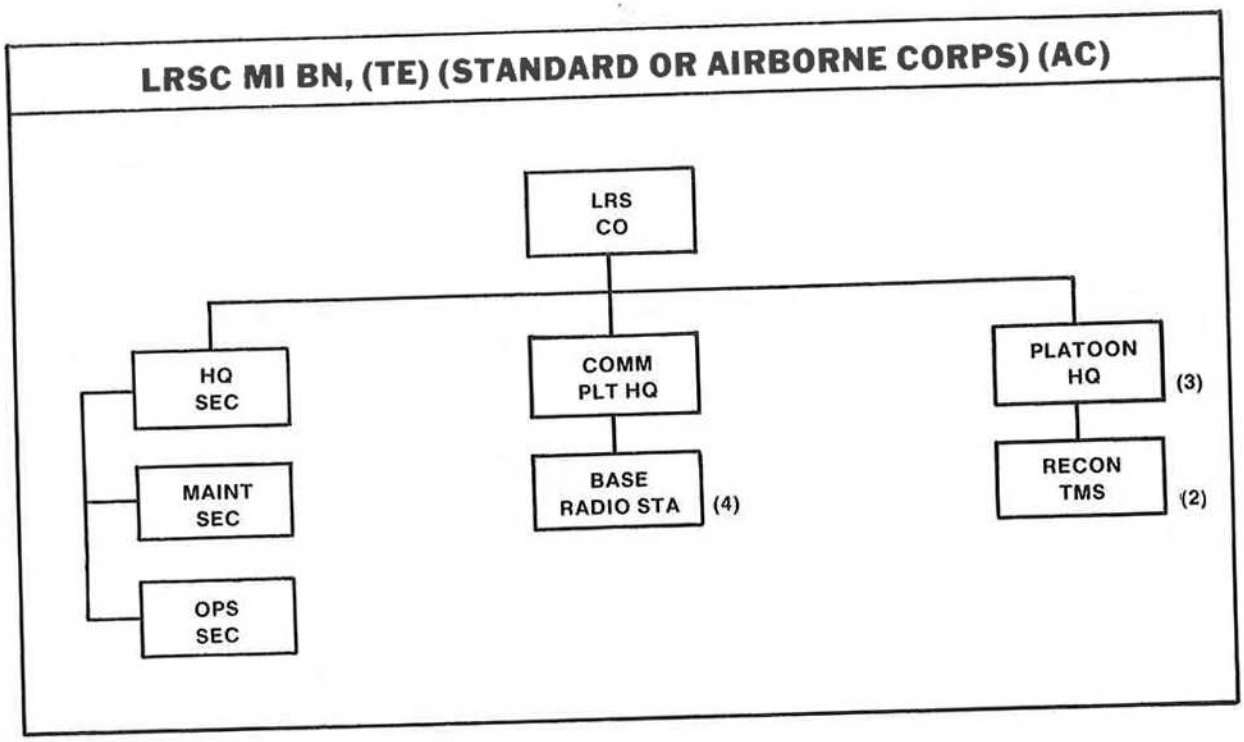
Voice Collection Platoon

The voice collection platoon is organic to the EW company. Its three-manned high frequency (HF) and VHF voice collection positions and three unmanned positions provide ground-based voice communication intercept, analysis, and reporting for the corps, assigned divisions, and separate brigades.

LONG-RANGE SURVEILLANCE COMPANY

The LRSC has a headquarters section, a maintenance section, an operations section, a communications platoon headquarters, and three platoon headquarters (see the following illustration).

The LRSC conducts long-range R&S as a behind the threat lines component of a long-range surveillance system; conducts stay behind operations; provides information on threat activities, terrain, and weather conditions; and employs sensors, photographic equipment, night-vision, and nonorganic devices as required.



The LRSC receives its mission tasking directly from the CM&D section of the CTOC support element. The G2 passes his surveillance requirements to the CM&D section of the CTOC support element. The CM&D selects those requirements best fulfilled by the LRSC and passes them as a mission tasking to the LRSC commander. The CM&D sections ensures that the tasked mission is long-range surveillance-capable, supports the collection plan, and complements all other collection efforts. These missions are formulated with the G3 and are coordinated with EAC to ensure that corps long-range surveillance operations are planned with full knowledge of EAC reconnaissance and strike capabilities which may be brought to bear in the corps area.

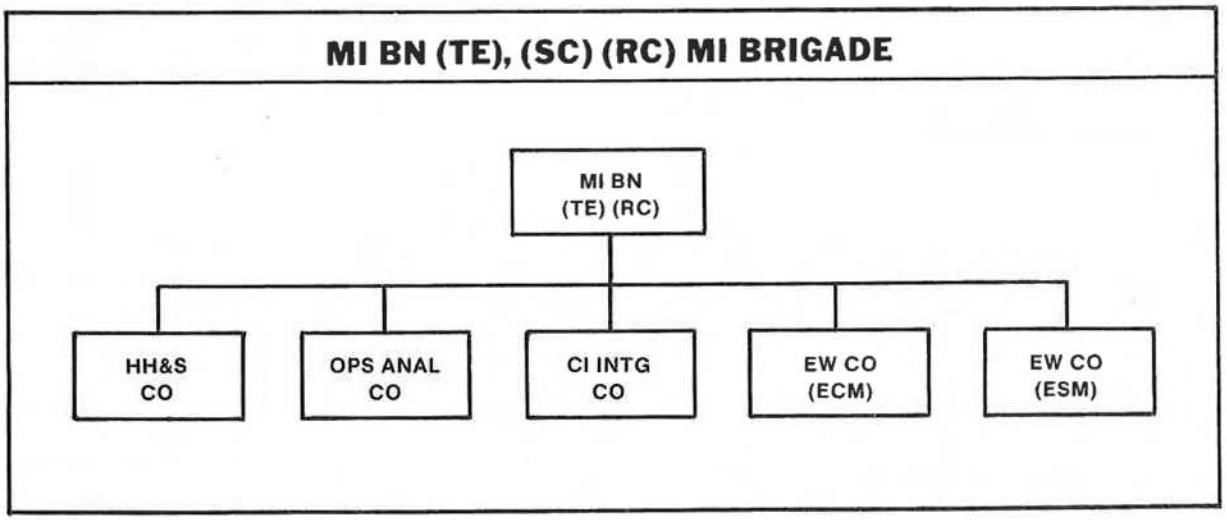
The LRSC TOC will normally locate at, or in close proximity to, the MI brigade S3. The requirements of the LRSC TOC for security, communications, logistic support, and isolation areas will determine the exact siting. This will be from 1 to 5 kilometers from the MI brigade. If necessary, the LRSC may deploy liaison officers or NCOs to the corps main headquarters or the deployment airfield.

LRSC communications with deployed surveillance teams will be accomplished using organic radio base stations. The link between the LRSC and the corps CM&D is the most secure and lowest profile link available. In most cases, this will be through normal use of the corps area communications system, to which the LRSC will be another subscriber. In exceptional cases, a direct point-to-point wire link may be used. If no other communications link is available, the LRSC will use couriers or secure FM radio.

Surveillance teams transmit to the LRSC, which passes information to the LRSC operations section. The operations section passes intelligence reports to the corps CM&D section. The frequency with which teams report will be determined by mission requirements and the threat environment. Every transmission from the surveillance teams creates a vulnerability, so the volume and timeliness of reporting must be balanced against the importance of the report and the dangers of immediate transmission. Items of the highest priority always are transmitted as soon as possible, but items of lesser importance are reported according to a transmission schedule controlled by the LRSC operations section.

RESERVE COMPONENT

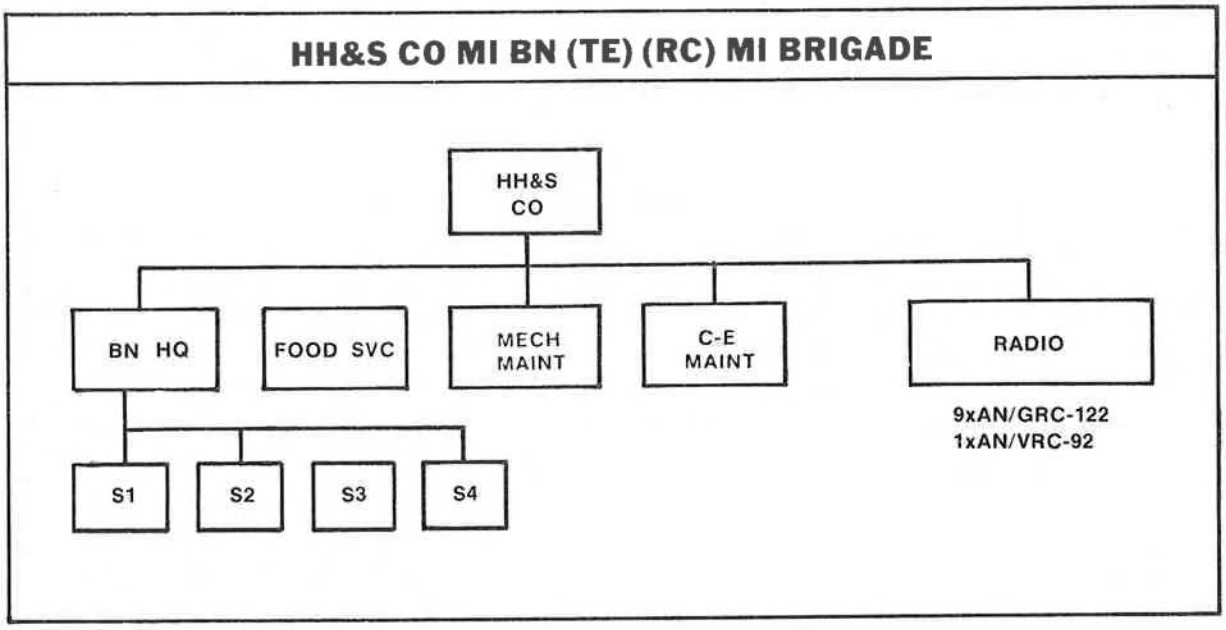
The MI battalion (TE) (RC) of the corps is organized to provide additional CI and document exploitation support (see the following illustration).



The MI battalion (TE) (RC) contains an HH&S company; an operations analysis company; a CI interrogation company; an EW company (ECM); and an EW company (ESM).

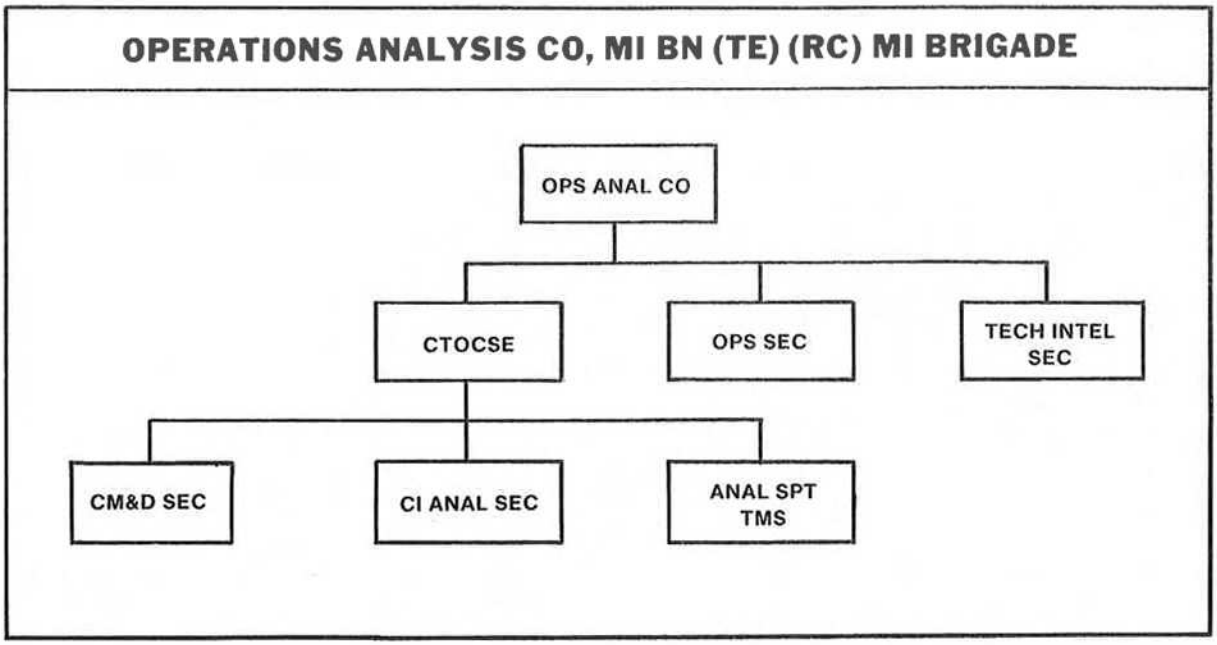
HEADQUARTERS, HEADQUARTERS AND SERVICE COMPANY

The HH&S company provides C2, consolidated communications, and maintenance and food service support to the battalion.



OPERATIONS ANALYSIS COMPANY

The operations analysis company consists of a company headquarters, a CTOC support element, an operations section, and a technical intelligence section. It provides personnel to augment the CTOC and the corps TCAE to handle the additional workload. (See the following illustration.)



CTOC Support Element

The CTOC support element provides personnel to the CM&D section and the CI analysis section of the active component CTOC.

Operations Section

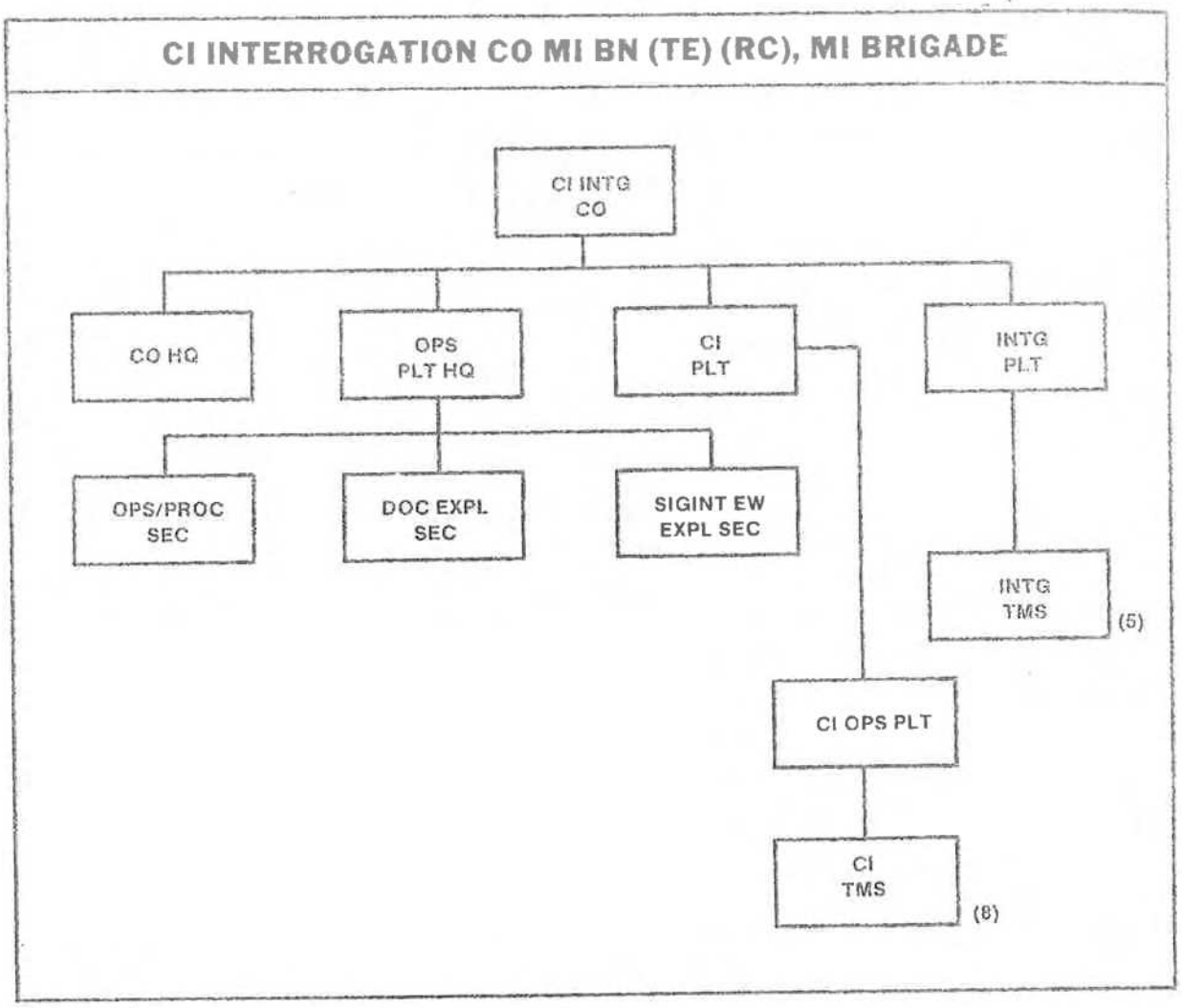
The operations section provides personnel to augment the division TCAE when EW assets are sent to that division.

Technical Intelligence Section

The technical intelligence section analyzes foreign material, supplies, and technical documents acquired as a by-product of battle. Included in this section is a packing and crating element. The purpose of technical intelligence is to prevent the enemy from having or maintaining technological superiority. They normally deploy in the COSCOM area to facilitate the evacuation of equipment but may locate near the EPW holding area. Want lists are received, and gathered information is reported to the CTOC CM&D section.

