

RIFLE COMPANY

ECCM

MAJOR P.J. DULIN

United States Marine Corps

The term "electronic counter-countermeasure" (ECCM) may conjure up images of super-sophisticated underground listening posts full of incomprehensible equipment, or perhaps aircraft electronically zapping enemy communications, radars, or missile guidance systems. Few people would think of ECCM in terms of laying communication wire or using runners in order to maintain radio silence. Nevertheless, both the electronic warfare (EW) wizards in their listening posts or planes and the rifle company soldiers laying wire are using ECCM techniques.

Convincing the riflemen that their efforts are important and effective, though, is another matter. For one thing, during most of their tactical training periods, their company's ECCM efforts may seem inconsequential because there is little or no tangible feedback from them. They also have difficulty understanding that most of their company's ECCM efforts are defensive in nature rather than offensive, that rather than being used to hack off an enemy's electronic warfare (EW) arm, they will be used more like a shield to blunt an enemy's EW sword thrust. That shield must remain raised at all times; if it is dropped, even for a second, the sword will strike home.

How, then, does a company hold onto its ECCM shield and use it to best advantage? Before that question can be answered, some definitions and explanations are in order.

Electronic warfare (EW) is officially subdivided into three general categories:

- Electronic support measures (ESMs)—direction finding and monitoring — are used to locate the geographic position of an enemy and to listen to his electronic signals.
- Electronic countermeasures (ECMs)—jamming and deception—are used to nullify an opponent's electronic equipment.
- Electronic counter-countermeasures (ECCMs)—protecting, evading, concealing, and covering—are used to negate an opponent's ECM attack on friendly electronics or to defeat his ESMs.

All three of these subcategories of EW are applied across the three radio frequency bands that a rifle company uses — high frequency (HF), very high frequency (VHF), and ultra



high frequency (UHF). In each of these bands, radio waves behave differently. This is especially true concerning ground waves, which travel through the air close to the ground, and skywaves, which travel to the upper atmosphere, bounce off the ionosphere, and come back down to the ground. This means that ECCM rules that work in one band will not necessarily work in another.

Specifically, the HF band uses both skywave and ground-wave communication. The skywave signal can give much greater range for communications and is the only way short of having a satellite that an individual radio can communicate over the horizon. But the atmosphere introduces rapidly changing variables that can affect the quality of skywave communications. For example, both time of day and atmospheric refractivity can affect how well communications perform.

Fortunately, there are some indicators that will help a radio operator decide whether he can use skywave communications. These indicators are the maximum usable frequency (MUF) and the lowest usable frequency (LUF), which can be computed daily by the battalion communications officer or the communications chief. These readings tell an HF radio operator whether his assigned frequency falls within the bracket of usable skywave frequencies. (One of the reasons for this bracket of frequencies is that the higher the frequency is, the less likely the waves are to bounce off the ionosphere and return to earth.)

In the VHF and UHF portions of the spectrum, there are

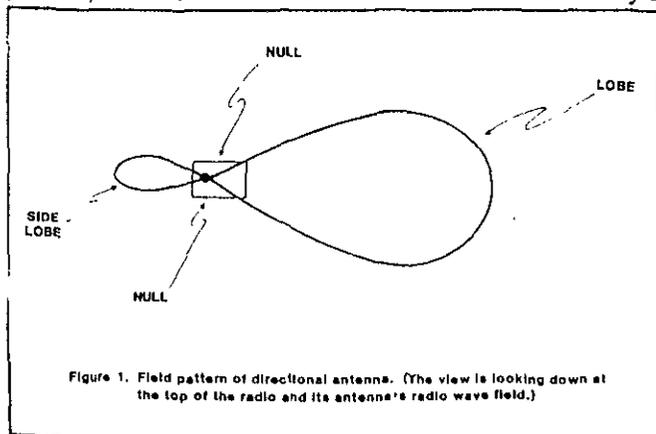
no skywave communications to speak of. The radio waves that are pointed toward the ionosphere pierce right through it and keep going out into space. The only way to get over-the-horizon communications with an individual VHF or UHF radio is to have a relay station such as a satellite or an aircraft. Otherwise, VHF and UHF signals must follow a groundwave path, which, for these frequencies, is commonly called line of sight (LOS) communications. Normally, if a radio operator can't see the point he wants to communicate with — if a mountain is in the way, for example — he can't communicate. The primary difference between VHF and UHF groundwaves is the number of obstacles in the line of sight that the waves can penetrate. For instance, heavy forests interfere more with UHF groundwave signals than they do with VHF groundwave signals.

Regardless of which type of groundwave signal is used, an important concept to understand is how to point the radio waves in the proper direction. To do this, quite simply, the radio operator uses his antennas.

For purposes of this article, there are two kinds of antennas — omnidirectional and directional. With an omnidirectional antenna, the radio waves travel outward 360 degrees in all directions just as the light from a table lamp travels out in all directions. Conversely, a directional antenna is pointed toward the desired direction of communication, just as a flashlight is focused in a single direction.

The directions in which antenna radio waves travel are generally known as field patterns. When a field pattern becomes focused, the beam of radio waves is referred to as a "lobe" (Figure 1). The areas where there are no radio beams are called "nulls." The width of a lobe (in degrees) and the direction in which it is pointed are determined by the type of antenna used. At company level, directional antennas are usually of the field expedient kind, because the antennas issued with company radios are predominantly omnidirectional.

