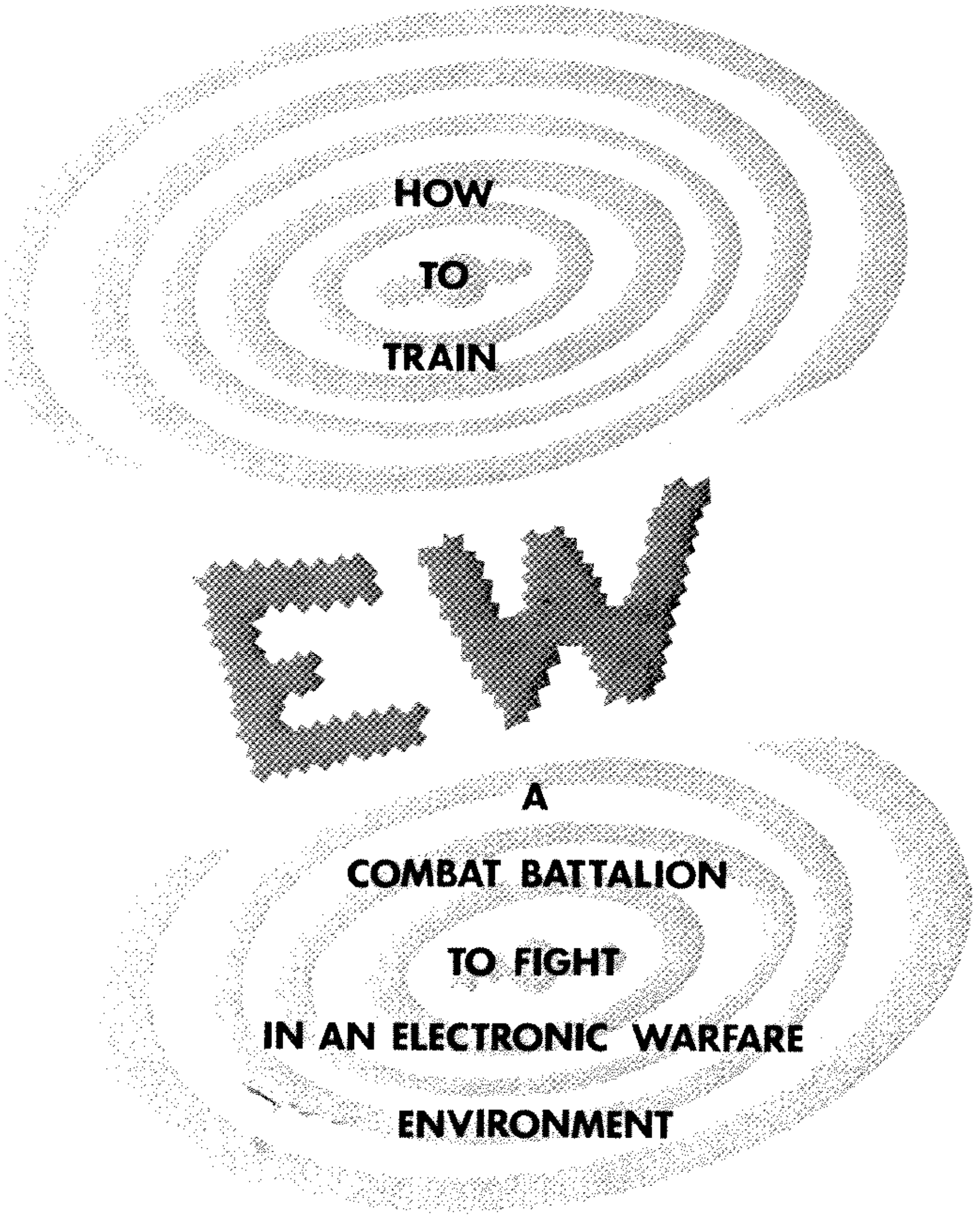
TC 32-10

DEPARTMENT OF THE ARMY TRAINING CIRCULAR



HOW TO TRAIN EW

A COMBAT BATTALION TO FIGHT IN AN ELECTRONIC WARFARE ENVIRONMENT

HEADQUARTERS, DEPARTMENT OF THE ARMY

JULY 1975

Users of this circular are encouraged to submit recommendations to improve its clarity or accuracy. Comments should be keyed to the specific page, paragraph, and line of the text to which they refer. Reasons should be provided for each comment to ensure understanding and permit complete evaluation. Comments should be prepared using DA Form 2028 (Recommended Changes to Publications) and forwarded direct to: Commander, US Army Security Agency Training Center and School, ATTN: IATPL–TL, Fort Devens, Massachusetts, 01433.

INTRODUCTION

This training circular provides training information for soldier-communicators and commanders who will be expected to operate in an electronic warfare environment.

Part I, For the Soldier, discusses the expected techniques which may be used against him and shows some of the steps that can be taken to reduce or prevent enemy success.

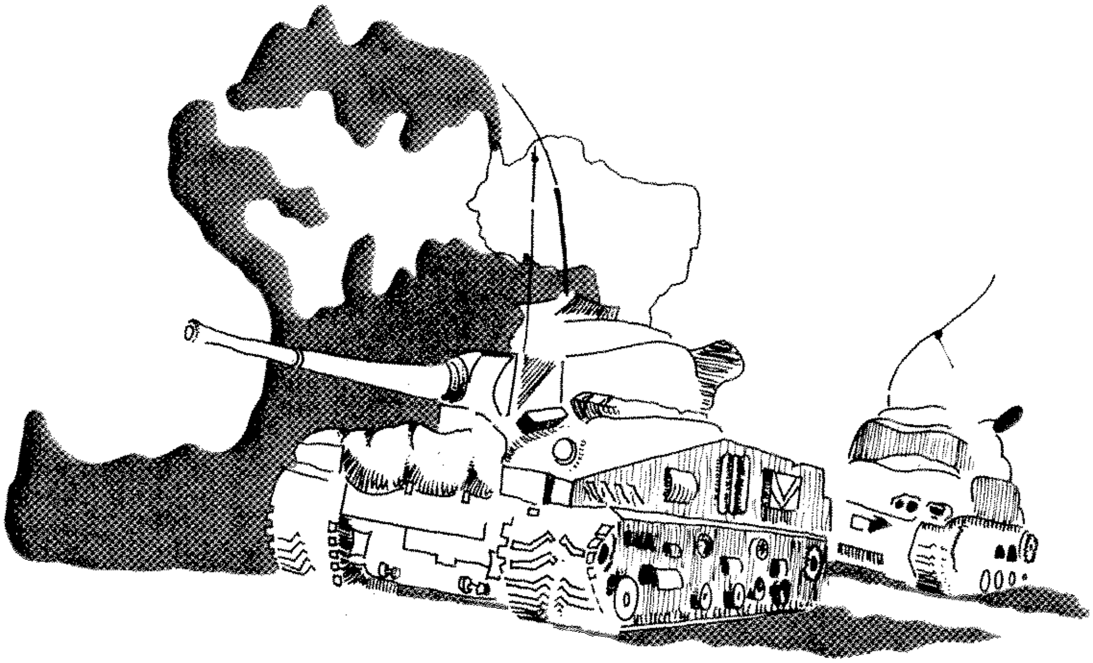
Part II, For the Commander, provides training information to help the commander organize and conduct electronic warfare training which will produce successful results on the field of battle.