CI INTERROGATION COMPANY

The CI interrogation company is organized as shown in the following illustration. The company provides the same support as the CI interrogation company of the MI battalion (TE) (AC), with the addition of the operations platoon.



Operations Platoon Headquarters

The operations platoon headquarters maintains the data base; provides the administrative support for the interrogation effort at the corps EPW holding area; and provides the planning, supervision, and coordination of EPW interrogation and document exploitation. The platoon leader--

- Performs intelligence coordination and liaison duties.
- Supervises translation and interpretation activities.
- Establishes and maintains a functional filing system.
- Determines procedures for reporting information to supported units.

Operations and Processing Section. The operations and processing section supports the document exploitation and interrogation activities of the company. It establishes and maintains a data base for use in analyzing and processing information. It reviews the corps collection requirements and ensures that those requirements are satisfied as quickly and completely as possible.

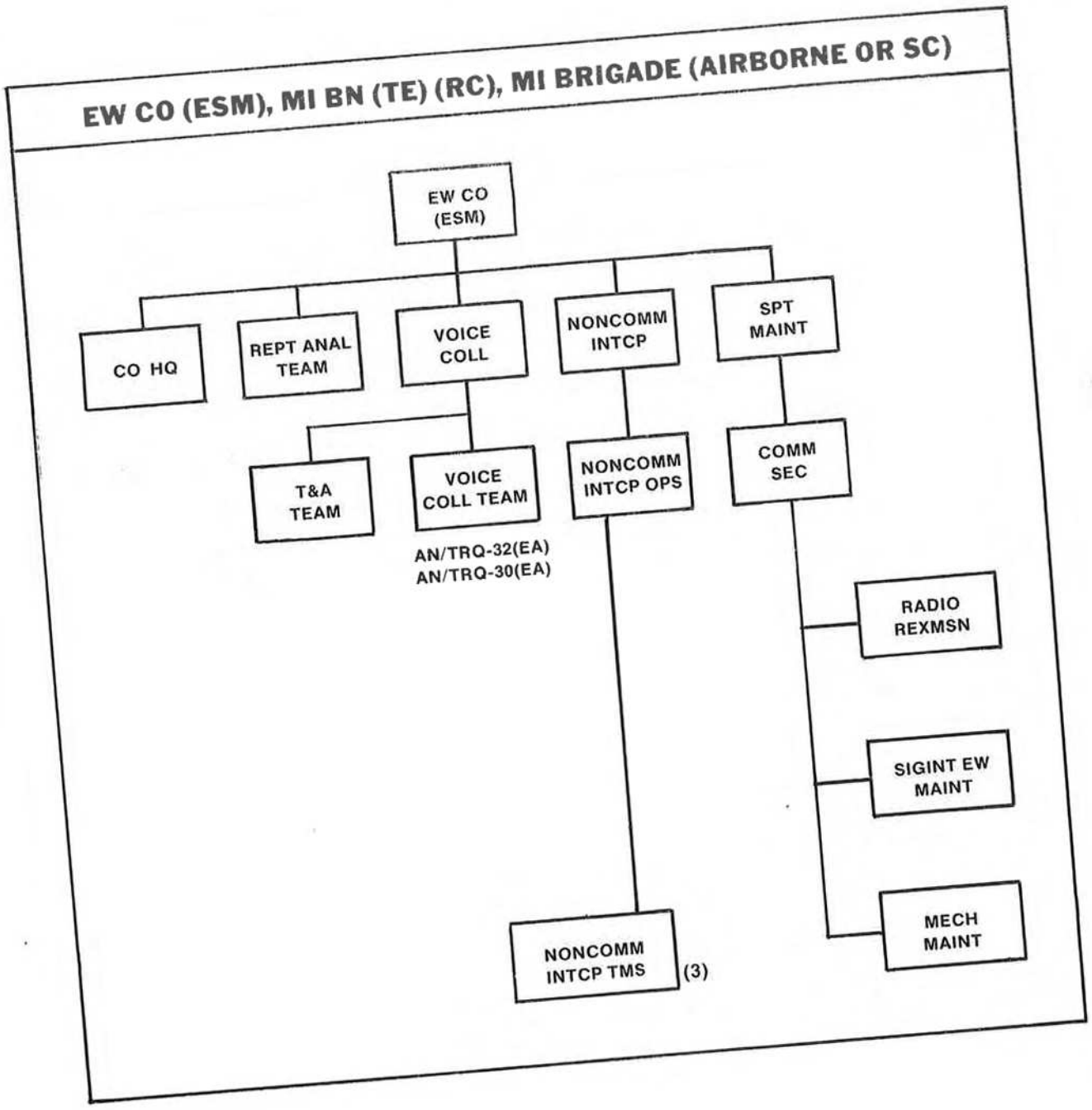
The ASPS of the CTOC support element provides the data base to the operations and processing section for use by interrogation personnel. In the planning and preparation of an interrogation, the interrogator may use this data base or, if additional information is needed, request it from the ASPS in the CTOC. It is also responsible for preparing final interrogation reports and, by using extracted information, updating the data base. It sends final interrogation reports to the CM&D section at the CTOC support element.

Document Exploitation Section. The document exploitation section translates and exploits CEDs of intelligence value, to include identification and initial screening of signal, SIGINT, and REC documents. It screens and categorizes all CEDs, translates selected documents, and reports obtained information in a timely manner. When translator personnel are not giving translation support, the platoon leader may detail them to provide interrogation support. This may be done more readily with the inclusion of local national translator personnel.

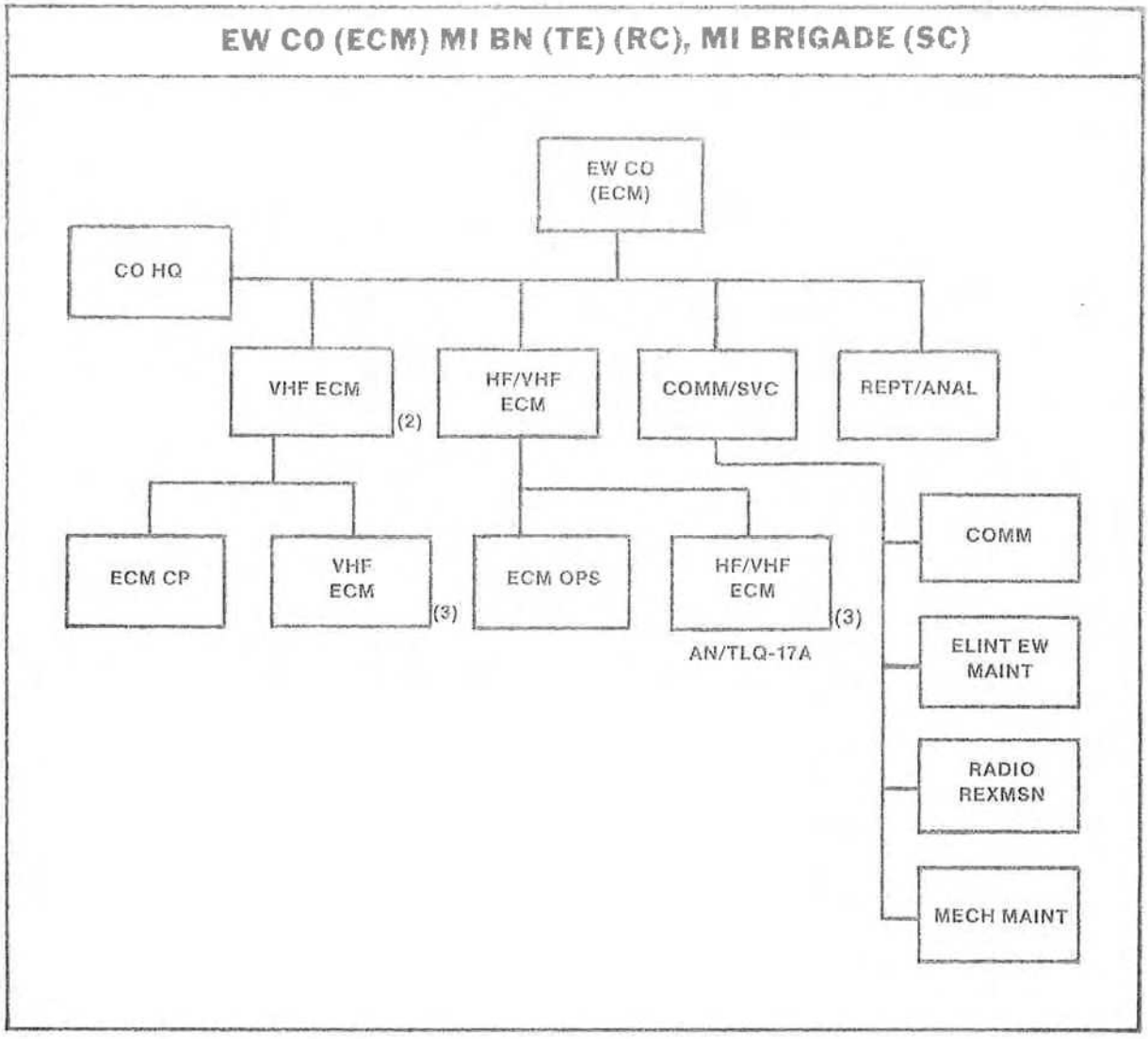
SIGINT EW Exploitation Section. The SIGINT EW exploitation section exploits SIGINT EW documents and equipment and assists interrogation teams to assist in the interrogation of captured REC, SIGINT, or signal personnel. It also provides coordination of evaluation and evacuation of documents and equipment.

ELECTRONIC WARFARE COMPANY

There are two EW companies in the MI battalion (TE) (RC): an EW company (ESM) and an EW company (ECM). (See the following two illustrations.)

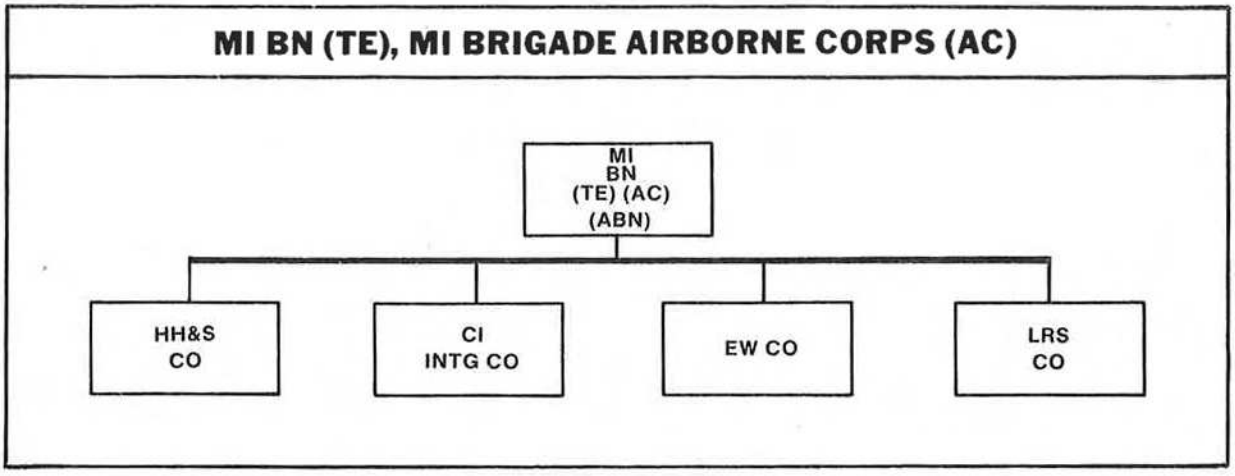

EW CO (ESM), MI BN (TE) (RC), MI BRIGADE (AIRBORNE OR SC)
EW CO (ESM)
CO HQ
REPT ANAL TEAM
VOICE COLL
NONCOMM INTCP
SPT MAINT
T&A TEAM
VOICE COLL TEAM
AN/TRQ-32(EA)
AN/TRQ-30(EA)
NONCOMM INTCP OPS
COMM SEC
RADIO REXMSN
SIGINT EW MAINT
MECH MAINT
NONCOMM INTCP TMS
(3)

EW CO (ECM)
MI BN (TE) (RC), MI BRIGADE (SC)



AIRBORNE CORPS (ACTIVE COMPONENT)

The MI battalion (TE) (airborne corps) (AC) is designed to support an airborne corps and its airborne divisions (see the following illustration). The battalion has increased CI and ECM capabilities.

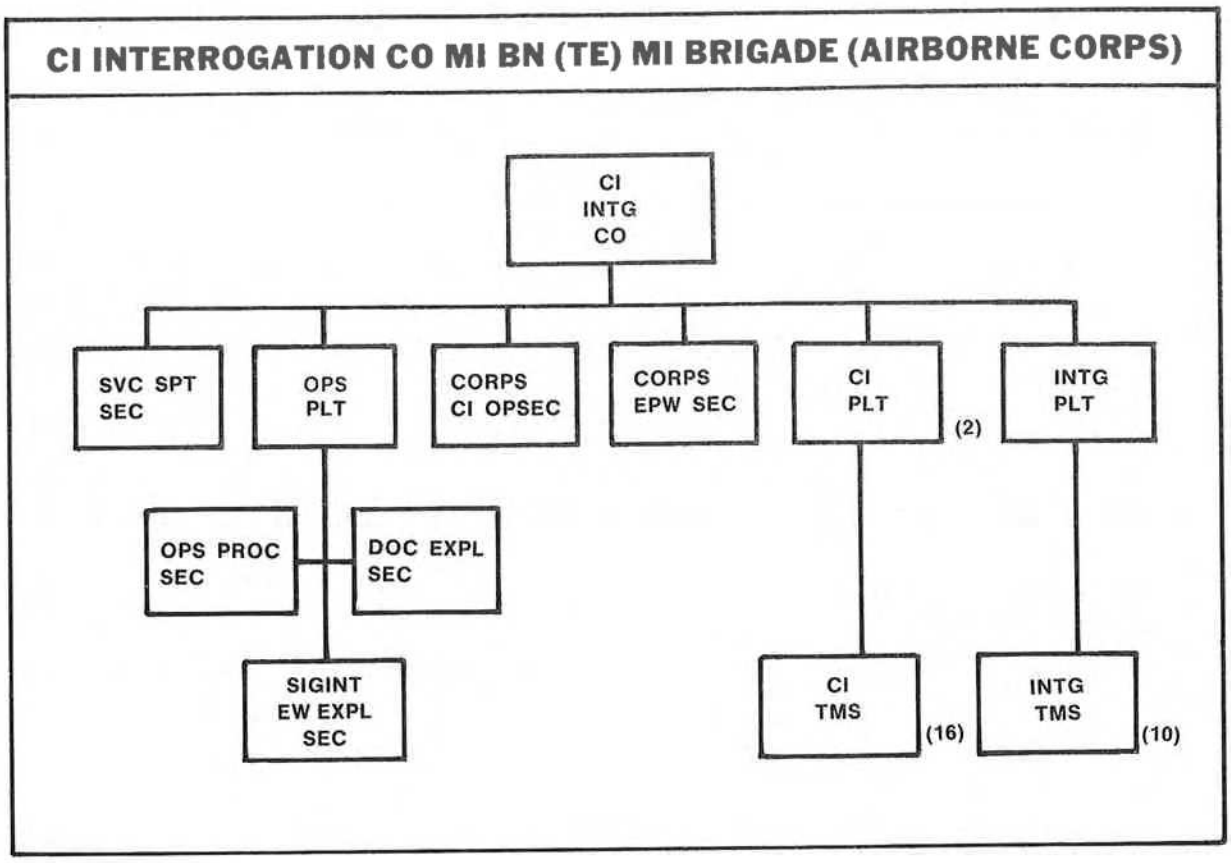


HEADQUARTERS, HEADQUARTERS AND SERVICE COMPANY (AC)

The HH&S company (airborne corps) is the same as the HH&S company, MI battalion (TE) (SC) (AC).

