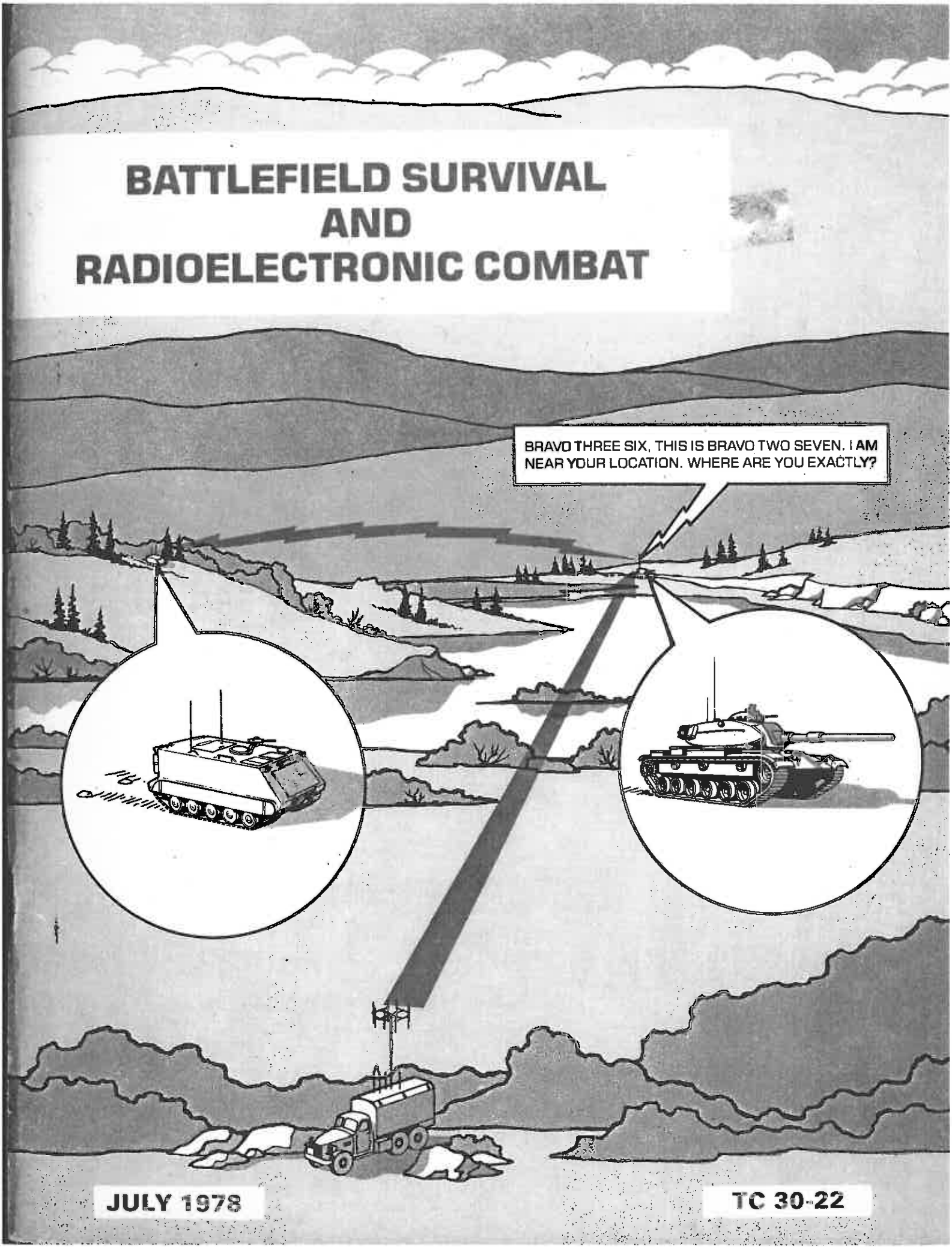
BATTLEFIELD SURVIVAL AND RADIOELECTRONIC COMBAT



JULY 1978

TC 30-22

Training Circular
No. 30-22

TC 30-22

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 7 July 1978

BATTLEFIELD SURVIVAL AND RADIOELECTRONIC COMBAT

CONTENTS

THIS TRAINING CIRCULAR WAS PREPARED BY HQ TRADOC, DCSORI. USERS ARE INVITED TO SEND COMMENTS AND SUGGESTED IMPROVEMENTS ON DA FORM 2028 (RECOMMENDED CHANGES TO PUBLICATIONS) TO HQ TRADOC, ATTN: DCSORI, FT MONROE, VA 23651

PREFACE

The purpose of this training circular is to provide information about the radioelectronic combat threat. The enemy integrates electronic intercept and direction-finding (DF) with suppressive fires and electronic jamming to deprive us of the full use of our tactical electronic emitters. This training circular explains how the direction-finding component of enemy radioelectronic combat is used, and how specific protective techniques may be applied to prevent United States Army units from becoming enemy electronic targets.

The word "he" or "his" in this publication is intended to include both the masculine and feminine genders and any exception to this will be so noted.

INTRODUCTION

The dependence that US forces place on communication will be more evident on the next battlefield than ever before. This reliance is primarily due to new developments in communication technology that continue to add to the overall effectiveness of our communication system.

However, as US history has taught us, we assume that the enemy knows our strong points, and that he will make every effort to hit us in our most critical areas. On the modern battlefield, our communication system will serve as the keystone upon which the command and control of our forces will depend. The enemy will try to destroy or disrupt at least 50 percent of our communication systems by using radioelectronic combat.

CHAPTER I
THE RADIOELECTRONIC COMBAT THREAT

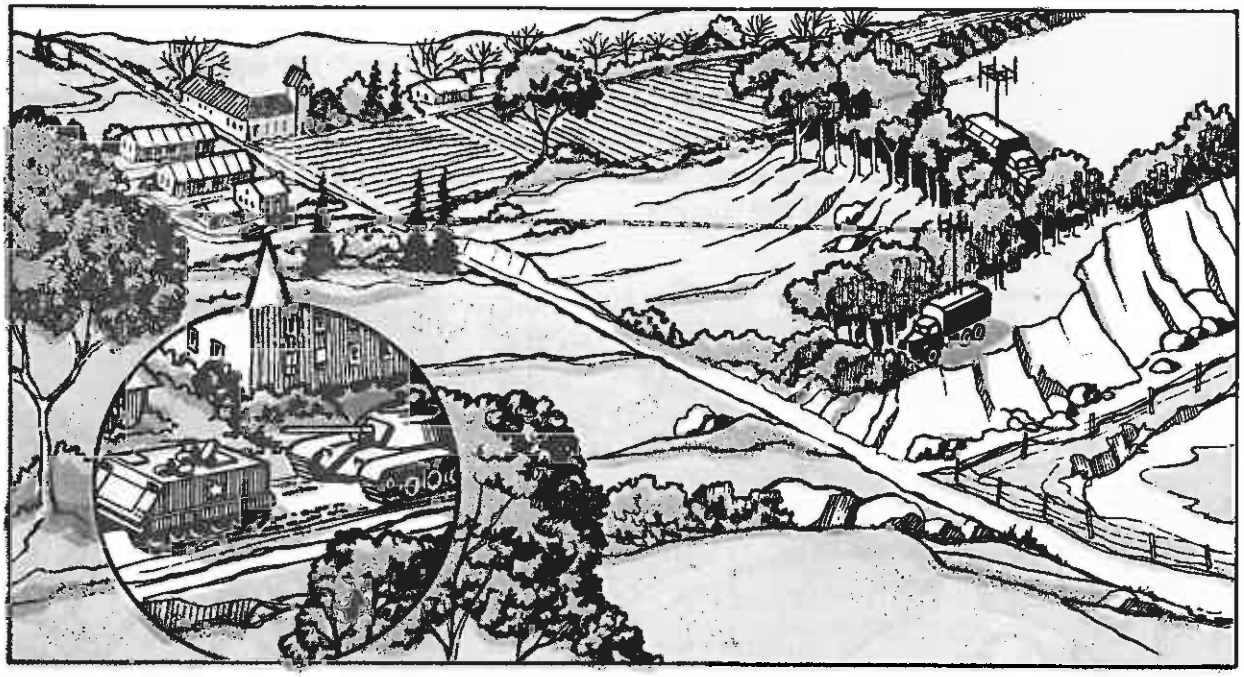
Radioelectronic combat is a term used by Soviet model forces to describe the integration of signals intelligence, intensive jamming, deception, and suppressive fires to deprive their adversary of command and control in combat.

To accomplish this objective, the enemy uses direction-finding as a method of determining the approximate relative direction or bearing of a transmitting antenna (radio or radar) from one, two, or, more commonly, three or more direction-finding positions.

A line bearing is determined by measuring the direction of arrival of an emitter's radio waves at the DF position.

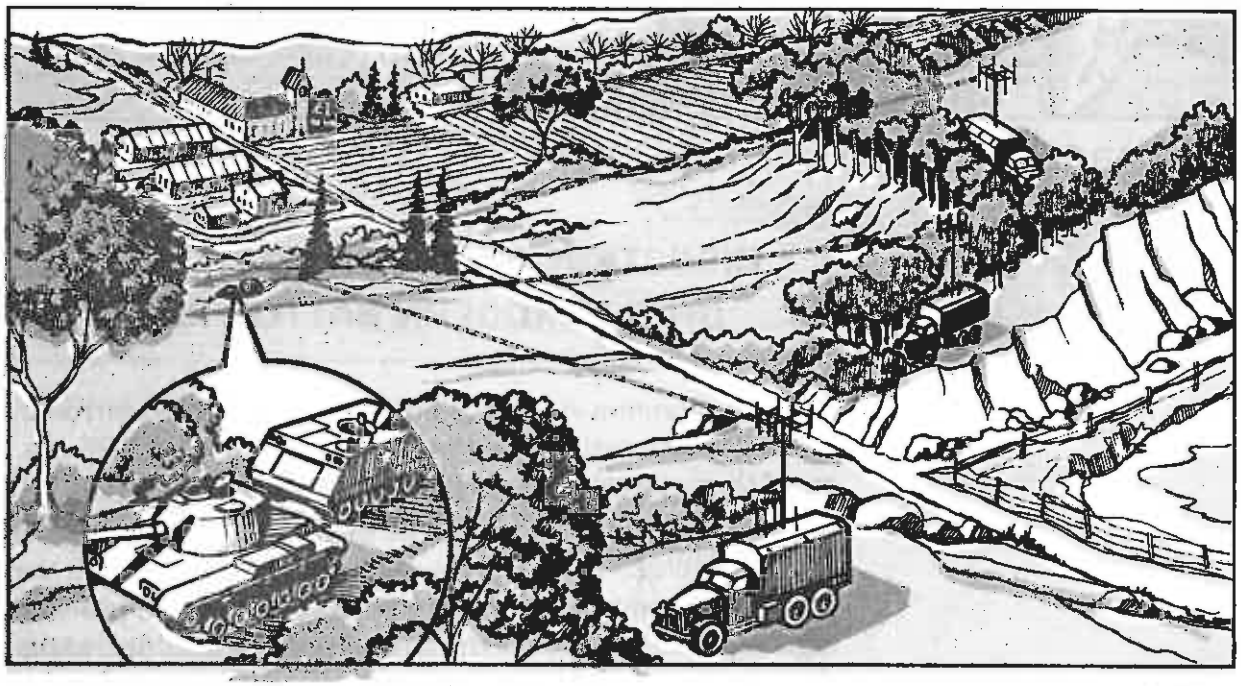
A BEARING

One radio direction-finding (RDF) bearing provides *approximate* direction, but not distance.



Two RDF bearings usually provide *approximate* direction and *some concept* of distance.

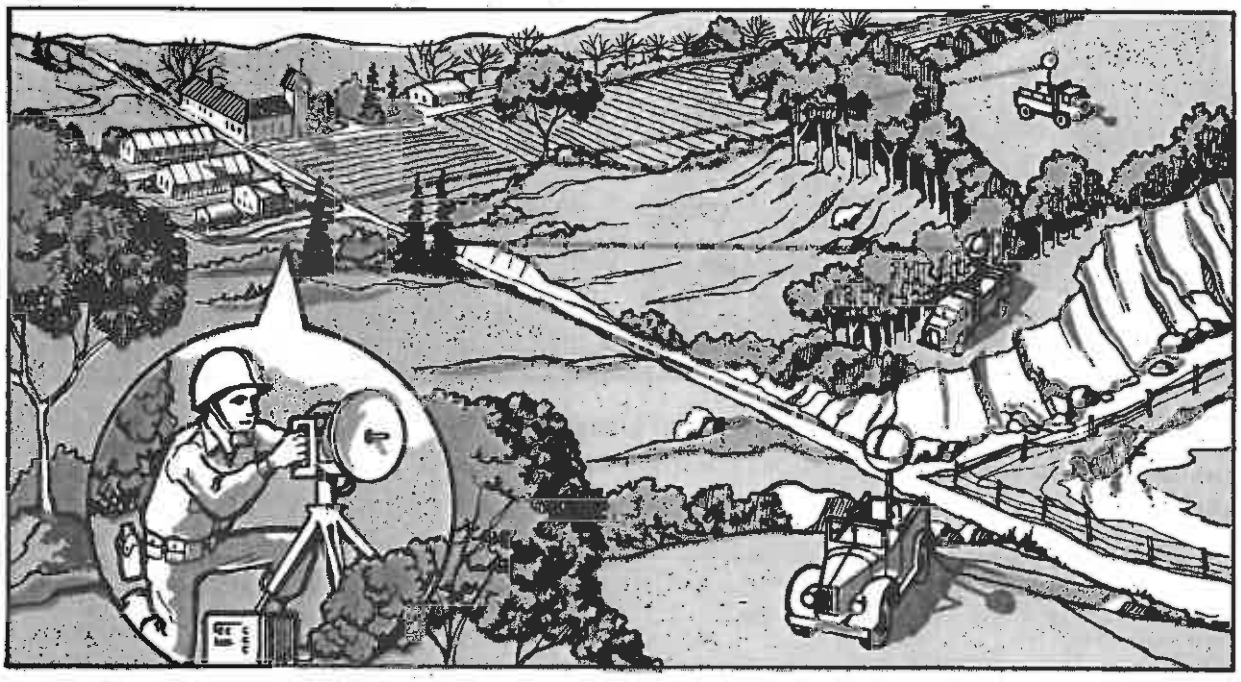
A CUT



Three or more RDF bearings are referred to as a fix. A fix usually provides sufficient direction and distance information to determine an *approximate* location.

A FIX

The same principle applies to locating radar equipment. In this case, the enemy uses DF equipment that is compatible with radar signals. Radars may be located more accurately than radios due to their signal characteristics, often within a triangle or circle having a radius of 50 to 200 meters.



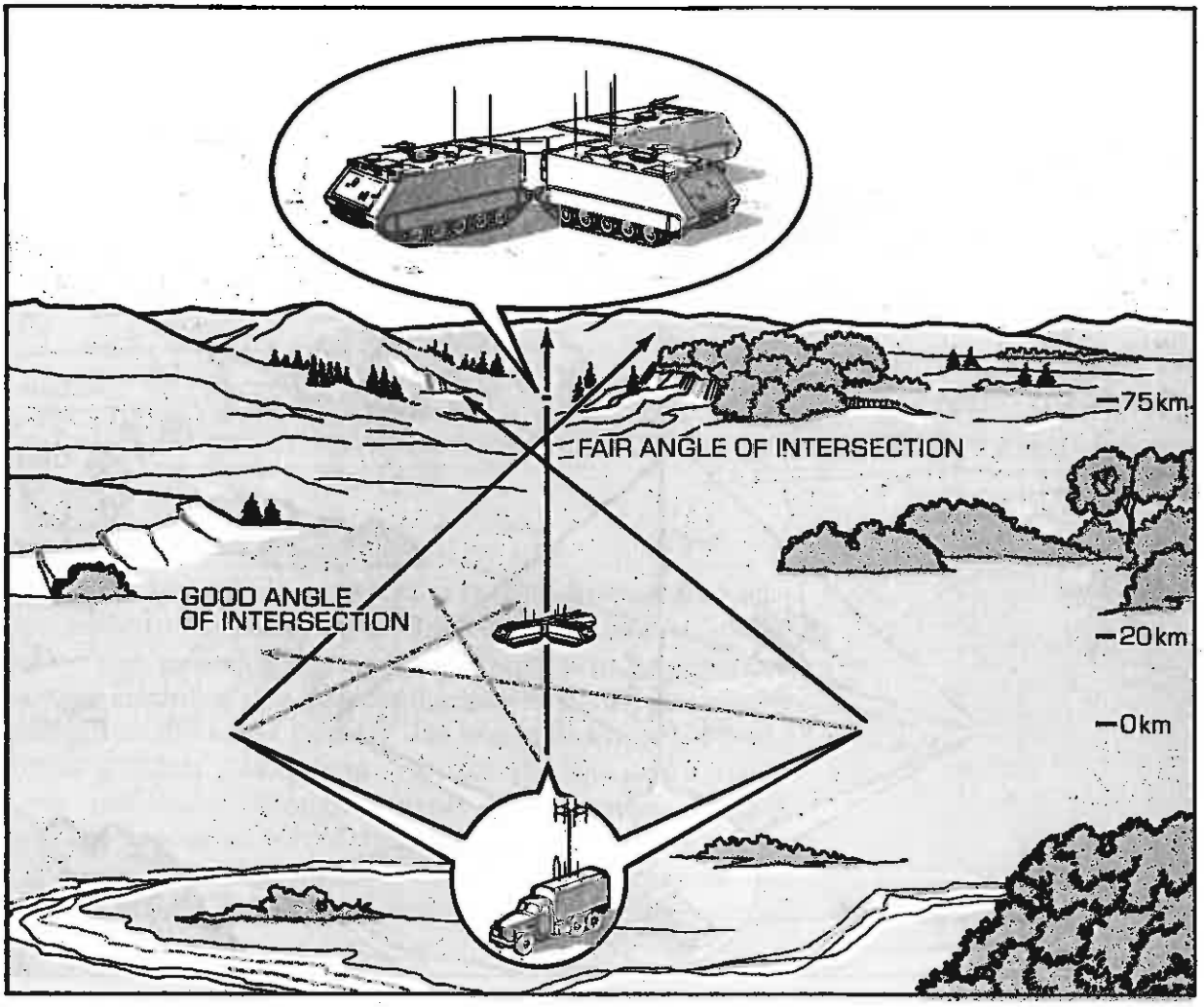
A RADAR FIX

DIRECTION-FINDING AND TACTICS ON THE MODERN BATTLEFIELD

Radio direction-finding is but one of the radioelectronic combat assets available to the enemy commander. RDF can assist the commander in making his tactical decisions by locating for him command posts, storage areas, and other types of important targets.

The RDF ground stations are positioned so as to provide high angle intersection of the lines of bearing thus providing a better fix area. The RDF stations may be located along a straight or concave baseline. These arrangements provide

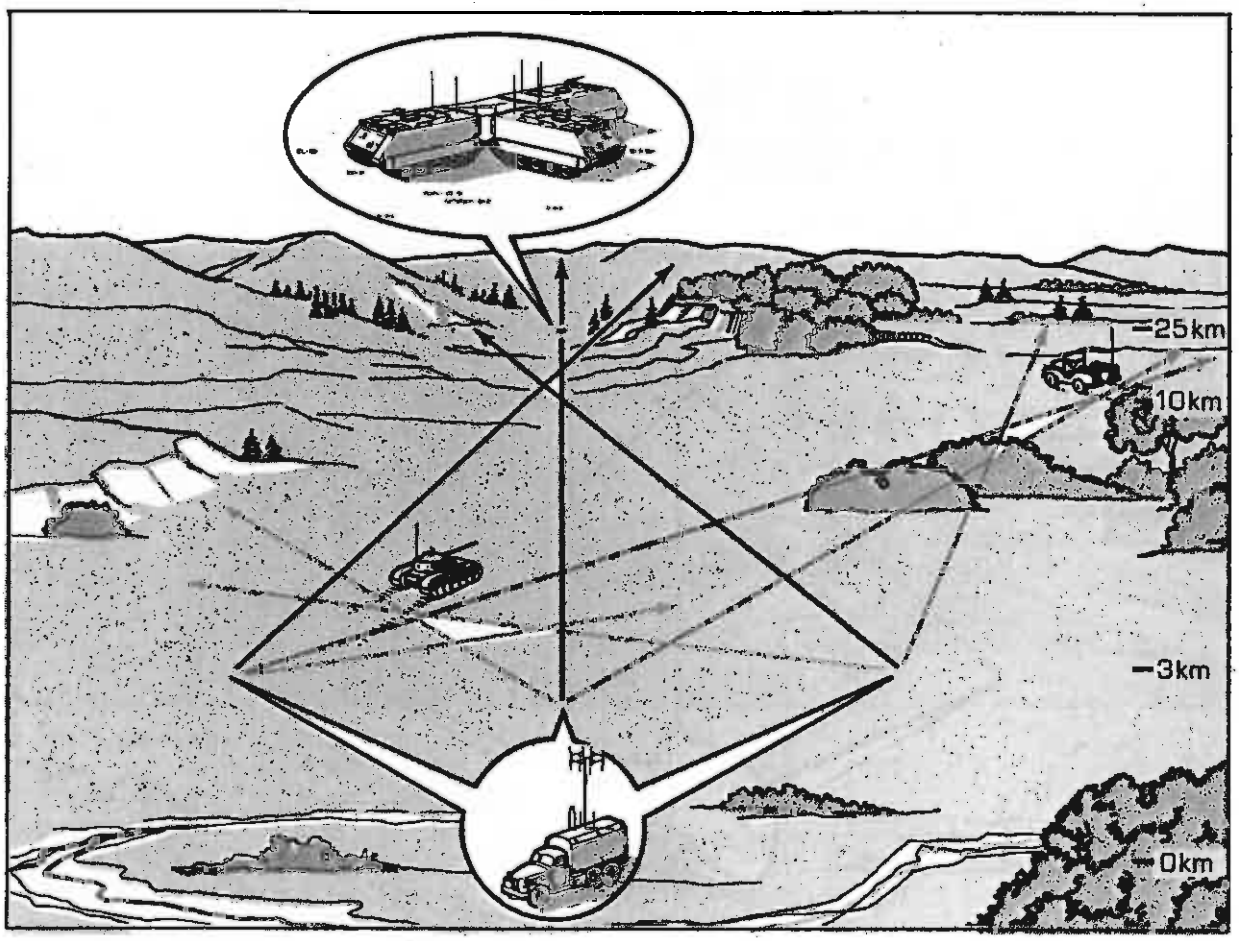
the best azimuth angles of intersection at short distances (within 20km) and fair angles of intersection at longer distances (75 km).



CONCAVE BASE LINE

In order to obtain the best bearings over a wide area, the enemy commander might locate his RDF stations in a triangular or quadrilateral base line pattern. These patterns provide fair angles of intersection on most transmitters in the area of coverage, but do not provide adequate angles of intersection on transmitters located near the forward edge of the battle area (FEBA).

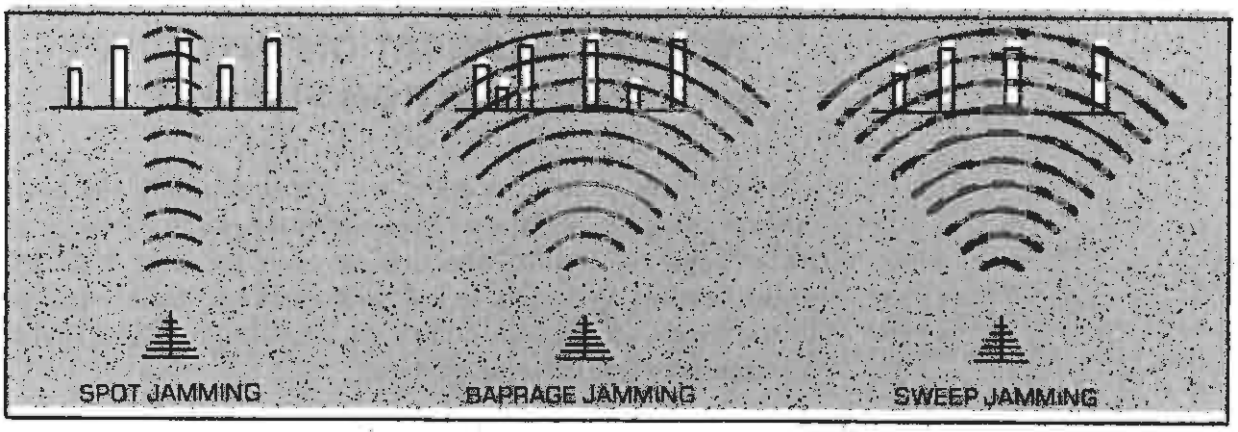
The pattern arrangement of RDF positions may reveal where the enemy commander intends to concentrate his efforts in an attack. Surveillance techniques which detect these employment patterns should be considered along with other indicators in determining enemy intentions.