PART I

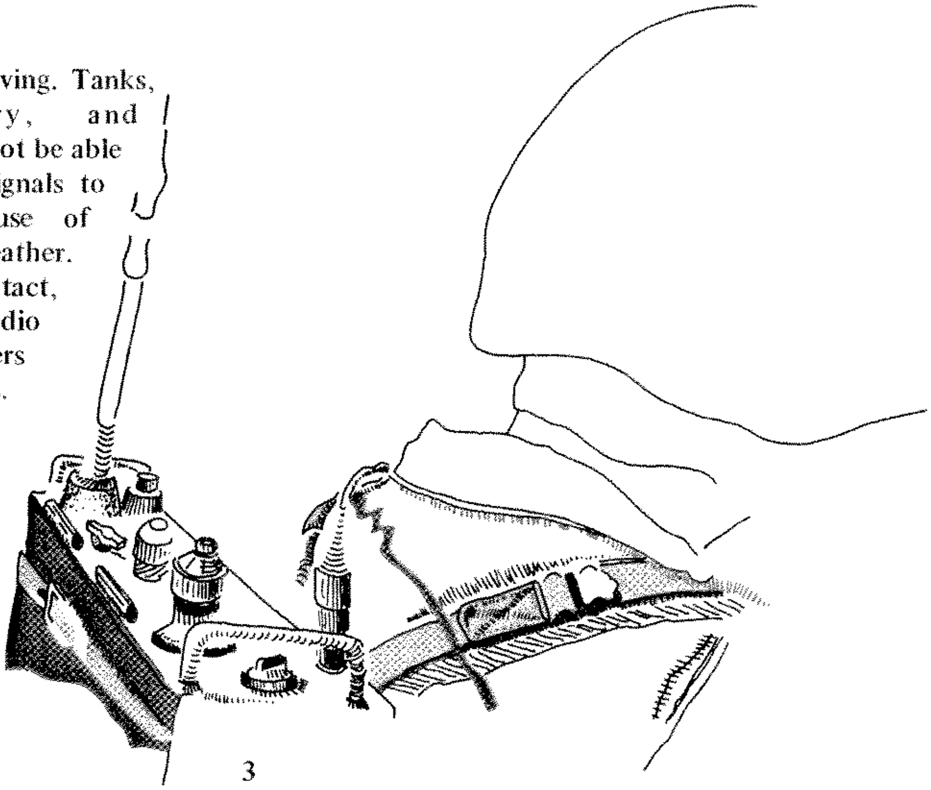
FOR THE SOLDIER

Electronic warfare, the so-called "Wizard War" or "War in the Ether" is not new. Armies have used it since World War I to favorably change the outcome of battle. It is not as mysterious as it appears and, through proper training and the use of common sense procedures, you can defeat it.

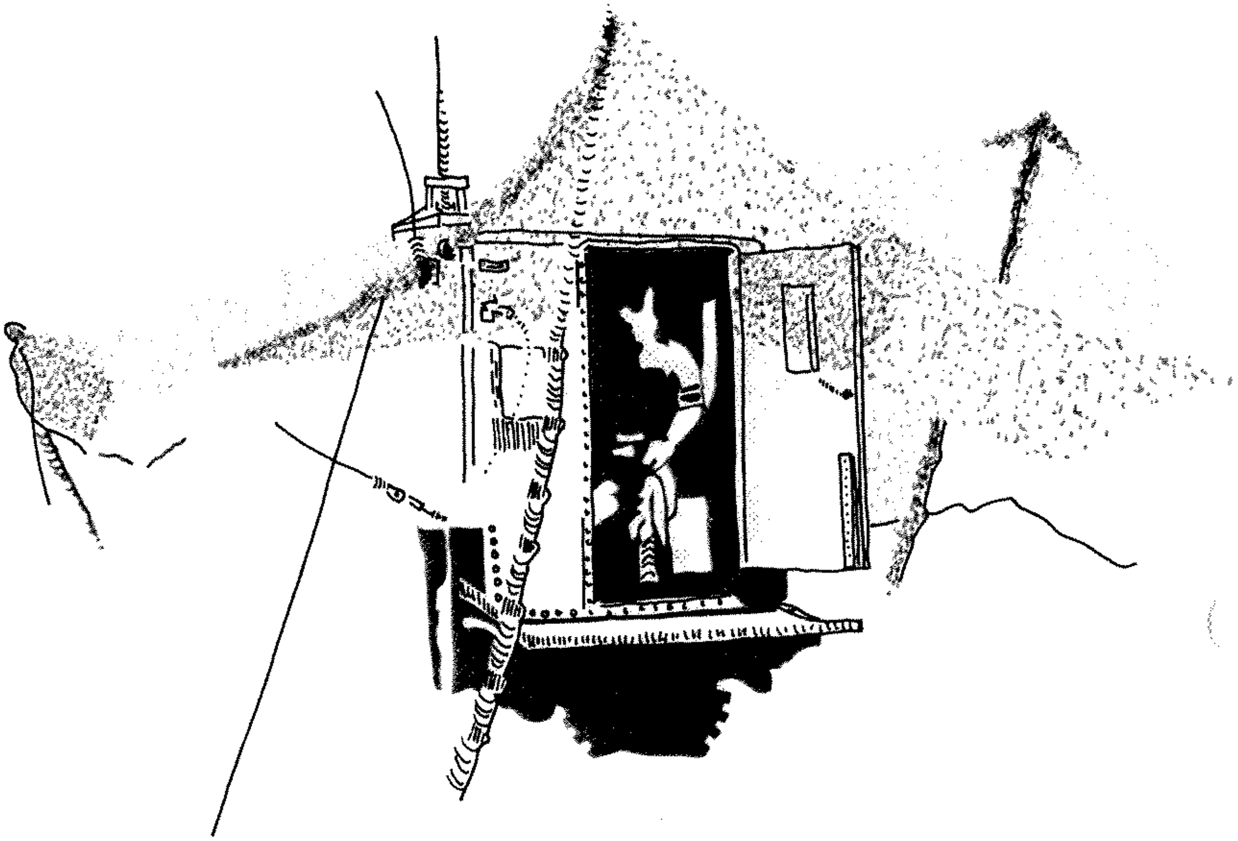
DURING BATTLE,
COMMAND AND CONTROL
IS USUALLY MAINTAINED
BY THE USE OF RADIO.



The action is fast moving. Tanks, mechanized infantry, and dismounted troops may not be able to use hand and arm signals to keep in contact because of terrain, darkness, or weather. Without visual contact, commanders rely on radio commo to get their orders out and to receive reports.



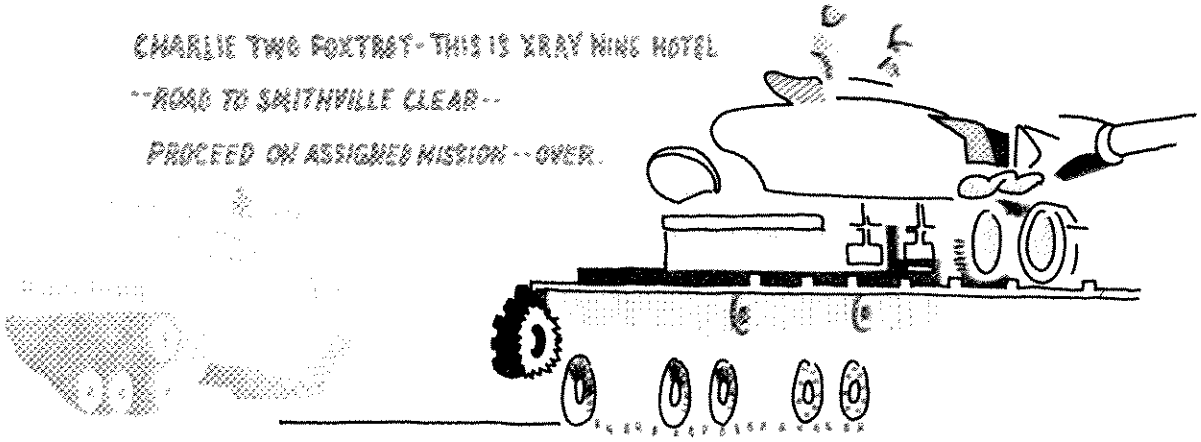
RADIO CAN PROVIDE THE ENEMY WITH INFORMATION THAT HE CAN USE TO CHANGE THE OUTCOME OF BATTLE.