CI INTERROGATION COMPANY

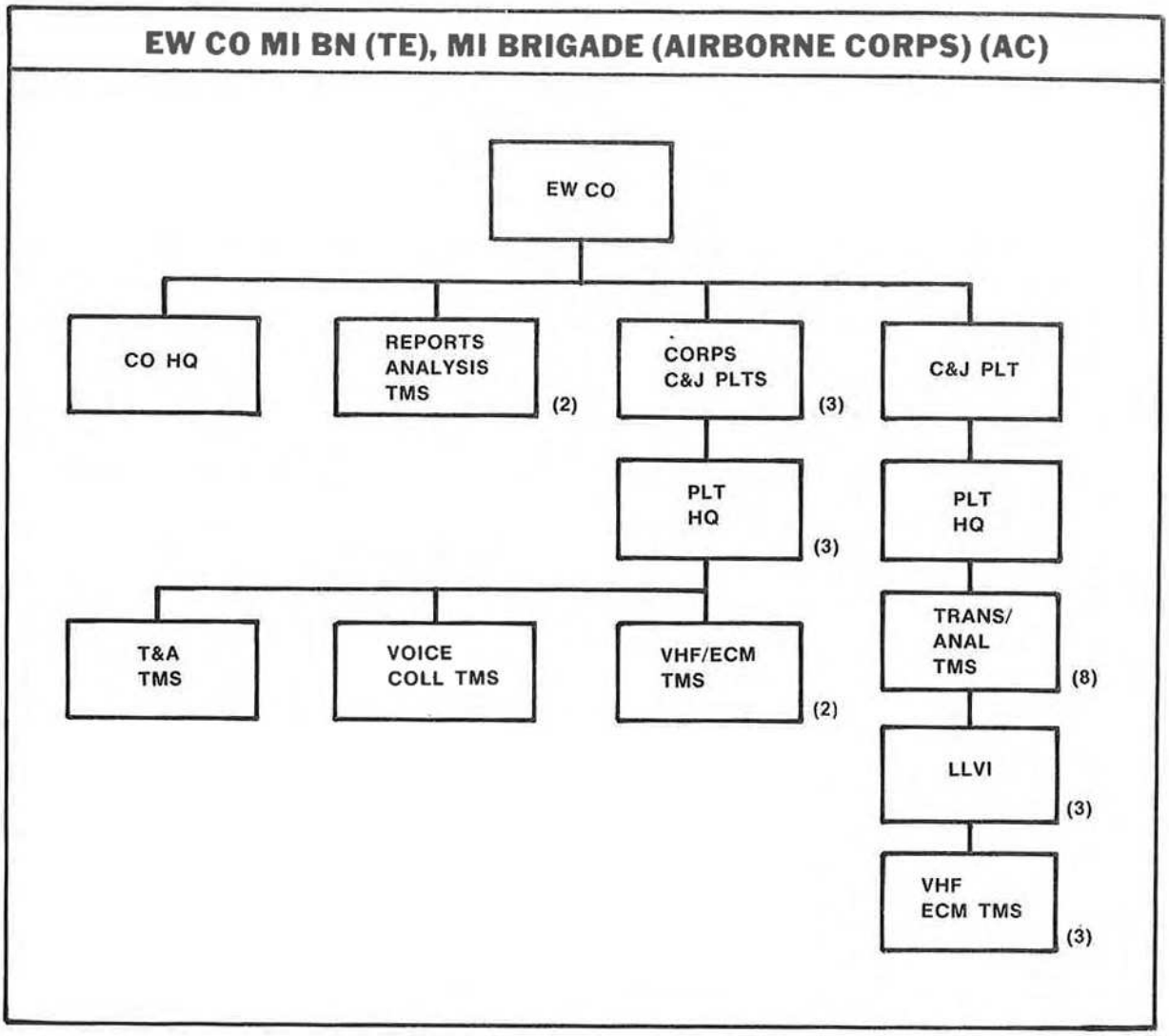
The CI interrogation company provides the same support as the CI interrogation company of the MI battalion (TE) (SC) (AC) with the addition of an operations platoon. (See the following illustration.) The operations platoon was described as part of the MI battalion (TE) (RC) of the standard corps.



ELECTRONIC WARFARE COMPANY

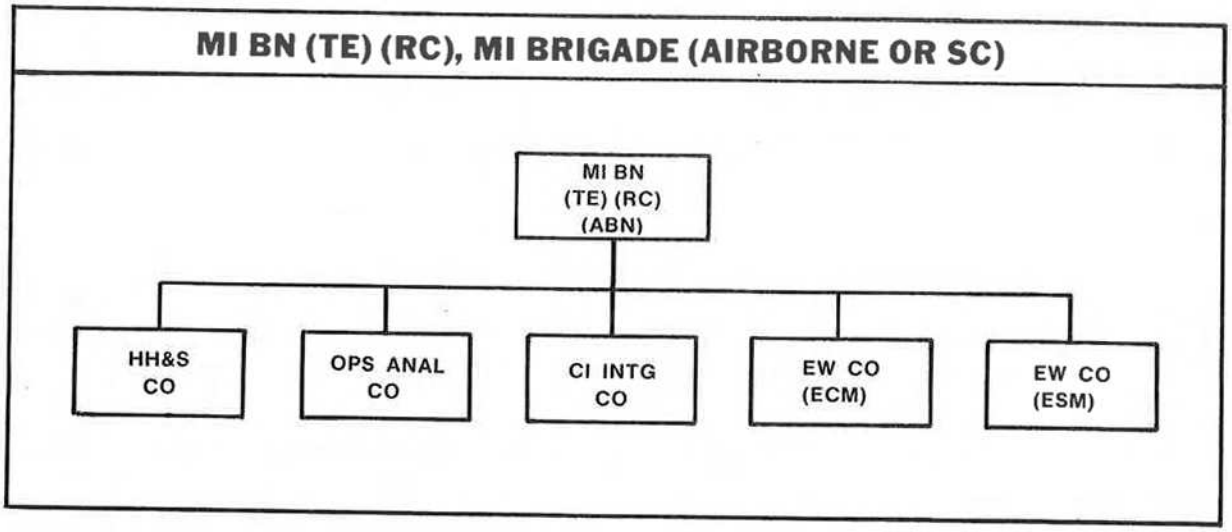
The EW company is organized as shown in the following illustration. The functions of the company are the same as those of the previously described EW companies.

EW CO
MI BN (TE), MI BRIGADE (AIRBORNE CORPS) (AC)



AIRBORNE CORPS (RESERVE COMPONENT)

The MI battalion (TE) (RC) of the airborne corps is organized the same as the MI battalion (TE) (SC) (RC). (See the following illustration.)



HEADQUARTERS, HEADQUARTERS AND SERVICE COMPANY

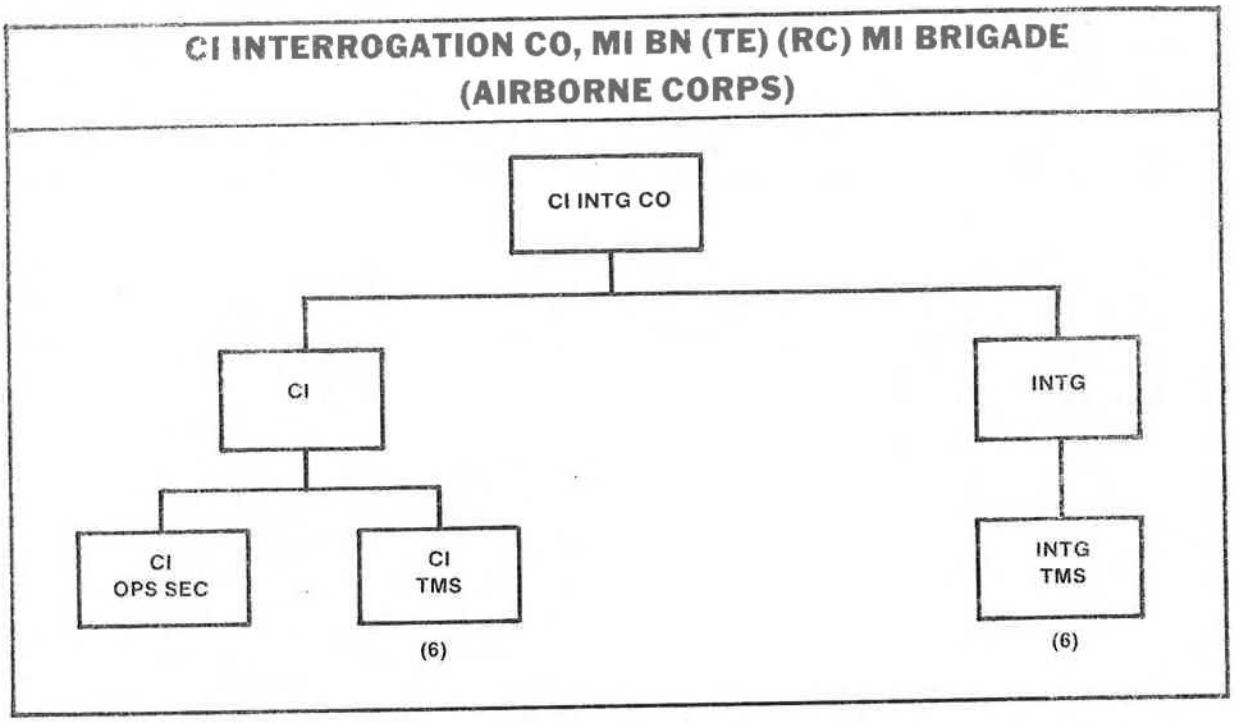
The HH&S company is identical to the MI battalion (TE) of the standard corps RC.

OPERATIONS ANALYSIS COMPANY

The operations-analysis company is identical to MI battalion (TE) of the standard corps RC.

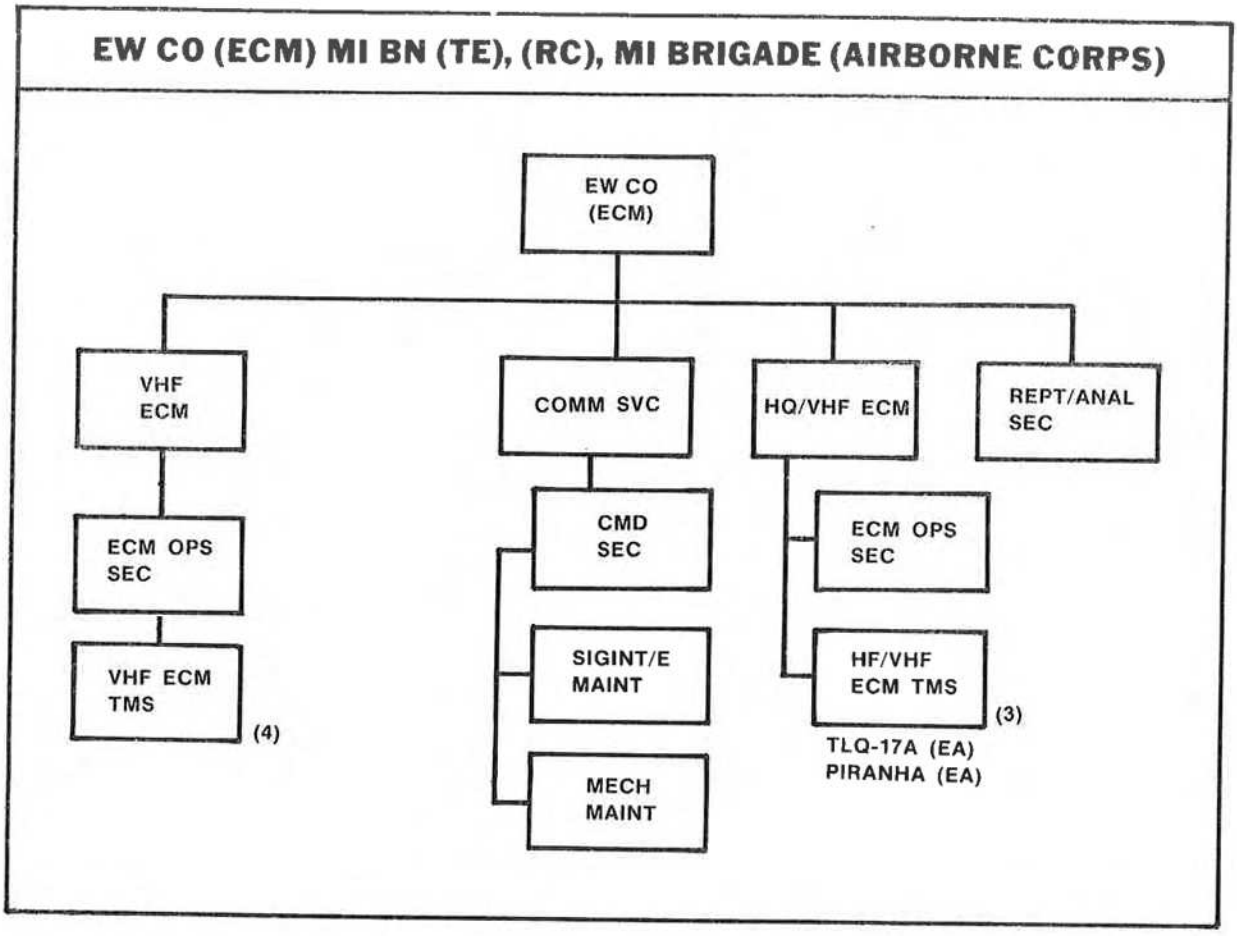
CI INTERROGATION COMPANY

The CI interrogation company (airborne, RC) is organized in a slightly different way: There is no operations platoon. (See the following illustration.)


CI INTERROGATION CO, MI BN (TE) (RC) MI BRIGADE
(AIRBORNE CORPS)
CI INTG CO
CI
INTG
CI
OPS SEC
CI
TMS
(6)
INTG
TMS
(6)

ELECTRONIC WARFARE COMPANY

The EW (ECM) company is organized as shown in the following illustration.



CI SUPPORT TO REAR OPERATIONS

REAR AREA IPB

CI personnel assist in the identification of enemy forces, integration of OPSEC into planning, terrain analysis, and appreciation of the enemy threat.

LIAISON

CI personnel provide liaison with police, civilian and MI agencies, and civil affairs units for the purpose of exchanging information or assistance. Cooperation between agencies is essential in defeating the rear area threat. Liaison is the key to this cooperation. Liaison will prevent duplication of effort, ensure maximum dissemination and use of intelligence, and assist in planning for unified efforts by the agencies involved. Liaison with local civil agencies may provide indications and warning intelligence.

THREAT AWARENESS TRAINING

Threat awareness training is an activity usually connected with peacetime missions. CI personnel provide training and information on the threat, responsibilities and channels for reporting suspicious activity, and security advice and assistance.

DEFENSIVE SOURCE OPERATIONS

Defensive source operations are conducted to provide indications and warning information on potential rear area activity. Defensive sources are individuals who serve as paid or unpaid informants for US intelligence SA personnel. They provide information on personalities and activities gained as a result of their routine daily activity. Examples include the local barber, storekeeper, or maid. Defensive source operations are established around critical areas to provide indications and warning information on potential rear area activity.

INCIDENT INVESTIGATIONS

Incident investigations, like all CI investigations, are directed by the control office or MI brigade headquarters. These investigations can lead to the identification and neutralization of perpetrators of hostile actions. These investigations include SAEDA and espionage investigations.

BLACK, GRAY and WHITE LISTS

Black, gray, and white lists identify personnel of CI interest. CI teams provide data used to compile these lists. Black lists contain the names of persons who are hostile to US interests and whose capture are of prime importance. Gray lists contain names of persons whose inclinations or attitudes toward US interests are uncertain. White lists contain names of persons who are favorably inclined toward US interests and need to be protected from threat targeting.

SCREENING and INTERROGATION

Screening and interrogation of refugees, line crossers, and defectors is a key service. CI personnel identify individuals of CI interest. These individuals may be persons who can provide information. Screening and interrogation may also identify enemy agents or special purpose troops, such as Committee of State Security (KGB) special purpose teams.

CI SUPPORT TO TERRORISM COUNTERACTION

CI personnel develop a data base on the terrorist threat. Information is assembled from open sources, criminal information, intelligence sources, and internal sources. CI personnel get this information through liaison with MPs, military and civilian intelligence, other civilian agencies, and through investigation of terrorist incidents.

VULNERABILITY ASSESSMENT

CI units provide assessment of the vulnerability of friendly units to the terrorist threat. CI personnel conduct vulnerability assessments which identify weaknesses in friendly security.

TERRORIST ACTIVITY PREDICTION

To predict terrorist activities, CI personnel analyze past terrorist activity to identify patterns or trends. These can aid them in predicting terrorist acts and targets.

RECOMMENDATION OF PROTECTIVE MEASURES

CI personnel recommend protective measures. Based on previous responsibilities, CI personnel recommend application of protective measures from terrorist activities.

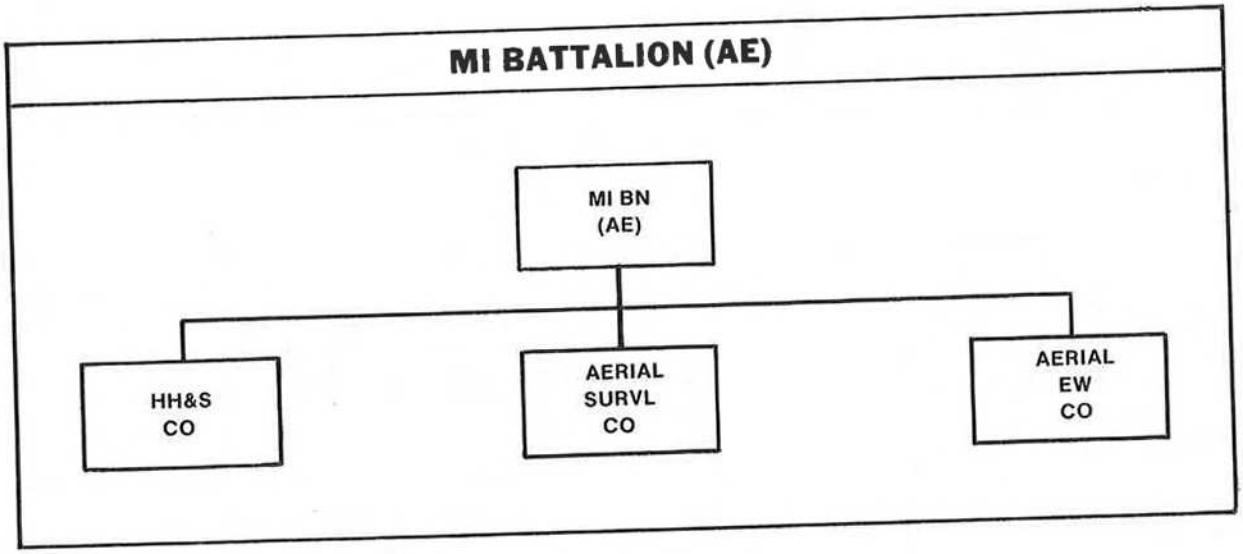
CI teams support deception operations by--

- Analyzing the threat collection capabilities. CI personnel identify the threat collection capabilities and the friendly vulnerability to this collection.
- Recommending methods through which false or misleading information can be channeled to the threat's collectors. CI personnel recommend which elements of information would be exposed to which collectors and the most effective and the least suspicious way of doing this.
- Collecting information used to evaluate the effectiveness of the deception operation.