TRIANGULAR BASE LINE

Efficient jamming depends on direction-finding as an analytical aid to select and generally locate target transmitters. The receiving element of the target transmitter is then selected for jamming, and the jammer's antenna is oriented

to the location indicated by RDF. ***Enemy doctrine establishes a requirement to jam US Army command, control, and weapon system communications when they cannot be destroyed by suppressive artillery fires.*** The three main types of jamming are illustrated below.



TYPES OF JAMMING

Spot jamming is used to jam certain individual frequencies without jamming other adjacent frequencies. It requires one jamming signal per frequency to be jammed. Barrage jamming allows several adjacent frequencies to be jammed at the same time by one high power, broad band jamming signal. Sweep jamming uses one signal and moves it up and down through a band of frequencies. This is basically a combination of spot and barrage jamming in that it allows several frequencies to be jammed in sequence, but all the jamming power is concentrated on one frequency at any one time.

Jamming can also support DF when used to block communication for a prolonged period. This causes the target station to create a backlog of traffic. When the jamming is terminated, the target station may then transmit continuously over a period to relieve the backlog. Prolonged transmission in these cases enables DF to obtain numerous bearings and thereby refine the fix area.

Enemy forces jam very high frequency (VHF), but they also depend on VHF for command and control of their own weapon systems. By using VHF directional antennas, enemy forces are able to control this problem.

They practice this technique in training. Enemy forces use VHF and ultra high frequency (UHF) multichannel communications at selected key levels. They also employ high frequency (HF) tactical communications as a back-up communication system down to tank platoon level.

NONCOMMUNICATION INTERCEPT AND DIRECTION-FINDING

A US Army division is allocated approximately 400 noncommunication emitters. These include such devices as radar sets, navigation beacons, aircraft landing systems, identification as friend or foe (IFF) devices, drone control units, fuzes, electro-optic devices, searchlights, and meteorological data-gathering systems.

Although these systems vary widely in their electronic characteristics and in their concept of deployment, in most cases they radiate electromagnetic energy into potentially hostile territory where it is vulnerable to intercept and analysis by enemy signals intelligence units.

INTERCEPT OF EMISSIONS

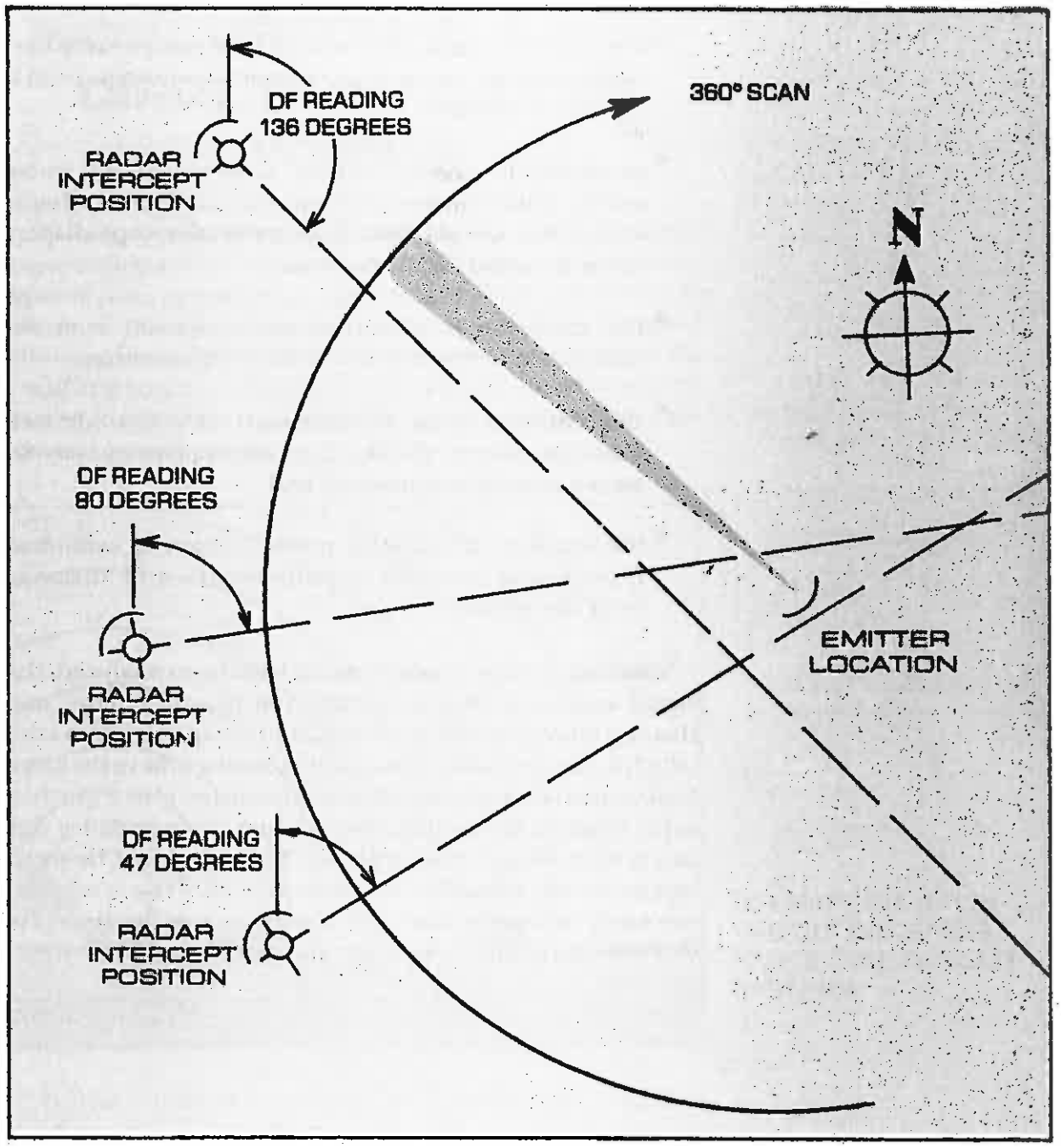
The two major factors considered in determining the interceptability of various noncommunication emitters are signal strength and the amount of operating time. Powerful radar signals can be intercepted at distances in excess of five times their operational range. That is to say, a radar with a maximum range of 5 kilometers searching for targets would be vulnerable to intercept at distances in excess of 25 kilometers. This is because the radar intercept operator intercepts the strong emitted signal and is not required to receive the weak echo signals required by the radar operator.

Early warning and surveillance radars must operate for prolonged periods of time to accomplish their surveillance mission, and are, therefore, extremely vulnerable to intercept.

Fire control and guidance radars operate at brief or intermittent periods, causing them to be less susceptible to intercept. However, regardless of the duration of the operating period, all radiations are vulnerable to intercept.

EMITTER LOCATION

Because of the sharpness of radar waves, highly directional antennas are able to provide very accurate direction-finding information. Direction-finding from two or more radar direction finders permits a radar emitter to be located as shown below.



EMITTER LOCATION USING DIRECTION-FINDING TECHNIQUES

SIGNAL ANALYSIS

Important signal information is contained in the technical characteristics of the noncommunication emitter signal and its direction of arrival. Signal analysis can reveal the type and function of the emitter; the direction of arrival information can permit location of the emitter. The basic characteristics of the emitted signal are:

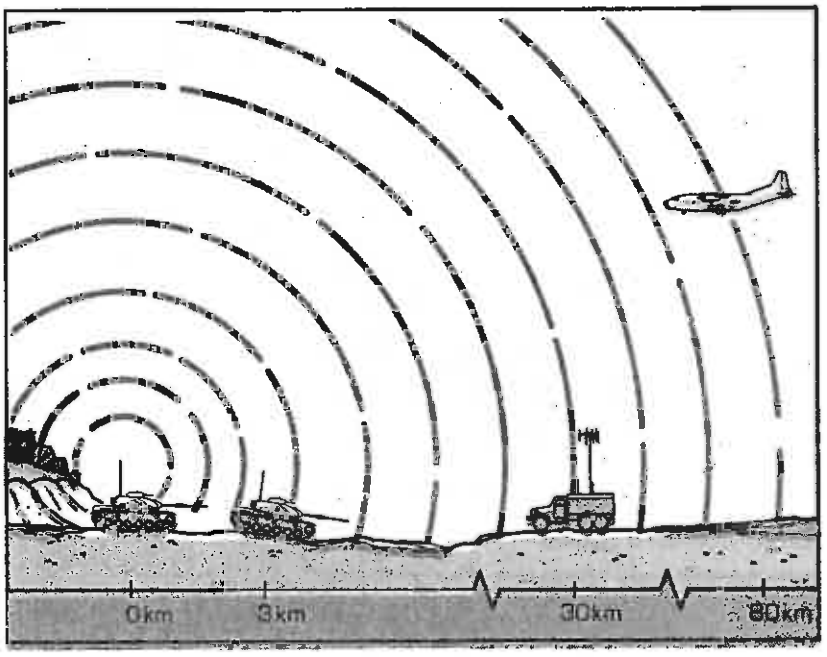
- the carrier frequency, which is obtained from the tuning dial of the receiver or, more accurately, from a frequency counter;
- modulation characteristics, which include pulse width, pulse recurrence frequency, and pulse shape, and which are obtained from an oscilloscope display of the detected video waveform;
- the direction of arrival, which is derived from the orientation of the directional receiving antennas;
- the antenna scan measurement, which is derived from the pattern displayed on an oscilloscope or observed audibly in a headset; and
- the amount of radiated power, which is estimated from signal strength measurements and distance from the emitter.

When all of these characteristics have been analyzed, the signal analyst is able to identify the type of emitter and thereby know the control function or weapon system with which it is associated. No two friendly emitters have the identical combination of the characteristics listed above. Further, some emitters have unique or unusual characteristics due to a system idiosyncrasy or defect. Because of this, they can be specifically identified or "fingerprinted." These emitters can easily be tracked from one location to another, thus providing valuable and reliable intelligence to the enemy commander.

CHAPTER II

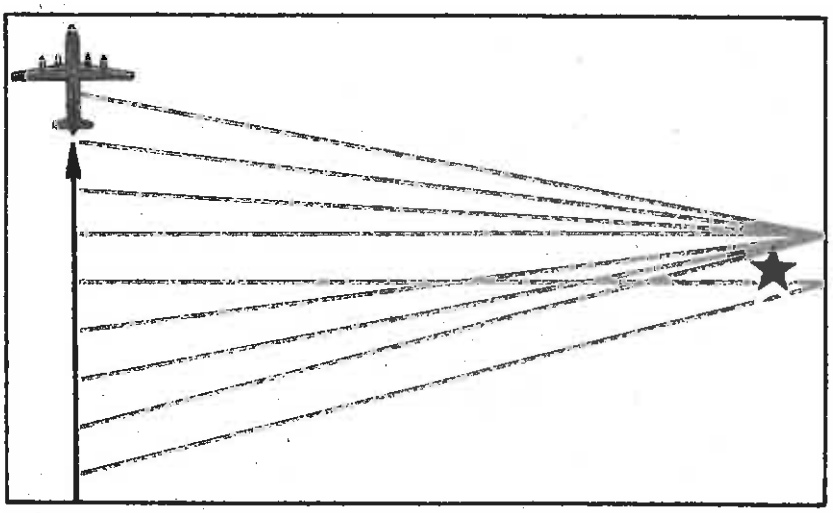
HOW AIRBORNE RADIO DIRECTION-FINDING WORKS

Airborne radio direction-finding (ARDF) is a radio direction-finding system mounted in a helicopter or a fixed-wing aircraft. The principles of operation of ARDF are similar to those of ground vehicle radio direction-finding. However, the use of an airborne platform increases the elevation of the receiving antenna, thereby enhancing the ability of the receiver to intercept radio signals at longer distances than ground based systems.



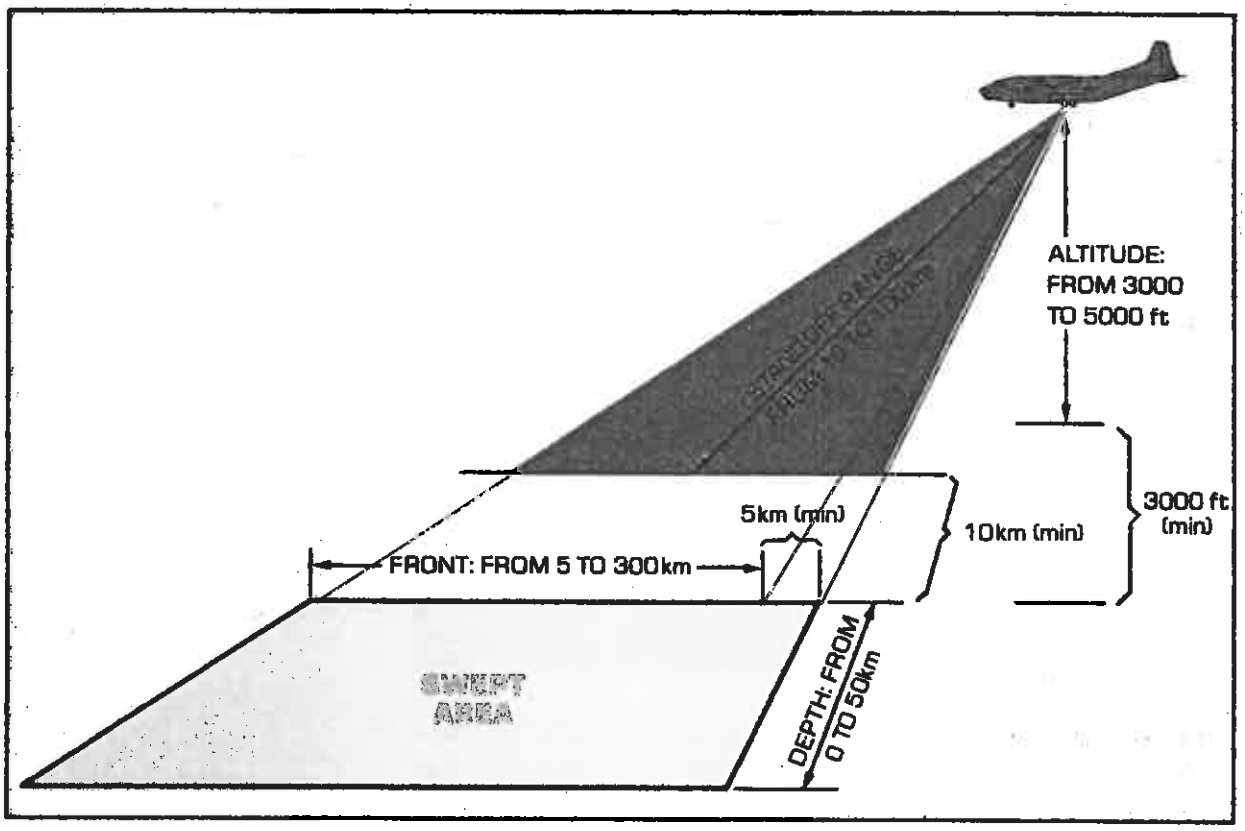
AIRCRAFT ELEVATION GREATLY INCREASES RANGE OVER GROUND SYSTEMS

Further, ARDF is not subject to as many effects of propagation error as is ground station RDF. An aircraft also has the advantage of taking a series of many successive bearings along its flight path.



AIRBORNE RADIO DIRECTION-FINDING FIX

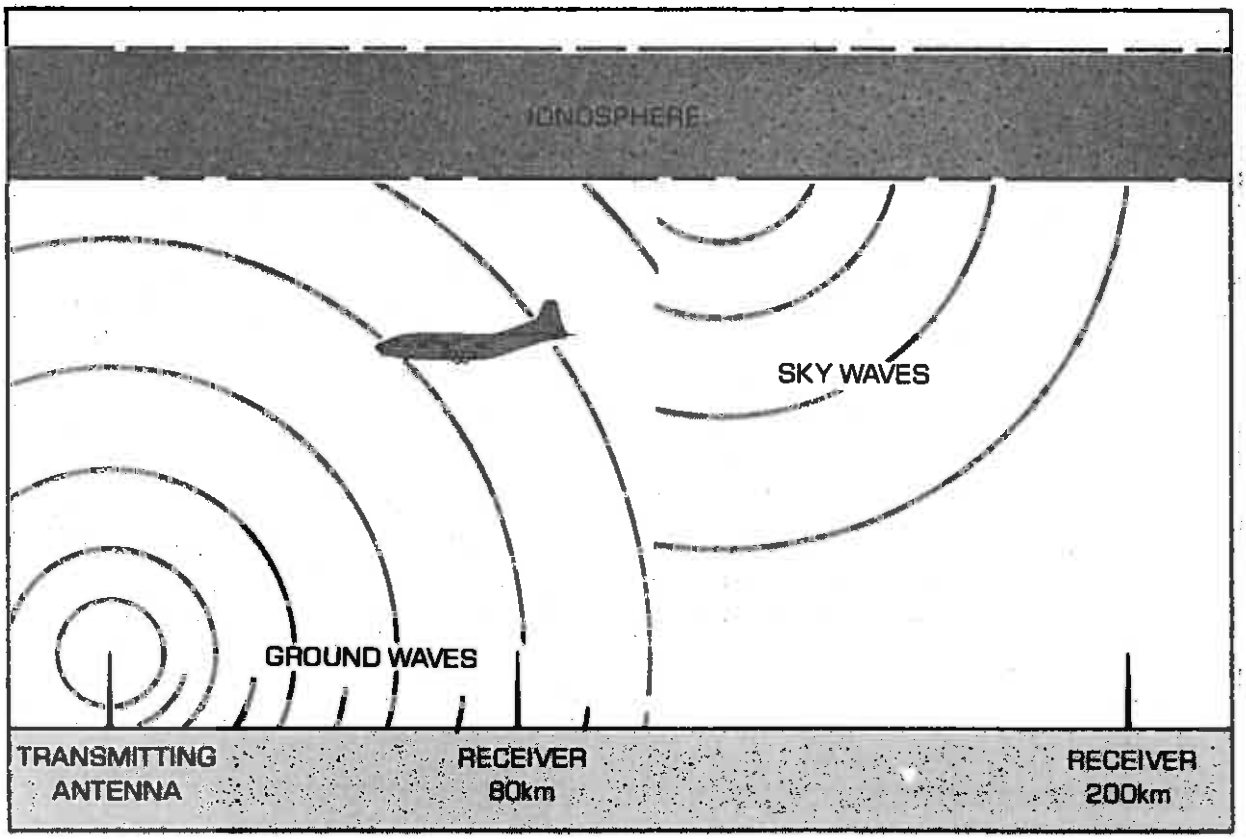
More azimuth readings and better accuracy are possible with ARDF, but the aircraft is required to remain on track long enough to acquire a wide base for the DF bearings. If the aircraft is diverted, as by antiaircraft fire, for example, the bearings will be distorted.



At ranges of 10 to 100 kilometers, and at altitudes of 3,000 to 5,000 feet, an ARDF aircraft can sweep a front of 5 to 300 kilometers at depths up to 50 kilometers. When an ARDF aircraft is kept 30 kilometers or more from the FEBA by suppressive fire, the ARDF target area may be larger. However, when the area is larger, the number of VHF target emitters on the same frequency within the area may be too large to effectively distinguish one from another.

HIGH FREQUENCY ARDF

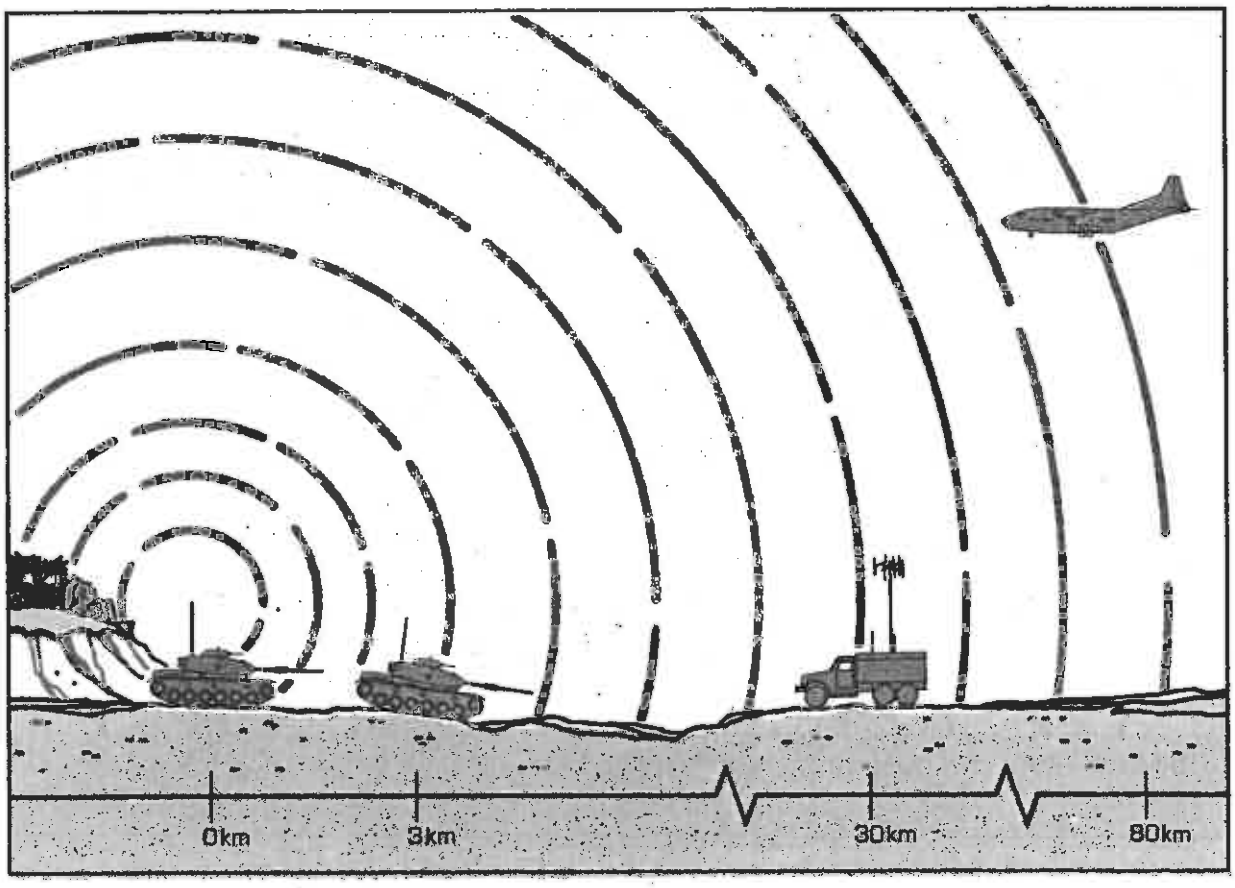
A simple radio transmitting antenna radiates waves in many directions, although the strength of the waves may be greater in certain directions and at certain angles above the ground. Both the sky wave and ground wave may be used in HF communications. Long-distance HF radio transmission operates principally by means of sky waves being refracted from the ionosphere to a receiving antenna on the earth's surface. High frequency airborne DF operations are conducted against these intentional and unintentional sky waves *prior to refraction.*



In short-distance HF radio transmissions, the ground wave rather than the sky wave is the principal means of communication. However, airborne DF is conducted against the unintentional by-product (sky wave) of this type of transmission. The distance from the transmitter at which these waves can be received by ARDF is affected by transmitter power output, type of antenna, terrain, and operating frequency. A typical distance is 80 kilometers. Although frequency affects wave propagation, the manner in which airborne DF operations are conducted against HF and VHF targets remains unchanged.

VERY HIGH FREQUENCY ARDF

The energy from a VHF transmitting antenna is normally radiated as an omnidirectional wave through the atmosphere to a receiving antenna located within line-of-sight. Airborne equipment, because of greater elevation, is capable of intercepting this line-of-sight transmission at greater distances than ground-based interceptors, thus enhancing its operations at extended ranges.