It is easy to forget that radio waves are difficult, if not impossible, to control. Once the transmitter is keyed, you have very little control over who can listen to the commo. All that the enemy needs to listen to your commo is a simple radio receiver.

THIS IS HOW YOUR RADIO BECOMES A SOURCE OF INTELLIGENCE FOR THE ENEMY.

1. The enemy listens to your radio traffic.


CHARLIE TWO FOXTROT- THIS IS XRAY NINE HOTEL
--ROAD TO SMITHVILLE CLEAR--
PROCEED ON ASSIGNED MISSION --OVER.

2. The enemy studies your commo using highly skilled analysts that can recognize your strengths and weaknesses.

3. The enemy reports your weaknesses to his commander, who will decide what action to take to exploit your weakness.

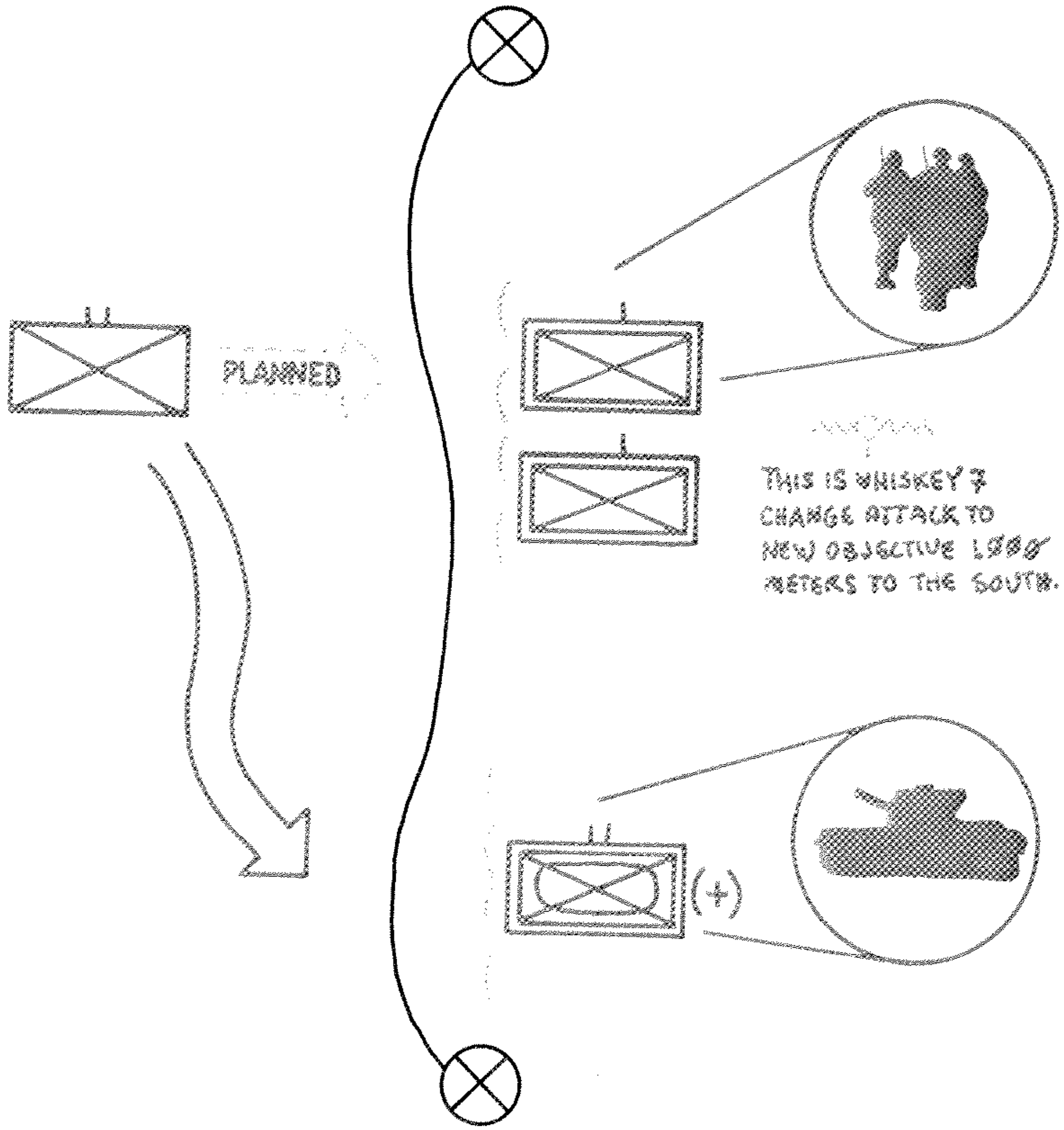
THIS IS WHAT THE ENEMY CAN DO.

1. The enemy commander may decide to deceive you because you do not authenticate properly. He can use soldiers skilled in the English language to enter your net and give you false instructions, such as:

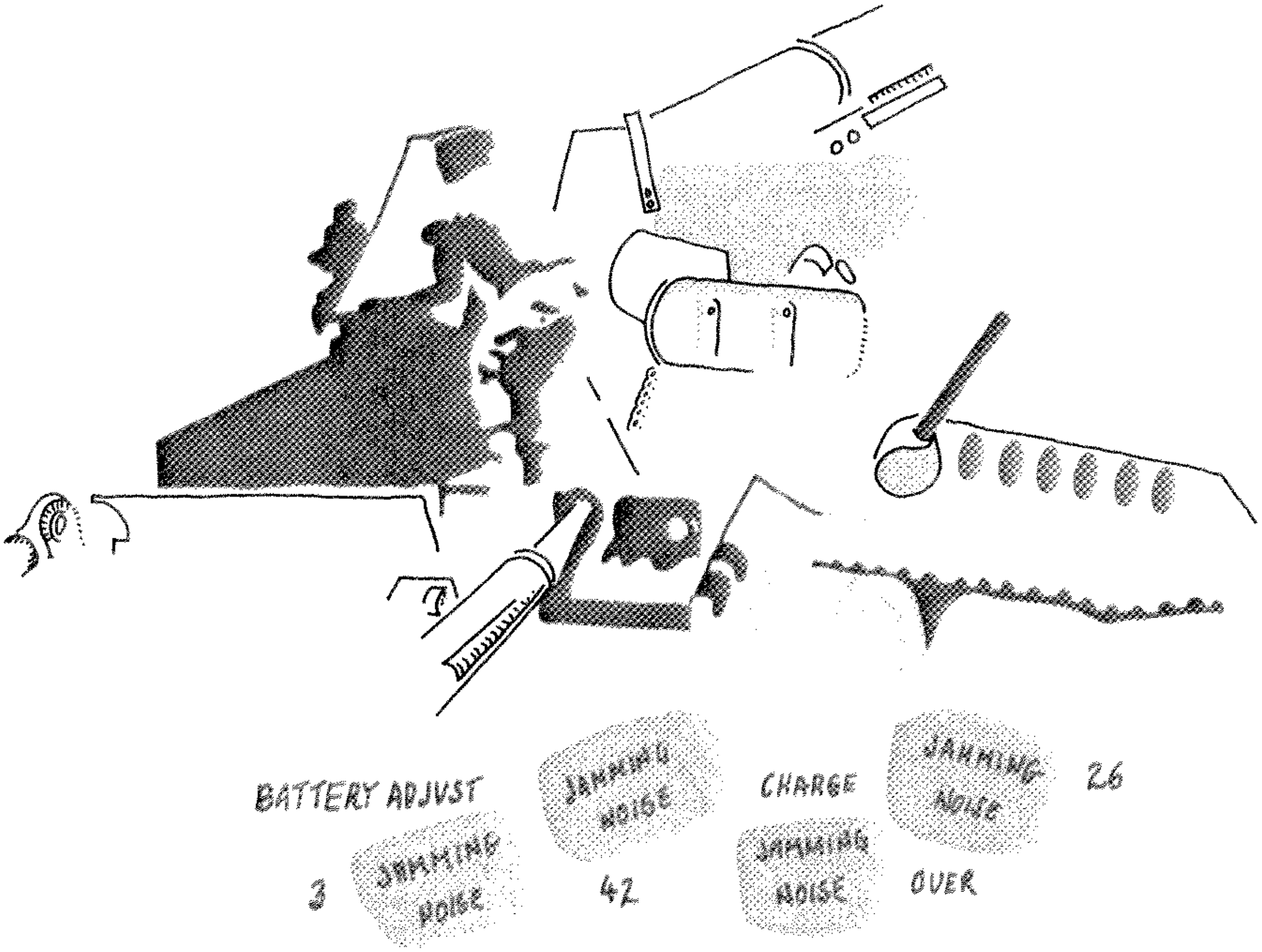
† Giving the coordinates of your CP to your own artillery units for a fire mission.