CHAPTER 8

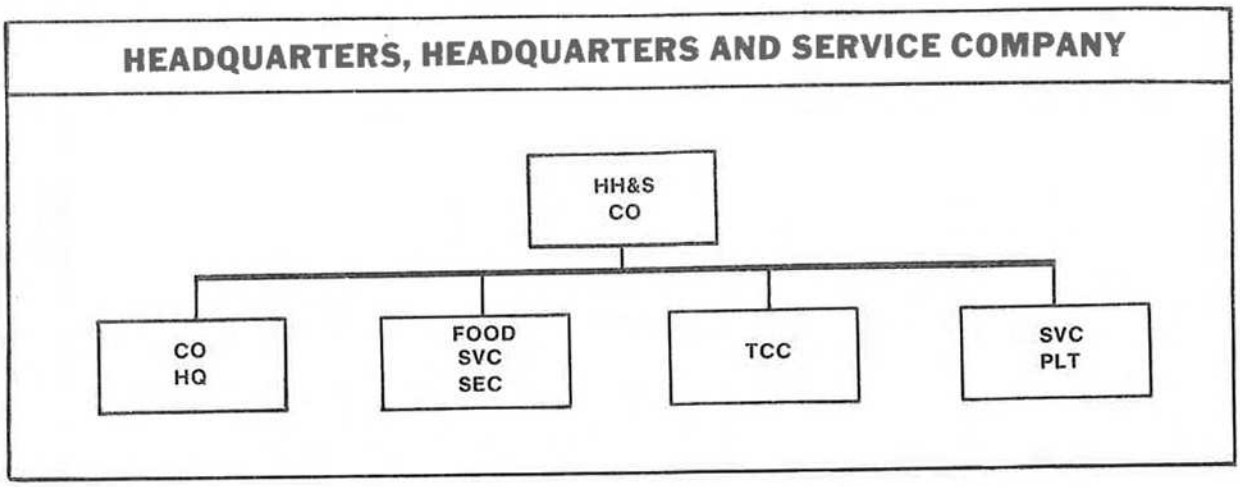
MI BATTALION (AERIAL EXPLOITATION)

The corps commander's mission is to fight the battle as one extended integrated operation. To do so, the commander must see the battlefield in-depth and be aware of what the enemy is doing, where they are, and what they intend to do. The MI battalion (AE) provides the corps commander with his organic "deep look" through aerial reconnaissance, surveillance, SIGINT collection, analysis, and reporting. The MI battalion (AE) is organized as shown below.



HEADQUARTERS, HEADQUARTERS AND SERVICE COMPANY

The HH&S company consists of the company headquarters, food service section, telecommunications center, and service platoon as shown in the following illustration.



The company headquarters provides C2 for elements assigned and attached to the company.

FOOD SERVICE SECTION

The food service section provides consolidated 24-hour food service support to the battalion. It establishes one dining facility at the corps airfield to support all battalion elements.

TELECOMMUNICATIONS CENTER

The TCC operates the battalion TCC, provides wire and switchboard service to the battalion headquarters, and terminates multichannel circuits between the battalion and the MI brigade and corps operations center.

SERVICE PLATOON

The service platoon provides consolidated logistical, aviation, medical, C-E maintenance, and mechanical maintenance support to the battalion.

The platoon headquarters supervises the operation of platoon elements and provides them with material control and accounting support.

The C-E maintenance section provides organizational maintenance of battalion communications equipment.

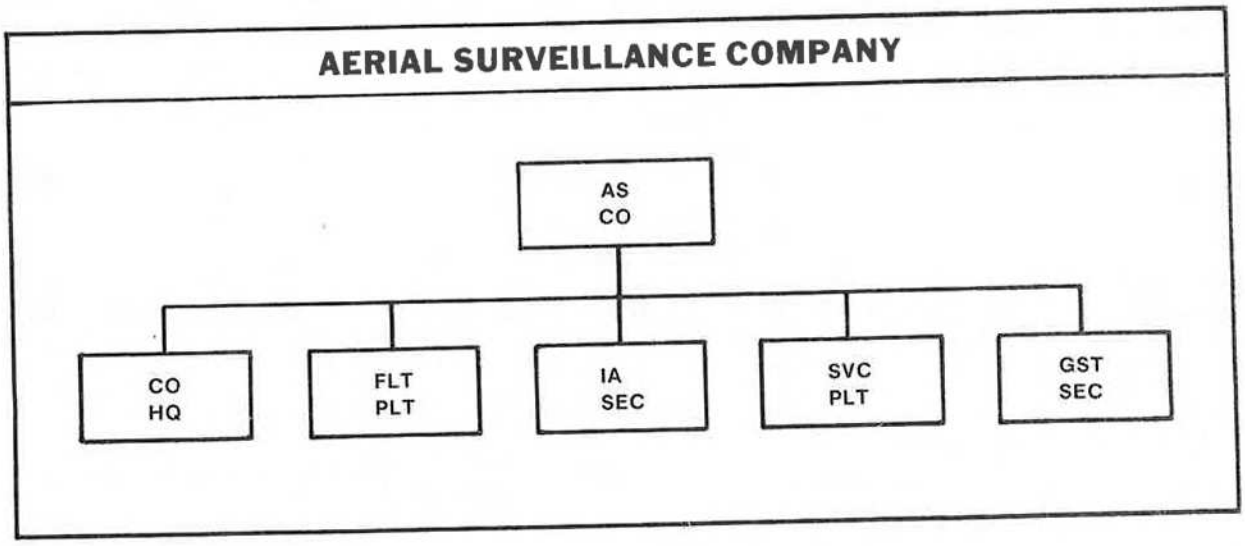
The mechanical maintenance section provides consolidated organizational maintenance for battalion vehicles, refrigerators, air conditioners, and power generating equipment. It also provides vehicle recovery service.

The aviation medical section provides aviation medical services and unit-level medical support to the battalion. It operates the battalion aid station and provides ground medical evacuation.

The airfield service section provides airfield service support to the battalion. Support includes aircraft fuel and oxygen and emergency airfield lighting.

AERIAL SURVEILLANCE COMPANY

The aerial surveillance company provides surveillance and reconnaissance support to the corps. The company plans and conducts aerial reconnaissance and surveillance of routes, zones, areas, coastlines, and borders using SLAR and photographic and visual means. Combat information and IMINT are reported to the supported unit and to the CTOC. All company assets, except for the ground sensor terminal (GST) section, normally operate at the corps fully instrumented airfield. The aerial surveillance company is organized as shown in the following illustration.



COMPANY HEADQUARTERS

The company headquarters provides C^2 for all assigned and attached elements. Subordinate to the company headquarters, the flight operations section is responsible for directing the flight operations of the company. It provides preflight planning information, processes flight plans, and coordinates ongoing missions. This section is responsible for the overall planning and scheduling of surveillance missions, in coordination with the imagery analysis section.

FLIGHT PLATOON

There is one flight platoon. Platoon headquarters supervises the operation of subordinate flight sections. They ensure that aircraft and crew members are available to meet mission requirements.

IMAGERY ANALYSIS SECTION

The imagery analysis section processes, analyzes, and reproduces photographic imagery obtained by the company. It produces IMINT and disseminates it to the CTOC. It receives mission tasking from the MI brigade operations center and works closely with the flight operations section for flight planning.

SERVICE PLATOON

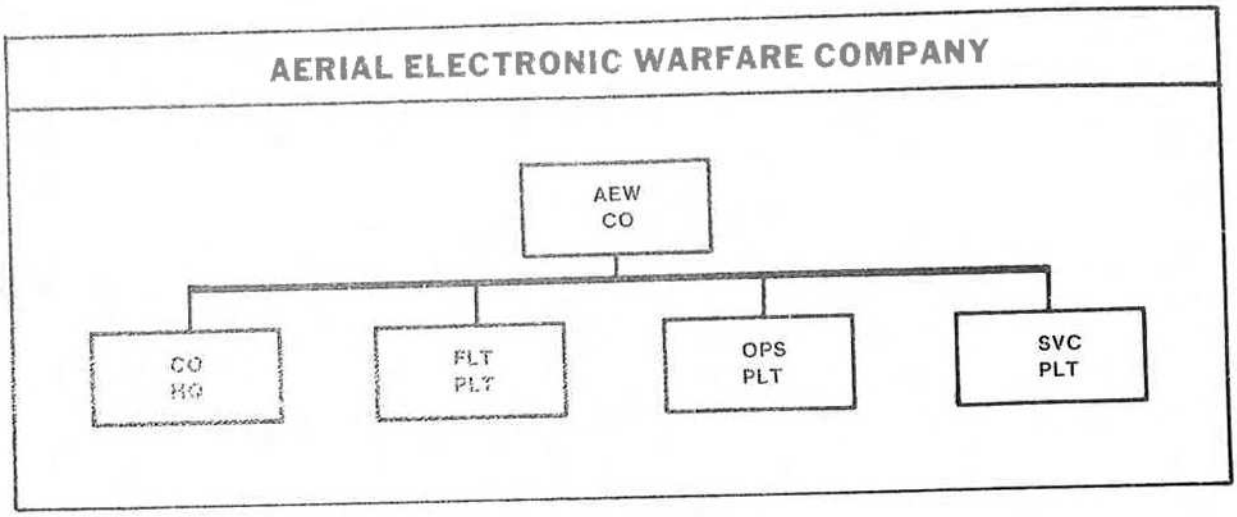
The service platoon maintains organic aircraft and surveillance systems. It is organized with a platoon headquarters, aviation unit maintenance (AVUM) section, and a surveillance systems repair section.

GROUND SENSOR TERMINAL

The GST provides near real time readout of SLAR imagery as it is acquired. Its eight teams normally deploy throughout the corps area to provide combat information to elements of the corps. Deployment is determined by the G2, and terminals normally include corps artillery, division, ACR, and any separate brigade.

AERIAL ELECTRONIC WARFARE COMPANY

The aerial EW company provides signal collection and processing support to the corps. In coordination with the MI battalion (AE) and MI brigade S3, the TCAE, and the G2 staff, it plans and conducts aerial SIGINT collection missions. It processes intercepted signals and reports combat information and intelligence data to the supported unit and to the TCAE in the MI brigade operations center. Company assets normally operate at the corps fully instrumented airfield. However, ground processing assets may be located elsewhere. The company is organized with a company headquarters, a flight platoon, an operations platoon, and a service platoon as shown in the following illustration.



COMPANY HEADQUARTERS

The company headquarters provides C^2 for all elements assigned or attached to the company.

FLIGHT PLATOON

The flight platoon provides aerial COMINT and ELINT collection support to the corps. It is organized with a platoon headquarters, a COMINT aircraft section, and an ELINT aircraft section. The COMINT section has RU-21H/RC-12D airborne VHF and ultra high frequency (UHF) intercept and location systems (GUARDRAIL) aircraft. The ELINT section has RV-1 airborne noncommunications emitter location and identification systems (QUICKLOOK) aircraft.

Platoon Headquarters

The platoon headquarters supervises the aircraft sections. It coordinates aircraft maintenance and schedules crews and aircraft based on mission tasking received through the operations platoon.

Communications Intelligence Aircraft Section

The COMINT aircraft section provides the GUARDRAIL aircraft and crews required to accomplish the aerial COMINT collection mission. Normally, two aircraft are flown simultaneously to provide a broad baseline for DF and signal intercept.

Noncommunications Electronic Intelligence Aircraft Section

The noncommunications ELINT aircraft section provides the QUICKLOOK aircraft and aviators to accomplish the aerial noncommunications ELINT collection mission. The systems operators are provided by the noncommunications ELINT processing section.

OPERATIONS PLATOON

The operations platoon performs ground-based processing and reporting of collected SIGINT data. It assists the flight platoon in determining the optimum flight track and altitude for mission accomplishment.

Platoon Headquarters

The platoon headquarters supervises subordinate sections. It receives EW mission tasking from MI battalion (operations) and immediately provides this information to the flight platoon. It assists the flight platoon in flight planning as it pertains to meeting signal collection requirements.

Collection and Direction-Finding Section

The collection and DF section remotely operates the collection and DF subsystems on board the GUARDRAIL aircraft from the GUARDRAIL integrated processing facility (IPF). Intercept and DF data are passed from the aircraft, while airborne, to the IPF where the data is recorded and processed for analysis and reporting.

Analysis and Reporting Section

The analysis and reporting section is responsible for analyzing data received from the GUARDRAIL aircraft and for reporting combat information, SIGINT TACREP, and technical control data to designated recipients. It is collocated with the collection and DF section in the IPF.

Noncommunications Electronic Intelligence Processing Section

The noncommunications ELINT processing section provides the ground processing, reporting, and tasking effort for the QUICKLOOK system. It programs the aerial collection system before takeoff and retrieves collected data from it after aircraft recovery. If the aircraft is within communications range, data is received during the mission. Processed data is reported to the TCAE. It also provides the ELINT systems operators for QUICKLOOK missions.

SERVICE PLATOON

The service platoon maintains assigned aircraft and SIGINT collection systems. It is organized with a platoon headquarters, AVUM section, and a signal maintenance section.

DEPLOYMENT

The MI battalion (AE) aircraft are self-deployable. Depending on the distance of deployment, additional aircraft maintenance preparation may be required. This additional maintenance may include the removal of the surveillance equipment and the outfitting internal or external fuel tanks. Extensive cross-country, overwater premission planning may be required.

The movement of personnel and equipment requires Air Force heavy lift support. It is imperative that unit and battalion movement plans be accurate, complete, and continuously revised to ensure timeliness during the actual deployment. Practice exercises are used as a tool to provide the commander a unit of measure of the unit's state of readiness to deploy. Before deployment, coordination is made with the corps of engineers to survey the airfield deploying to and locate inertial navigation equipment coordinates for both the IPF and inertial navigation system maintenance equipment.

OPERATIONS AND SENSOR SYSTEMS

Looking deep into threat territory, the battalion finds and follows enemy forces through their physical and electronic signatures. The MI battalion (AE) provides continuous surveillance of the battlefield. It uncovers critical targets that are inaccessible to corps ground-based systems. It also verifies and expands information provided by other systems. Through its aerial signal collection and surveillance operations, the MI battalion (AE) makes a significant contribution toward satisfying the commander's critical information needs for both the close-in and interdiction battles. Battalion assets include--

- GUARDRAIL for communications intelligence.
- QUICKLOOK for noncommunications intelligence.
- Mohawk aircraft with the SLAR system for detection of enemy movers and with camera systems for aerial photography.

MOHAWK

The aerial surveillance company is equipped with OV-1D Mohawk aircraft. This aircraft can be equipped with photographic and SLAR sensors. Not all OV-1D aircraft are so equipped. Each system is described briefly.

Aerial Photography

The aerial photography capabilities of the company provide both square-format and panoramic views of the reconnaissance target. Each of the aircraft assigned to the company may be equipped with one square-format camera and two panoramic cameras.

The square-format camera provides five possible views of any given target based on the camera position selected. While in flight, the camera may be positioned for high or low oblique or vertical views of the target. Each oblique position provides a side view of the target with the view angle depending on the position selected. The vertical position provides an overhead view of the target.

Lens cones available for use with this camera range from wide angle to telephotographic. Selected and installed before flight, the lens cones provide increased flexibility for the system.

Additionally, the square-format camera may be used for night vertical photography. When the aircraft is equipped with an electronic photoflash and an appropriate lens cone, the system may be used for photographic reconnaissance at altitudes 1,500 to 2,000 feet above ground level.

The two panoramic cameras on each aircraft provide a horizon-to-horizon view of the target area. One camera, mounted in the nose of the aircraft, provides a very low-level side view of the target as the aircraft approaches. The second camera is mounted in the belly of the aircraft and provides a wide vertical view of the target.

The aerial photography systems can be used for reconnaissance of both enemy and friendly targets. However, the air defense threat must be thoroughly evaluated for each mission because the camera systems require that the aircraft fly over (or close to) the target.

Reconnaissance of large areas, routes, or several point targets separated by impassable terrain or obstacles may be accomplished by one aircraft sortie. Resulting imagery may be exploited immediately or retained for future use. Aerial photography is excellent for use in support of OPSEC and rear operations.

Besides the limitations posed by threat air defenses, a number of other factors may also affect the effectiveness of aerial photography:

- Smoke, blowing dust or sand, and weather conditions, such as clouds, rain, fog, or snow may obscure the target.
- The camera systems are not capable of in-flight processing and do not provide in-flight readouts. These systems require the aircraft to return to base to have the systems downloaded and the film processed. The imagery must then be interpreted before it can be used.
- Processing and interpretation delay the dissemination of valuable target data.

Side-Looking Airborne Radar

SLAR is a moving target detector capable of providing stand-off surveillance of large areas. It can cover selected areas at various ranges on either or both sides of the aircraft flight path. Information collected by SLAR is presented in near real time in the aircraft and simultaneously transmitted to ground data terminals.

GSTs, when provided by tables of organization and equipment, are normally located with the imagery analysis section and the CTOC, divisions, corps artillery, ACR, and separate brigade. In-flight reports are used when GSTs are not available or to augment information downlinked to the terminals.