In conclusion, airborne radio direction-finding provides the enemy with approximate location of emitters associated with US forces for subsequent destruction, deception, or continued observation for electronic warfare intelligence exploitation.

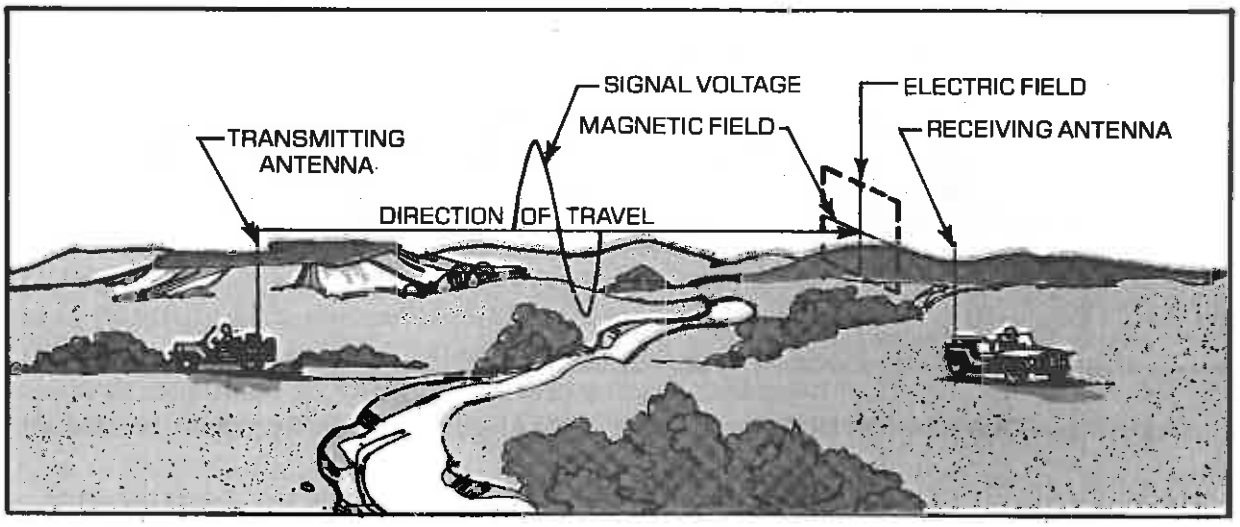
CHAPTER III
RADIO WAVES

The ability of a direction-finding station to intercept and then determine a bearing on a target transmitter depends on its ability to receive a "usable" signal. A usable signal depends on the characteristics of radio waves. There are two principal ways in which radio waves travel from the transmitter to a receiver or direction-finder: by means of the ground wave, which spreads directly from transmitter to receiver through or just above the soil or sea, and by means of the sky wave, which travels up to the electronically conducting layers in the earth's upper atmosphere and then is reflected back by them to earth.

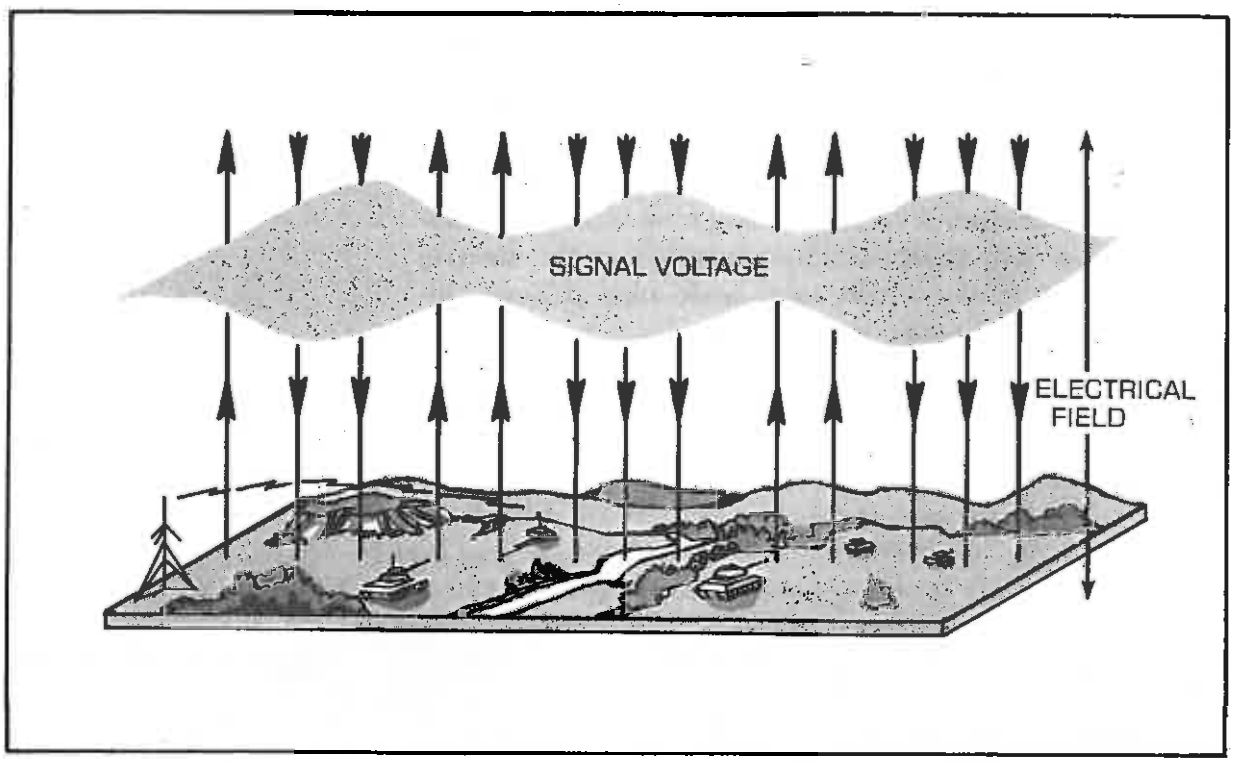
Long-distance (600 kilometers+), high frequency (3 to 30 MHz) radio transmission takes place principally by means of the sky wave. Short-distance high frequency transmission (50 kilometers) uses the ground wave. Tactical FM communications, like the AN/PRC-77, use VHF. Very high frequency (30 to 300 MHz), often called tactical FM communications, is a radio, line-of-sight, short-distance (40 to 80 kilometers) radio transmission method. Both the AN/PRC-77 and the AN/VRC-46 series radios use a portion of the VHF spectrum (30 to 76 MHz). The range of the VHF ground wave depends on the unobstructed line-of-sight distance from the transmitting to the receiving antenna, the height and type of the antennas, and the effective power output of the transmitter. Enemy direction-finding can be restricted by controlling the direction and power of our radio's ground wave. Use the lowest power necessary to communicate.

ANTENNA POLARIZATION AND DIRECTIVITY

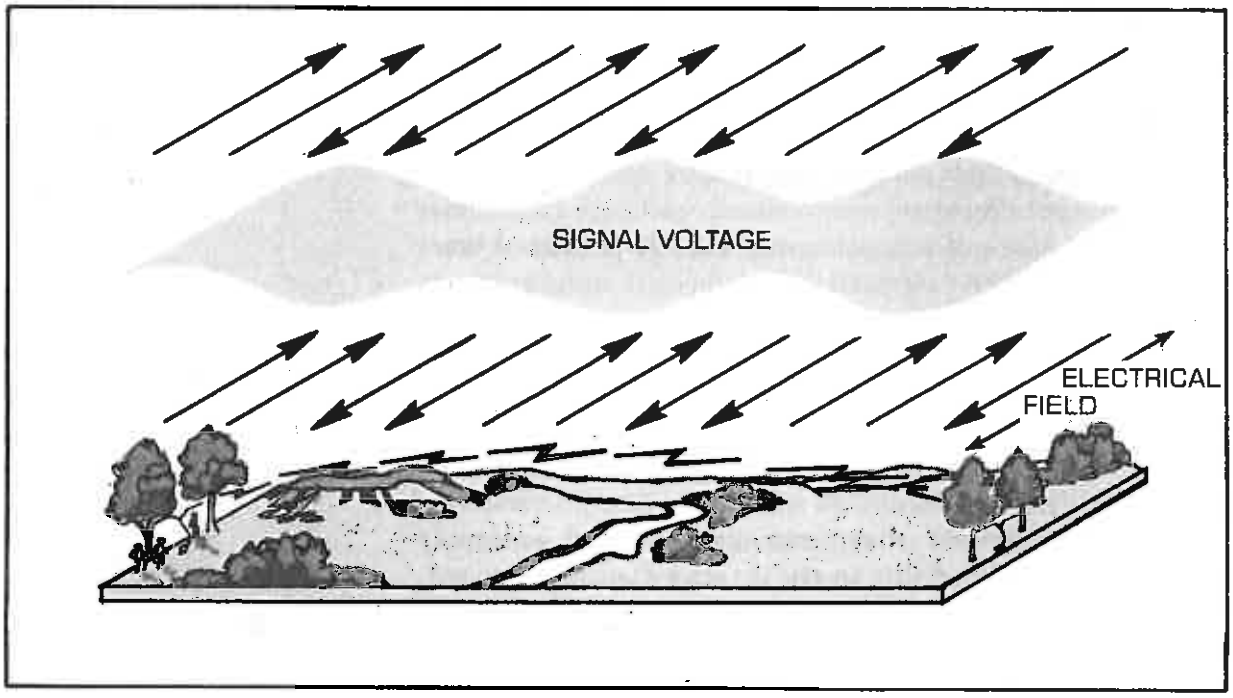
When power is delivered to an antenna, a radiation field is established which travels from the transmitting antenna into space and thence to a receiving antenna. The radiation field has two components, referred to as the electric and magnetic fields, which form a definite pattern depending on the type of antenna used.



Polarization of a radiated wave is determined by the direction of the lines of force making up the electric field. Lines of force at right angles to the earth are called *vertically polarized*; lines which are parallel to the earth are called *horizontally polarized.* Vertically polarized antennas are used for efficient reception of vertically polarized lines of force; similarly, horizontally polarized antennas are used for efficient reception of horizontally polarized lines of force. Commanders at every echelon should understand how to use vertically and horizontally polarized antennas to their best advantage. The unit communications-electronics (CE) officer should be consulted with regard to the proper use of all antennas. The commander needs to understand that vertically polarized antennas provide the best flexibility in the attack when rapid movement detracts from enemy DF. When transmitting in heavily wooded areas and in many defensive situations, horizontally polarized antennas provide the best security and longer range.



VERTICAL POLARIZATION USING VERTICALLY POLARIZED, OMNIDIRECTIONAL ANTENNAS



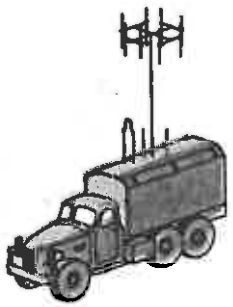
HORIZONTAL POLARIZATION USING HORIZONTALLY POLARIZED ANTENNAS

Either vertically or horizontally polarized antennas may be used with VHF radios. Vertically polarized antennas, such as whips, are more common for military communications because they produce an omnidirectional signal (radiating in 360 degrees) and, hence, are very versatile. However, omnidirectional signals are more vulnerable to intercept and DF by the enemy. Horizontally polarized antennas, on the other hand, are more directional. Using horizontally polarized antennas reduces the vulnerability to intercept and direction finding because the Adcock RDF antenna system used by the enemy is more effective against vertically polarized signals. The horizontally polarized signal will create bearing error in the Adcock antenna system. Both vertically and horizontally polarized antennas can produce dead areas called nulls — zero signal — which can be pointed toward the enemy when steerable directional antennas are used. This also will reduce the vulnerability of radio emitters to intercept and direction finding. Vertically polarized VHF signals are also stronger at 30 to 50 MHz with antenna heights under 10 feet. Above 50 MHz there is no practical difference between the signal strength produced by vertically or horizontally polarized antennas.

Various types of directional antenna systems can be used in RDF. Two of the more common types, the Adcock and the loop, are discussed below.

THE ADCOCK RDF ANTENNA

The Adcock type RDF antenna used by the enemy usually consists of two to eight spaced vertical antennas connected in opposition. There are other variations, but the illustration shown to the right is typical. It is most efficient against the vertically polarized component of an incoming radio wave. The advantage to the Adcock antenna is that it is especially reliable for VHF signals at a point beyond strong ground wave range — an area to the rear of the FEBA, for example.

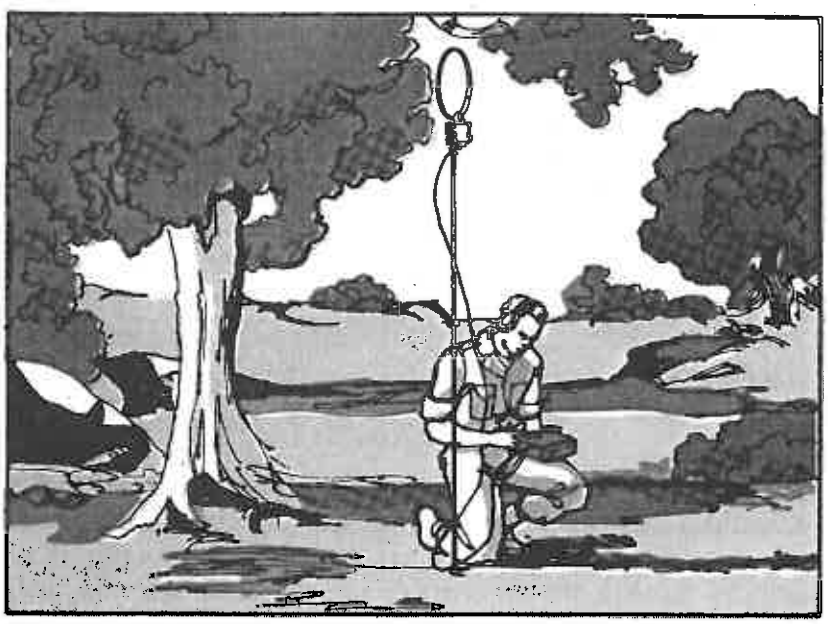


As a result, when the vertically polarized component of a radio wave predominates, as is now the case with US Army tactical communications using omnidirectional antennas, the Adcock antenna is very effective and has little,

if any, polarization error. *Its chief weakness is its limited effectiveness in detecting horizontally polarized antennas.* In addition, the Adcock antenna and its connecting cables are comparatively complicated to adjust. Good calibration of the Adcock at a new site is very difficult to obtain and is seriously affected by changing weather conditions. Nevertheless, the Adcock-type antenna remains more than adequate for enemy forces so long as the US Army relies heavily on vertically polarized, omnidirectional, VHF antennas for tactical communications.

LOOP ANTENNAS

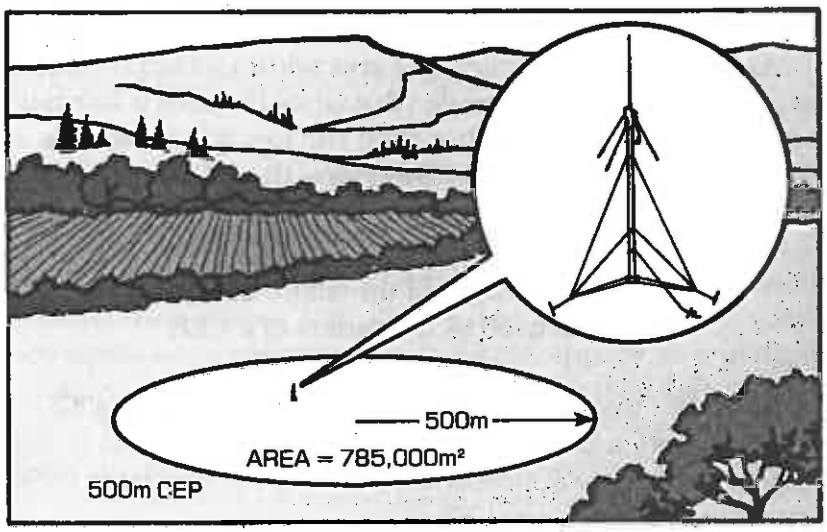
Enemy forces may also use spaced loop, rotatable loop, and other type loop tactical VHF direction-finding antennas. Like the Adcock, the spaced loop is a vertically polarized antenna. It consists of two parallel loops fixed coaxially to the ends of a boom which may be rotated. Several variations are available and RDF positions of this type may be mobile. The spaced loop antenna is not very suitable for tactical conditions. It requires considerable time to install and calibrate, has poor sensitivity, and bearing ambiguity is difficult to discern. As a result, its accuracy is limited. However, other HF and VHF loop antennas do have tactical application.



CHAPTER IV
TARGET LOCATION AND CEP

Direction-finding accuracy is mostly determined by the power and antenna directivity of the target transmitter, by electromagnetic influences which affect radio wave propagation, and by the capability of direction-finding equipment and operations. Because rather complicated mathematical formulas are applied to determine the effect of these influences, RDF accuracy was previously expressed for tactical use, with respect to rules of probability and standard deviation, as an equivalent circular error probability (CEP).

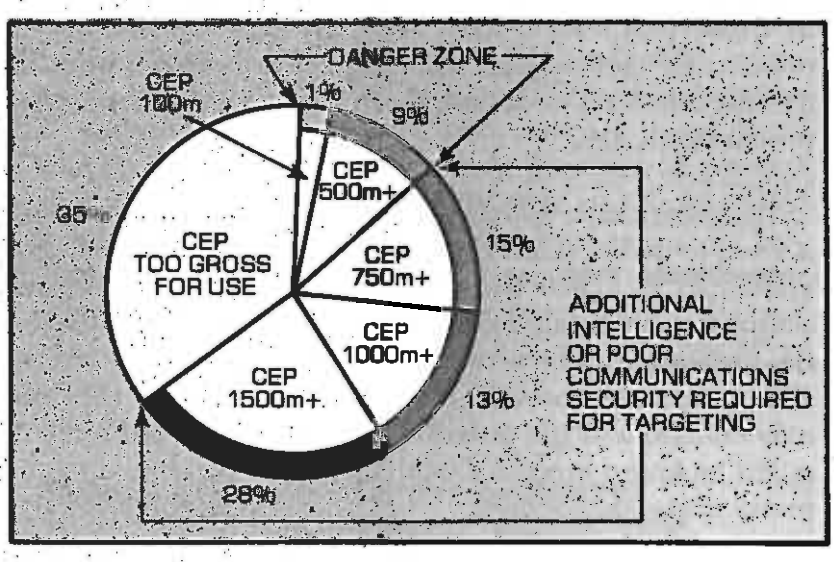
The term CEP is usually associated with artillery where it is used to define delivery accuracy of a weapon or weapon system. A CEP in RDF is expressed in terms of a CEP of a given size plus a percentage figure. The percentage figure indicates the likelihood that the target antenna is located within the area covered by the CEP. It should be noted that this area may contain a single antenna or several antennas such as might be found around a battalion or higher echelon command post.



In the example shown on the preceding page, when a 500m CEP is reported with a 90 percent probability, there is a 90 percent chance that the target transmitter is located somewhere within the area defined by that 500m radius.

Fortunately, that information by itself is only of marginal value in the acquisition of targets. But as mentioned earlier, most enemy signal intelligence (SIGINT) analysts apply CEP information in conjunction with poor signal security (SIGSEC) on our part to complete the transmitter location process.

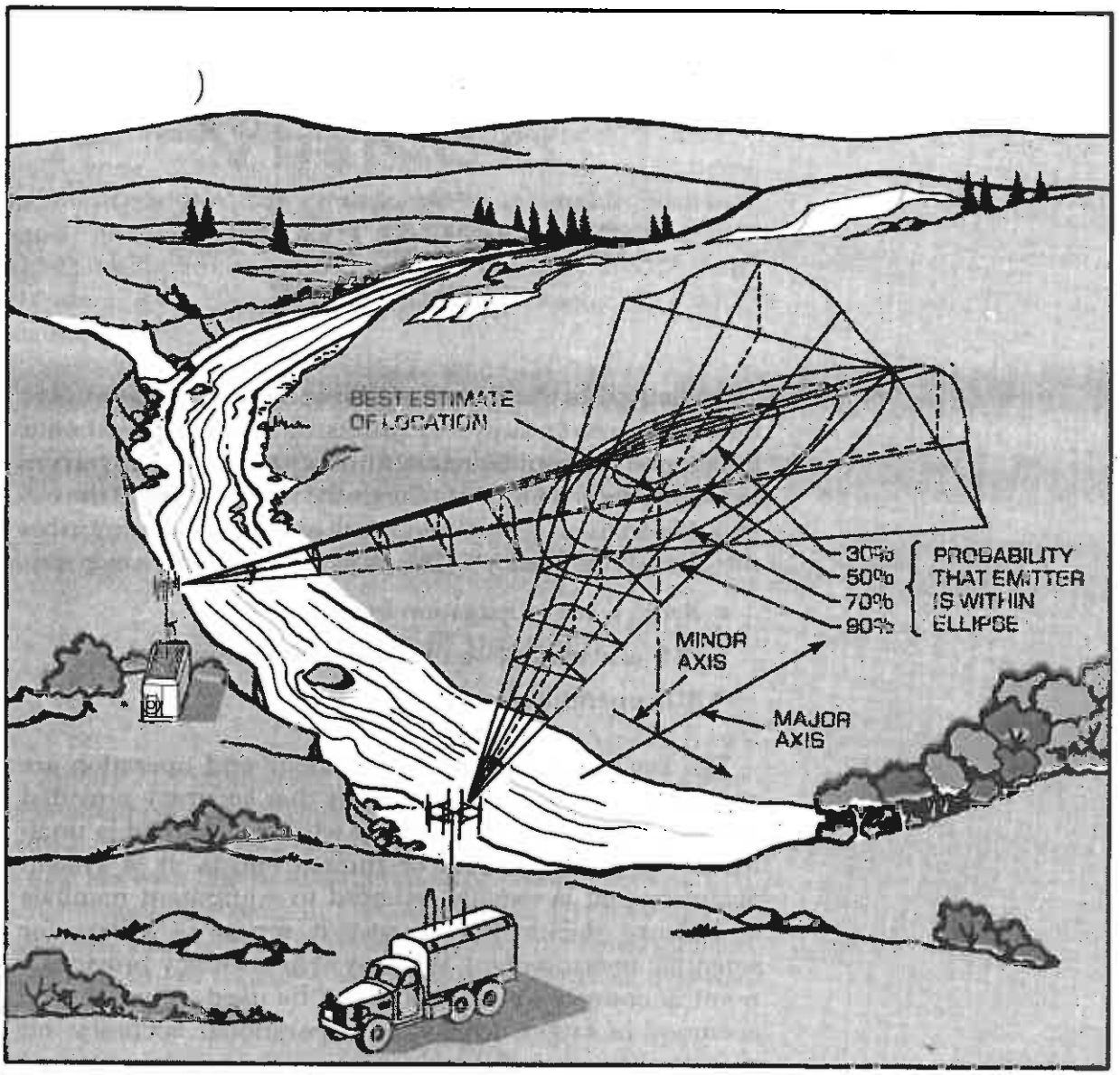
The following illustration shows how tactical RDF is measured in meters of CEP.



As the term CEP implies, the area within which the object is probably located is circular. But since the area is normally viewed from the side rather than the top, it is treated as an ellipse rather than a circle. Therefore, the CEP model would be expressed like this:

> 50% of the length of the major axis of an ellipse is used as the radius of a CEP.

Although the development and construction of a CEP is complicated, a basic understanding of the process is necessary in order to appreciate the enemy's potential to locate our transmitters using CEP.



MODEL OF ELLIPTIC ERROR PROBABILITY

Due to the advent of computer-assisted RDF, it is important to also become aware of how an elliptic error probability (EEP) is derived and how the EEP ellipse is used. An EEP provides a more accurate location when plotted than does a CEP. If one had the ability to actually see radio wave propagation, it would appear in a manner similar to that illustrated. The RDF bearings form an ellipse. Usually three or more bearings are used to determine an RDF fix, but only two RDF stations are illustrated in the example to reduce diagram clutter.

CHAPTER V

CAUSES OF RDF ERRORS

Realizing that the enemy will direct DF against US forces to develop targets for suppressive fires, US commanders should know enough about direction-finding to avoid as many errors as possible when initiating electronic warfare against the enemy. Mistakes made by US units will only aid the enemy in his direction-finding efforts. The chief causes of RDF error are:

- Radio wave propagation irregularity
- RDF and emitter equipment inconsistencies
- RDF operator mistakes.