† Directing an attacking force away from his weak positions or formations, giving them time to move forces into the area or to clear the area entirely.

† Directing your unit toward a much stronger enemy unit.



2. Or, the enemy commander may decide to foul up your commo by jamming your channel so that you can't get your messages through at the most critical time.



THIS IS WHAT YOU CAN DO.

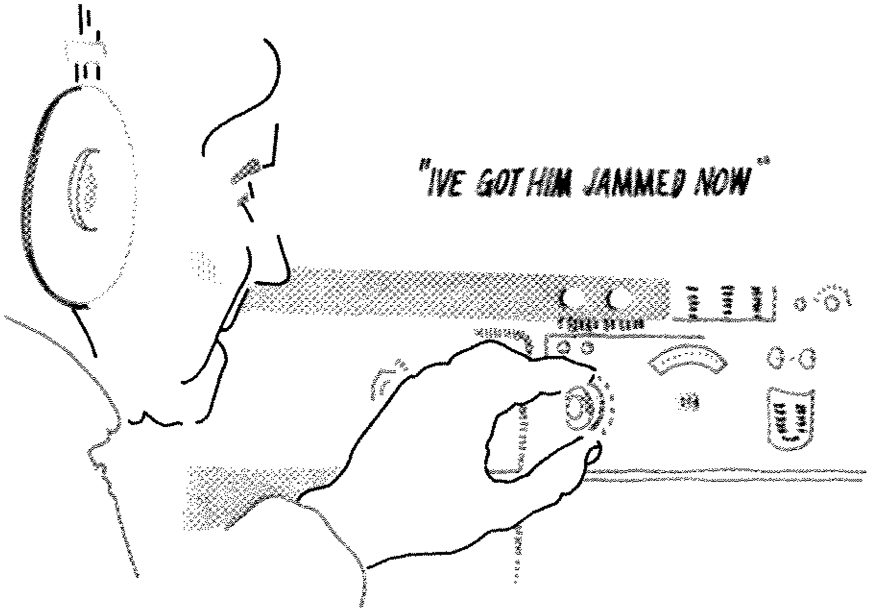
But if you follow these rules you can defeat it.

1. Jamming is more difficult to contend with. First you have to be sure that you are being jammed.

† Distinguish between jamming and receiver trouble. When receiving interference, disconnect the antenna from the binding post. If the noise decreases, then the interference is coming through the antenna from outside the set. The trouble is in the set if the noise does not decrease.

† Distinguish jamming from local interference. If the noise decreases when the antenna is disconnected, there is a possibility that it may be caused by local interference. Try tuning several hundred kilohertz on each side of the signal frequency to which you are tuned. If there is no change in intensity, then you are receiving electrical interference from a nearby source (power line, generator set, or radar set). When you have decided that the interference is enemy jamming, then do the following:

† Never say that you are being jammed. If you do, the enemy knows that he is being successful.



† Next, you should try to work through the jamming. Ask and give *say again* as necessary. If that doesn't work, and you have an idea of the direction from which the jamming is coming, try to get a natural obstacle between your receiver and his jammer.

† Change antennas. For example, use a directional antenna if it will help you get through.

† If you can, retune your equipment so that it is slightly above or below your assigned frequency. Of course, with receivers which incorporate preset channels, this is not possible.

† Also, you might try:

Using another station in the net to relay, or –
Using AM instead of FM or vice versa, or –
Using a landline if available, or –
Using a messenger.

† Above all – continue to operate. The last step you should consider is to change to your alternate frequency. Only do this as a last resort, when the traffic you have is so important that it has to reach the other guy NOW and no other way is possible.

2. The enemy's attempts to deceive you can be defeated by the following:

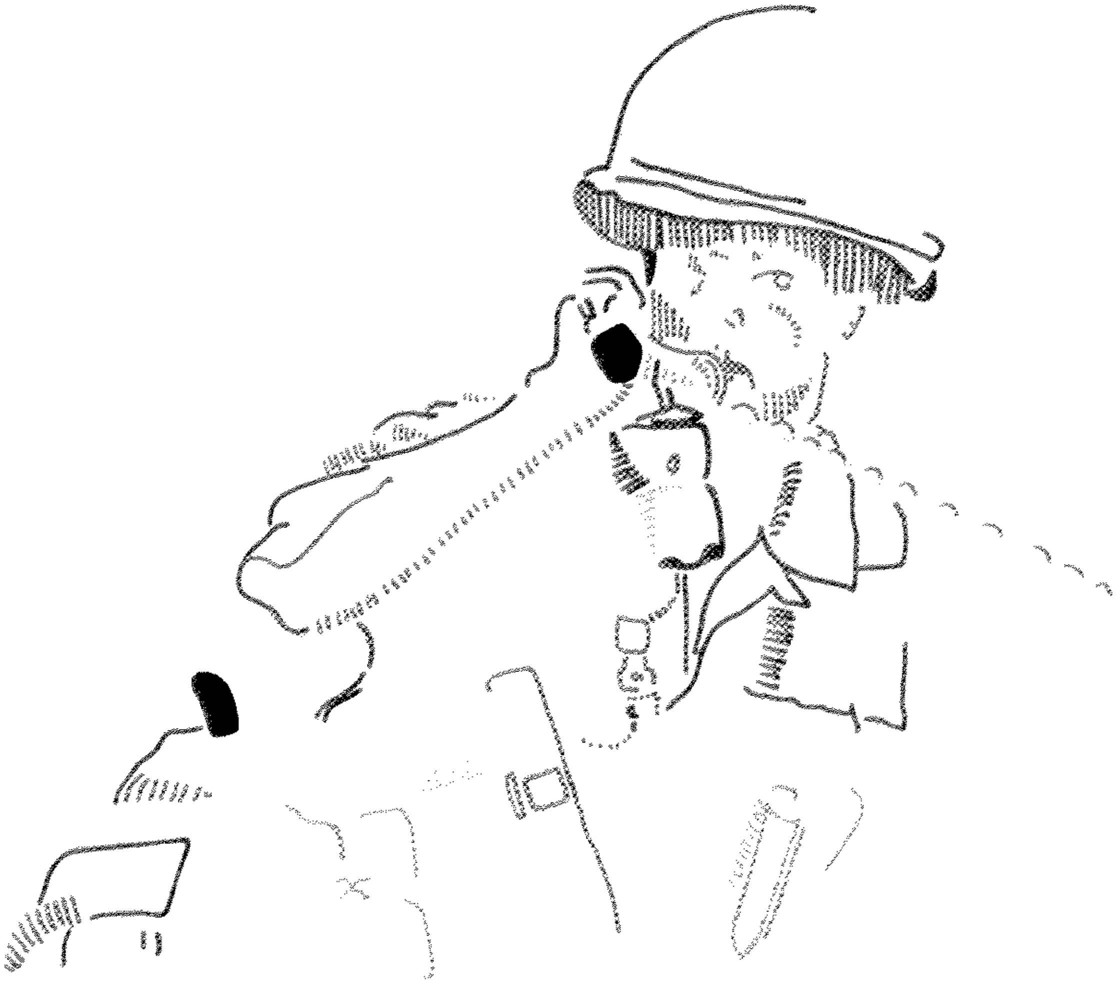
† *Communicate only when necessary.* Don't jawbone on the radio.