SLAR has a near all-weather capability and is equally effective day or night. Its stand-off capability places it out of range of threat forward air defense systems. However, stand-off operations decrease the range of SLAR coverage beyond the FLOT.

QUICKLOOK

QUICKLOOK is an airborne ELINT collection and emitter location system. It provides commanders with identification, location, and deployment of noncommunications emitters. The system is mounted in the RV-1D aircraft.

The QUICKLOOK provides classification and location of electronic emitters to a ground-based data collection and emitter location facility by digital data link. The aerial portion of the system consists of a countermeasures receiving set and a digital data link.

The countermeasures set collects and processes data it receives from enemy ground-based emitters detected along the flight path of the aircraft. Upon the return of the aircraft to its airfield, the collected information is removed from the receiving set data files for analysis. The receiving set can also respond to control signals transmitted from the ground-based support facility via the digital data link. The countermeasures set receiving this signal collects specific data and relays the collected data to the ground-based support facility.

The digital data link provides secure two-way data communications between the countermeasures set in the aircraft and the ground processing station.

Ground equipment of the QUICKLOOK system is related to mission operation and is used to control the intercept equipment in the aircraft. Other items of ground equipment are used in a support role to keep the aircraft available to perform assigned missions. Included are--

- A ground support facility for performing preflight and postflight operations. It performs flight-line checkout and loads and unloads mission programs and data in the on-board computer files.

- A semitrailer maintenance facility for performing organizational maintenance on the QUICKLOOK system.

- An operational support facility or ground processor mounted in a semitrailer. This provides a capability to construct tapes containing EOB files. One can then enter the variable parameters into the system's operational programs, interpret collected data, and provide a hard-copy printout of mission results.

The ground processor receives the collected data. The operator passes combat information directly to the user by the fastest means available. Processed data is forwarded to the group operations center. QUICKLOOK also has an encrypted down link to the electronic processing and dissemination system (EPDS).

Like the GUARDRAIL, QUICKLOOK missions are flown in a stand-off mode. An elongated flight profile parallel to the FLOT is used. Distance from the FLOT depends on the mission, terrain, and air defense threat. Each leg of the flight track is of sufficient length to establish an adequate baseline consistent with anticipated ranges to the targets. Mission time is dependent on flight speed, altitude, and the distance from the airfield to the flight track.

GUARDRAIL

GUARDRAIL provides collection and emitter location information for threat communications. It intercepts enemy VHF, UHF, and limited HF communications emitters and provides locational information on HF and VHF emitters. It processes the information and reports it to users over secure, direct communications links in near real time. The system consists of--

- A remotely controlled collection and data transmitting system aboard an RU-21H (GRV) or RC-12D (IGR) aircraft. The systems are different in the two airframes.

- GS and maintenance equipment.

- An IPF.

- A commander's tactical terminal (CTT).

The IPF operator remotely controls the airborne collection equipment, processes data received from the aircraft, and transmits the processed information through the aircraft to the CTT. CTTs are collocated with MI operations centers at corps, divisions, ACRs, and separate brigades. The CTT can provide teletype and secure UHF voice intelligence reports.

Two or three aircraft are normally employed for each mission to optimize emitter location. Continuous maximum spacing between aircraft is desired to establish the longest DF baseline.

The aircraft flies over friendly controlled areas in a stand-off mode. The nature of the terrain, anticipated location of target emitters, and the enemy air defense threat dictate the distance behind the FLOT and altitude for each mission. Missions must be flown within range and LOS of the target emitters. Additionally, the aircraft must maintain LOS to each other; and one of the aircraft must maintain LOS to the IPF and CTT.

MISSION REQUIREMENTS

Aerial surveillance and signal collection missions are initiated at the CTOC. Elements of the CTOC develop the corps collection and surveillance plans based on intelligence and ESM requirements. These plans generate surveillance and collection missions.

Aerial surveillance and signal collection missions are either preplanned or immediate. Preplanned missions based on corps requirements identified during planning are most effective because they allow time for planning, coordinating, and briefing. They also permit more efficient use of limited USAF and organic resources through consolidation of requirements.

Immediate missions are used to satisfy urgent, unanticipated requirements for information of immediate tactical value. Some aircraft and aircrews may be placed on ground alert, or preplanned missions may be diverted in-flight to satisfy immediate mission requirements.

The CM&D, CTOC, passes mission requirements to the MI brigade operations center TCAE in the form of mission tasking. The operations center, through correlation and refinement, translates mission tasking into asset tasking. MI battalion (AE) assets are then selected and tasked based on mission priorities and the capabilities, deployment, and status of MI battalion (AE) assets. Collocation of the CTOC and the brigade S3 facilitate this process.

Tasking instructions are keyed to the specific needs of the asset tasked. They convey all information and coordinating instructions necessary to accomplish the mission. They normally include--

° Task objective.

° Type of target.

° Type of system to be used.

° Mission and reporting priorities.

° Coordinating and reporting instructions.

° Time the mission is conducted or when the information is required.

° Trace of the FLOT.

° Enemy air defense threat.

° Friendly air defense plan and airspace entry approval.

° Air-ground communications frequencies and call signs.

° Other background or supporting information.

Air reconnaissance request formats may be used to transmit tasking instructions for aerial R&S missions. They are the--

° Joint tactical air R&S request form for joint operations conducted only by US forces.

° Air reconnaissance request and task message for NATO operations.

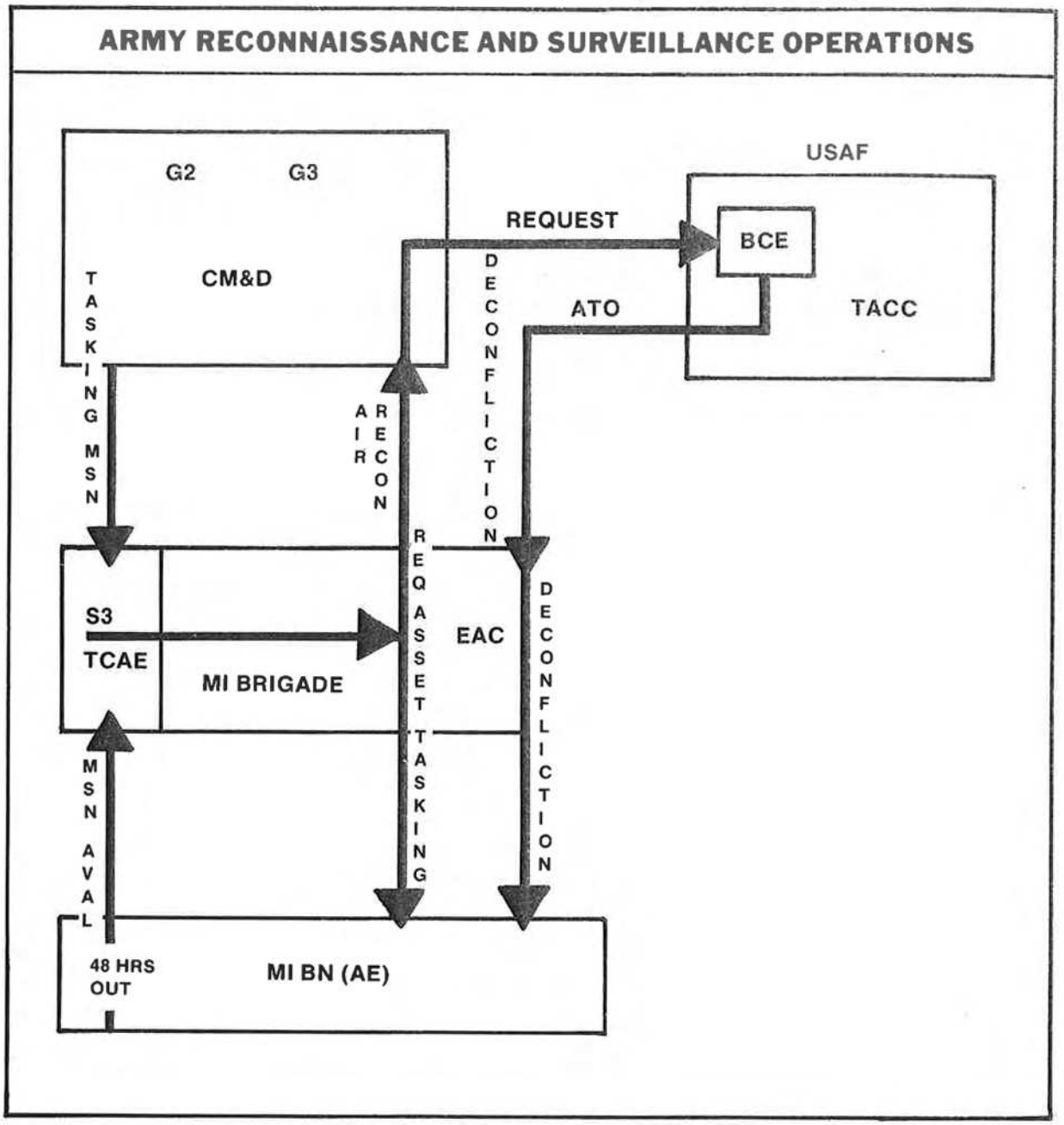
The joint tactical air R&S request form is published in Change 2, Volume II, JCS Publication 12. The air reconnaissance request and task message conforms to the requirements of STANAG 3277.

Tasking for MI battalion (AE) assets is transmitted from the brigade operations center TCAE to the battalion S3 operations center (see the following illustration). All missions are coordinated with the Air Force TACC for inclusion in the daily air tasking order. Each mission will receive special transponder codes, frequencies, and block times which are reflected in air tasking orders and tasking messages.

The battalion S3 section coordinates tasking with the appropriate company and keeps the commander informed of projected and ongoing operations. The commander ensures that the companies are deployed and supported to meet mission requirements. He also ensures the most efficient use of battalion resources in response to mission requirements.

Signal collection tasking is forwarded from the TCAE to the operations platoon of the aerial EW company. Besides the information above, the tasking message includes current EOB and technical data on enemy emitters pertinent to the mission. The operations platoon notifies the flight platoon leader who schedules the aircraft and crew.

Asset tasking for the aerial surveillance company is directed to the imagery analysis section. The imagery analysis section refines the mission to specific target areas and coverage and determines the number of aircraft and type sensors required. If the time of execution is not specified in the message, the imagery analysis section determines the optimum time to fly the mission. To facilitate flight planning and the scheduling of aircraft sensors and aircrews, it passes mission tasking to the company flight operations section when it is received.



To ensure that aircrews thoroughly understand the requirements of the mission, they are briefed by the flight platoon and the company operations section. The imagery analysis section participates in the briefing for aerial surveillance missions. The briefing should include the mission requirements and available--

° Friendly and enemy situation.

° Dispositions.

° Air defense threat.

° Weather data.

° Minimum risk routes and low-level transit routes.

° Artillery trajectory areas.

° Air defense artillery weapon engagement zones.

° Identification of friend or foe codes.

° Other airspace restrictions in effect.

A general briefing for all aircrews may be given daily. This briefing provides pertinent information about tactical operations for the next 24 hours and aids in reducing the amount of information that is presented at the preflight briefing.

Flight tracks and profiles are determined, based on mission requirements, aircraft capabilities, threat, and weather constraints. Weather is a vital element of mission planning and execution. USAF-generated weather information on current projected conditions along flight tracks is provided to the aircrews in preflight briefings. The planned flight route and profile may have to be changed due to weather conditions.

Effective flight planning is paramount to the success of aerial surveillance and signal collection operations. The responsibility for flight planning is shared by the unit commander, operations personnel, flight platoon and section leaders, and aircrews.

Careful map reconnaissance is conducted during premission planning to take advantage of the best flight orbits and routes. The aircrew is briefed by the S2 on the locations and fire fans of all known surface-to-air missiles that could engage the aircraft during the mission. Evasive tactics are planned by the aircrew. Flight altitude, stand-off distances, and tracks are selected to provide the optimum combination of mission accomplishment and protection from threat air defense systems.

Takeoff times are scheduled to meet the time-on-station time as specified in the tasking message. If the tasking message does not specify the time on station, it is computed to ensure that the information is available when it is needed.

When flight plans are completed and approved by the company flight operations officer, they are filed with the appropriate air traffic control facility. The flight operations section maintains the flight schedule, based on flight plans.

While the aircrew prepares for the mission, the aircraft maintenance section supervises the preparation of the aircraft and sensor systems for the mission. When mission requirements are critical, a backup aircraft is prepared along with the mission aircraft. Should maintenance requirements or other factors prevent use of the mission aircraft, the backup aircraft is launched in its place.

MISSION EXECUTION

Mission execution must conform to the requirements in the tasking instructions and the planned mission. While the aircraft and crew are the key players, the success of the mission relies on support that has been planned and coordinated. Any deviation from the plan must be reported to every element involved in the mission.

During aircraft runup, all systems are checked. A system failure or malfunction requires immediate analysis and a decision whether to continue or abort the mission. A backup aircraft is used for urgent missions. Any delays are reported to the group operations center and ground terminal sections.

Immediately following takeoff, the aircrew reports to the appropriate air traffic control facility and the sector operations center or ground-controlled intercept site in whose sector they are operating. They also coordinate with other friendly units according to the planned mission.

Mission aircraft take off to meet the on-station time. Missions are flown with the aid of the on-board internal navigation system which continuously updates and displays the location of the aircraft. This technique increases the accuracy and quality of the collected data.

Sensor equipment is turned on when the aircraft reaches the designated flight track or target area. The aircrew reports when they arrive and when they depart from their mission station.

IN-FLIGHT REPORTS

In reporting information, the primary consideration is to pass essential data, within acceptable time limits, to the unit or agency that needs it or is able to take appropriate action. Normally, this will be the unit that requested or directed the mission. However, other elements may need the collected information. The reporting system must provide for immediate reporting of combat information and timely reporting of other information.

Visual reconnaissance is part of every aerial mission. The aircrew submits in-flight reports on any significant information noted visually. In-flight reports are transmitted to the company operations center which, in turn, forwards them to the brigade operations center, the corps CM&D section, or other elements that need them. The aircrew may report combat information directly to the unit that requested the mission, to the FSE, or to other units in whose area they observe activity. Ground equipment operators may also submit in-flight reports of significant information.

Secure and reliable communications are vital to in-flight reporting. Normally, FM secure radio is used. HF radio provides an alternate means. HF communications are effective at greater ranges and when the aircraft is flying at a low altitude. HF communications, however, suffer from two disadvantages: they cannot be easily secured--encryption requires the use of manual coding of each message, and they require prior coordination with ground elements to arrange for compatible radio sets.

POSTMISSION OPERATIONS

Postmission operations include the preparation of the aircraft and sensors for the next mission, debriefing the aircrew, submitting postflight reports, and processing data taken from the aircraft.

Debriefings provide a method of extracting critical information resulting from observations during the flight. They are designed to expand on in-flight reports and to obtain information not previously reported. Normally, this includes visual information about the enemy, weather, and terrain.

Flight personnel are questioned regarding all aspects of the mission during the postflight debriefings. These include--

° Mission results and the degree of mission accomplishment.

° Enemy activity and other observations: who, what, when, and where.

° A damage report as applicable.

The debriefing officer also obtains any additional information that is not directly related to the mission, but is of value. Weather observations are examples of such information.

The aerial EW company operations platoon leader, or his representative, debriefs aircrews following signal collection missions. He reports pertinent information to the group operations center.

Postmission functions of a GUARDRAIL mission include completing the analysis of data obtained during the flight. Postmission reports are forwarded to the corps operations center.

If the QUICKLOOK performed properly during the mission, there will be little postmission activity required. However, a break in the data link requires a dump of mission data into the preflight and postflight vehicle where the data is recorded on cassette tape. The data is processed and analyzed in the ground processor. Reports are prepared and transmitted to the brigade operations center through the multichannel or RATT system.

Following an aerial surveillance mission, the imagery is immediately delivered to the imagery analysis section for processing and interpretation. The aircrew is debriefed by flight operations and imagery analysis personnel. Information obtained from the debriefing is included in the reconnaissance exploitation report (RECCEXREP).

IMAGERY REPORTS

The imagery analysis section rapidly inspects the imagery for combat information and information needed to answer specific mission requirements. Based on the aircrew debriefing and initial readout of imagery, it submits the RECCEXREP to the CTOC. The possible, but no later than 45 minutes after engine shutdown.

However, a mission report (MISREP) may be used to report negative mission results. If used, the MISREP must be submitted within 30 minutes after engine shutdown.

If the mission required prints, they are developed and delivered to the message center for further delivery to the requesting unit.

The initial photographic interpretation report (IPIR) and supplemental photographic interpretation report (SUPIR) are used to report information obtained through a systematic review of imagery. They are used to report information not previously reported and to provide additional details. Both reports use the same format. They are transmitted to the brigade operations center, which then passes the information to the CTOC. This process closes the asset-tasking requirement. These reports may be prepared either manually or by automatic data processing.

The IPIR is submitted as soon as possible, but not later than 4 hours after engine shutdown. It is used to report on programmed mission objectives or other vital information in reasonable proximity to the objective.

The SUPIR is used to report additional information or to provide supplemental information. It is disseminated quickly and may be transmitted in fragments to facilitate transmission.

The aerial surveillance company imagery analysis section works closely with the imagery analysis section of the CTOC support element. They exchange data concerning mission requirements. The capabilities and status of aerial surveillance and imagery analysis are coordinated with the brigade S3 operations center. The CTOC imagery analysis section provides backup support when the quantity of imagery requiring exploitation exceeds the capabilities of the aerial surveillance company imagery analysis section. Because of delays in imagery delivery, the CTOC imagery analysis section handles the least time-sensitive requirements. The aerial surveillance company imagery analysis section responds to requests for hard-copy imagery within its capability.