The key words are system accuracy and operation accuracy of RDF. System accuracy is that accuracy provided within an electronics laboratory when equipment is unaffected by environmental or human effects. It is system accuracy that is usually reported in equipment manuals and Threat documents because it serves as a base for scientific measurement. While system accuracy provides a point of comparison, it should not be used to predict the accuracy of target acquisition. Operational accuracy, on the other hand, is field accuracy — the results obtained by experience during training exercises or combat. Let us examine, in general terms, the principal causes of RDF error and their effect on RDF accuracy.

RADIO WAVE PROPAGATION ERROR

One example of a radio wave propagation effect is the multipath error which occurs when a radio wave produces both a reflective and an instant component wave, each arriving at different times and possibly appearing out of phase. The DF operator hears the same signal twice. As

a result, the direction-finding station has difficulty determining the true signal. Where the received signal arrives from two or more paths, the RDF operator will read an azimuth that is in error and biased. Errors up to 10 degrees can result from such a condition. The VHF multipath error may be caused by other metal equipment located near the RDF equipment, by manmade obstructions, or by terrain which may distort the path of the signal. Multipath error occurs more frequently at VHF than HF since a smaller area can act as a reflector to a VHF signal.

All this is important because when VHF radio operators deliberately place terrain obstacles to radio wave propagation between the intended receiver and the enemy RDF, they take advantage of the potential effect of multipath error. This technique is called "masking," and we'll talk more about masking in Chapter VI.

RDF EQUIPMENT ERROR

Tactical RDF equipment is designed to perform with a system accuracy within plus or minus 2 degrees. Accuracy within plus or minus 2 degrees is the same as a total error of 4 degrees with regard to target plotting. System accuracy is what is generally given in Threat manuals. The operational accuracy, also referred to as field accuracy, of enemy tactical RDF equipment is usually within plus or minus 3.5 degrees (total 0 to 7 degrees).

Strategic or semipermanent RDF equipment, usually targeted at HF communications and located well behind the FEBA, is usually not more accurate than plus or minus 2 degrees; but the greater distance between the target transmitter and the RDF site results in larger linear error and in a CEP close to 50 kilometers. Nevertheless, strategic RDF plays an important role in detecting major troop movements. The Soviets probably used strategic RDF and communications intelligence (COMINT) to detect a temporary gap between the German Fourth and Sixth Panzer Armies confronting Stalingrad on 13 July 1942, which allowed two-thirds of the Soviet forces trapped across the Don River to escape — a significant factor in the Soviet victory at Stalingrad.

RDF OPERATOR ERROR

Radio direction-finding equipment operators can also contribute considerable error to RDF equipment by making even minor mistakes in many operational and land navigational functions for which they are responsible. Additionally, tactical RDF equipment can seldom be verified, or operator error distinguished from equipment or propagation error. This is important because RDF is susceptible to deception.

DECEPTION OPERATIONS AGAINST RDF

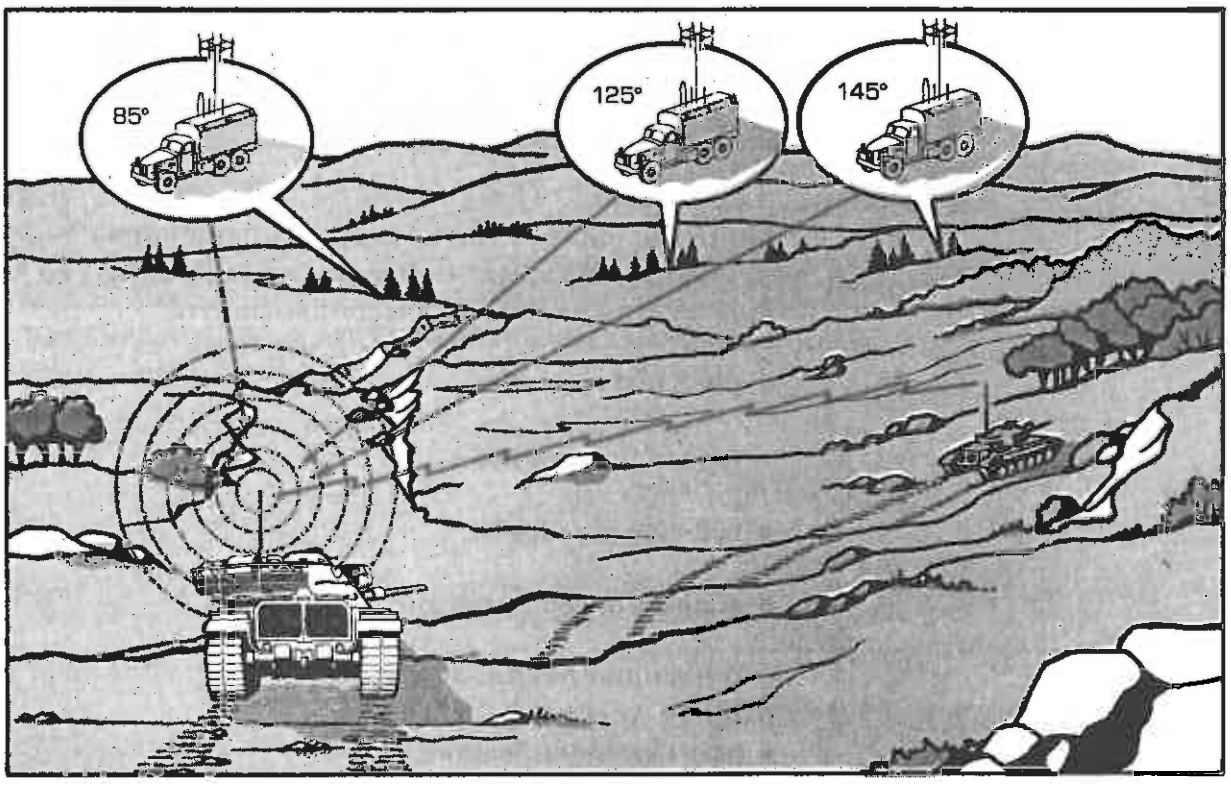
Radio direction-finding data enable analysts to determine the approximate location of an active transmitter whose signal has been intercepted and from which RDF bearings were taken. These bearings in themselves do not provide sufficient information to correctly identify the transmitter. Identification is usually provided through analysis of signals. If enemy SIGINT analysts are deceived into believing that a specific transmitter is assigned to, say, a division tactical command post, RDF may reinforce that conclusion. This is especially true if RDF reports that the transmitter is indeed located where a division command post should be located with respect to the FEBA and other boundaries. Other deceptive techniques against reconnaissance, which could include decoy equipment and installations, would further reinforce the deception. By contrast, an otherwise flawless deception plan not supported by electronic deception could be detected easily by enemy RDF.

The use of speech-security equipment (NESTOR or VINSON) with VHF radios does not provide protection against DF. Speech-security devices prevent clear text revelation of unit identity or call-sign identity; but if only command and control nets use these devices, identification of key emitters by RDF can still be accomplished. In fact, when only key command and control nets within a unit use speech-security equipment, this practice greatly assists enemy RDF operators in identifying command post transmitters.

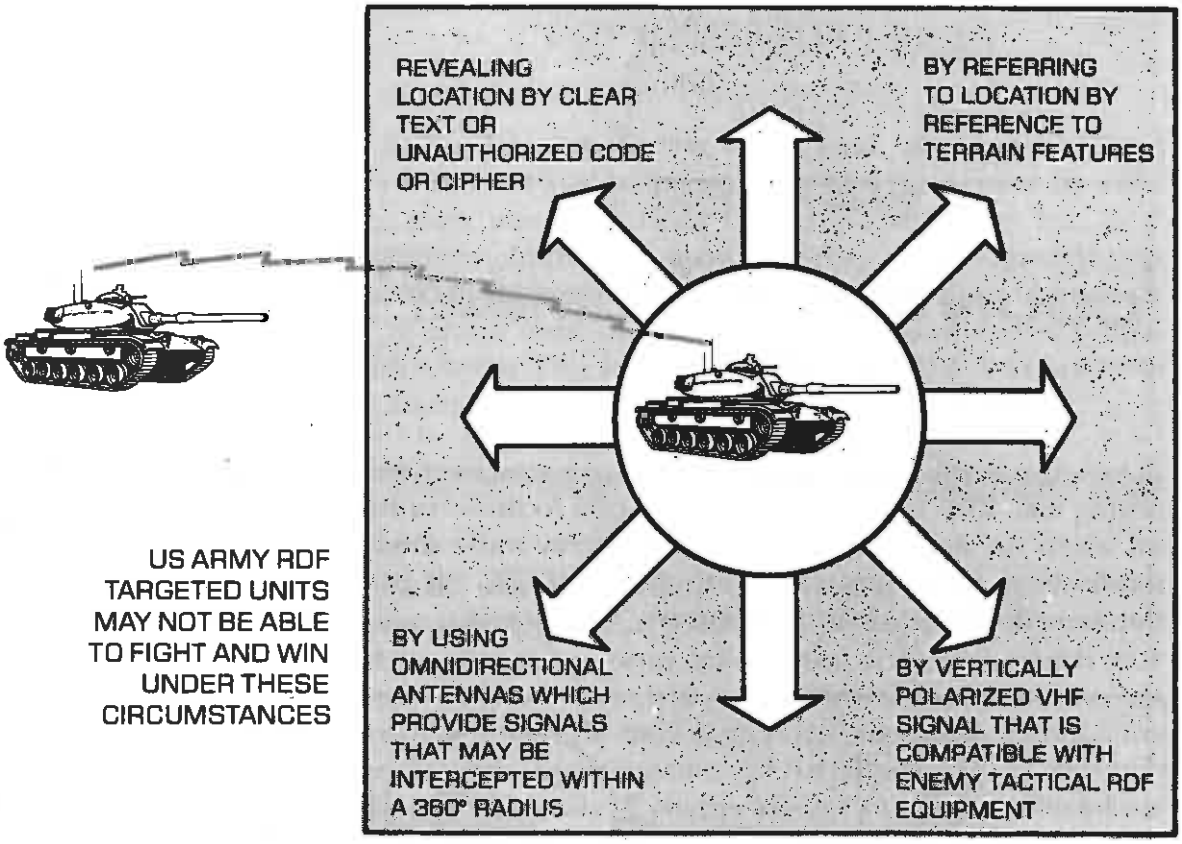
CHAPTER VI

COUNTER-DF COMBAT STEPS

Once the battle begins and our units are attacking and moving fast, RDF is not a significant threat to those units. But when we stop or go into defense, enemy radio direction-finding, in conjunction with poor SIGSEC on our part, provides targets for suppression — free targets.



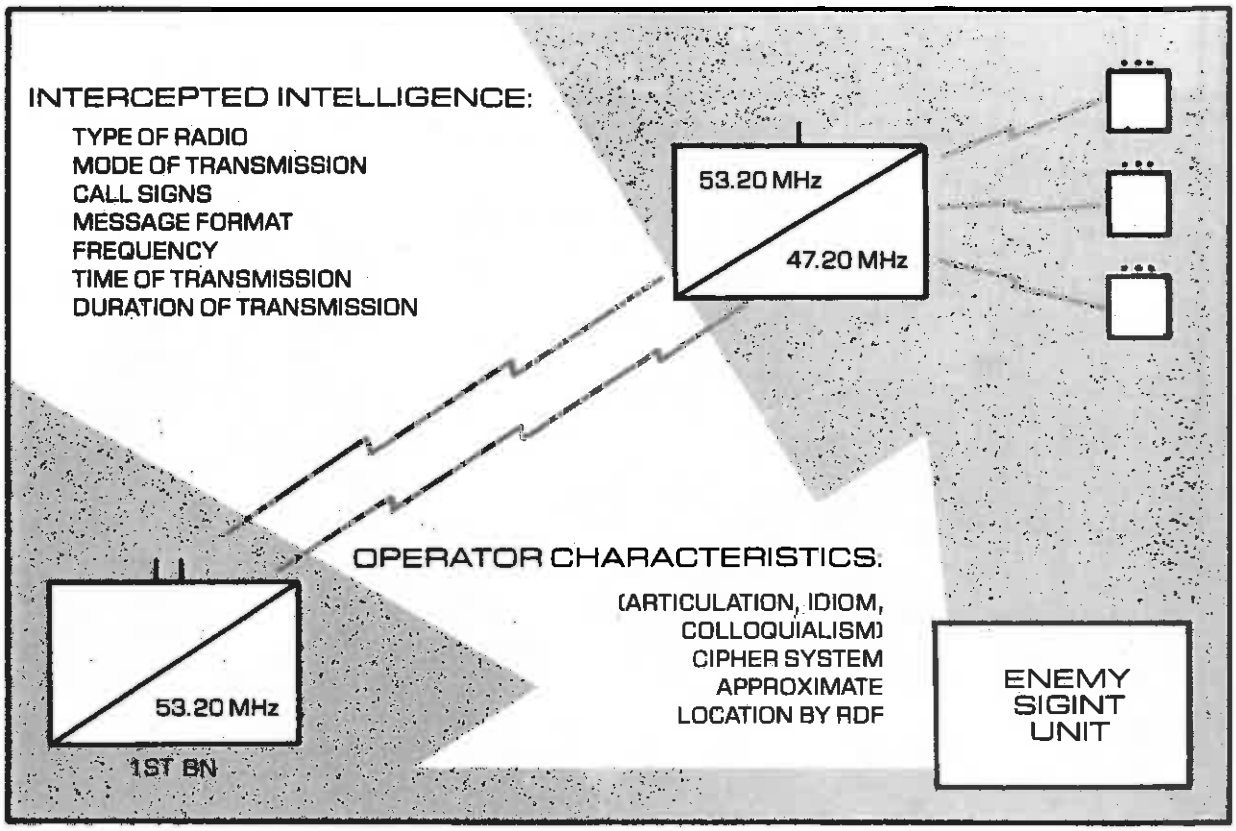
Poor communications security (COMSEC) during field training exercises allows location by RDF of many divisional, brigade, battalion, and company command posts with an accuracy of 100 to 250 meters, sufficient for destruction.



Electronic emitters can be used to identify units, weapons, and command posts because unit identity can be simply determined by one or a combination of:

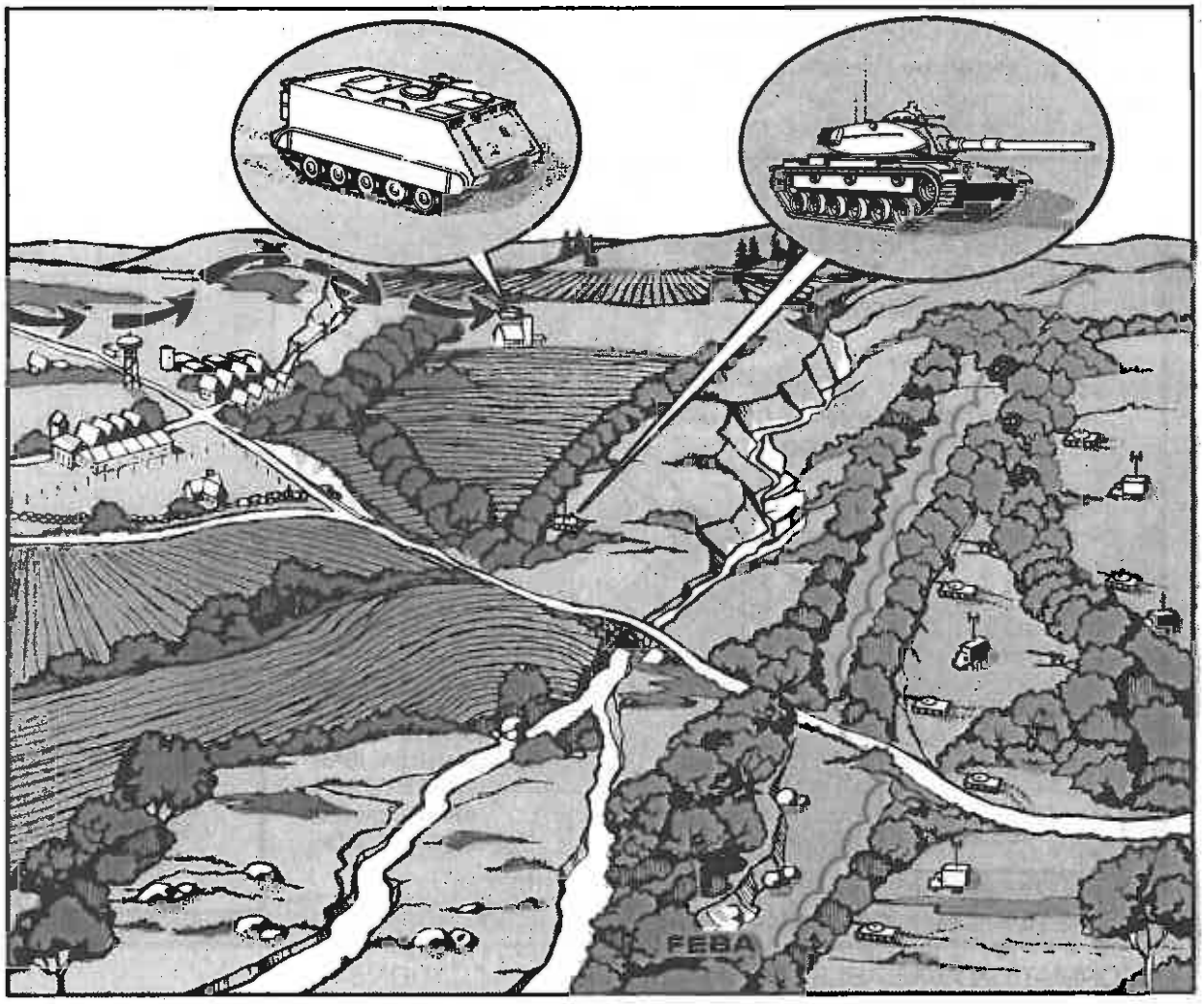
- plain text revelation,
- type of transmitter,
- call-sign peculiarity,
- analysis of communication traffic,
- transmitter modulation,
- operator identification,
- duration and frequency of messages,
- analysis of unauthorized codes or ciphers, and
- misuse of authorized call signs, codes, or ciphers.

All of these bits of information are used in conjunction with an analysis of the general location of a unit on the battlefield provided by direction-finding to locate it more precisely.

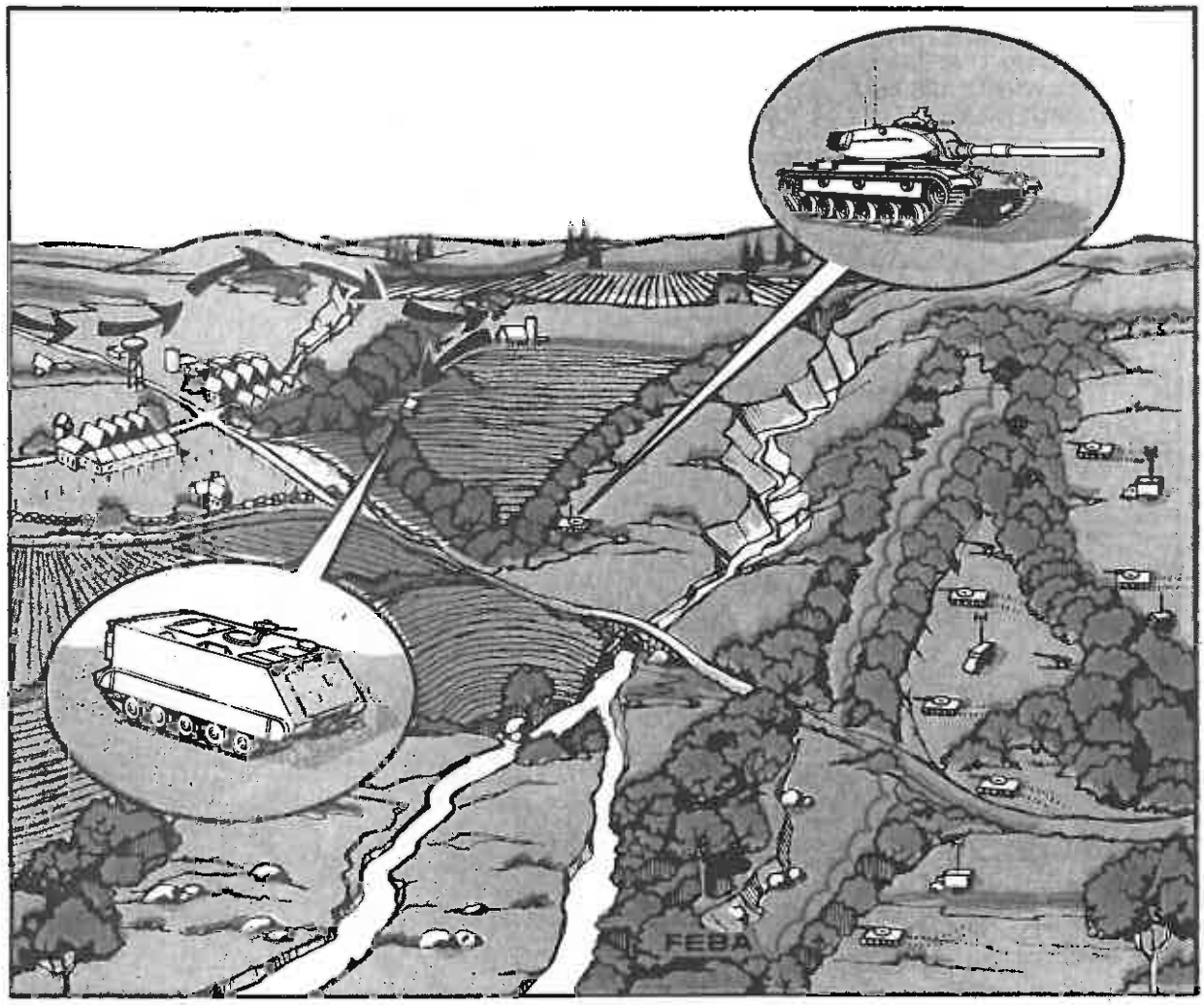


INFORMATION AVAILABLE FROM RADIO COMMUNICATIONS

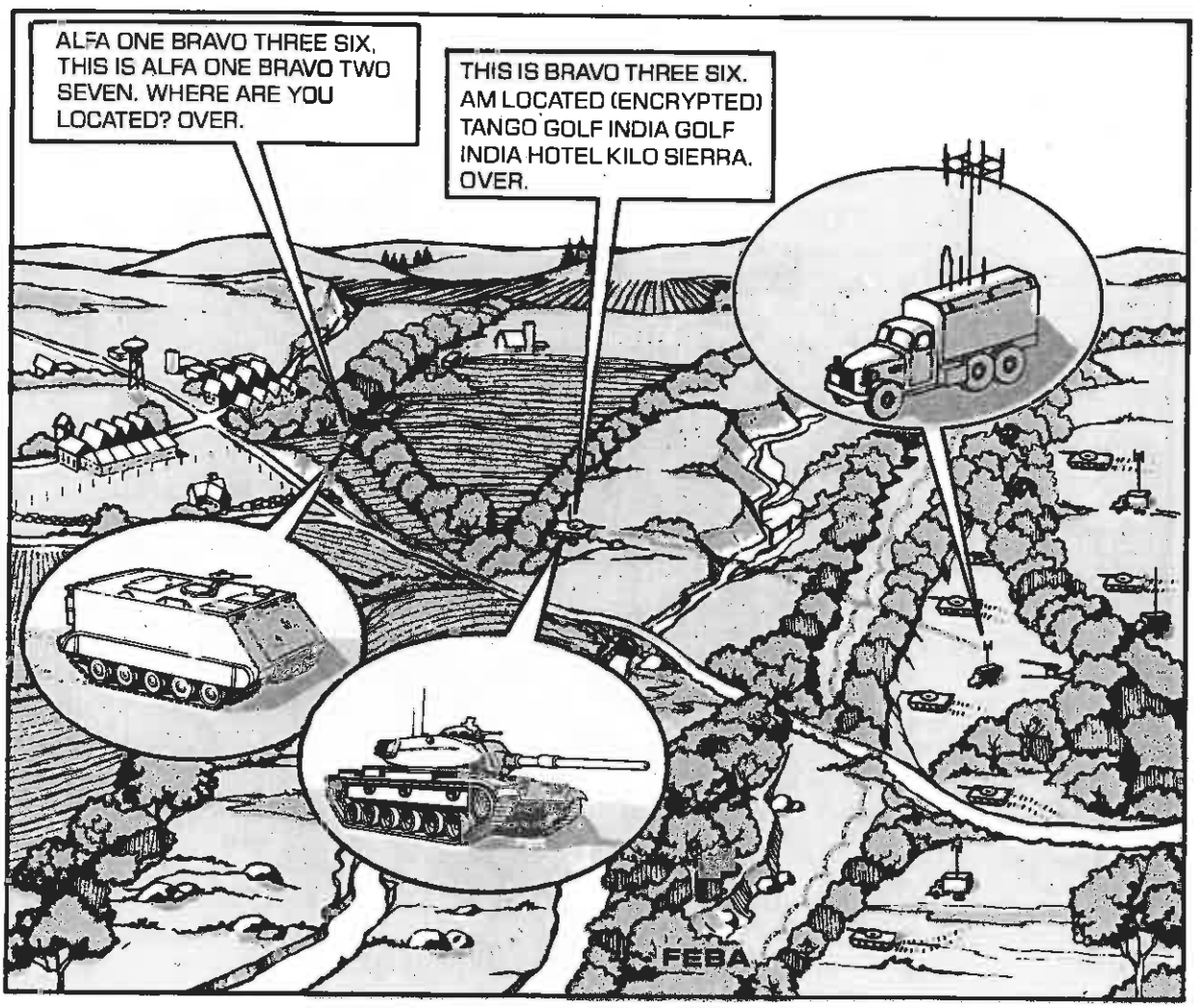
And now, a short horror story. . .



