ECCM TRAINING: REDUCING THE REC THREAT

by 1st Lt. Carol L. Donohue

There is a great deal of misunderstanding in the military today concerning Radioelectronic Combat (REC) and what it can do to us and our communications. Some soldiers believe it cannot affect us; others believe it is so powerful that we cannot defend against it. Both are serious misconceptions. REC could conceivably negate enough of our communications to disrupt control, but if we practice good electronic counter countermeasures (ECCM), we can decrease its effectiveness.

What is REC and what can it do to you? Radioelectronic Combat or REC is the Soviet term used to describe the integration of signals intelligence (SIGINT), intensive jamming, deception, and suppressive fires to deprive us of command and control. It is a real threat to our communications and will play a major role in any future conflict. Therefore, we must train all our communicators to defend against it.

ECCM is anything you do to ensure you and your radio are safe when you communicate. ECCM can be either preventive or remedial. Good preventive ECCM will counter any REC effort to locate you by direction finding (DF). The effects of DF can be reduced by several techniques.

One way is to prevent your transmission from reaching them at all. This is done by masking — putting an obstacle between you and the enemy's direction finders. If you used a directional antenna, this would not be necessary; however, most of our units have omnidirectional antennas.

Masking can sometimes be difficult or impossible because you may not be able to communicate if you mask properly. One solution would be to move to another site; but this, too, may be difficult. If you must remain at a site which prohibits masking, then you must be very cautious. Don't use the radio at all if you don't need it. Use alternate means to send your message, especially if it is long and/or routine. When you must use the radio, keep it short; always use proper prowords and call signs. Write your message down before transmitting if you have the time; this will prevent unnecessary delays. The shorter your message, the better your chance of avoiding DF; an ideal transmission time is 20 seconds or less.

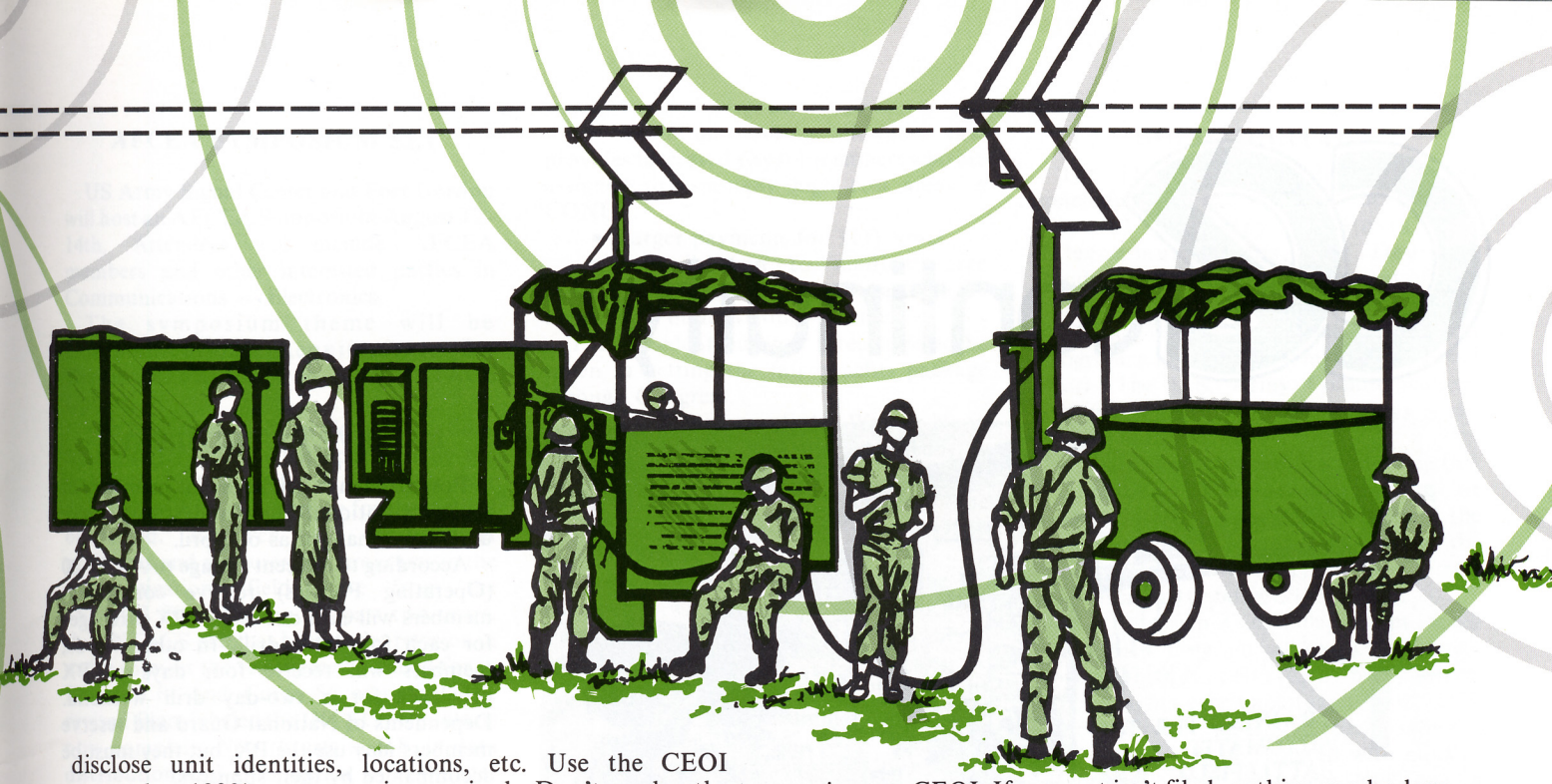
The effects of DF can also be reduced by using low power. This could prevent your signal from reaching the enemy. You should never use more power than is necessary to communicate; if you can do so effectively at a low power setting, why use high power and risk being intercepted?