APPENDIX

MILITARY INTELLIGENCE COMMUNICATIONS

Every aspect of IEW operations is dominated by the requirement for rapid, reliable, and secure communications. MI assets cannot perform the mission unless they are effectively tasked and controlled; nor is collected, analyzed information valuable unless it is transmitted in a timely manner to combat elements which require it.

MI COMMUNCIATIONS MEANS

MI tactical communications requirements are met with an integrated system built from various communications assets belonging to several echelons of signal elements. Those assets include systems for encrypted single channel and bulk-encrypted multichannel communications which may be transmitted over tropospheric scatter, tactical satellite, or standard UHF and VHF communications carriers. Those carrier systems are terminated with various communications and special purpose terminals belonging to either the MI brigade (EAC), tactical exploitation of national capabilities, national agencies, or the corps signal brigade. Integral to that system is the network of Joint Tactical Communications System (TRITAC) automated switches which have access to the worldwide automatic digital network (AUTODIN). More traditional MI nets and point-to-point circuitry include tactical RATT, tactical FM radio, and the commander, US forces or Army forces special security network.

The establishment of the tactical automated switch and the eventual fielding of mobile subscriber equipment as the priority means of communications for SCI data and voice traffic as well as for MI logistical and administrative traffic provides new flexibility and speed of installation for MI communications requirements. Special purpose MI vans, organic teletypewriter vans and stand-alone teletypewriter terminals, and in some cases, terminals provided by national agencies, either tie directly into TRITAC terminals or through other communications carriers into those switches. Based upon message headers, those signals are then automatically routed between switches and have access through the tactical system into AUTODIN and the defense special security communications system (DSSCS). The TRITAC network permits quick reentry of MI-dependent vans into other TRITAC nodes based upon tactical considerations. The concept of dual homing off multiple switches also provides reliability necessary for continuous intelligence support.

Point-to-point HF RATT is a slow, but reliable, high signature method for sending message traffic. It is the primary backup means of MI SSO communications and is used for tasking and reporting. Messages are received in the form of page copy. RATT personnel and equipment are provided by the CTOC RATT and TCAE RATT platoons of the communications company of the MI battalion (operations). Other RATT communciations are provided by the radio section within the headquarters, MI battalion (TE). HF RATT can be remoted from the van and should be managed in that manner whenever possible.

FM voice is the primary means of communication for C^2 and for MI administrative and logistical coordination. At division, ACR, and separate brigade, FM radio within the MI battalion (TE) company frequently provides the only tasking and reporting capabilities between specific elements.

Voice communications over wire are installed by the following means: (1) Digital security voice terminals may operate at the SCI level. They are requested for installation from the corps signal brigade. They are encrypted at the user terminal. (2) Protected distribution telephones operate at the secret level. They are also provided by the corps signal brigade. Those circuits are bulk-encrypted between switches and must be inspected continuously between the switch and the telephone terminal. (3) Tactical telephones are manual switches organic to the brigade and are used for internal, nonsecure telephones only.

Net radio interface is flexible, timely, and provides the MI commander with the ability to enter wire circuits from his tactical mobile radio. Net radio interface facilities are requested through the Army air signal center by supporting signal elements.

Couriers are assigned to the TCC platoons within the MI battalion (operations). They provide a secure means of local delivery for large or bulky items or large quantities of routine message traffic. This means is dependent upon the tactical situation.

The following eight illustrations and charts show brigade and corps communications net requirements.

FUNDAMENTALS FOR PLANNING MI BRIGADE COMMUNICATIONS

The user has the responsibility to install, operate, and maintain equipment which terminates circuitry provided by the corps signal brigade.

SCI TCCs are established by the MI brigade at the CTOC, brigade tactical operations center, MI battalion (TE) operations center, and MI battalion (AE) operations center.

Over-the-counter general service TCCs are the responsbility of the corps signal brigade.

The enhanced tactical users terminal is always installed for the corps commander at the CTOC.

The TCAE is designed for internodal configuration at the brigade tactical operations center. TCAE circuits at locations other than the brigade tactical operations center are supported through SCI TCCs or by stand-alone teletypewriter terminals.

The EPDS is normally accessed through EAC communications.

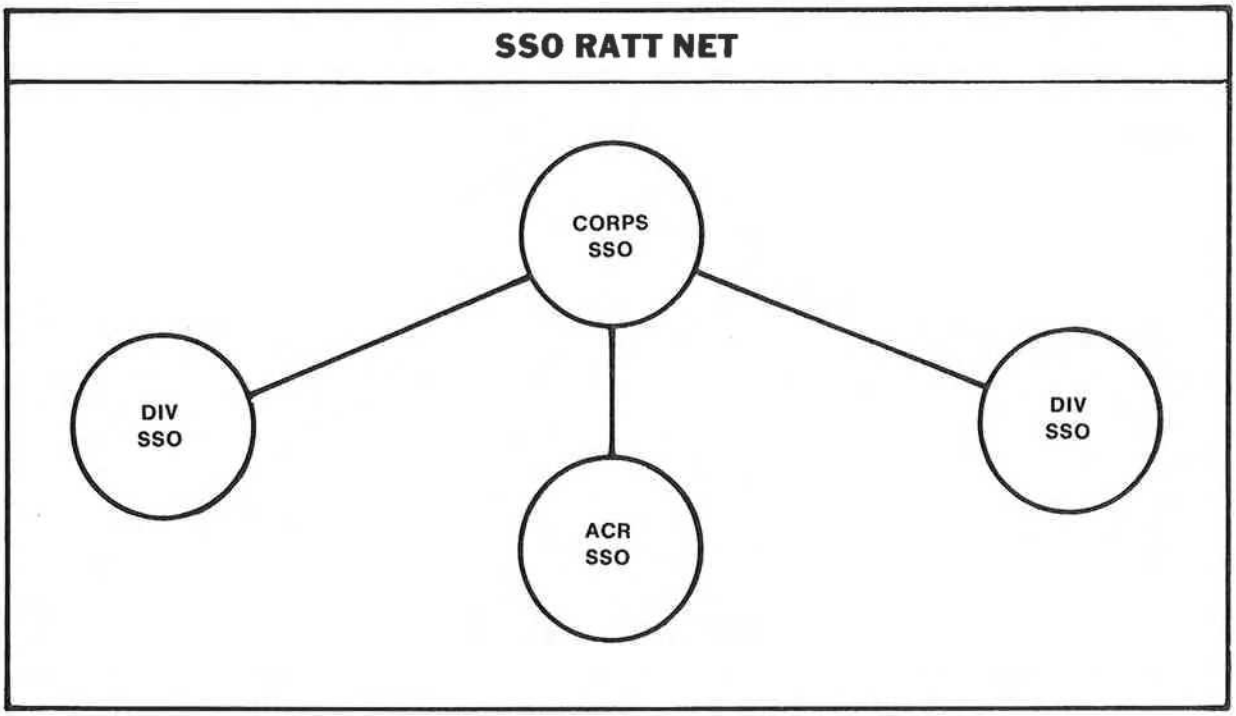
The QUICKLOOK van requires access to over-the-counter service provided by general service TCCs.

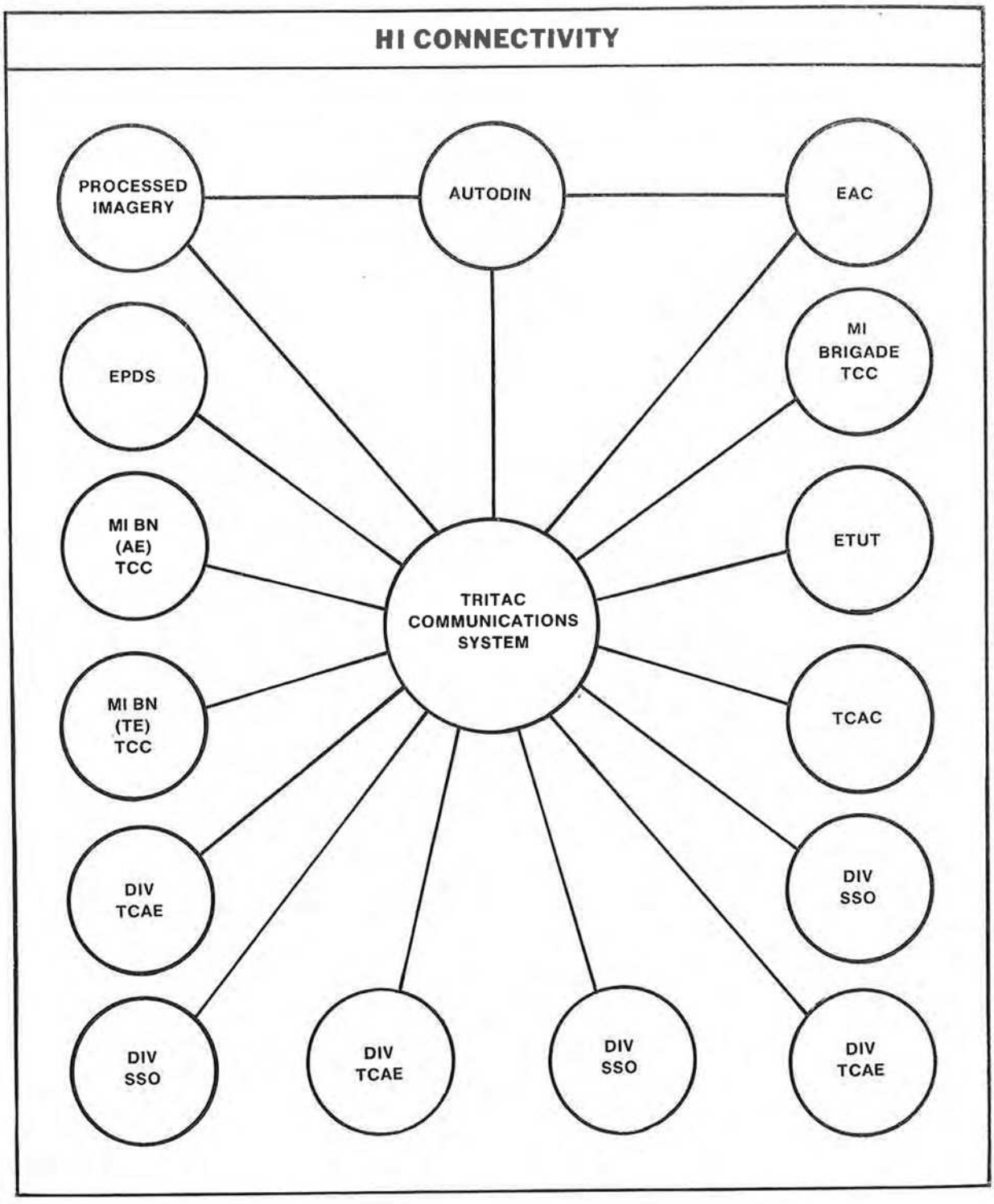
Critical terminals should be dual homed off multiple switches.

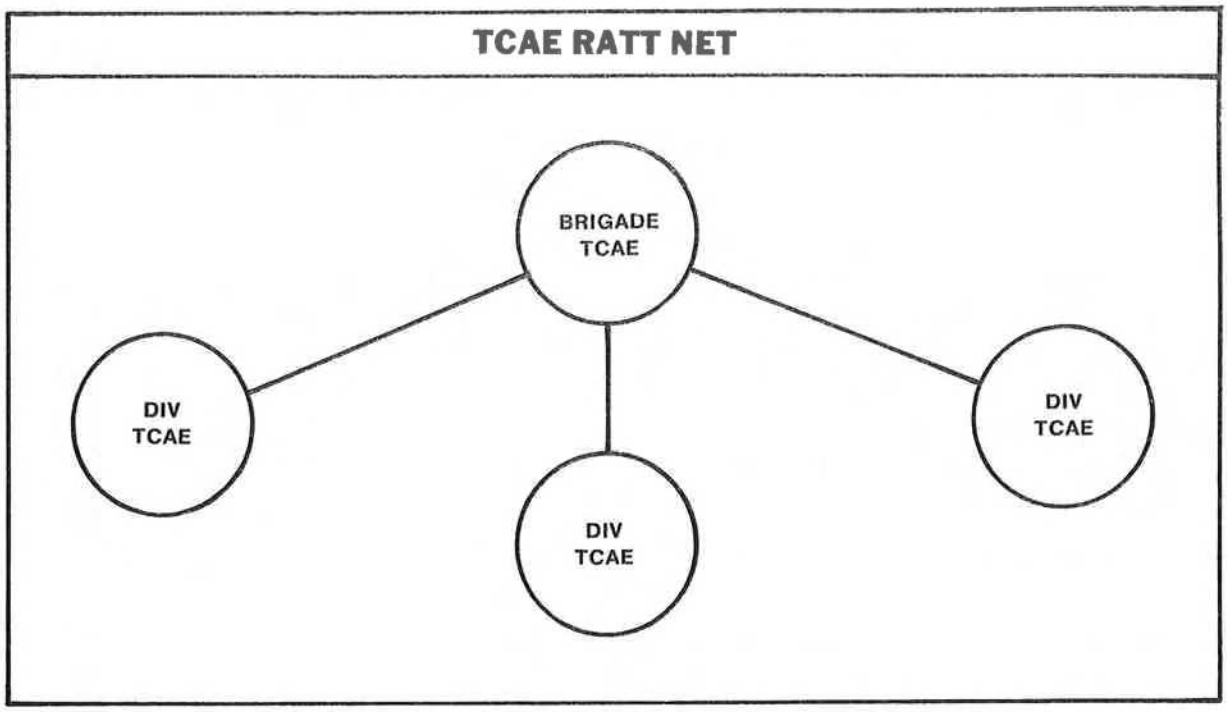
Organic COMSEC is available at the brigade tactical operations center.

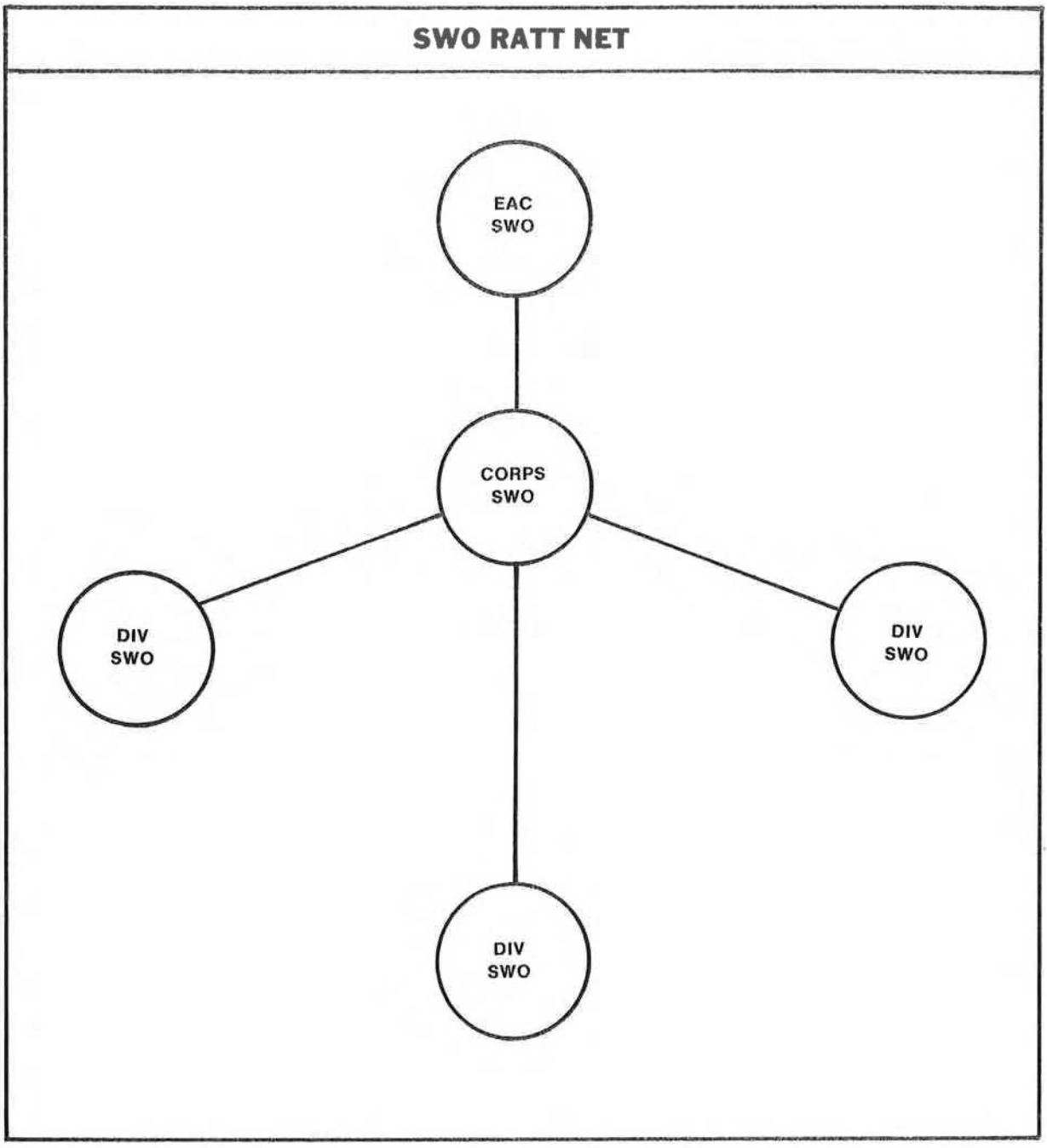
The communications platoon of both the MI battalion (AE) and MI battalion (TE) operate TCC and switchboard service to their respective battalions.