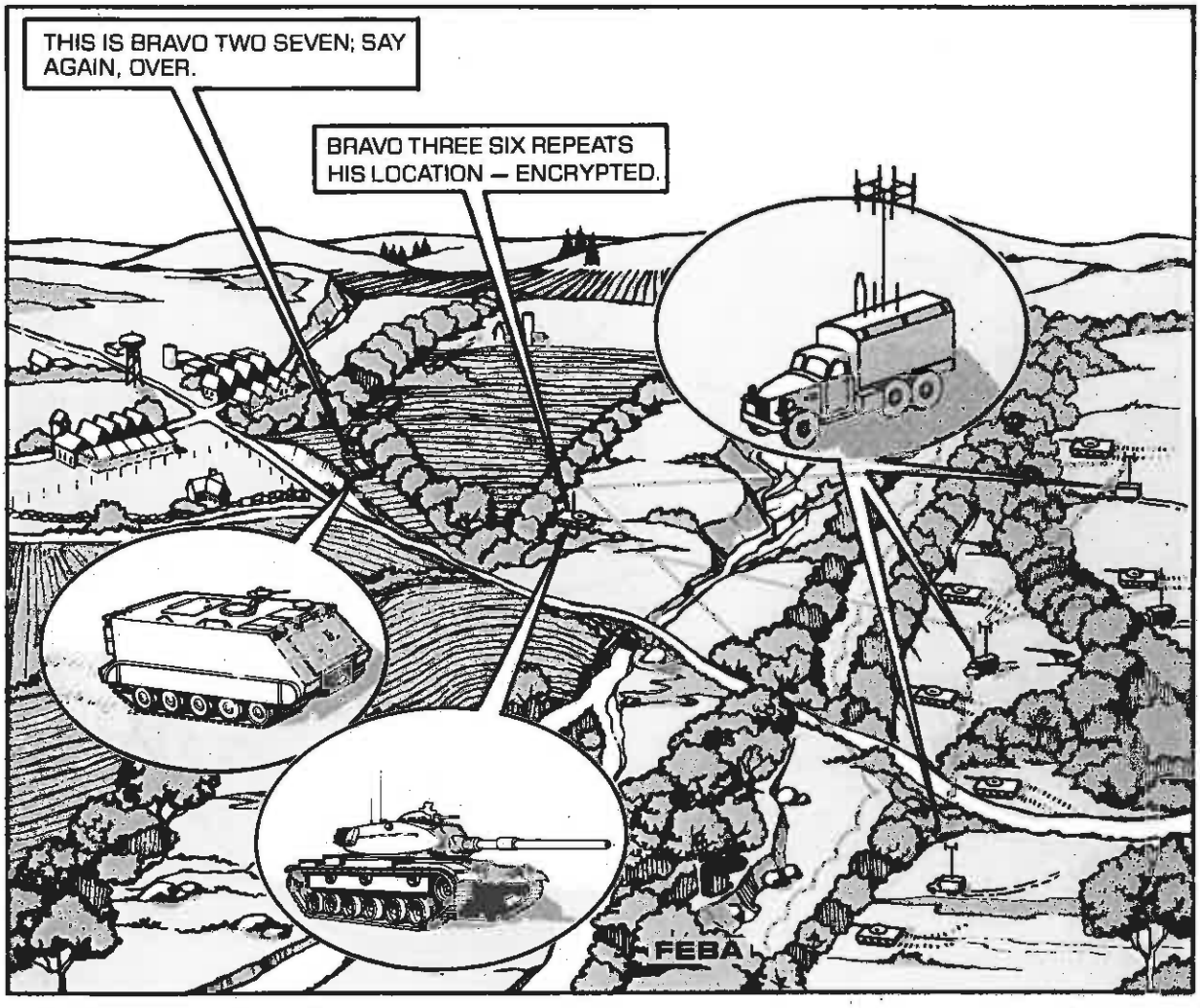
A US Army mechanized force prepares to attack an enemy position on the hill mass to the east. One of its tank units is located off the adjacent road in a woodline near the bank of the stream. The tank unit is concealed and in defilade awaiting the arrival of a friendly mechanized unit, approaching north and west of the town, prior to attacking the enemy position.



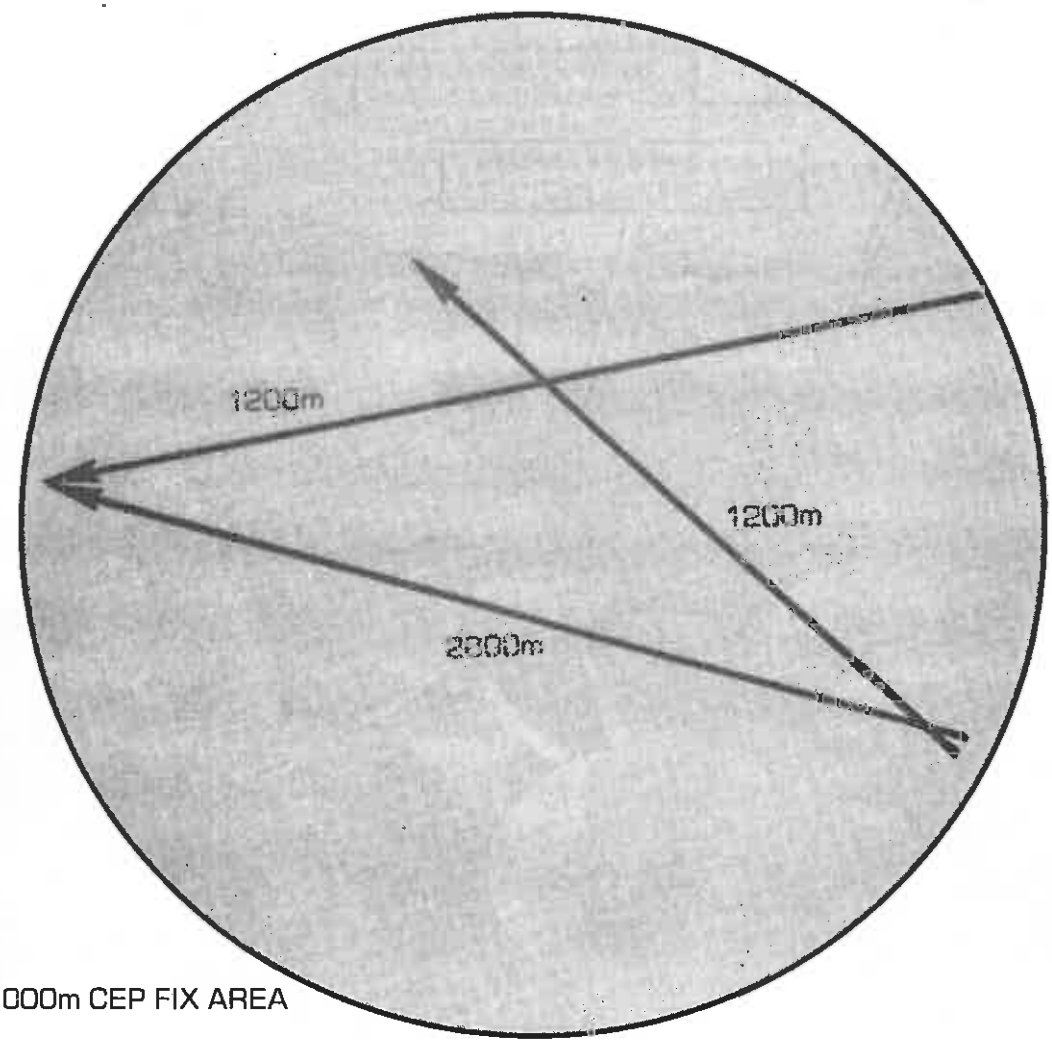
The mechanized infantry unit has passed north of the town and is approaching the tank unit while taking full advantage of all concealing terrain. At this point, both units remain visually unobserved by the enemy.



As the mechanized infantry unit approaches the general location of the tank unit, the commander requests additional information about the tank unit's location. Communication time is about 10 seconds. The enemy operator monitoring the command net intercepts the transmission and records it.

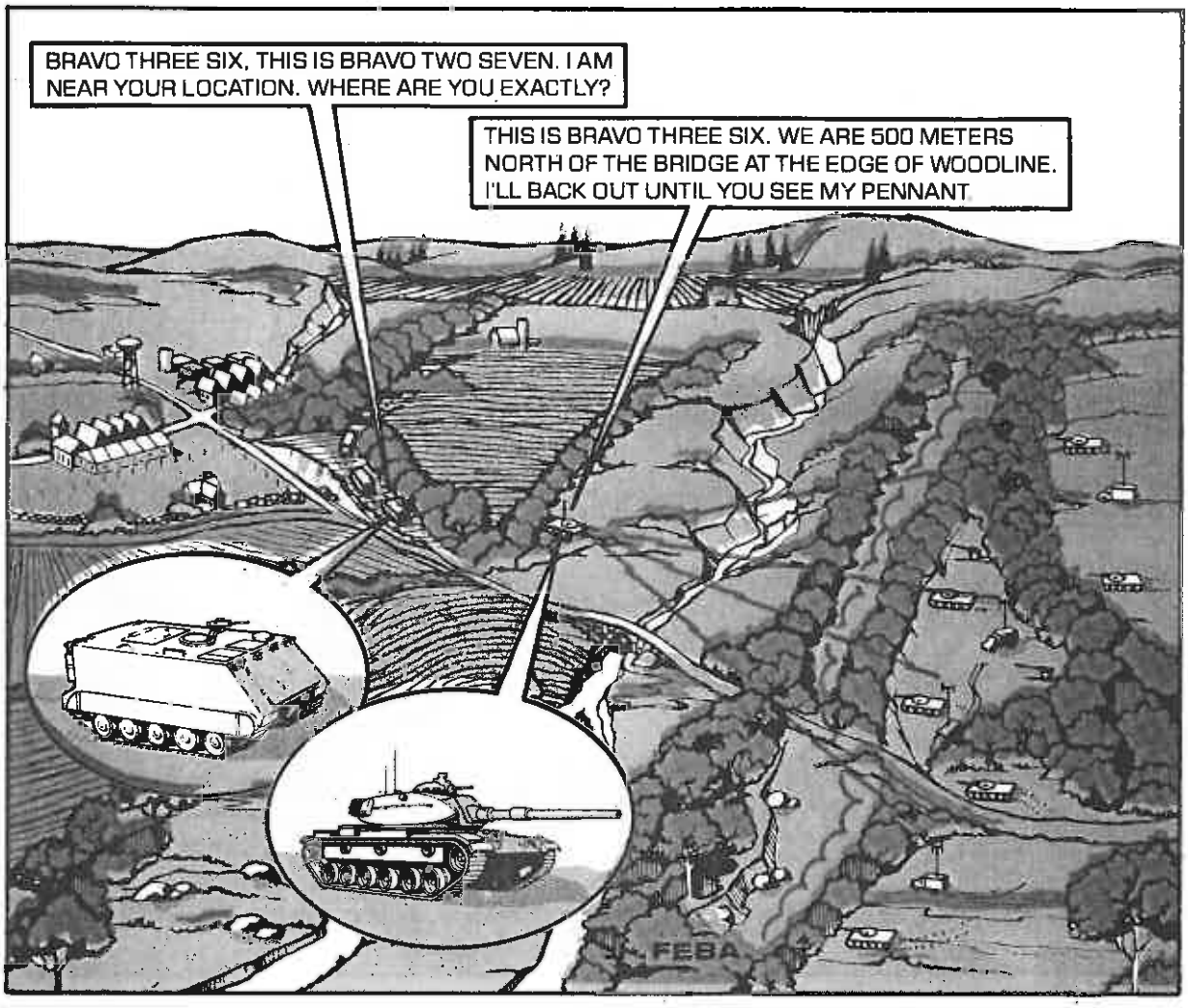


Total time for the entire communication transmission is about 45 seconds. The enemy RDF net has had more than adequate time to determine the azimuth from each of its three positions to the tank unit. The area within the triangle on the picture represents the approximate RDF fix.

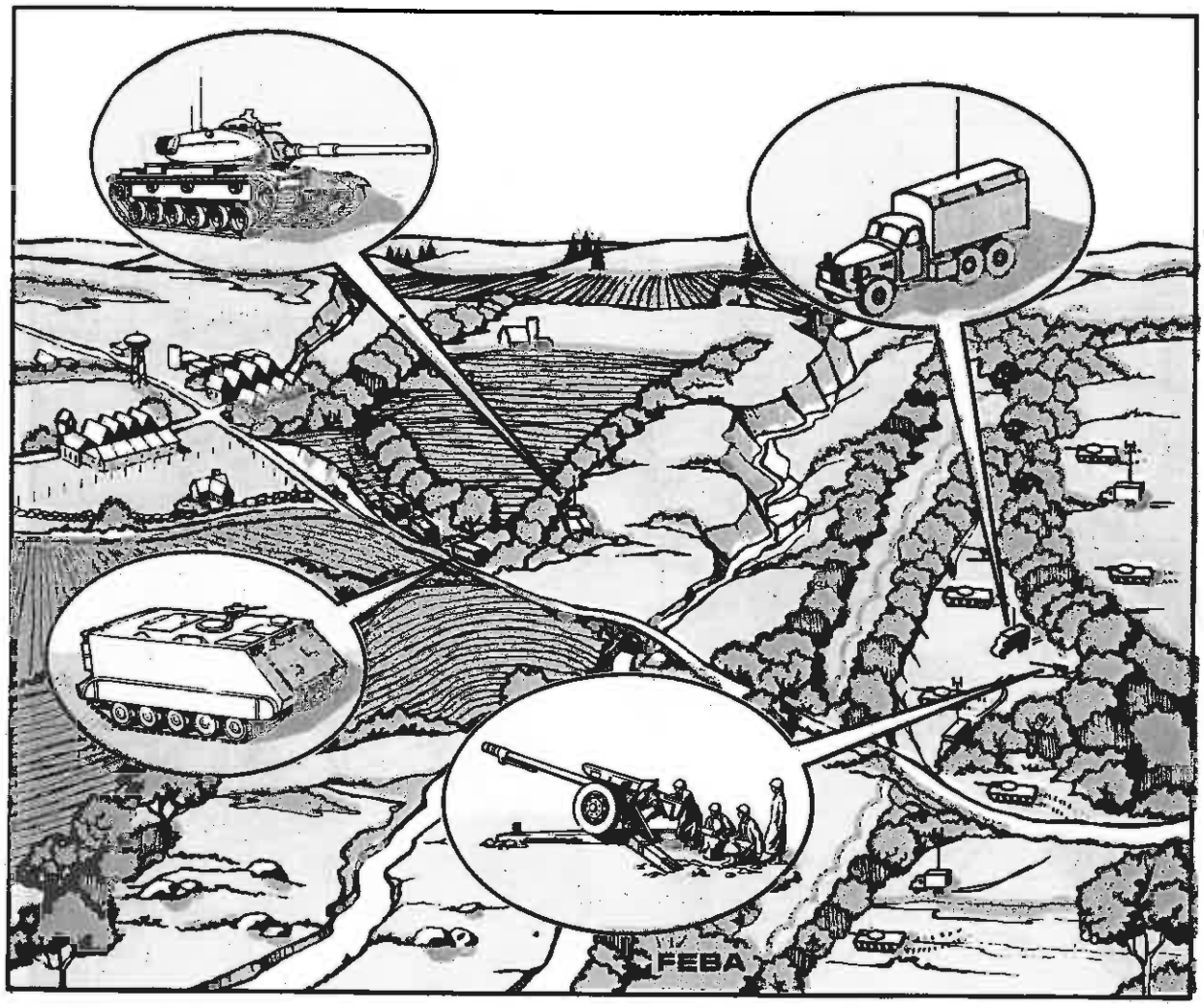


A 1000m CEP FIX AREA

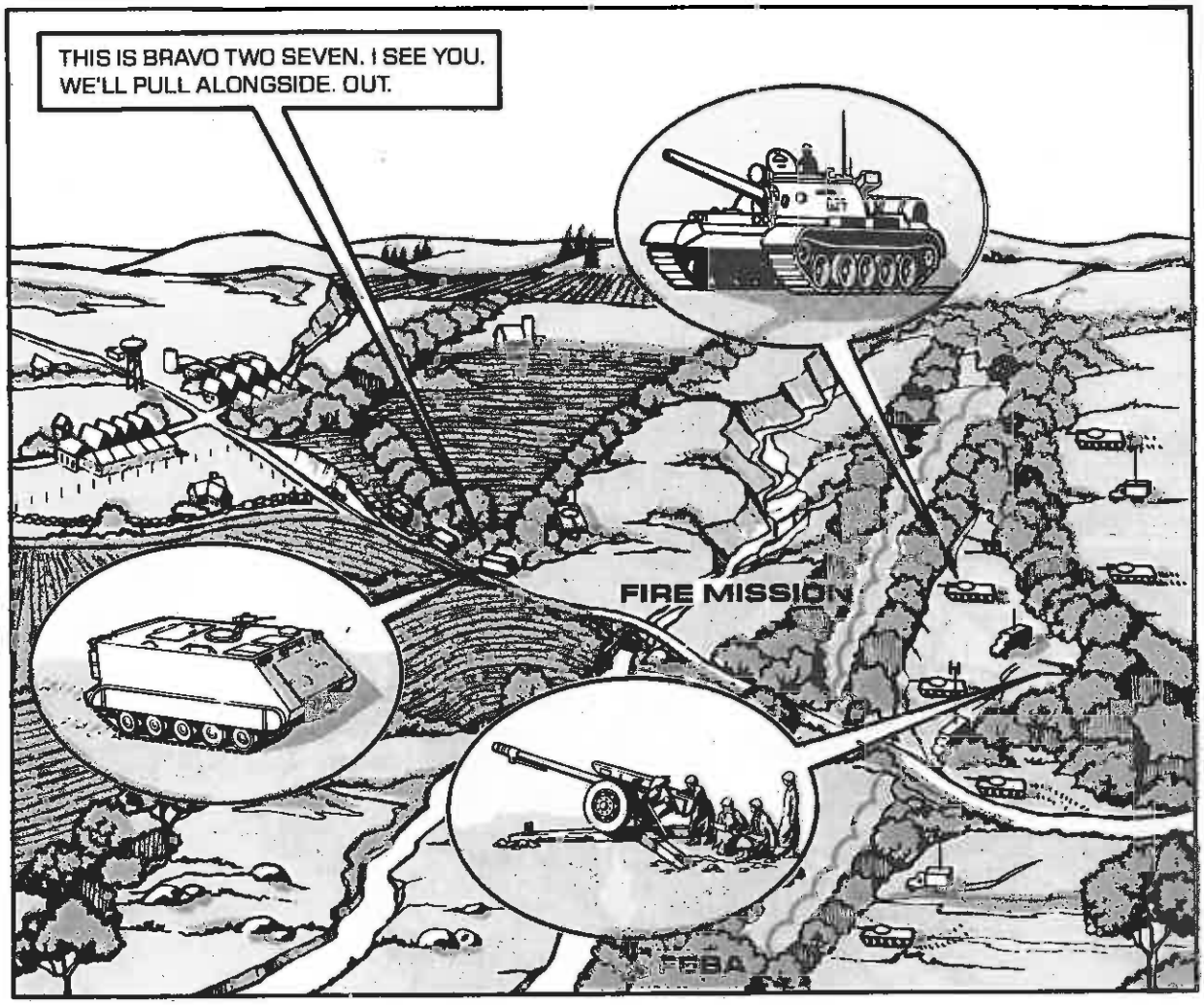
The area of the fix remains too large for accurate targeting or to risk exposing the enemy's firing positions on the hill to the front. The gridded location of the tank platoon reported in the communication was properly encrypted and remains unintelligible to the enemy. In fact, most things are being done correctly. A combined arms team is being used to attack fortified positions, and the team is using concealed avenues of approach. However, the enemy knows that one unit (mechanized) is advancing towards another unit (tank) located within the triangular area delineated by RDF. The enemy knows there will soon be two targets within the triangular area. Elementary call-sign analysis further suggests that separate units are involved. If the new automated communications-electronics operations instructions (CEOI) are not used correctly, prior tactical call-sign analysis by the enemy will indicate that a tank unit and a mechanized unit are involved. Plain text revelation involving the use of terms peculiar to armor or mechanized infantry operations will also allow this conclusion.



BRAVO 27 is now about 1000 meters from the tank unit, but is unable to see the concealed tanks. But BRAVO 27 has no intention of remaining in the open or of getting lost near the FEBA.



Meanwhile, on the hill to the front, enemy gunners have received preliminary information for a fire mission. Traverse and elevation are completed, the guns are loaded, and the gunners are awaiting the order to fire. Only the most basic analysis was required to locate the "bridge" within the vicinity of the RDF location. From there, the woodline was readily located. There was more than adequate information with which to provide a target.

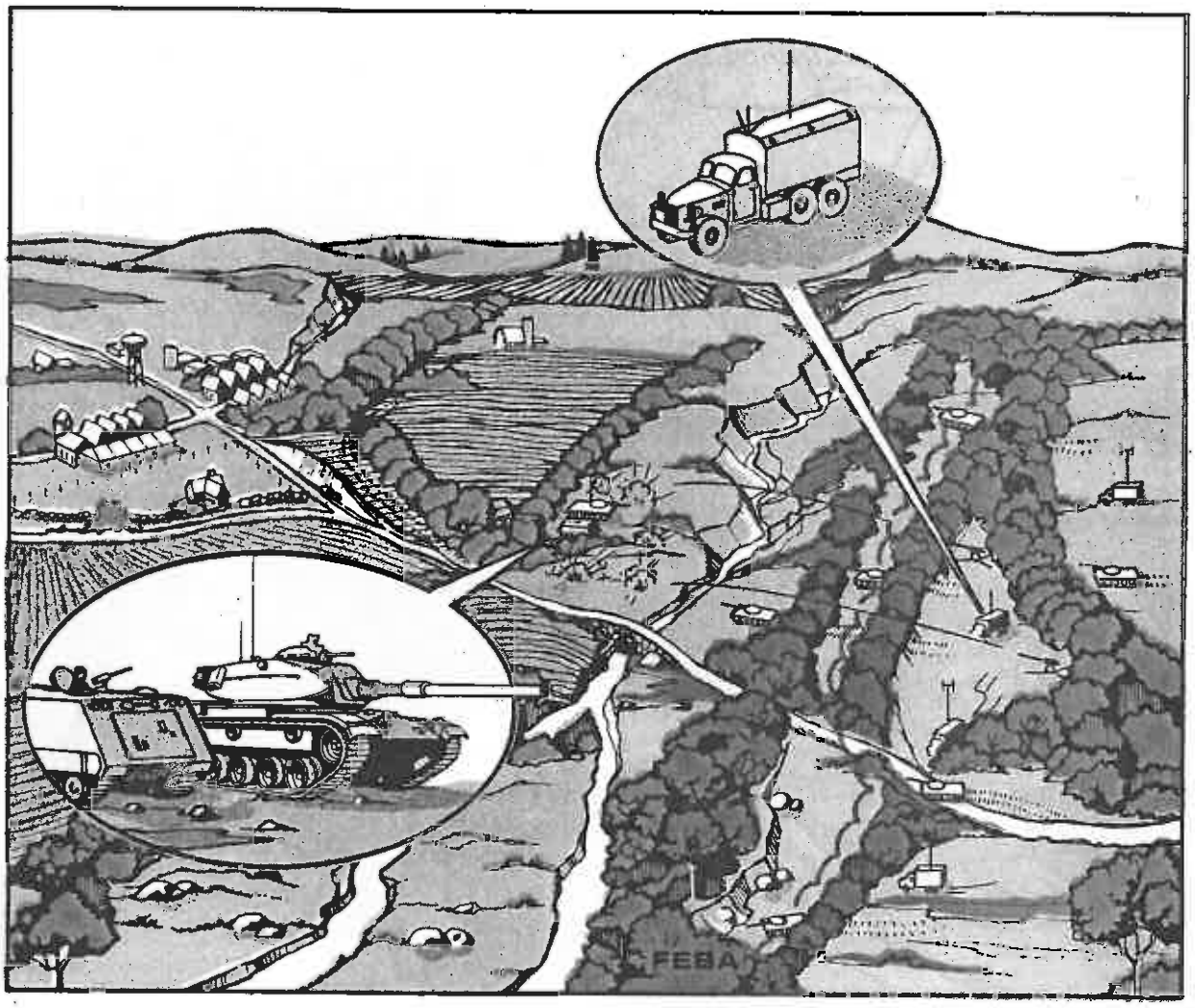


The enemy artillery commander allows another minute or so for the APCs to close with the tanks and for hatches to open, and then the APC and tank engines are muffled by the sound of exploding artillery aimed 500 meters north of the bridge at the edge of the woodline.