† *Use proper radiotelephone procedure.* No shortcuts, nothing fancy, just plain, simple, and correct radiotelephone procedures that you learned in a service school or during unit training.

† *Authenticate when required.* Know how to use your authentication system. Compromises occur when you don't know how the challenge and reply works. If you are uncertain, ask your supervisor – he'll talk it over with you and explain it. If you have any questions on why it is necessary to authenticate or why a home-made system is dangerous, ask your commo officer. (Also, see DA Cir 380–8, Mandatory Authentication Requirements.)

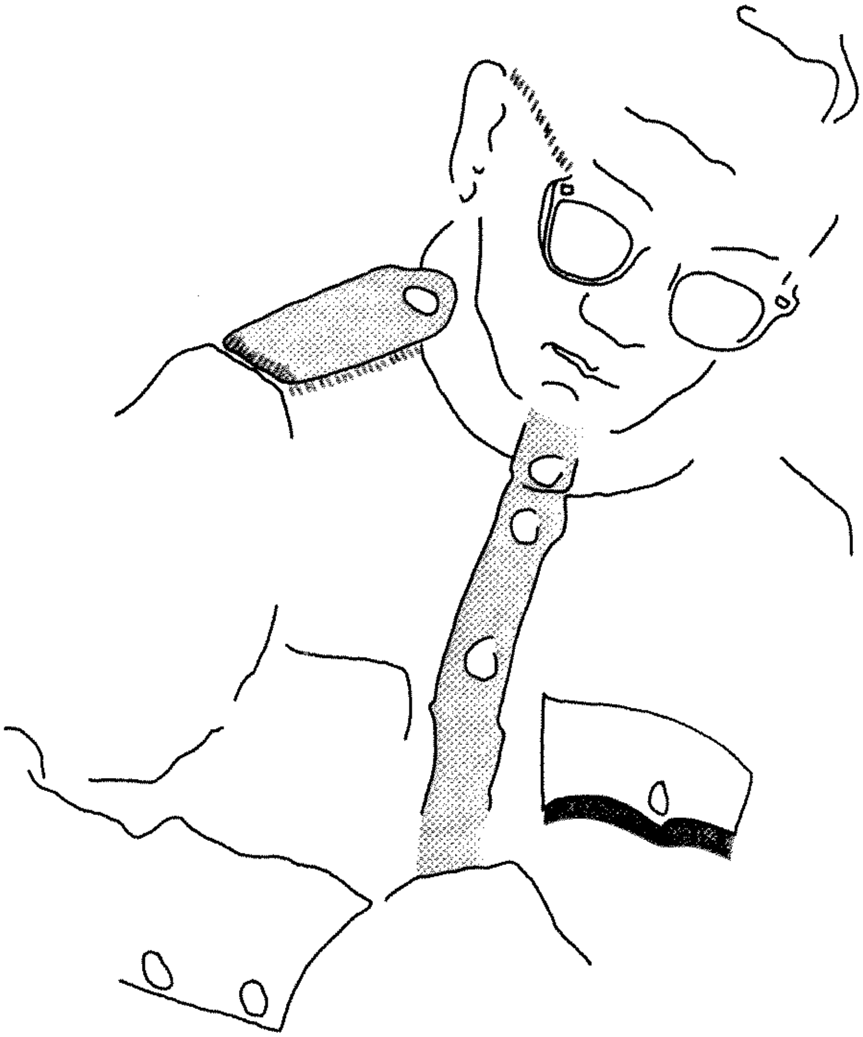
† *Use short transmissions.* Keep the length of radio transmissions under 8 seconds whenever possible. Short transmissions lessen the chance of the enemy fixing your location with direction finders or exploiting your communications.

† *Do not keep to a schedule.* Vary times for "commo checks."



† *Never, Never,* send traffic in anything but an approved cryptosystem. Cryptanalysts love the guy who thinks he can come up with a new code that can't be broken. A solution to your locally produced code can be done in about as much time as it takes to solve the daily crossword puzzle.

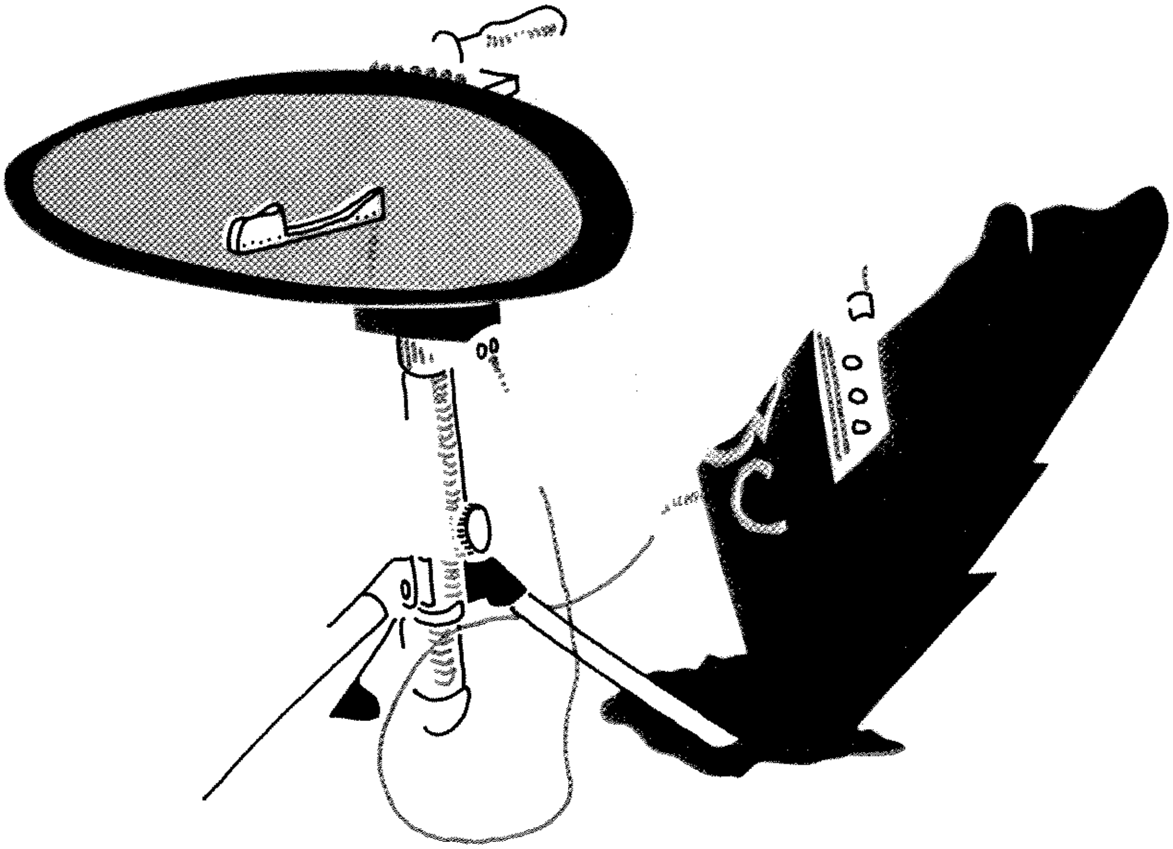
Make no mistake about this, cryptanalysts are as good at their job as you are at yours (maybe even better). They like their work and they've been doing it for a long time. THEY ARE EXPERTS.