Processed imagery is available through the AUTODIN and DSSCS.

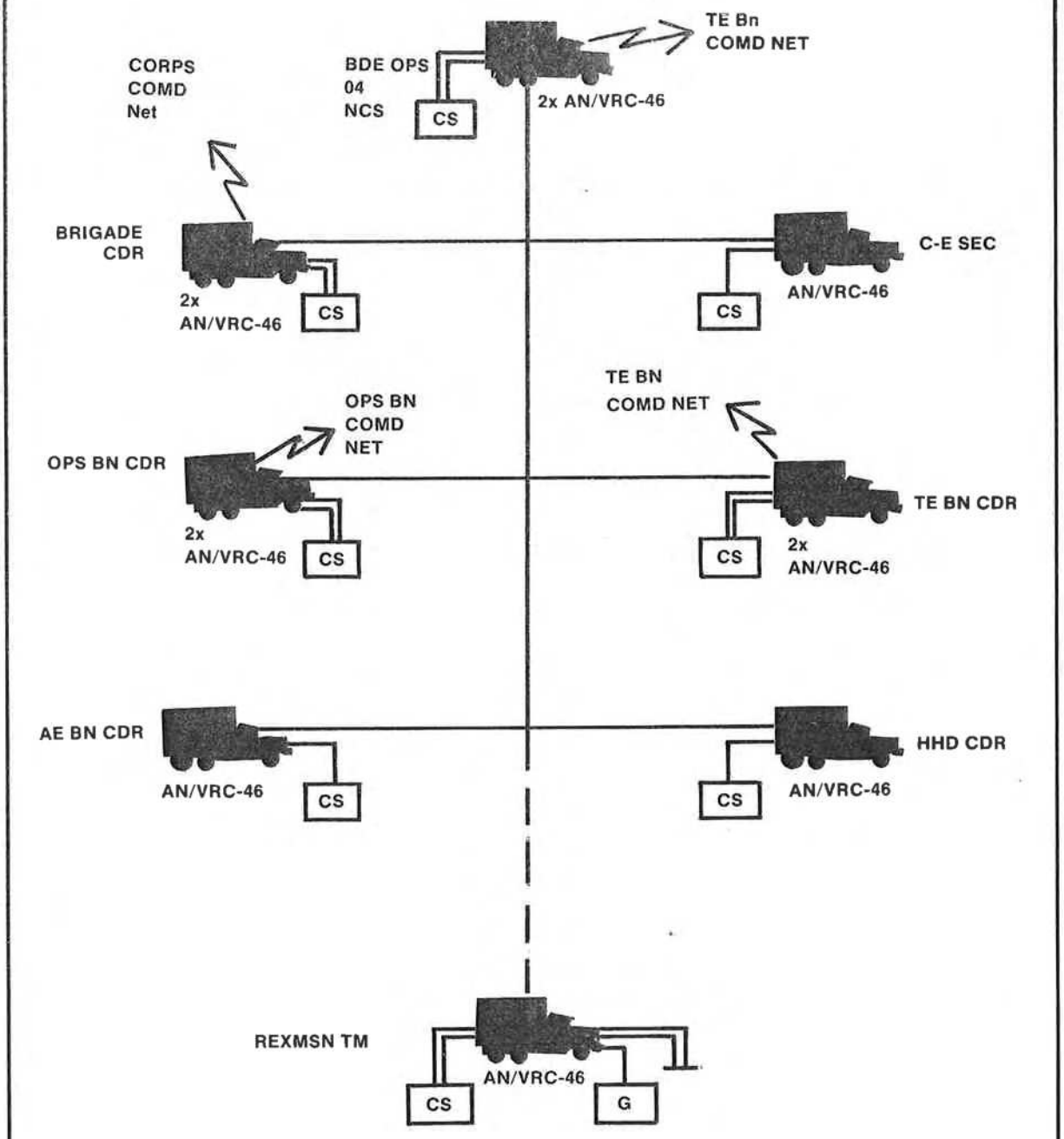



HI CONNECTIVITY
PROCESSED IMAGERY
AUTODIN
EAC
EPDS
MI BRIGADE TCC
MI BN (AE) TCC
ETUT
TRITAC COMMUNICATIONS SYSTEM
MI BN (TE) TCC
TCAC
DIV TCAE
DIV SSO
DIV SSO
DIV TCAE
DIV SSO
DIV TCAE

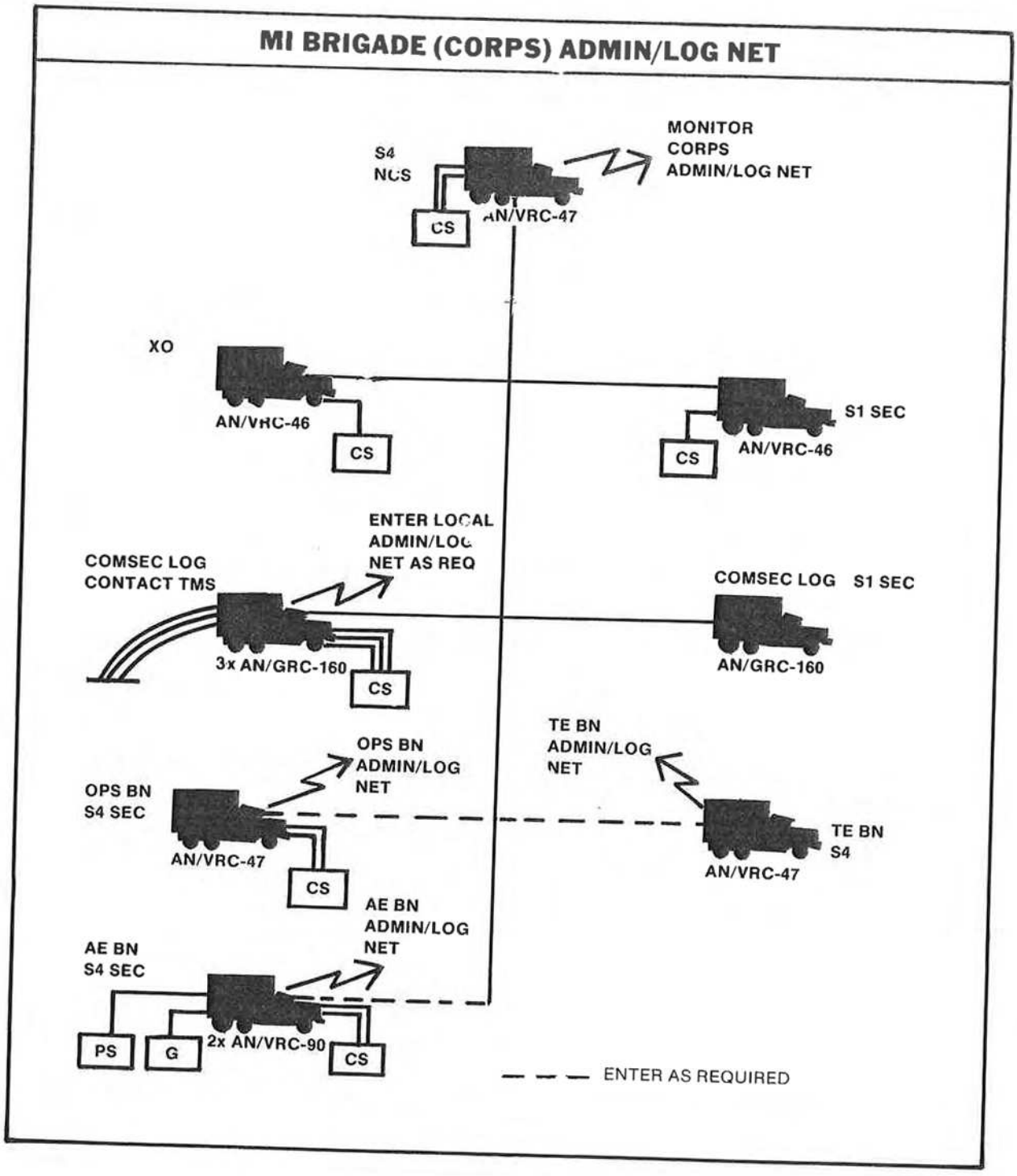

TCAE RATT NET
BRIGADE TCAE
DIV TCAE
DIV TCAE
DIV TCAE


SWO RATT NET
EAC
SWO
CORPS
SWO
DIV
SWO
DIV
SWO
DIV
SWO

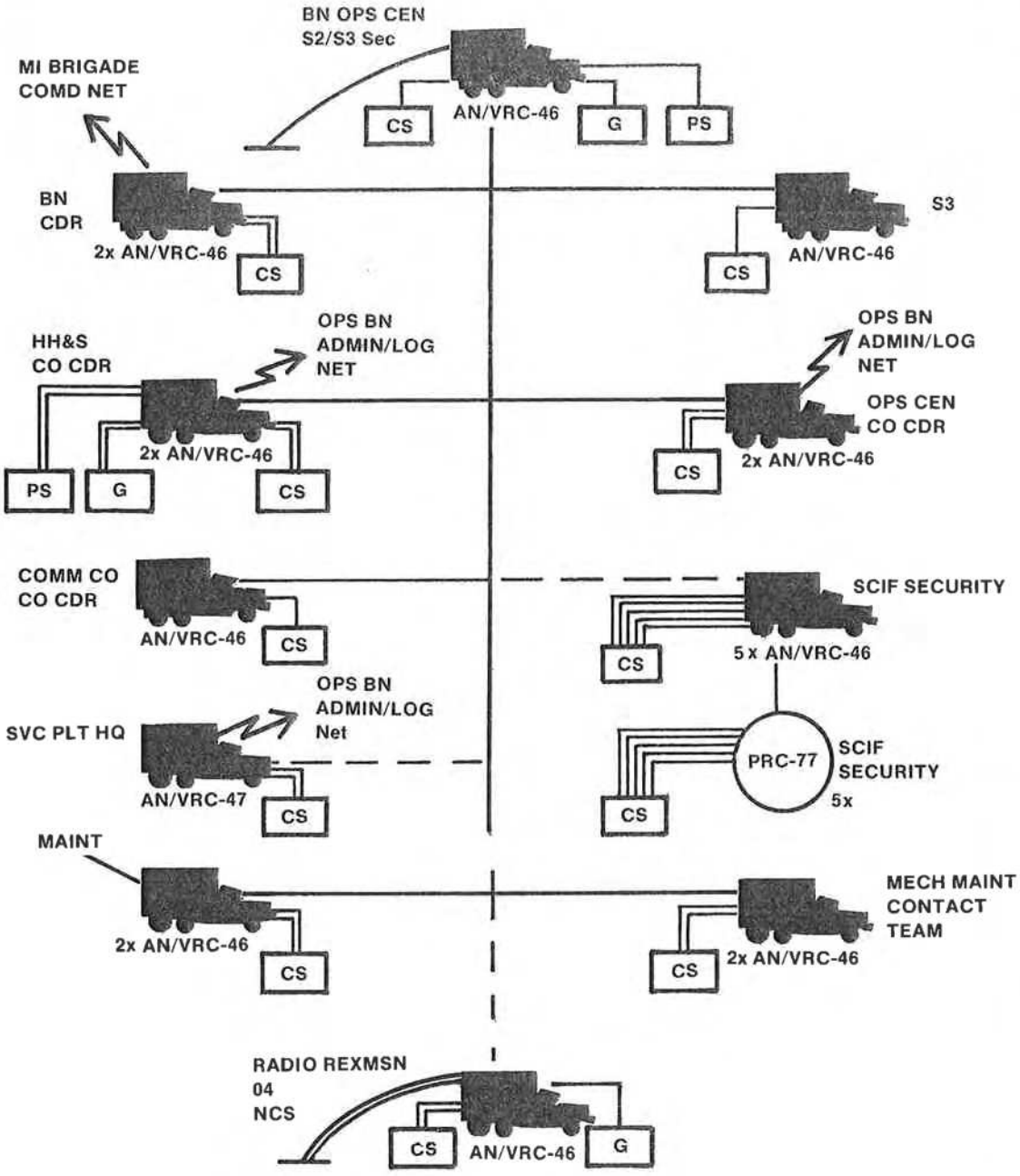
MI BRIGADE CORPS COMD NET



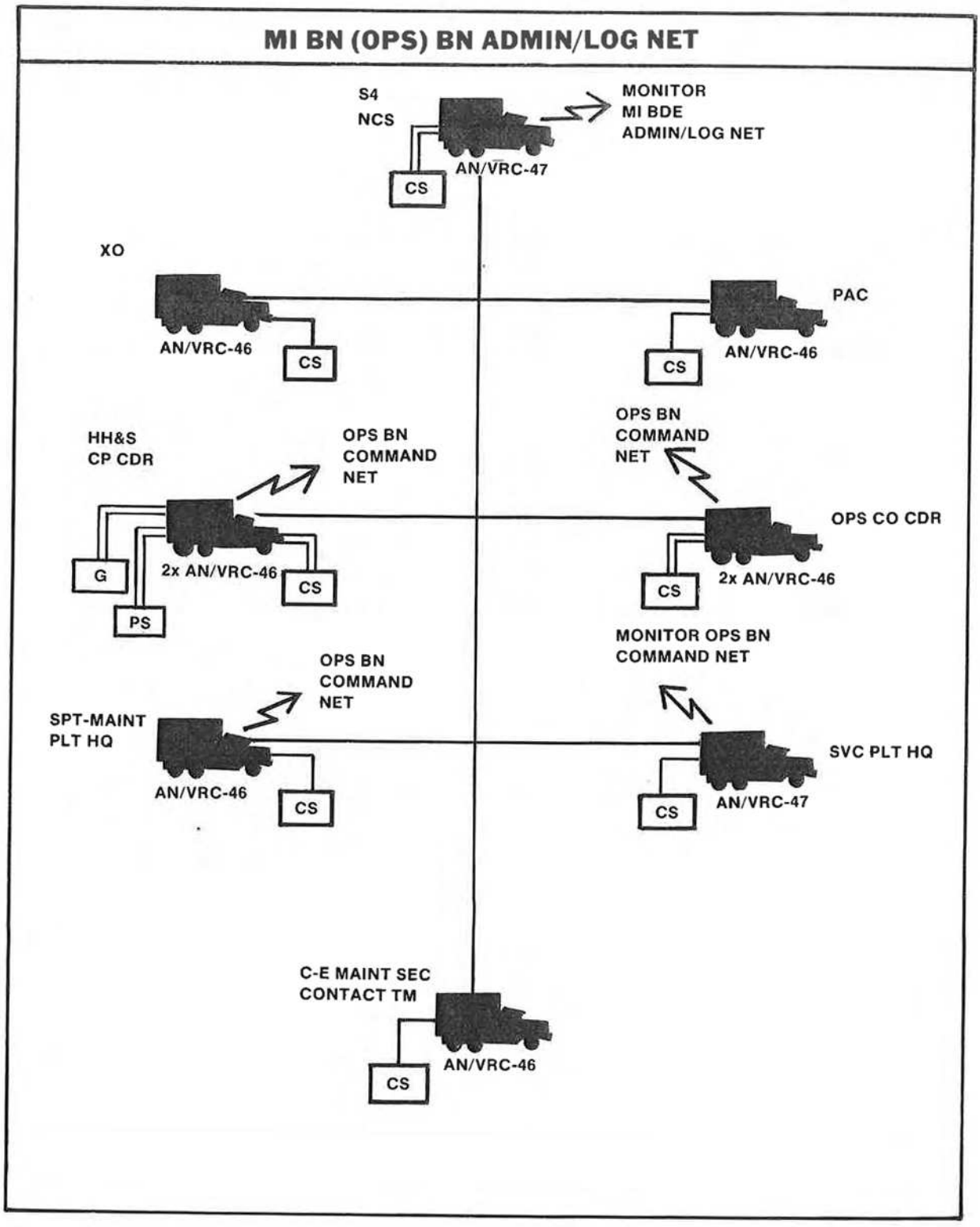
NOTE: This net is used by the MI brigade commander for command and control, coordination, and reporting.


MI BRIGADE (CORPS) ADMIN/LOG NET
S4
NCS
CS
AN/VRC-47
MONITOR
CORPS
ADMIN/LOG NET
XO
AN/VRC-46
CS
CS
AN/VRC-46
S1 SEC
ENTER LOCAL
ADMIN/LOG
NET AS REQ
COMSEC LOG
CONTACT TMS
3x AN/GRC-160
CS
COMSEC LOG S1 SEC
AN/GRC-160
TE BN
ADMIN/LOG
NET
OPS BN
ADMIN/LOG
NET
OPS BN
S4 SEC
AN/VRC-47
CS
TE BN
S4
AN/VRC-47
AE BN
ADMIN/LOG
NET
AE BN
S4 SEC
PS
G
2x AN/VRC-90
CS
ENTER AS REQUIRED

MI BRIGADE (CORPS) MI BN (OPS) COMD/OPS NET (VHF/FM)



NOTE: This net provides the battalion commander with command and control, communications for the battalion.