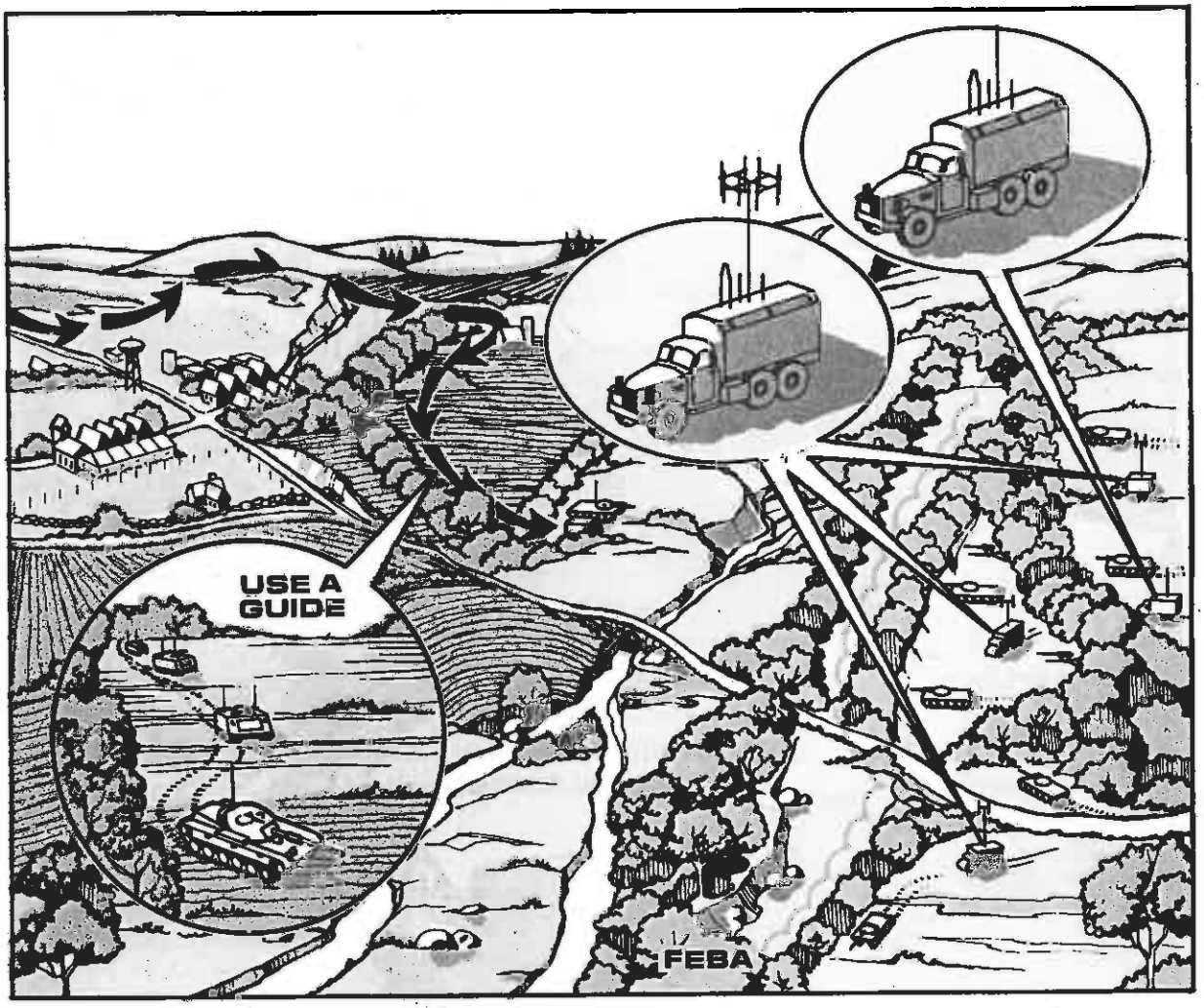
Hopefully, the lesson to be learned from this horror story is not that enemy RDF is highly accurate, but that . . .

POOR COMSEC IS SUICIDE!

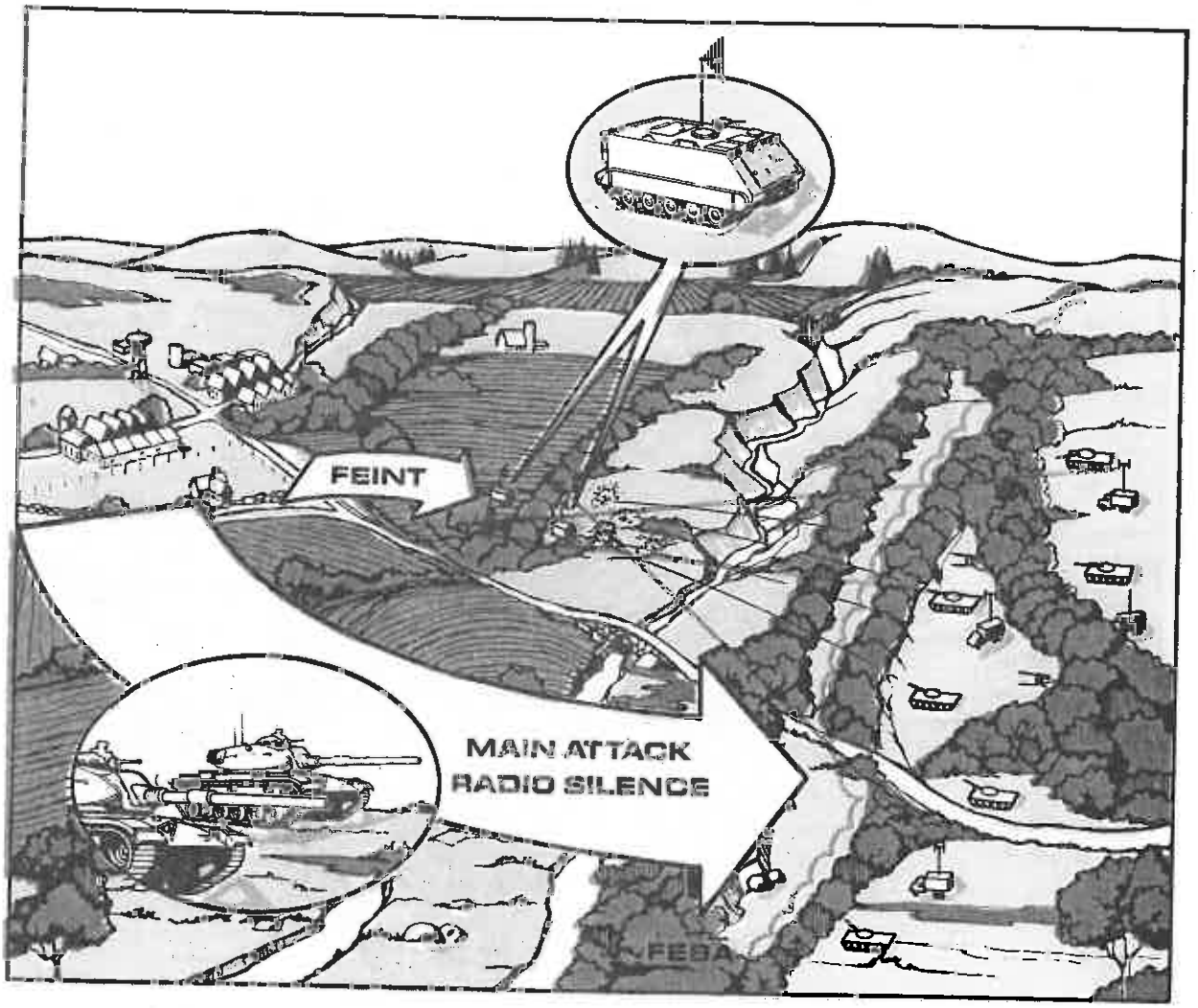
During a three-day maneuver in 1975, about 60 percent of all battalion and brigade command posts within a US Army division were located to within 500 meters in this manner.



If the enemy is unable to destroy our friendly unit by suppressive fires, he will target the friendly unit's receivers for radio jamming during the attack on his positions when command and control by our forces is critical. Radio direction-finding and poor COMSEC permit the enemy to accurately direct his jammers against our radios for maximum effectiveness.



In the preceding scenario, the use of a predetermined approach route for the mechanized infantry unit, and the use of guides provided by the tank unit could have avoided the use of communication. This is one method that enemy forces use to reduce communication.



This scenario also provided an excellent opportunity for electronic deception. A feint suggesting a frontal attack north of the road could have been simulated with only one tank and one APC using noise broadcast equipment to simulate the engine sounds of tanks and APCs of a larger force. Loudspeakers and recording equipment could have been used to broadcast recorded tank and APC noise.

Manipulative communications deception by the tank and APC indicating a much larger force would have contributed additional realism to the feint by feeding the enemy false RDF conclusions. Meanwhile, the actual force conducting the main attack approaches from the south with emission control (radio silence). The enemy's artillery is directed to the wooded, but then unoccupied, area "500 meters north of the bridge"; the attack is successful and casualties hopefully reduced.

While deception is a good idea, it must be carefully planned and coordinated with the battle commander and adjacent units. Since the enemy may also use ground radar to verify these targets, the deception force should include a deception array.

A radio signal provides information even when protected by code or cipher.

Electronic emitters can provide the enemy with the detection, general location, and possible identity of the transmitting unit.

You can beat RDF by using the following techniques:

1. Transmit as quickly as possible, then get off the air; organize message content beforehand to minimize transmission time, and consider not transmitting the message by radio or telephone if alternative means exist; do not peak traffic before an attack.
2. Reduce transmit power to the minimum level required to permit communications.
3. Use mobile antennas where practical.
4. Use horizontally polarized directional antennas where tactical utility permits.
5. Remote radios 1 kilometer or more.
6. Use decoy antennas.
7. Use encryption devices to prevent the enemy from refining RDF locations with measurement data provided through poor COMSEC; use proper call signs; employ random transmissions rather than working on a schedule to reduce the enemy's chance of interception.
8. Use Morse code where practical.

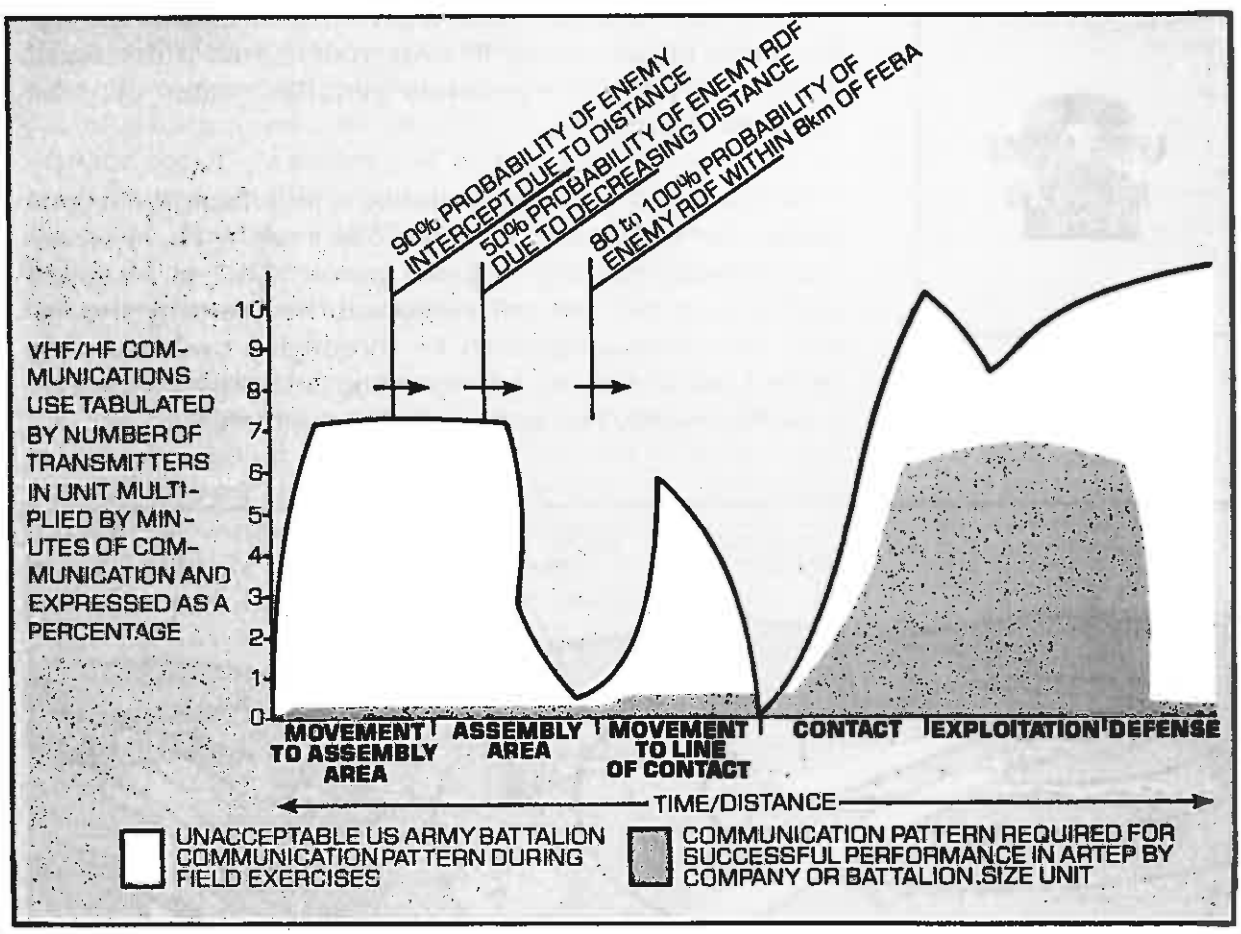
9. Site radio stations with obstacles between them and the enemy to reduce the possibility of intercept.
10. Use proper authentication procedures.
11. Train radio operators.
12. Take special care with radars and microwave transmitters.
13. Take special care with jammers.
14. Change call signs, frequencies, and schedules.

REDUCE COMMUNICATION TIME

A highly effective method for reducing the chance a signal will be intercepted by the enemy is to reduce communication time. You should try to limit conversations to less than 30 seconds. A 20-second signal is ideal. Once station identity is confirmed *(ALPHA ONE BRAVO ONE SIX, THIS IS ALPHA ONE BRAVO TWO SEVEN),* eliminate call sign redundancy by using the last letter of the changing portion of the call sign plus the suffix *(BRAVO ONE SIX, THIS IS BRAVO TWO SEVEN).* Where practical, you should also use personnel as guides rather than providing direction and location over the radio.

Short communication time is not as critical during the battle, but short communication as a counter-RDF technique is vital during the preparation phase and during the approach to the objective, or in the defense. Also, since the discovery of the displacement of a reinforcing unit is critical, the reserve force should not use radio communications unless necessary.

An observant enemy notices that in too many instances US Army tactical communications may be used as a substitute for complete battle planning. Analysis of US tactical communications, illustrated in the following graph, indicates that most communications used in training exercises are explanatory, not directive in nature. Tactical communications should be used to convey decisions rapidly, key standing operating procedures, and direct alternative courses of action.



VHF/HF COMMUNICATION PERFORMANCE REQUIRED FOR SUCCESSFUL ARTEP VERSUS PREVIOUS HISTORICAL PERFORMANCES.

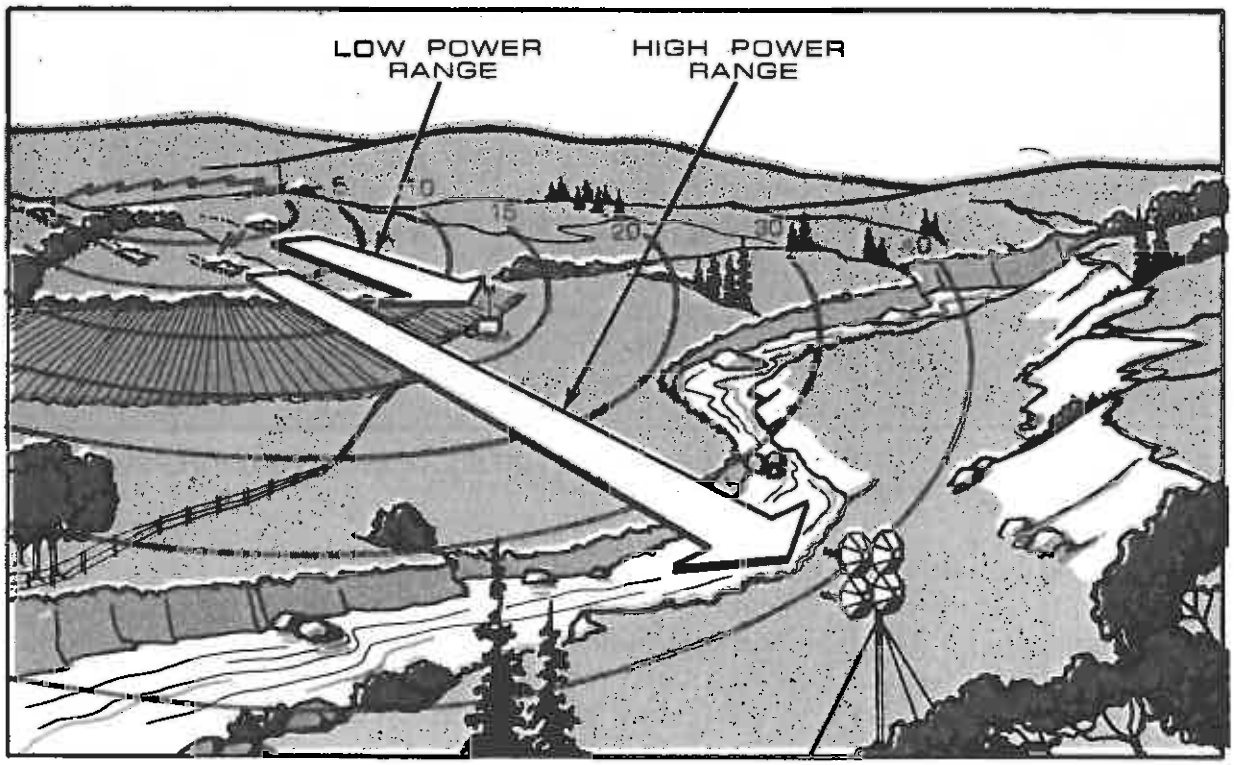
Execution of the battle must be inherent in training, planning, ingenuity, and teamwork. Vulnerability of communications to intercept and direction-finding is indicated by the large volume and context of communications noted on command links prior to contact with the enemy. This pattern uniquely distinguishes the US Army in the attack prior to its departure from the assembly area.

Additionally, the communication pattern depicted in the graph defies electronic concealment. There is too much traffic to be concealed. By contrast, the preferred communication pattern (indicated by the shaded area on the graph) can be concealed prior to contact.

Vulnerability to enemy RDF increases as the FEBA is approached.

When you transmit on low power, you reduce the opportunity for an enemy to hear your signal. If the signal can't be heard, the transmitter can't be located by radio direction-finding.

Obviously, if your own station can't hear the signal either, the radio is of little use. The trick, then, is to use only enough effective radiated power (ERP) to be heard within your net, but not enough to be heard by the enemy. This is accomplished by thoroughly understanding radio wave behavior, and by using low power wherever possible and the best antenna for each situation.



Unfortunately, tactical VHF radios have only two power settings: *low* and *high*. Most operators use only the high setting because they incorrectly think high power is better and that the low power position is useless. Let us look at the following example.

A tank platoon will operate in formations in which its tanks will be separated from one another by about 100 to 1000 meters. Even when the tank's VHF/FM radio is set on low power,

the radio transmits an effective signal which may be received by radio direction finders at a distance well in excess of 10 kilometers, and perhaps as far as 30 kilometers. On the higher power setting, a radio direction finder may be able to intercept the signal at a distance of 30 to 80 kilometers. Airborne radio direction-finding can certainly intercept the high power signal at a distance of 80 kilometers. Since US Army tactical radios do not have variable power controls like commercial radios, we must resort to expedients.

One simple operating procedure to reduce the ERP of the AN/VRC-12 and AN/PRC-77 family of radios, using a low power setting, is to bend and tie the AS-1729 whip antenna toward the ground. This technique will reduce the ERP at certain frequencies, particularly between 60 and 76 MHz. Bending the antenna will also deform the radiation pattern in the horizontal plane, which is another counter-RDF technique. See Chapter 2, Operator's Manual, TM 11-5820-667-12, for additional information. Always use Antenna Tip Assembly, FSN 5820-437-2353, to prevent eye damage from tied-down antennas.

CAUTION

DO NOT TRANSMIT USING ONLY THE ANTENNA STUB OR NO ANTENNA

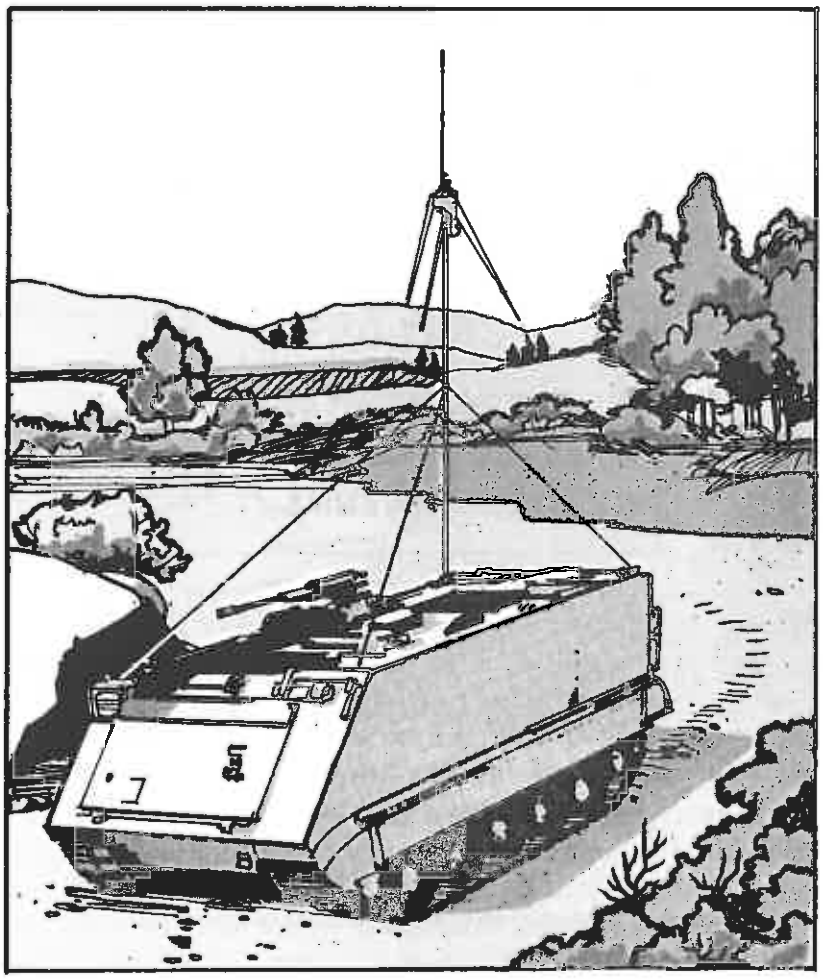
Using the AN/VRC or AN/PRC-77 family of radios without an antenna, or with only the antenna stub, results in severe mismatch of the power output stage. At certain frequencies, this mismatch is so severe that the maximum safe operating limits for the power amplifier transistor could be exceeded causing permanent damage to the radio.