Once you suspect you have been deceived or jammed, you must report the incident so that a special report can be made through channels. Reporting procedures should be in your SOP or CEOI.

WHAT ABOUT GROUND SURVEILLANCE RADAR?

A special problem exists with your ground surveillance radar (GSR). In order for this equipment to do its job, it must radiate into enemy territory, which means that it can be intercepted.



There is not much that you can do about this, except to provide as little information as possible to the enemy. Follow these guidelines: (Also, see FM 32–6.)

1. Operate the equipment according to the instructions.
2. Select proper target background.
3. When tuning the equipment, aim it away from the FEBA, not toward the enemy.
4. Operate the GSR only when you have to. When you don't have a mission, turn it off.
5. Report any jamming attempts immediately.

PART II

FOR THE COMMANDER

Electronic countermeasures have been used to alter the course of battle. Because of its importance as a weapons system, you must expect the enemy to use jamming and deception against you. To be prepared to operate in an electronic warfare environment, you must train your operators to defeat jamming and deception techniques during all phases of unit training.

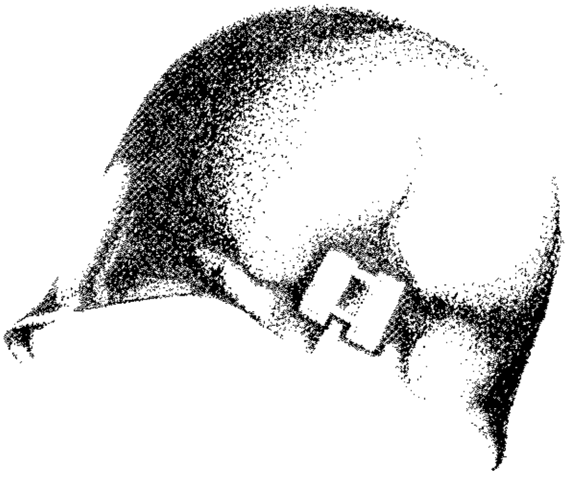
Operator actions related to jamming and deception are contained in Part I. From these fundamentals, you can develop a training program that will allow your unit to perform its mission in an electronic warfare environment.

Advice and assistance in the conduct and evaluation of your training is available through Army Security Agency (ASA) sources, either from an ASA unit or from the SIGINT Support Element/Electronic Warfare Element (SSE/EWE) located at division or separate brigade level.

Improved communications security and electronics discipline provide less opportunity for the enemy and ensure that you will be able to successfully complete your mission.

Ensure your unit has a meaningful and workable COMSEC annex to the unit FSOP or TACSOP. The unit Signal Officer, prefix "E" trained staff personnel, and local ASA personnel are excellent sources of information for writing a COMSEC SOP.

WHAT CAN YOU, AS A COMMANDER, DO TO IMPROVE THE TECHNIQUES AND PROCEDURES USED BY YOUR SOLDIERS?



1. Evaluate your communications. During all phases of training, listen to your nets to ensure that the operators are following the procedures outlined in the CEOI and CESI. If you note any irregularities, correct them.

2. Ensure that all equipment operates at the lowest power that will get the job done.

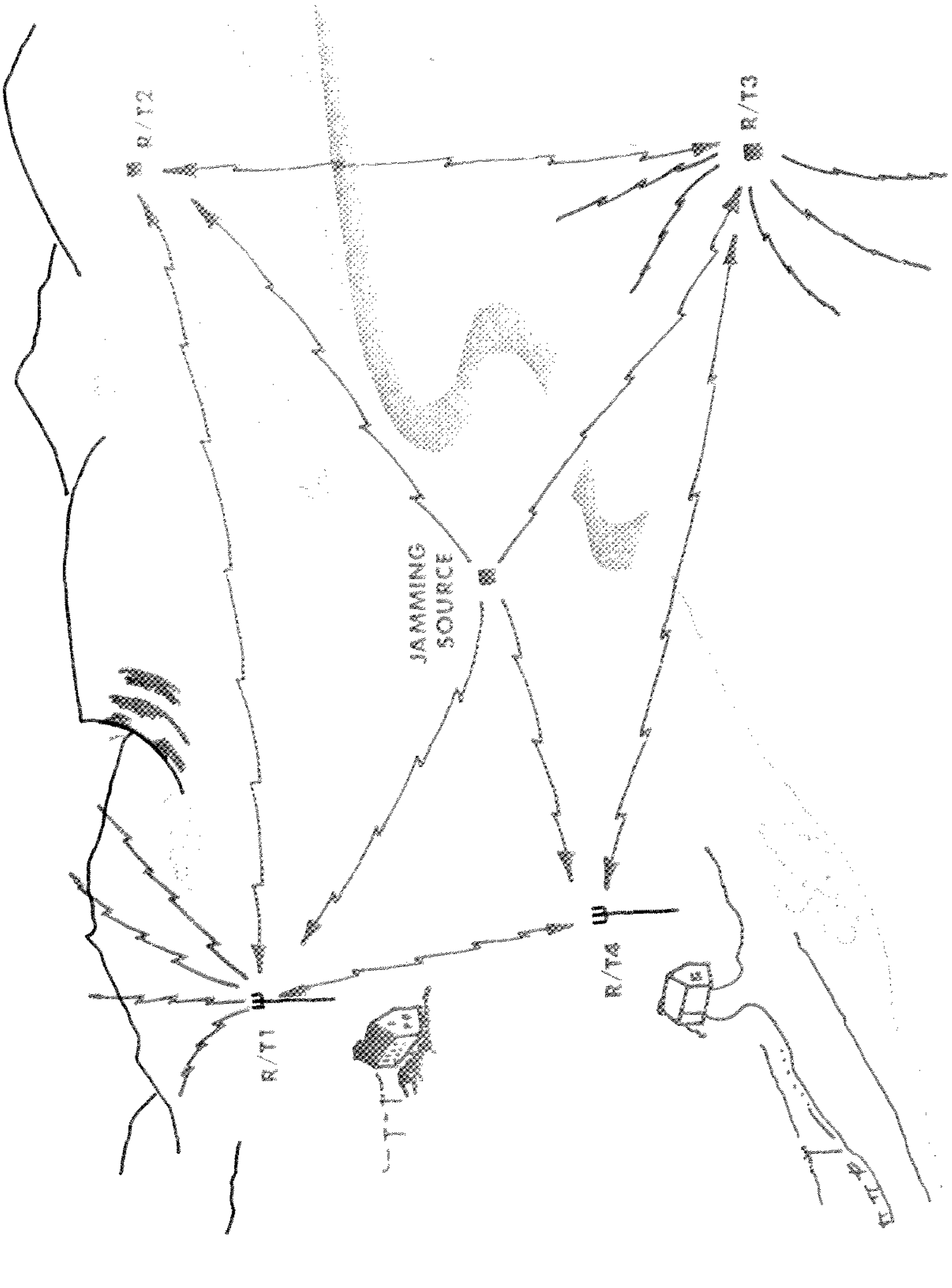
3. Expose your operators to jamming. There are several methods that you can use to simulate a jamming signal.