MI BN (OPS) BN ADMIN/LOG NET
S4
NCS
MONITOR
MI BDE
ADMIN/LOG NET
AN/VRC-47
CS
XO
AN/VRC-46
CS
PAC
AN/VRC-46
CS
HH&S
CP CDR
OPS BN
COMMAND
NET
G
2x AN/VRC-46
CS
PS
OPS BN
COMMAND
NET
OPS CO CDR
CS
2x AN/VRC-46
MONITOR OPS BN
COMMAND NET
OPS BN
COMMAND
NET
SPT-MAINT
PLT HQ
AN/VRC-46
CS
SVC PLT HQ
CS
AN/VRC-47
C-E MAINT SEC
CONTACT TM
AN/VRC-46
CS

GLOSSARY

A

AC	active component
accy	accuracy
ACR	armored cavalry regiment
ADA	air defense artillery
ADC	area damage control
admin	administration
AE	aerial exploitation
AEW	aerial electronic warfare
AM	amplitude modulated
ammo	ammunition
AO	area of operations
AOE	Army of Excellence
arty	artillery
AS	aerial surveillance
ASPS	all-source production section
ASOC	air support operations center
atk	attack
ATO	air tasking order
AUTODIN	automatic digital network
AVUM	aviation unit maintenance

B

BCE	battlefield coordination element
BDE	battlefield deception element
bde	brigade
bn	battalion
bat	battle
btry	battery

C

C^2	command and control
C^3	command, control, and communications
C^3CM	command, control, and communications countermeasures
C^3I	command, control, communications, and intelligence
cat	category
cdr	commander
C-E	Communications-Electronics
CED	captured enemy document
cen	center
CEWI	combat electronic warfare and intelligence
CI	counterintelligence
CIA	Central Intelligence Agency

CIDC	Criminal investigation division command
CM&D	collection mangement and dissemination
co	company
COLT	combat observing lasing teams
comd	command
COMINT	communications intelligence
COMJAM	communications jamming
COMM	communications
COMSEC	communications security
con	control
CONUS	Continental United States
coord	coordination
COSCOM	corps support command
CP	command post
CR	3CR, three crater rays that cross, same caliber and type, within specified period
CR&GPS	one crater ray and a related grid-producing source (source could be a target indicator)
CS	close support
CSS	combat service support
CTOC	corps tactical operations center
CTOCSE	CTOC support element
CTT	commander's tactical terminal

D

DA	Department of Army
DCI	Director Central Intelligence
DCSINT	Deputy Chief of Staff, Intelligence
DF	direction finding
DNE	do not engage
DOD	Department of Defense
DOJ	Department of Justice
DS	direct support
DSSCS	defense special security communications system

E

EAC	echelons above corps
EACIC	echelons above corps intelligence center
ECB	echelons corps and below
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures
EEFI	essential elements of friendly information
elm	element
ELINT	electronic intelligence
engr	engineer
ENSCE	enemy situation correlation element
EOB	electronic order of battle
EPDS	electronic processing and disseminating system
EPW	enemy prisoner of war

ESM	electronic support measures
ETUT	enhanced tactical users terminal
EW	electronic warfare

F

FA	field artillery
FAAO	field artillery aerial observer
FBI	Federal Bureau of Investigation
FDC	fire direction center
FEBA	forward edge of battle area
FID	foreign internal defense
FLOT	forward line of own troops
FM	field manual/frequency modulated
FS	fire support
FSCOORD	fire support coordinator
FSE	fire support element

G

G1	Assistant Chief of Staff, G1, Personnel
G2	Assistant Chief of Staff, G2, Intelligence
G3	Assistant Chief of staff, G3, Operations
G4	Assistant Chief of Staff, G4, Logistics
G	ground
GBDF	ground based direction finding
GRV	GUARDRAIL V
GS	general support
GSA	General Services Administration
GSM	ground station module
GST	ground sensor terminal

H

HF	high frequency
HHD	headquarters and headquarters detachment
HH&S	headquarters, headquarters and service
HH&SC	headquarters, headquarters and service company
HOIS	hostile intelligence services
HPT	high payoff target
HQ	headquarters
HUMINT	human intelligence
HVT	high value target

I

IA	imagery analysis
IEW	intelligence and electronic warfare
IGR	Improved GUARDRAIL
IMINT	imagery intelligence
INSCOM	US Army Intelligence and Security Command
IPB	intelligence preparation of the battlefield

IPF	integrated processing facility
IPIR	initial photograpic interpretation report
IPW	prisoner of war interrogation
IR	information requirements
ITAC	intelligence threat analysis center
J	
J2	Intelligence Directorate
J-SEAD	joint suppression of enemy air defenses
K	
KGB	Committee of State Security
km	kilometer
L	
lang	language
LIC	low-intensity conflict
LLVI	low level voice intercept
LOC	lines of communication
log	logistics
LOS	line of sight
LRS	long-range surveillance
LRSC	long-range surveillance company
LRSU	long-range surveillance unit
M	
maint	maintenance
MASINT	measurement and signature intelligence
MCS	master control station
mech	mechanized
METT-T	mission, enemy, terrain, troops, and time available
MI	military intelligence
MISREP	mission report
MLR	main line of resistance
MOS	military occupational specialty
MP	military police
MPI	military police investigator
MSC	major subordinate command
msn	mission
MTLR	moving target-locating radar
mvr	maneuver
N	
NAI	named area of interest
NATO	North Atlantic Treaty Organization
NCA	national command authority
NCO	noncommisioned officer

noncomm	noncommunications
NSA	National Security Agency

O

OB	order of battle
OCONUS	outside Continental United States
OMG	operational maneuver group
ops	operations
OPCON	operational control
OPSEC	operations security

P

PAC	personnel and administration center
photo	photography
PIR	priority intelligence requirements
plns	plans
PM	provost marshal
PMO	provost marshal's office
PS	power supply
POL	petroleum, oils, and lubricants
proc	processing
PSYOP	psychological operations

R

RA	rear area
R&S	reconnaissance and surveillance
RATT	radio teletypewriter
RC	reserve component
RDO	radio
REC	radio electronic combat (not a US term)
RECCEXREP	reconnaissance exploitation report
recon	reconnaissance
reinf	reinforce
req	request
rexmsn	retransmission
rept	reporting
RPV	remotely piloted vehicle
RS	remote sensor
RSR	resource status report
RSTA	reconnaissance, surveillance, and target acquisition

S

S1	Adjutant (US Army)
S2	Intelligence Officer (US Army)
S3	Operations and Training Officer (US Army)
SA	special agent
SAEDA	Subversion and Espionage Directed Against the US Army and Deliberate Security Violations
SC	standard corps

SCARF	standard collection asset request format
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SEAD	suppression of enemy air defenses
sec	section
SI	special intelligence
SIGINT	signals intelligence
SITMAP	situation map
SIGSEC	signal security
SIR	specific information requirements
SLAR	side-looking airborne radar
SOF	special operations forces
SOFA	Status of Forces Agreement
SOP	standing operating procedure
spt	support
SSO	special security office
SUPIR	supplemental photographic interpretation report
sqd	squad
sus	suspected
svc	service
SWO	staff weather officer

T

T&A	Transcription and analysis
TAC	tactical
TACC	tactical air control center
TACELINT	tactical electronic intelligence
TACFIRE	tactical fire direction system
TACREP	tactical report
TAI	target area of interest
TCAE	technical control and analysis element
TCC	telecommunications center
TE	tactical exploitation
tech	technical
tfc	traffic
tgting	targeting
tm	team
tms	teams
TOC	tactical operations center
TRADOC	US Army Training and Doctrine Command
TRITAC	Joint Tactical Communications System
TSS	target selection standards
TTY	teletypewriter
TVA	target value analysis

U

UHF	ultra-high frequency
US	United States
USAF	United States Air Force

V

VHF	very high frequency

W

wea	weather
WLR	weapon-locating radar
wpn	weapon
WOC	wing operation center

X

XO	executive officer

REFERENCES

REQUIRED PUBLICATIONS

Required publications are sources that users must read in order to understand or to comply with this publication.

Army Regulations (ARs)

190-30	Military Police Investigations
190-52	Countering Terrorism and Other Major Disruptions on Military Installations
195-5	Evidence Procedures
381-10	US Army Intelligence Activities
381-12	Subversion and Espionage Directed Against US Army (SAEDA)
381-20	US Army Counterintelligence Activities

Field Manuals (FMs)

6-20	Fire Support in Combined Arms Operations
34-1	Intelligence and Electronic Warfare Operations
34-37	Echelons Above Corps Intelligence and Electronic Warfare Operations
34-60	Counterintelligence
34-60A(S)	Counterintelligence Operations (U)
34-80	Brigade and Battalion Intelligence and Electronic Warfare Operations
100-2-2	Soviet Army Specialized Warfare and Rear Support
100-5	Operations
100-15(TEST)	Larger Unit Operations

Miscellaneous Publications

JCS Pub 12, Vol 2	Tactical Command and Control Planning Guidance and Procedures for Joint Operations
DIAM 50-3(0)	Physical Security Standards for Sensitive Compartmented Information Facilities

Standardization Agreements (STANAGs)

3277	Air Reconnaissance Request/Task Form

STANAGs and QSTAGs may be obtained from the Naval Publications and Forms Center (NPFC), 5801 Tabor Avenue, Philadelphia, PA 19120.

COMMAND

Command publications cannot be obtained through Armywide resupply channels. Determine availability by contacting the address shown. Field circulars (FCs) expire three years from the date of publication unless sooner rescinded.

Field Circulars (FCs)

100-20	Low-Intensity Conflict, July 1986, US Army Command and General Staff College, Fort Leavenworth, Kansas 66027-6900

Index

aerial photography, 8-7
agents, 5-16
in place, 5-16
confusion, 5-16
provacative, 5-16
sleeper, 5-17
mass-recruited, 5-17
airborne corps (RC), 7-20
AirLand Battle
close operations, 2-2
deep operations, 2-2
rear operations, 2-1, 5-20
asset tasking, 3-1
attack criteria, 4-6

battlefield coordination element (BCE), 6-11
battlefield deception element (BDE), 6-12
battle planning, 4-8

command and control (C^2), 2-7
assigned, 3-6
attached, 3-6
OPCON, 3-6
organic, 3-6
communications security, 6-18
company headquarters, 7-7, 8-4
corps command post, 2-6
main CP, 2-6
CTOC, 2-6
corps operational concept, 4-0
corps resources, 2-4
corps staff
ASPS, 6-8
CI analysis section, 6-10
CM&D, 3-1, 6-4
CTOC, 2-6
CTOC support element, 3-3, 6-0, 6-4
EW section, 6-11
FSE, 2-5
G2, 2-11
imagery analysis section, 6-10, 8-4
OPSEC staff element, 6-11
processing and reporting section, 6-14
S3, 3-5
SSO, 2-12
terrain team, 6-10
weather team, 6-10
corps support command (COSCOM), 5-20
counterintelligence
defensive source operations (DSO), 7-23
HOIS, 1-3
platoon, 7-4
support to rear operations, 7-23
CTOC telecommunications platoon, 6-19

deception, 2-11, 6-12
deep attack helicopter operations, 2-5
defense special security communications system (DSSCS), A-1
direction finding, 2-15

Echelons above corps intelligence center (EACIC), 2-10
echelon corps and below (ECB), 6-12
electronic warfare, 1-3, 2-11
ECCM, 1-3
ECM, 1-3
deception, 1-3, 2-11
electronic order of battle (EOB), 6-10
ESM, 1-3, 2-11
jamming, 1-3

fire support planning, 4-4
flight tracks, 8-14
fronts, 5-18

ground sensor terminal (GST), 8-3, 8-4
GUARDRAIL, 8-10

intelligence, 2-8
categories, 2-9
operational level of war, 2-10
strategic, 2-8

analysis,
indications and warning, 2-11

intelligence and electronic warfare

agility, 2-1
close operations, 2-2
deep operations, 2-2
depth, 2-1
initiative, 2-0
rear operations, 2-1
syncronization, 2-1

intelligence preparation of the battlefield, 4-11, 5-20, 6-9

area of interest evaluation, 5-22
named areas of interest, 2-15
terrain analysis, 5-23
threat evaluation, 5-20
threat integration, 5-24
weather analysis, 5-23

interrogation

EPW, 7-4
PWI, 2-14, 7-4, 7-3

joint suppression of enemy air defenses (J-SEAD), 4-1

low intensity conflict, 1-4, 5-4

categories, 5-4
definition, 5-4
intelligence requirements, 5-7

master control station (MCS), 6-12

MI battalions

aerial exploitation, 2-14, 8-1
operations, 2-14, 6-0
tactical exploitation, 2-14, 7-0

MI brigade, 2-13

MI companies

aerial electronic warfare, 8-4
aerial surveillance company, 8-3
CI interrogation company. 7-2, 7-12, 7-17
electronic warfare company, 7-6, 7-14, 7-18
headquarters, headquarters and service company, 6-1, 7-1
long-range surveillance, 7-8
operations company, 6-2

national command authority (NCA), 2-8

Noncommunications intercept, 7-8

operational manuever group (OMG), 5-19

operations and sensor systems, 8-7

aerial photography, 8-7
GUARDRAIL, 8-10
MOHAWK, 8-7
QUICKLOOK, 8-9
sidelooking airborne radar, 8-9

operations center, 3-3

CTOC support element, 3-3
TCAE, 3-4

operations security measures, 2-11, 5-1

order of battle files, 6-9

platoons

C-E, 7-2
CI, 7-4
CTOC TCC, 6-19
CTOC TTY, 6-19
flight, 8-4, 8-5
mechanical maintenance, 7-2
noncommunications intercept, 7-8
operations, 8-6
service, 8-2, 8-4, 8-6
service support, 7-7
support and maintenance, 6-18
TCAE TCC, 6-19
TCAE TTY, 6-19
VHF ECM, 7-8
voice collection, 7-8

principles of war, 3-7

economy of force, 3-9
objective, 3-9
security, 3-9
simplicity, 3-9
unity of command, 3-9

processing, 6-14

IPB, 4-13, 6-9
OB files, 6-9
SITMAPs, 6-9
target folders, 6-9

QUICKLOOK, 8-9

radioelectronic combat (REC), 1-4

reconnaissance, surveillance, and target acquisition (RSTA) 2-12

reports

imagery, 8-17
in-flight, 8-15
IPIR, 8-17
mission (MISREP), 8-17
reconnaissance exploitation (RECCEXREP), 8-16
resource status (RSR), 6-13
SUPIR, 8-17

SCIF security squad, 6-3

sections

analysis and reporting, 8-6
C-E-IEW maintenance, 7-7
CI analysis, 6-10
collection and direction finding, 8-6
communications intelligence aircraft, 8-5
corps PWI operations, 7-3
document exploitation, 7-14
EW section, 6-11
food service, 7-2, 8-2
imagery analysis, 6-10, 8-4
noncommunications electronic intelligence processing, 8-6
noncommunications intercept operations, 7-8
operations and processing, 7-14
processing and reporting, 6-14
reports and analysis, 7-7
SIGINT EW exploitation, 7-14
SIGINT integration, 6-16
tactical ELINT, 6-17
technical intelligence, 7-12

sensitive compartmented information facility (SCIF), 2-6

signal security, 2-12

EEFI, 2-12

sidelooking airborne radar, 2-5

situation development, 1-2, 2-10

situation maps, 6-9

special operations, 5-1

desert, 5-2
POL, 5-2
jungle, 5-2
mountain, 5-3
LIC, 5-4
mission, 5-4
LOS, 5-1
river crossing, 5-2
winter, 5-3

specific information requirements (SIR), 5-7, 6-6

suppression of enemy air defenses (SEAD), 2-6, 4-17

suspected targets, 4-13

tactical air control center (TACC), 4-5

tactical fire direction system (TACFIRE), 2-6

target categories, 4-13

target defined, 4-13

target development, 1-3, 2-11

attack guidance matrix, 4-15
high payoff target list, 4-11, 4-12
high payoff targets, 4-11, 6-14
high value target list, 4-11, 4-12
high value targets, 2-5, 4-11
target areas of interest (TAI), 2-11
target selection standards, 4-13
target value analysis, 4-11

target engagement, 4-4

target folders, 6-9

targeting process, 2-3, 4-10

assessment, 4-11, 4-17
attack, 4-11, 4-16
focus, 4-11
information processing, 4-11, 4-13
sensor tasking, 4-11, 4-12

task organization, 3-7

combat task organizing, 3-7

tasking

assets, 3-3
missions,
DS, 3-7

GS, 3-7
GS reinforcing, 3-7
reinforcing, 3-7
teams
cryptanalysis, 6-16
terrain, 6-10
traffic analysis, 6-15
USAF weather, 6-10
technical control and analysis element (TCAE), 3-4, 3-5, 6-0, 6-12
telecommunications center, 6-19, 8-2
terrorism, 5-9
antiterrorism, 5-10
counterterrorism, 5-10
special warfare operations, 5-14
threat level I, 5-16
threat level II, 5-17
threat level III, 5-18

By Order of the Secretary of the Army:

CARL E. VUONO
General, United States Army
Chief of Staff

Official:

R. L. DILWORTH
Brigadier General, United States Army
The Adjutant General

DISTRIBUTION:

Active Army, USAR, and ARNG: To be distributed in accordance with DA Form 12-11A, Requirements for Corps I EW Ops (Qty rqr block no. 1121); MI Group, G EW I (Corps) (Qty rqr block no. 480); MI Bn, C EW I (Ops/Corps) (Qty rqr block no. 481); MI Bn, C EW I (Aerial Exploitation/Corps) (Qty rqr block no. 482); and MI Bn, C EW I Tactical Exploitation/Corps (Qty rqr block no. 1120).

18140

☆U.S. GOVERNMENT PRINTING OFFICE: 2000-461-711/21187