Another method of reducing ERP and of distorting the radiation pattern in the horizontal plane is to carry the AN/PRC-77 upside down with the antenna tip a foot above the soil. This technique will usually provide a good strong surface wave within a radius of 5 kilometers, while reducing the radius of the direct wave most usable to RDF and ARDF.

Use the smallest antenna which will permit effective communication. Do not hesitate to take the extra step of changing from a ground plane antenna to a short whip antenna whenever possible.

USE A MOBILE ANTENNA

A reduced height VHF ground plane antenna (RC-292) can be mounted into a pole holder attached to the front bumper of an M151, M715 truck, or to an APC and secured with guy wires. This procedure provides a highly mobile command post and antenna array. Where terrain permits, this technique is superior to remoting antennas since it allows for greater mobility. The mobile RC-292 has excellent applications in desert operations.

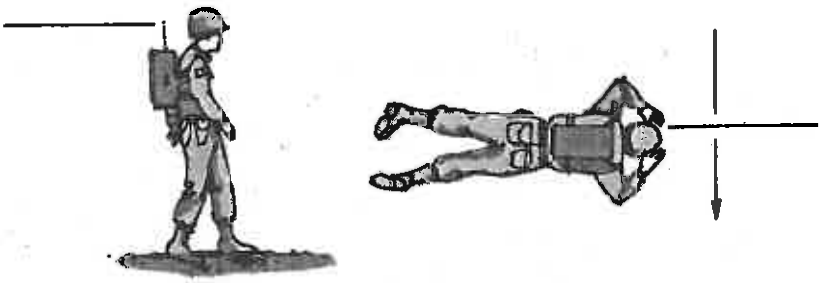


CAUTION: This antenna produces a large radiating pattern and long communication ranges. Use low power when possible.

USE DIRECTIONAL, HORIZONTALLY POLARIZED ANTENNAS

For all-around versatility, the omnidirectional, vertically polarized antenna cannot be beaten. The flexibility provided by omnidirectional antennas is important to the commander during the attack when it is difficult to maintain correct orientation for horizontally polarized, directional antennas.

Vertically polarized, omnidirectional antennas are required for communication between moving vehicles. However, when electronic counter-counter measures (ECCM) are considered, the omnidirectional antenna has one chief disadvantage. Omnidirectional antenna signals travel in a 360-degree pattern and usually well across the FEBA where they are susceptible to intercept and RDF. Directional, horizontally polarized antennas should be considered for lateral communications whenever possible.

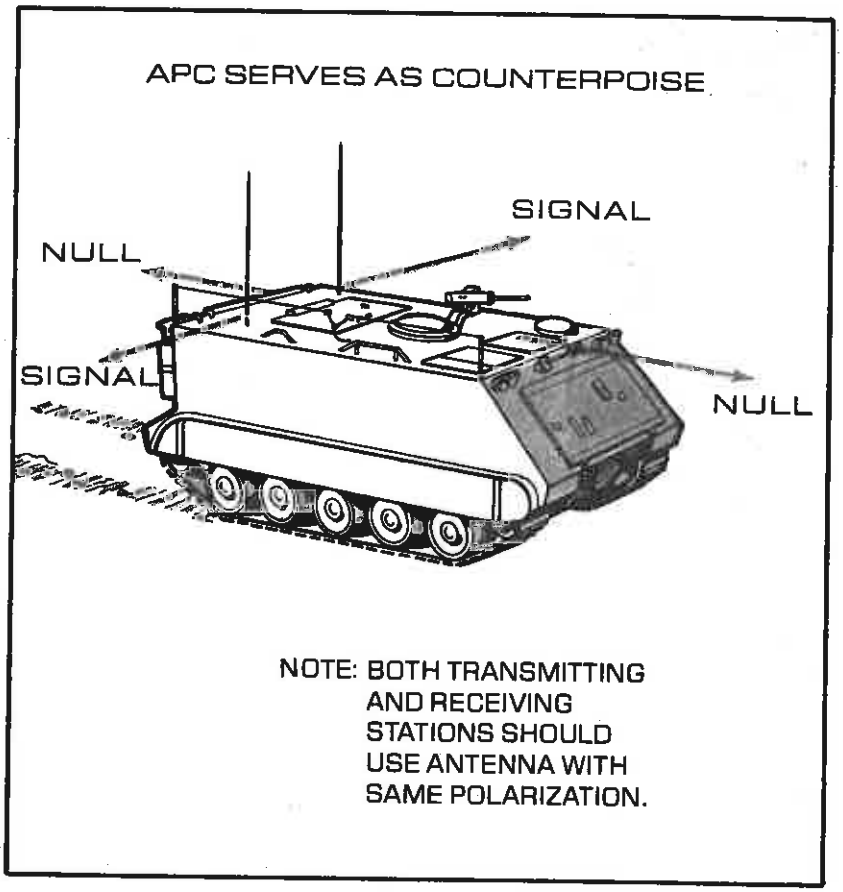


ANTENNA HORIZONTAL; RADIATION DIRECTIONAL AND AT RIGHT ANGLES TO ANTENNA

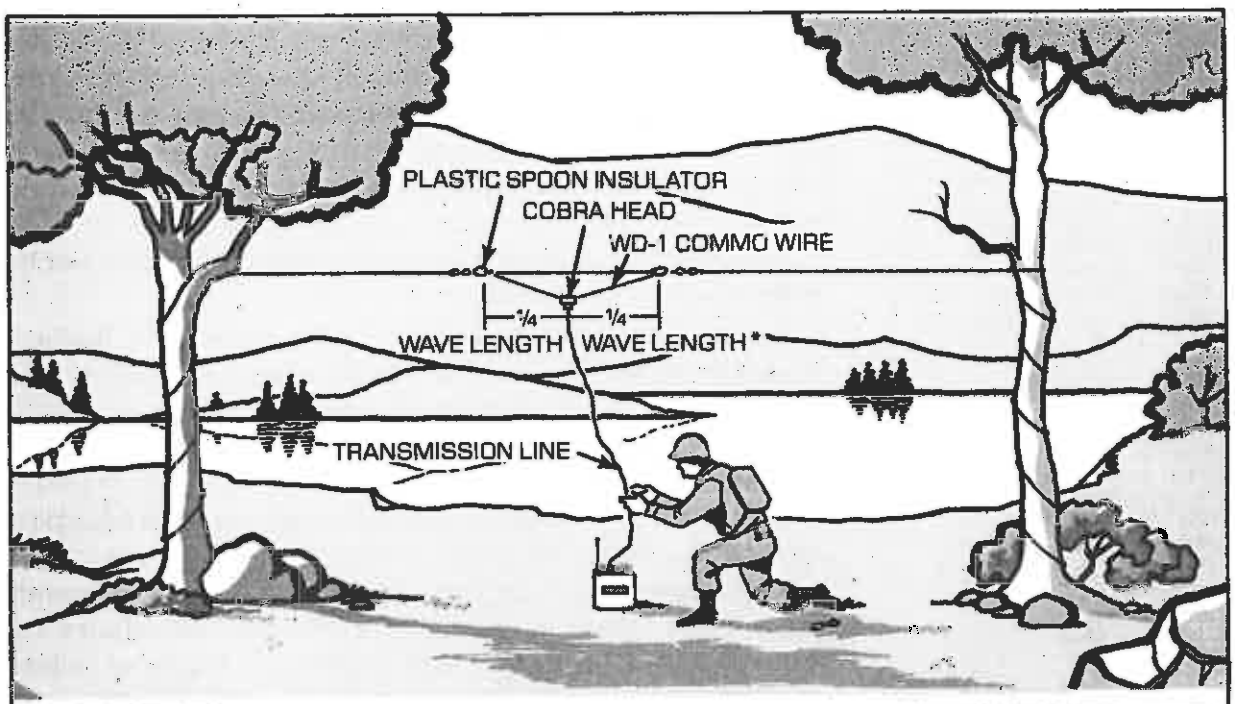
Enemy forces primarily use Adcock and vertical loop RDF antennas which are designed to achieve best performance when receiving vertically polarized radio waves. A horizontally transmitting VHF antenna will radiate a predominantly horizontally polarized wave to a considerable distance (10 to 40 kilometers) from the transmitter. The horizontally polarized wave will create bearing error in an Adcock antenna and a very large error in a vertical loop antenna. This may cause an error as much as five times as great as the usual operational error, or about 20 degrees, creating unusable RDF bearings. It is impossible for an RDF operator to continually adjust tactical, ground-operated RDF equipment, particularly Adcock antennas, to compensate for both vertical and horizontal waves.

If US forces would use both vertically and horizontally polarized, omnidirectional and directional VHF antennas, and good COMSEC practices, direction-finding would become very difficult and expensive for our adversary.

End or center-fed, one-half wave or one-quarter wave, directional antennas offer many advantages with VHF radios. A doublet antenna is an example. By increasing ERP in the desired direction, it provides a more directional signal which can reduce the enemy's ability to intercept the signal by 20 to 40 percent while providing a 20 percent greater range, especially in wooded areas. This is a useful ECCM technique.



A VHF directional antenna is small, only 9 feet long for a frequency of 50 MHz, or 6.5 feet for a frequency of 70 MHz. An antenna of this size is easily concealed. Doublets are also easily constructed from copper wire (or landline), a "cobra head," and two plastic C-ration spoons as insulators.



Horizontally polarized, center-fed, doublet antenna for AN/PRC-25 or -77 radio. See TM 11-2651 and TM 11-5820-4 67-15.

*Formula for ½ wave antenna:

$$\text{Antenna Length (in feet)} = \frac{468}{\text{Frequency (in MHz)}}$$

*Formula for ¼ wave antenna:

$$\text{Antenna Length (in feet)} = \frac{234}{\text{Frequency (in MHz)}}$$

There are, of course, drawbacks. For example, when one station uses a horizontally polarized antenna, the other station should also use a horizontally polarized antenna. Correct antenna orientation between both stations is also important, but the advantages, particularly in a defensive situation, warrant consideration of this technique wherever practical. Also, antennas of this type are not suitable for fast moving offensive operations. A directional, horizontally polarized antenna provides the commander an alternative to, but not necessarily a substitute for, the directional, vertically polarized antenna.

Half-wave, horizontally polarized VHF antennas offer a number of advantages over vertically polarized antennas:

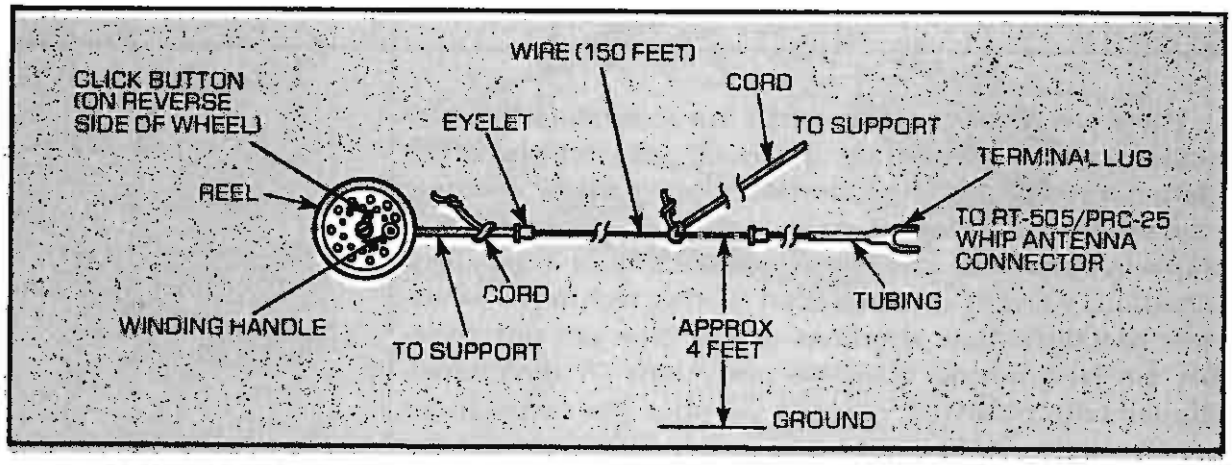
- The horizontal antenna produces a more stable signal in the presence of interference (jamming).
- The horizontal antenna produces a more stable signal when used in or near dense woods.
- The horizontal antenna is more readily camouflaged without loss of signal.

- Small changes in antenna location do not cause large variations in signal strength.
- The horizontal antenna is less susceptible to direction-finding because of polarization, and because its signal can be directed to intended recipients and away from enemy RDF in most instances.

Horizontally polarized antennas may be constructed by following instructions in:

- TM 11-5820-667-12 (Long Wire for AN/PRC-77 Radio)
- TM 11-2651 (Antenna Groups AN/GRA-4 and -12, Center-Fed Doublet)
- TM 11-5820-467-15 (Antenna Group AN/GRA-50)

While the information provided in these manuals is tailored for HF applications, the dipole dimensions can be readily scaled down for the particular operating frequency in the VHF range at the proper 50-ohm impedance required by the AN/PRC-12 and AN/PRC-77 family of radios. The AT 984A/G can be used to make an end-fed antenna for AN/PRC-77 radio; see TM 11-5820-667-12.



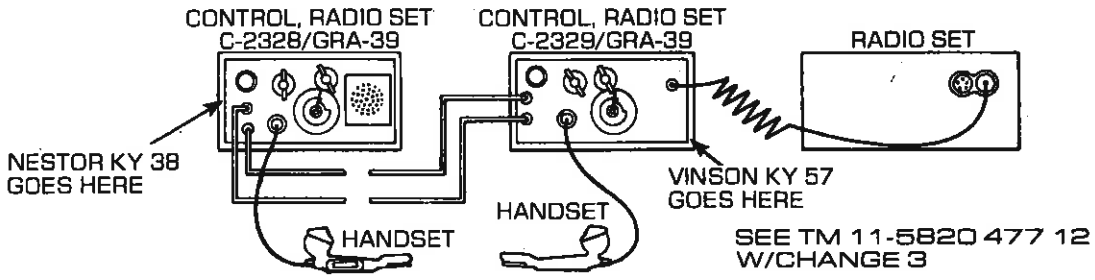
THE RF CABLE ASSEMBLY CG-692/U CAN BE USED TO FEED A DOUBLET ANTENNA

REMOTE OPERATION OF RADIOS

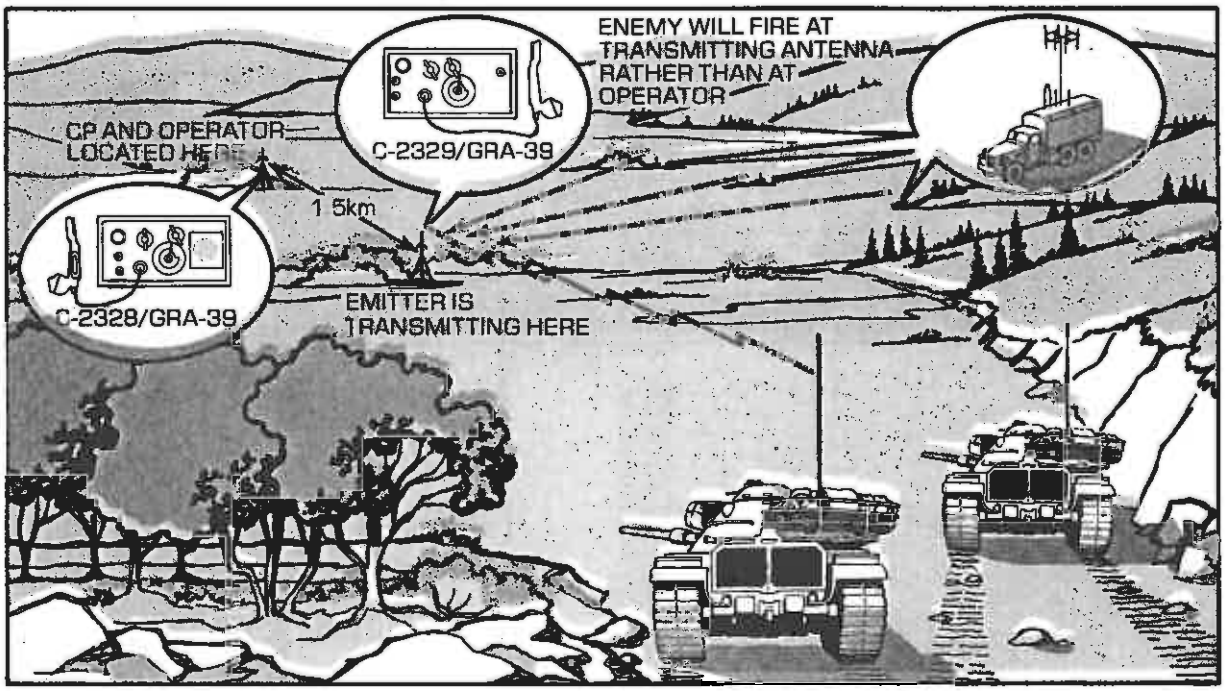
The AN/GRA-39 radio set control group allows the operator to remote the radio up to 3.2 kilometers. It should be noted that there is no practical advantage to be gained by installing the radio and antenna away from the command post (remoting) unless the distance is 1 kilometer or more. The error inherent in RDF equipment does not provide for a consistent accuracy less than 1 kilometer.

During most battlefield situations, DF analysts can be expected to regard the DF fix and its attendant CEP as a clue to a transmitter's location. Map analysis, other information, and textual revelation are applied to refine the fix for targeting data. Further, even when using NESTOR speech security equipment, the remoting cables are subject to exploitation by inductive-type line interdiction (wiretap) devices, devices that need not touch the cable.

Also, remoting cables may cause radiation leak after being subject to vehicle traffic. In some instances, radiation-leaking cable arrays may provide a better target than the antenna. Deceptive command post location probably offers better survival than remoted antennas unless the remoted distance is 1 kilometer or more.



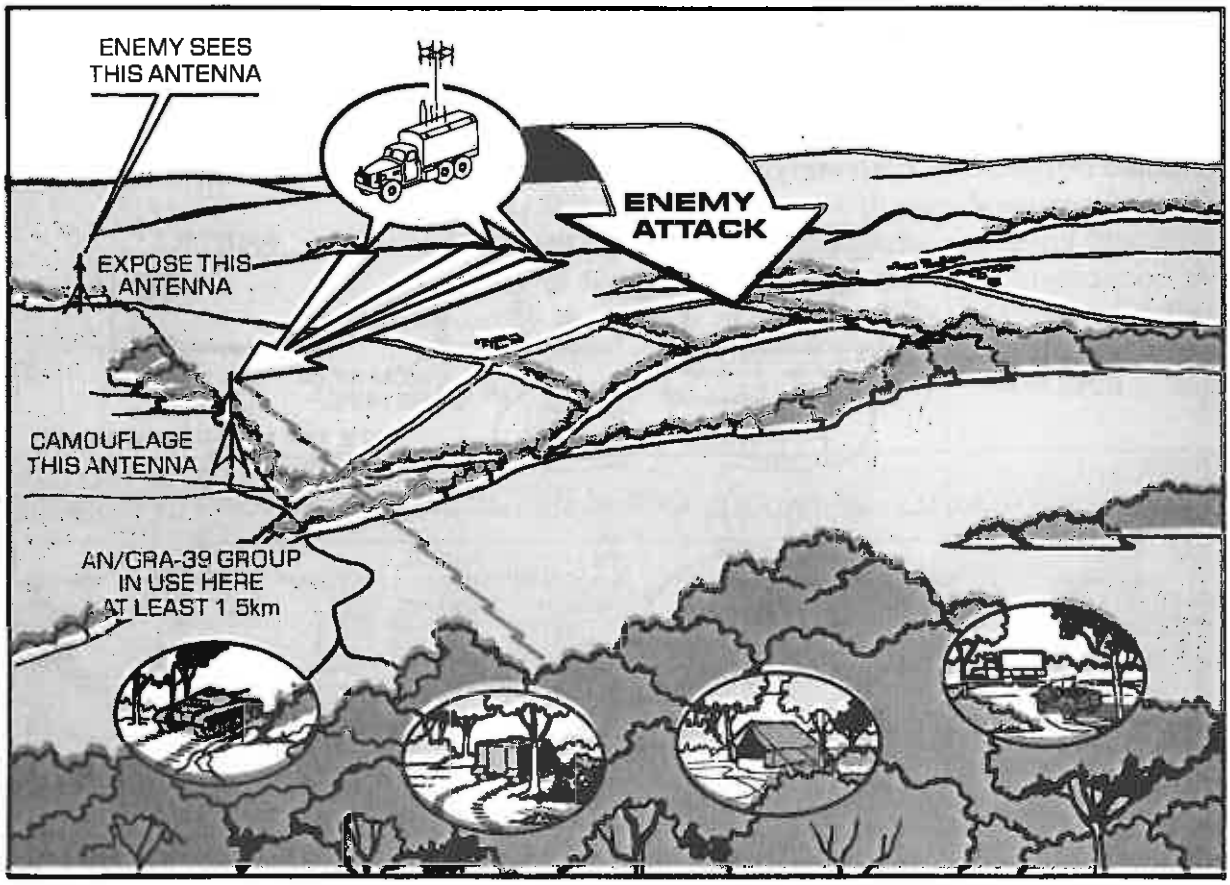
AN/GRA-39A HAS CALL LIGHT ADDED; AN/GRA-39B HAS CALL LIGHT AND RFI CIRCUITRY



USE OF THE AN/GRA-39 RADIO SET CONTROL GROUP (REMOTING ANTENNA SET)

USE DECOY ANTENNAS

When available and practical, surplus or decoy antennas should be erected in credible antenna locations within 2000 to 5000 meters of the command post. Enemy intelligence analysts are inclined to place special emphasis on photographs or reconnaissance reports of visible antenna arrays which appear within the CEP provided by RDF. The real antennas, especially distinctive microwave antennas, must be carefully camouflaged.



Use the KAL 61-DRYAD or other appropriate encryption system for all numbers (map coordinates, distances, dates, and times). When used with an NSA-accredited brevity list, the KAL 61 can also encrypt words, phrases, and short standardized messages. Do not assist the enemy by making approximate RDF locations precise due to poor COMSEC. Never discuss past, present, or future locations in plain text.