† Operate a regular communications transmitter at a power setting that is higher than the radios that you are trying to jam. Key the microphone whenever the other stations are trying to talk.

† Use a tape recorder and place your microphone near the recorder's speaker. You can create your own jamming tapes by recording noise, music, or any other type of signal.

† Use a transistor radio tuned to a spot on the tuning dial where there is no station. The noise on the empty frequency (channel) plus any ignition noise of your vehicle make an excellent jamming signal.

† Obtain an Interference Generator, SG–886T/UR (FSN 6940–474–9495) from your local Training Aids Services Office. The Instruction Manual (IM 11–6940–210–14) tells you how to connect the equipment to your communications gear and shows how the equipment can be used to jam. The SG–886T/UR is also intended to improve the ability of the operator to recognize some of the fundamental types of jamming. This ability is required when reporting jamming incidents. Once you have obtained a jamming source and have determined which piece of equipment will be used as the jammer, the location of the jammer must be determined. Locate the transmitter so that it is closer to the intended target than the other stations in the net. (See figure on page 15) After the jammer is in position, operate it for short periods and listen when the jammer is off to determine if the operators noticed the presence of the jammer on the channel. The periods of ON–time can be increased when it is apparent that the operators are trying to get a message through. As the jamming effectiveness increases, the operators' frustration at not being able to get the message through also increases. Ideally, the messages should be delayed past the time when they can be acted upon. You may want to get a local ASA unit to perform jamming during field exercises. If your operators know how to react to jamming during a training exercise, you can be confident that they will be able to communicate during battle.


R/T2
R/T3
JAMMING SOURCE
R/T1
R/T4

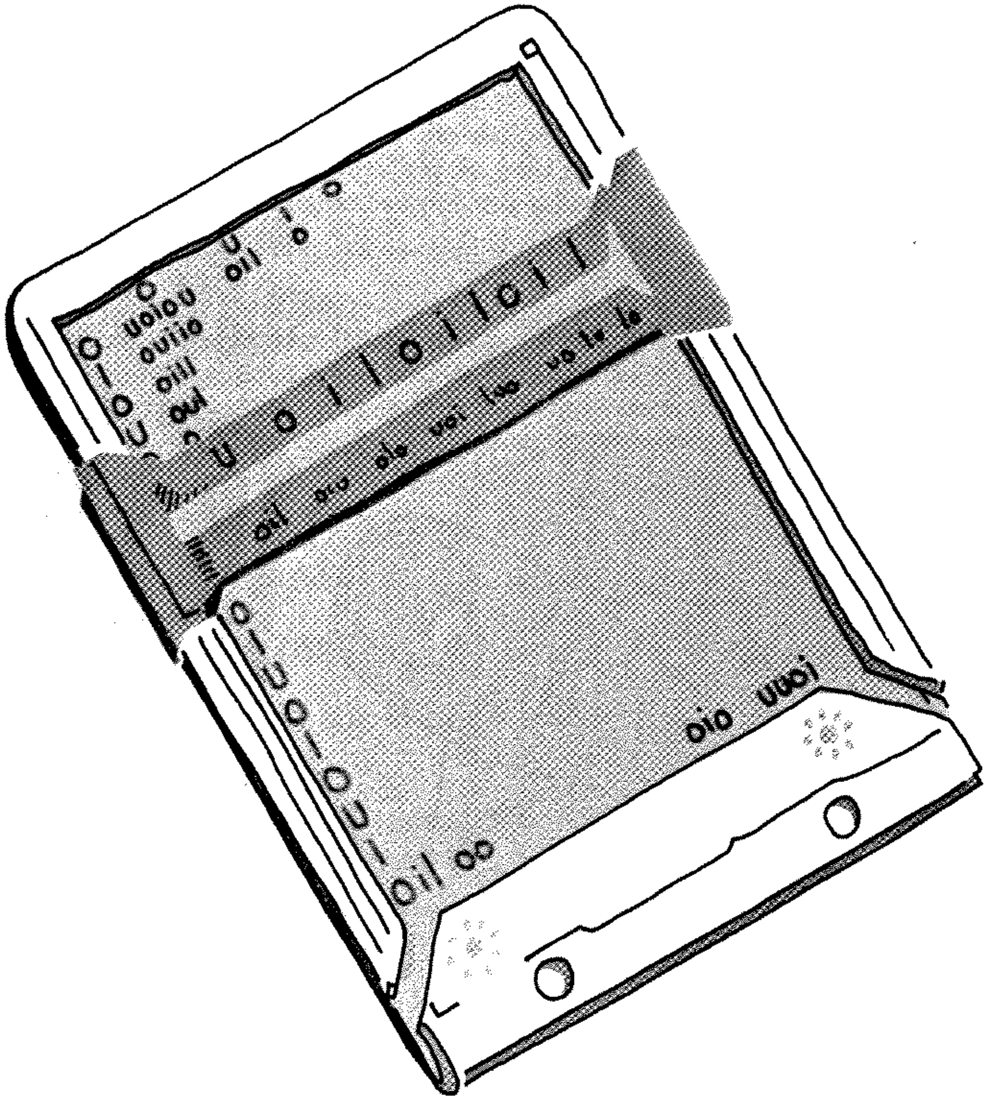
4. *Train operators to authenticate.*

† Operators must be trained to defeat communications deception. An enemy can pass false instructions to your unit when your operators fail to require authentication. To defeat deception, authentication must be used properly. The most widely used authentication system is DRYAD. The operating instructions are contained in NAO 3 ( ). They are readily available and training versions of the tables are not classified. They bear the protective marking "For Official Use Only," to keep them from unauthorized sources. Since your communicators require the tables for practice, they MUST be made available to them.