Using secure communications will not prevent DF; they may not understand what you are saying, but they can still pick up your signal. The same rules will apply to both secure and nonsecure communications.

When doing maintenance on your equipment, use dummy load or aim your signal away from the enemy. Frequencies should be changed at irregular intervals; every 24 hours may not be often enough. The division C-E officer can schedule changes as often as need be. If you can do it only once a day, don't do it at the same time each day. Another good practice is to change operators when you change frequencies. Some operator characteristics are so distinct that they will be easily recognized and identified. Transmitting stations/antennas should be relocated frequently. You should not remain in the same location long enough to be identified. All of these measures should be practiced religiously. Omitting any one could be fatal, not only to you, but to your unit.

Let us suppose that we have been unsuccessful in preventing DF and the enemy knows our frequency and location. They have several options. They can monitor for intelligence purposes, jam to disrupt control, confuse by deception, or call for artillery fires. Once they have your location, it takes approximately three minutes for them to make a decision about what to do with you. If they decide to use suppressive fires, it will be too late for remedial measures. You would not be able to move fast enough even if you knew when to move. This is why we emphasize preventive measures; learn them and practice them without fail.

What if the enemy decides to monitor your communications for intelligence purposes? Unless your equipment is secure, you cannot prevent his listening; but you can prevent his gathering any information of value. If you use proper radio-telephone procedures, he will not hear anything he can use against you. Encrypt any messages or parts of messages that contain vital information. Never



disclose unit identities, locations, etc. Use the CEOI correctly; 100% accuracy is required. Don't make the enemy's job easy.

Next, let us consider deception; imitative communications deception or ICD involves an attempt by the enemy to enter your net and give erroneous orders. If you allow him to do this, the situation will become confused and lives could be lost. For instance, he could tell you to move and then call for artillery on your new location. What should you do when you get conflicting orders or any orders for that matter? Authentication is the answer every time. It is the only way to be sure you are not talking to the enemy; they are well trained in the English language.

The remaining possibility is jamming. Jamming is any noise or sound that the enemy uses to disrupt your communications. It is difficult for even highly trained operators to recognize. Effective jamming could easily be mistaken for atmospheric interference or equipment malfunction. Once jamming has been identified as the source of the problem, the operator must take steps to counter it; these should be taken automatically. Don't stop transmitting and never disclose over a jammed link information which acknowledges enemy jamming and/or its effectiveness. The transmitting station should switch to high power; this should increase the signal-to-jamming ratio enough to allow message reception. Also, try detuning (a small shift in operating frequency); adjusting band pass, BFO, and/or gain control; changing transmission mode, antenna polarization or the antenna itself. If none of these improves your reception, change frequency (if you are authorized to do so). As a last resort, move to a new location; it may be enough just to move your antenna. Any or all of these measures may be necessary; you should be familiar with all of them. Your goal is to communicate; don't let the enemy deprive you of your goal.

Any incident of jamming, intrusion (attempted deception), or interference should be reported immediately to your supervisor. A written report should follow as soon as possible; the instructions for interference/MIJI (Meaconing, Instrusion, Jamming, Interference) reporting are in your CEOI. If a report isn't filed, nothing can be done about it.

We have discussed many "what if's," but we can never assume that REC isn't out there working against us. We must be prepared or we will not survive the next conflict. To do this we must be well-trained, and the training must begin now. Much reference material is available and can be obtained by writing to the address below:

Commander
USASC&FG
ATTN: ATZHCD-D
Fort Gordon, Georgia 30905

Our first priority now should be training; however, you cannot train an operator to counter REC effectively in the classroom. It should be done in a field situation with actual equipment. Sitting in a classroom listening to a tape of jamming signals will probably put everybody to sleep. Expose your operators to jamming by any means available to you. If your unit has EW personnel, ask them to use their jammers; this is the best way to teach defensive techniques. Another method is to use a jamming simulator (SG-886A-T/UR) which is available through your local Training Aids Support Center. It is small and simple to use; no special training is required. A tape of jamming signals or any kind of noise played on the radio will suffice for training purposes. The idea is to get the operator to react correctly and automatically when jamming is suspected.

Training to defend against deception is much easier; all you need is a compatible radio. Set up a dummy station and pass traffic. Tell them to do something which will expend a lot of energy needlessly and waste time; maybe they will ask for authentication the next time they receive an order. With a little imagination this can be a lesson they will not soon forget. It only takes a couple of people to do this, and it can be done in conjunction with any type of field training.

Let's not be caught unprepared. The military is dependent upon its operators. If we can't communicate, we have no control. We cannot win without good operators. Isn't it time we got serious about ECCM?