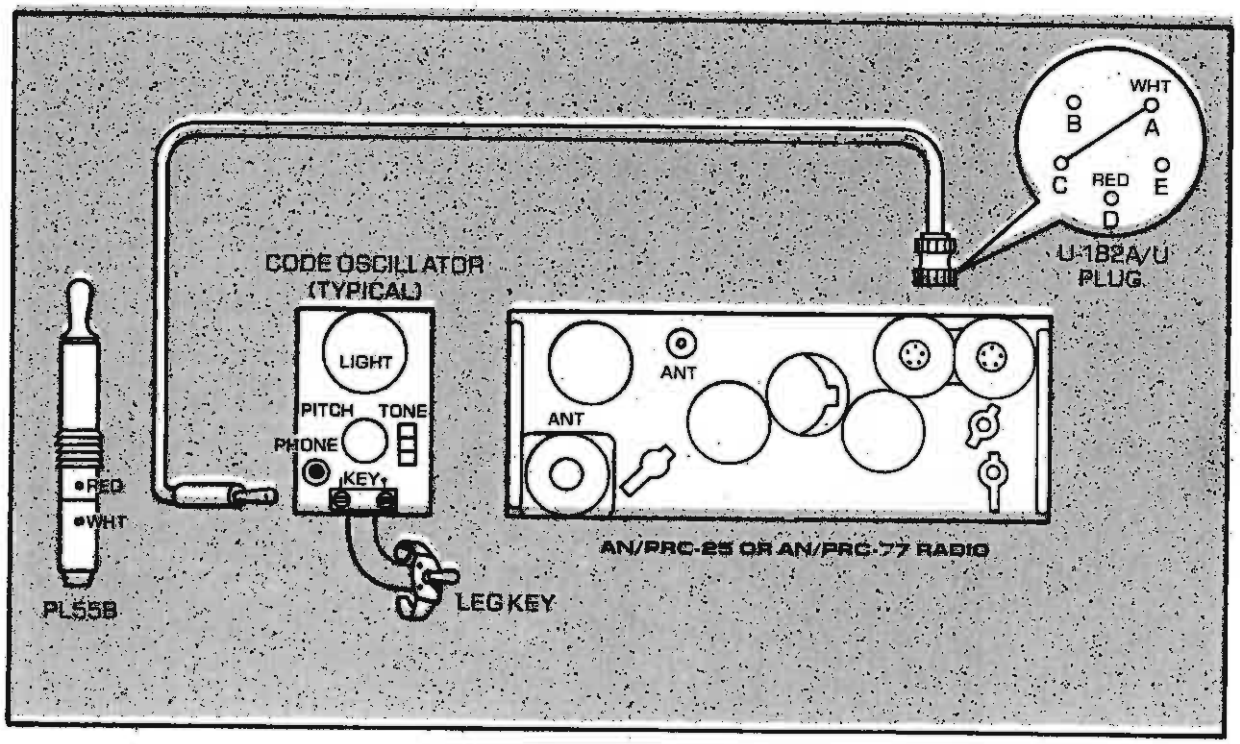
USE YOUR ENCRYPTION SYSTEM

GOOD COMSEC...

SECURE COMMUNICATIONS FOR TACTICAL UNITS

CONSIDER USE OF MORSE CODE

Communication time can also be reduced by using an inexpensive (less than $15) radio code tone oscillator. Used to practice Morse code, and obtainable at most radio supply stores, the oscillator can be attached to the audio input of FM/VHF radios. This adaptation permits the transmitting of short duration Morse code tone signals in place of long duration voice signals. The signal is clear, sharp, and perceptible at a greater distance than voice; and, when used with a directional antenna, Morse code is an excellent COMSEC technique. Radiotelegrapher's Q and Z signals may serve as a basis for a divisional Morse code system. Special forces and long-range reconnaissance units put FM/Morse code to good use in Vietnam.



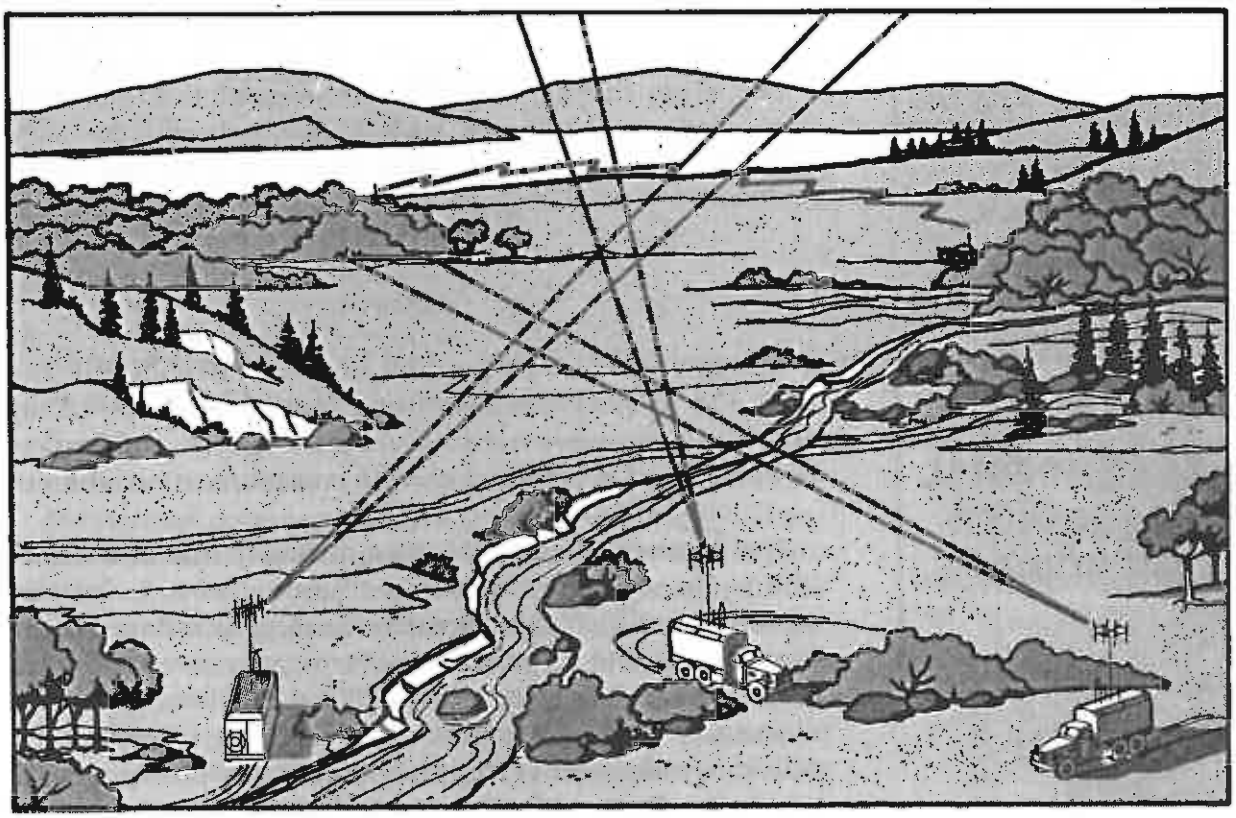
This idea is a technique from the field. Consult the unit C-E Officer for proper use of this technique over controlled VHF nets.

MASK ANTENNAS

Antenna masking is the technique of hiding radio signals behind terrain. It is an inexpensive method to confuse RDF.

Very high frequency radio waves bend and bounce; they are reflected by buildings and mountains and absorbed by trees. When this happens, it is difficult to determine the original direction from which the waves were transmitted, although the hearability of the signal is affected very little. A radio operator can use this principle to his advantage by placing terrain obstacles between the transmitter and the FEBA, thus affording an unblocked path to the intended receivers.

Hills and dense forests also serve as obstacles. Lakes serve as trampolines. A radio operator should erect antennas as low as adequate communication permits and, in all cases, antennas should be camouflaged to blend with terrain.



Be aware of imitative communications deception. Authenticate! Imitative communications deception is frequently used by an enemy to prolong communications. Radio direction-finding thrives on prolonged communications. Don't be caught by the lure. If you'll remember our short horror story, enemy forces were able to determine the approximate location of the tank unit in well under 60 seconds of transmission time. Do not respond to calls that you cannot authenticate with certainty; it might be an enemy operator practicing imitative communications deception.

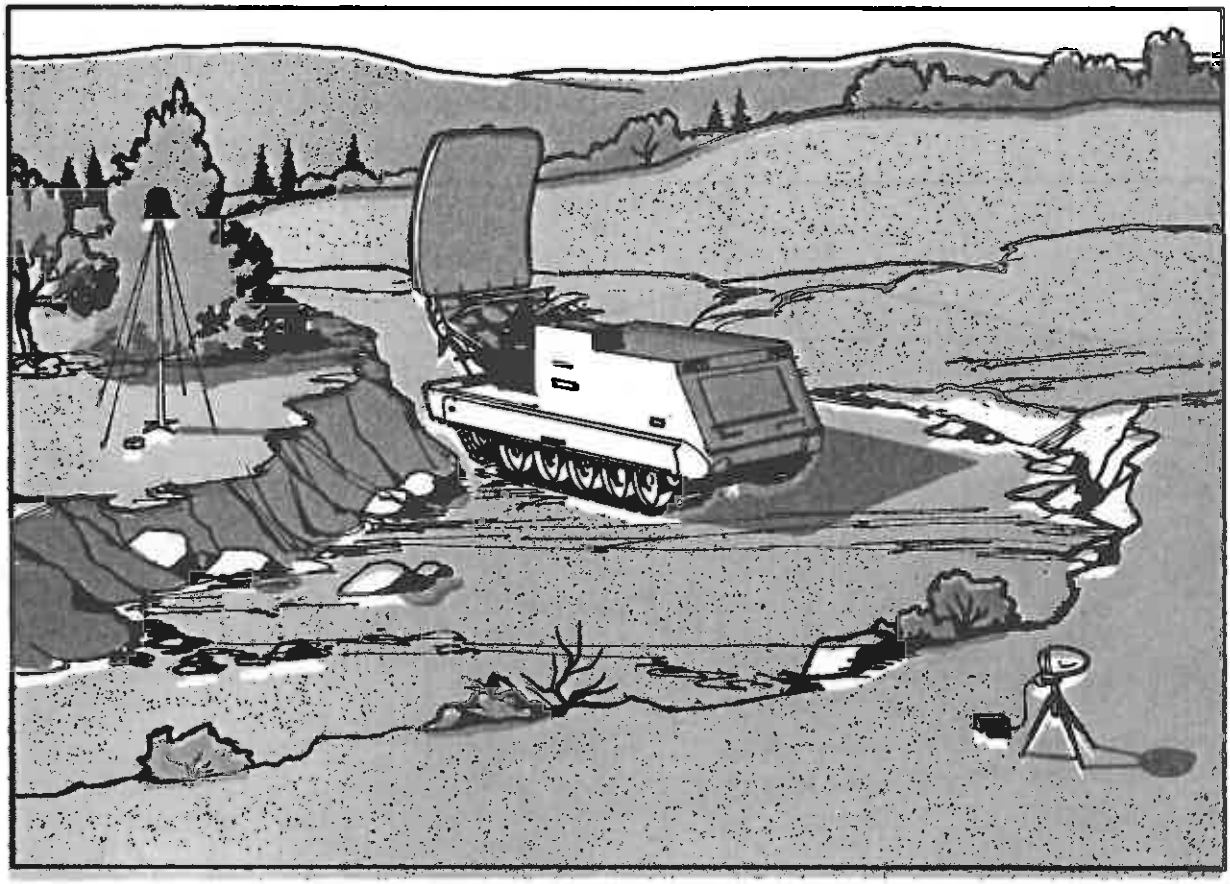
Operation of a vehicle, for example, is a comparatively simple task for most US Army personnel; nevertheless, a definitive training and licensing program is required to insure personal and group safety as well as to prevent equipment abuse. In combat, misuse of the radio through ignorance or carelessness can result in the death of an entire unit.

Use of any tactical radio should be restricted to individuals, especially officers, who continually demonstrate equal qualification in both radio-operator skills ***and*** COMSEC.

Though this circular pertains chiefly to RDF of VHF and UHF, FM, single-channel communication emitters, radars and VHF microwave transmitters pose special problems to be considered in conjunction with communication emitters.

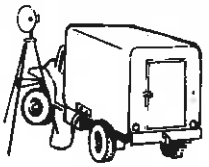
The nature of a radar wave as opposed to that of an HF or VHF radio wave makes direction-finding of a radar very accurate and lucrative. Direction-finding of radars can be very precise — to within a CEP of 50 meters at a range of 10 to 20 kilometers. This accuracy is sufficient for directing immediate and effective artillery fire. Too frequently, US Army units collocate radars with radio transmitters, especially in artillery units. Even when the radar operator practices good electronic security (ELSEC), the combination of radar signal and radio traffic provides considerably more SIGINT to the

enemy than when emitters are separated. This is an opportunity for better use of landline communications. Do not locate radars near communication centers or command and control areas. Insure that radar equipment operators practice good ELSEC.

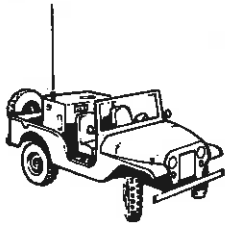


THE BEST RDF TARGETS ON THE BATTLEFIELD

Microwave communications systems use highly directional antennas. An RDF set has to be directly in the path of the microwave signal before it is effective, and still the distance to the transmitter is difficult to measure accurately. It is not uncommon, however, to observe microwave system operators using an HF or VHF radio with an omnidirectional antenna to communicate from one end of a microwave link to the other. High frequency or VHF communications usually reflect service traffic distinctly familiar only to microwave systems used at command posts.



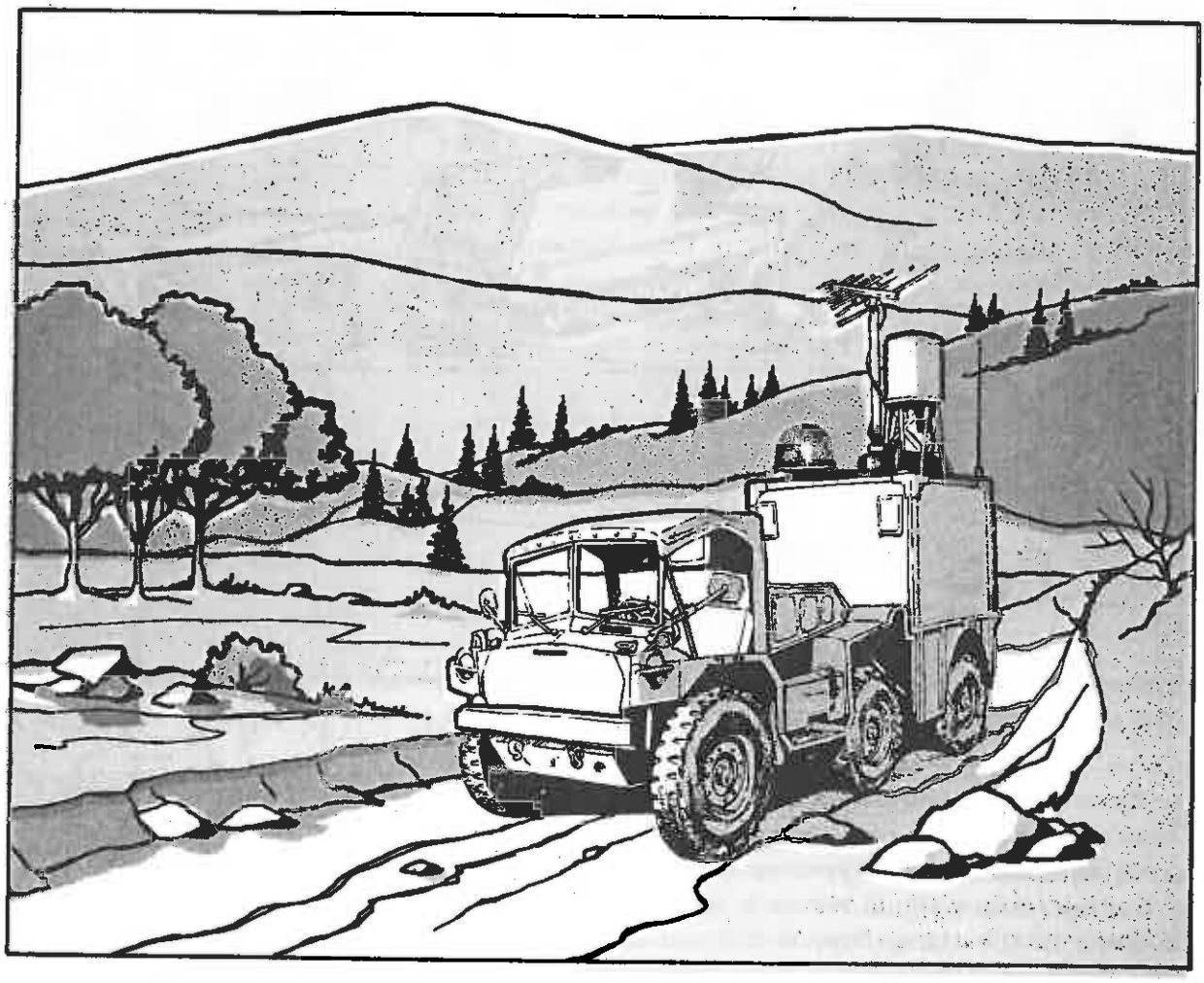
MULTICHANNEL LINK



AN/GRC 106 HF
VOICE ORDER WIRE

TAKE SPECIAL CARE WITH JAMMERS

Friendly jammers are also among the biggest RDF electromagnetic targets on the battlefield. No longer can these high radiation devices be deployed to the highest terrain to operate with impunity for extended periods. The modern battlefield requires mobile jammers, capable of moving constantly while still operating. The high amount of radiated power and the peculiar signal transmitted by jammers enable enemy RDF to easily identify them as targets for suppressive fires. Deployment of tactical jammers requires optimum signal security tactics.



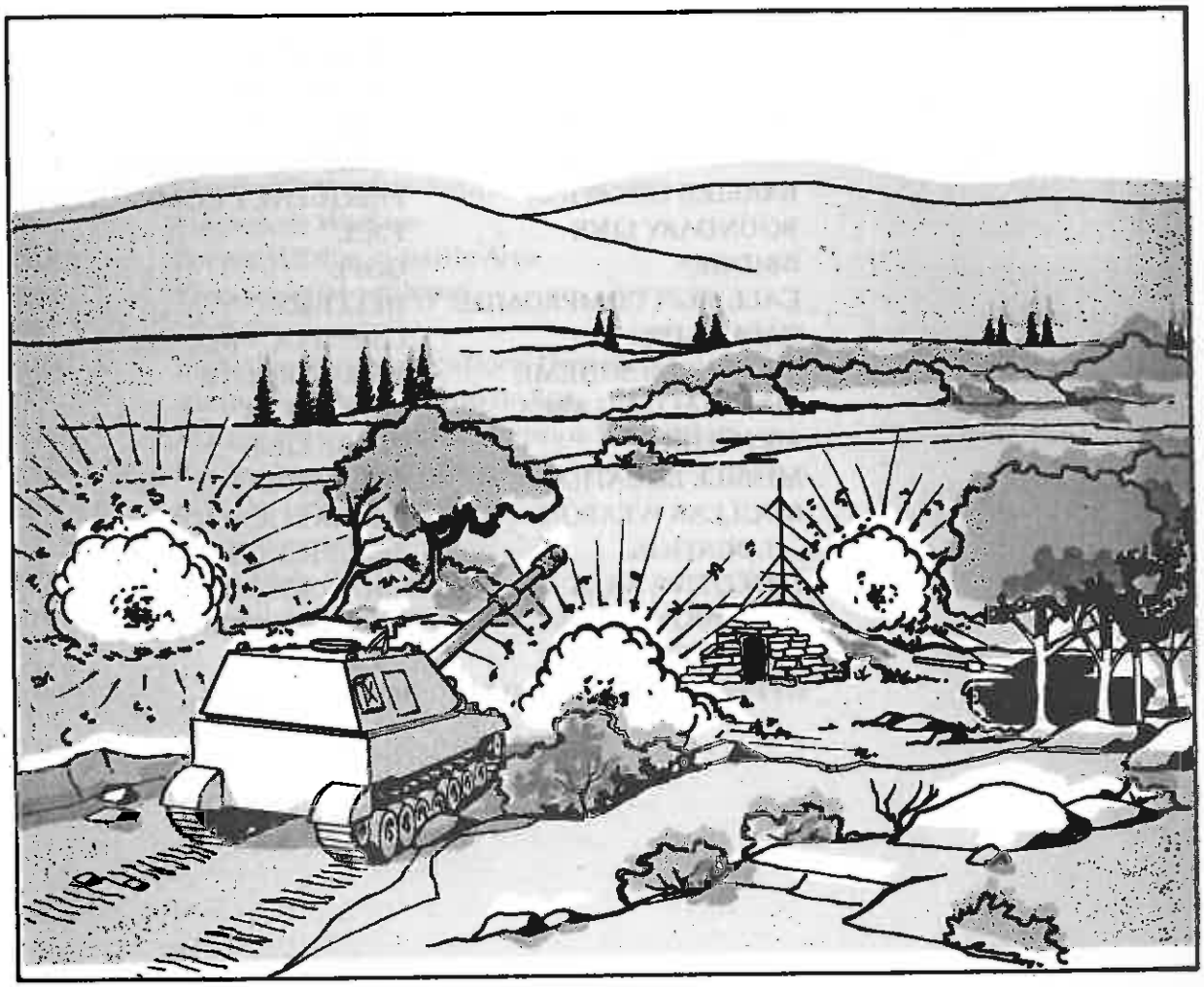
Jammers must radiate large power levels across the FEBA and be located close to the FEBA. These conditions create considerable vulnerability with a high probability of intercept and accurate DF locations.

CHANGE CALL SIGNS, FREQUENCIES, SCHEDULES

Change call signs, frequencies, and schedules at least every 24 hours; change call-sign suffixes as well. Don't circumvent the automated CEOI. These techniques reduce the enemy's ability to analyze RDF reports in conjunction with COMINT.

Electronic emitters can reveal locations of units, weapons, and command posts because these locations can be approximately determined by direction-finding and then refined to an accuracy sufficient for target acquisition by:

- plain text revelation,
- reference to terrain features by the operator, and
- terrain analysis.



APPENDIX A

INFORMATION MOST OFTEN REVEALED USING PLAIN TEXT

RADIO OPERATORS USING PLAIN TEXT MOST OFTEN REVEAL:

ADA LOCATION
AIRBORNE LAUNCH AREA
AIRHEAD
AIRSTRIKE TARGETS
ASP
ARMOR LOCATION
ASSAULT STRIP
ARTY LOCATION
ARTY TARGETS
AUTHENTICATION FAILURE
AVENUE OF APPROACH
BARRIER LOCATION
BOUNDARY LINE
BRIDGE
CALL SIGN COMPROMISE
CAPABILITY
MANEUVER SCHEME
MARSHALLING AREA
MINE FIELD
MISSILE LOCATION
NUCLEAR WEAPON LOCATION
OBJECTIVE AREA
OBSERVATION POST
OFFENSIVE PLANS
OFFENSE VULNERABILITY
COMMAND POST
COMMUNICATION SITE
CONCENTRATIONS (TROOP)
CONVOY (TIME - LOCATION)
DEFENSE POSITION
DEPLOYMENT SCHEME
DGZ
DZ/LZ/PZ
EVASION ROUTE
FEBA
FORWARD STAGING AO
FREQUENCY COMPROMISE
FSCL
GOPL
HELI PAD
LRRP (LOC - ROUTE)
PATROL ROUTE
PERIMETER
PHASE LINE
POL SUPPLY
RADAR LOCATION
RESUPPLY LOCATION
SHORTAGES (CRITICAL)
TACTICAL OPERATION CENTER
VIP LOCATIONS

APPENDIX B

GLOSSARY

AAA	Antiaircraft Artillery
AM	Amplitude Modulated
APC	Armored Personnel Carrier
ARDF	Airborne Radio Direction Finding
CEOI	Communications-Electronics Operating Instructions
CEP	Circular Error Probability
COMINT	Communications Intelligence
COMSEC	Communications Security
DF	Direction-Finding
ECCM	Electronic Counter-Counter Measures
ECM	Electronic Counter Measures
EEP	Elliptic Error Probability
ELSEC	Electronic Security
ERP	Effective Radiated Power
ESM	Electronic Warfare Support Measures
EW	Electronic Warfare
FEBA	Forward Edge of Battle Area
FM	Frequency Modulated
HF	High Frequency
ICD	Imitative Communications Deception
IFF	Identification as Friend or Foe
MCD	Manipulative Communications Deception
RDF	Radio Direction Finding
SIGINT	Signals Intelligence
SIGSEC	Signal Security
UHF	Ultra High Frequency
VHF	Very High Frequency

By Order of the Secretary of the Army:

BERNARD W. ROGERS
General, United States Army
Chief of Staff

Official:

J. C. PENNINGTON
Brigadier General, United States Army
The Adjutant General

DISTRIBUTION:

Active Army and USAR: To be distributed in accordance with DA Form 12-11B, Requirements for Combat Intelligence (Qty rqr block no. 273); and Electronic Warfare (U) (Qty rqr block no. 325).

ARNG: To be distributed in accordance with DA Form 12-11B, Requirements for Combat Intelligence (Qty rqr block no. 273).

Additional copies can be requisitioned (DA Form 17) from the US Army Adjutant General Publications Center, 2800 Eastern Boulevard, Baltimore, MD 21200.

☆ U.S. GOVERNMENT PRINTING OFFICE: 1978—735-082/ 233