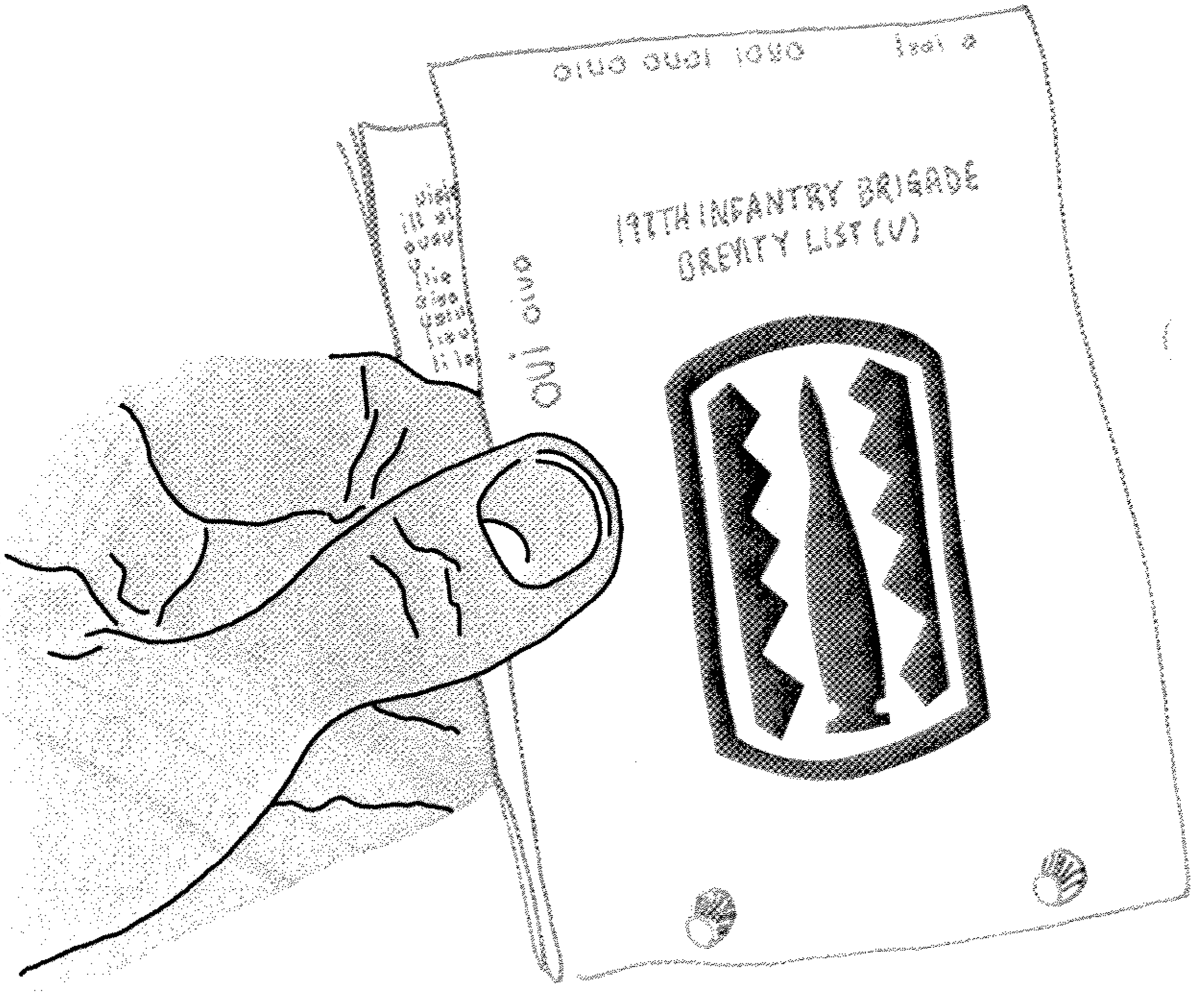
† Operators must know when to authenticate and how to do it. A challenge-reply authentication system will be used whenever possible. When using a challenge-reply type of system, the called party will always make the first challenge. When a caller desires authentication, he must invite a challenge by stating that he is prepared to authenticate.

5. *Train operators to use cryptosystems and brevity lists.*

† **The numeral cryptosystem, DRYAD, is not difficult to use, but your operators need practice so that the encipher-decipher operations become second nature to them.**



† Brevity lists are unclassified and bear the marking "For Official Use Only." Training is an official use. Operators need practice with brevity lists so that they can find the items easily and speedily. The code groups in the brevity list must be encoded using the DRYAD system prior to transmission. REMEMBER THAT BREVITY LISTS DO NOT PROVIDE SECURITY.



† Remember to train your officers because in many instances they are the users of communications equipment.

> *An effective training situation can be created by preparing typical messages that can be expected in your unit. Give the soldiers the DRYAD system and brevity lists, then have them encrypt the messages and pass them to other soldiers to decrypt. Check the results. You can even organize the soldiers into teams and have them compete. Remember that speed and accuracy are equally important. The results of this type of training will be a complete familiarity with the tools that your personnel will be using.*

6. *Expose operators to deception.* To train your operators to defeat deception, obtain the assistance of another unit. Have personnel attempt to give your operators false commands during an exercise. Do not give the commander and personnel of the other unit your current authentication system. When the "bogus" personnel enter one of your nets and get challenged, have them call on another net and try to get the reply to the challenge, then go back to the original net with the correct reply. Instruct your operators not to wait more than 20–25 seconds for a reply. The challenge and reply system is designed to operate quickly. Any delay in answering a challenge may be caused by a deception attempt.

7. *Evaluate the use of Ground Surveillance Radars.* The use of Ground Surveillance Radars (GSR), forces the commander to consider the benefits to be gained as opposed to the information that will be provided to the enemy. Even when the decision is made to use GSR's, you must provide strict control over their operation. To reduce the chances of intercept by the enemy, you must ensure that your unit does not provide a pattern of operation or a unit signature that is unique and which can be used to identify your unit from others. Some of the steps that you can take to reduce the information provided to the enemy are:

† Ensure that all personnel follow the operating instructions for the equipment.

† Use only the number of GSR's that will do the job. Why use three when two will do?

† Ensure that equipment is properly maintained. Defective equipment can provide a unique signature.

† Carefully select the operating positions of the GSR in an attempt to provide background masking and side lobe absorption. (See FM 32–6.)

† Follow the CEOI precisely.

† Inspect all GSR sites to check compliance with sound site procedures.

8. *Instruct operators on what to report.* All instances of Meaconing, Intrusion, Jamming, and Interference (MIJI) must be reported. Operators must be trained on what to report and how to do it. Ensure that your CEOI contains the reporting instructions, addressees, and format of the report.

9. *Use the CEOI.* Train personnel how to use the CEOI. Ensure that they know what to do if copies of the CEOI are lost, stolen, or compromised.

EVALUATION OF YOUR UNIT

You can evaluate the performance of your unit based on the following pass/fail criteria:

1. Did operators use proper radiotelephone procedure?
2. Did operators use authentication properly?
3. Did deception succeed because the operator failed to authenticate?
4. Was traffic sent in approved cryptosystems only?
5. Were transmissions kept as short as possible?
6. Was jamming effectiveness discussed over the air?
7. Did the operator try to work through the jamming?
8. Did the operator try to relocate his antenna?
9. Did the operator use a different antenna?
10. Were alternate means used when available?
11. Were proper receiver tuning techniques employed?
12. Did the operator change to an alternate frequency when available?
13. Did the operator report the jamming or deception attempt?
14. Were GSR's properly used?
15. Did GSR operators tune equipment properly?
16. Were GSR's properly maintained?

As the combat readiness of your unit increases, contact an ASA unit for assistance to the evaluation of your electronic warfare training.

What was said of the Roman army must become a description of the US Army—

"They do not wait for war to begin before handling their arms, nor do they sit idle in peacetime . . ."

Josephus, First Century, AD

By Order of the Secretary of the Army:

FRED C. WEYAND
General, United States Army
Chief of Staff

Official:

VERNE L. BOWERS
Major General, United States Army
The Adjutant General

Distribution:

Active Army, ARNG, USAR: To be distributed in accordance with DA Form 12-11A requirements for the Infantry Battalions (Qty rqr block no. 79); Military Training Management (Qty rqr block no. 158), and DA Form 12-11B requirements for Electronic Warfare (Qty rqr block no. 325).

☆ U. S. GOVERNMENT PRINTING OFFICE : 1975 O - 578-728