On the assumption that a company commander, in terms of tactical communications, is interested primarily in shielding his voice radios, some ECCM techniques have been consolidated and boiled down to three checklists, which are included here. The techniques shown apply only to three specific radios: the AN/PRC-104, which handles the HF band (Table 1); the AN/PRC-77, which handles the VHF band (Table 2); and the AN/PRC-75, which handles the UHF band (Table 3). If these three radios can be shielded from an enemy's



EW capabilities, then the company's major fire support nets and command and control nets can be maintained.

To use these tables, a radio operator follows a three-step process:

- He finds out from the S-2 what combination of EW capabilities the enemy has.
- He determines whether his company is conducting offensive operations (taking objectives) or defensive operations (digging in).

• He looks at the table under the appropriate enemy EW capability and then under the appropriate column — offense or defense. Everywhere there is an "X" in this column, he uses the ECCM technique shown on the far left of the table. If the enemy has more than one of these EW capabilities, the radio operator uses every technique that has an X marked beside it, even if it is marked in only one of the multiple EW capability columns that apply to his situation.

An operator's ECCM actions, as shown in the tables, are divided into two general classifications. The first classification I call "methods ECCMs" — techniques an operator can use to minimize enemy ESMS and ECMs relying only on the equipment available with the standard radios. Methods ECCMs are the operator's actions that do not involve the use of additional hardware. The second classification, which I call "hardware ECCMs," are actions that do involve the construction or introduction of additional hardware elements.

Under these two broad classifications, the four basic EW capabilities — monitoring, direction finding, deception, jamming — can be analyzed and possible tactics can be formulated for each classification of company level ECCM actions.

Monitoring

First, in order to understand how an enemy monitors our radios, let's review the geometry of a general tactical situation and begin to make some distinctions as to how that geometry changes during fluid wartime operations. Referring to Figure 2, our radios will be located primarily along the forward edge of the battle area (FEBA) with the rifle companies. One to two kilometers behind these front lines will be the battalion command post (CP). The enemy's ability to monitor is located on the opposite side of the FEBA from friendly units within relatively short range.

The Soviets, for example, have a large number of radios that can intercept our signals, with many of these available to their front line combat forces and not just to their specialized EW units. Consequently, monitoring should always be considered a threat, even when friendly intelligence sources report no specialized enemy EW unit in the area.

In both offensive and defensive operations, the distances between front line and battalion CP radio links remain relatively the same. As a result, the primary emphasis is on groundwave rather than skywave propagation, since the distances involved are normally less than 25 kilometers. There are some clear distinctions, however, between these two types of operations. These distinctions can be summarized in the word "mobility." Company level radios have only one type of

antenna for an operator on the move — the whip antenna, which is omnidirectional and limited to groundwave propagation. In addition, offensive mobility affects communications in that it reduces the number of alternate methods of communication available to the company, such as wire-linked field phones. This results in additional reliance on the radios as the essential communication link. Throughout both offensive and defensive operations, then, the ECCM objective is to avoid being listened to by the enemy.

To ensure a distinct understanding of when to apply specific techniques of "methods ECCM" and when not to, the appropriate tactics must be defined separately for offensive and defensive operations.

Since in offensive operations no rapidly responsive alternate means of communication is available to the company, it must rely on its radios as its *primary means of communicating* with its platoons, its supporting arms, and the battalion CP. Since the company *must* talk by radio, it really has only four ECCM techniques with which to counter *monitoring*:

Brevity codes. The battalion S-3 can pre-establish codes to indicate accomplished tasks or standard phrases. The extent to which these codes are used is left to the individual units involved, but too many can become confusing and counterproductive.

Short-burst transmissions. This technique consists of limiting transmissions to three seconds or less, which makes it more difficult for the enemy to identify and monitor a friendly frequency. But operators must not fall victim to the common misinterpretation that they can carry on a conversation using a series of 50 or 60 three-second bursts. This is not good ECCM, because the enemy will find the frequency. The three-second burst is *most useful* when used in conjunction with a brevity code.

Alternate frequencies. At randomly prescribed times during the day, or when there is *some indication of enemy monitoring activity*, the operator can temporarily frustrate that

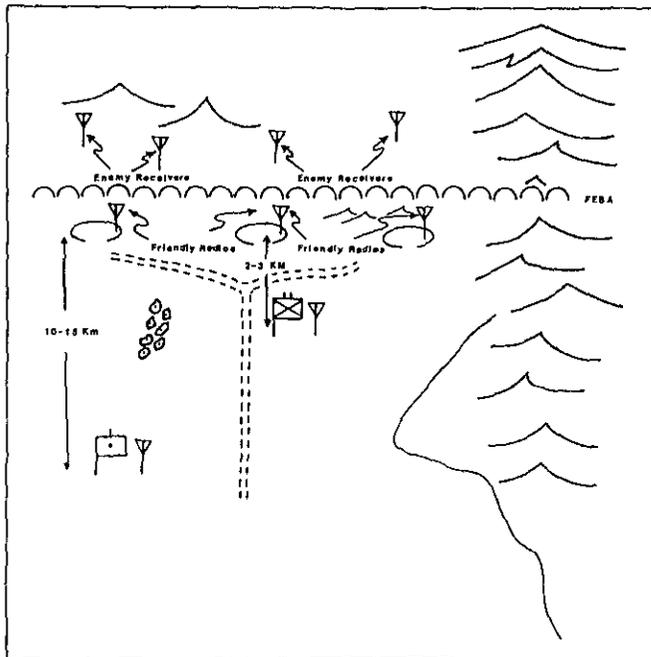


Figure 2. General Tactical Situation.

Overall Company Ops ECCM Technique	ENEMY EW CAPABILITIES								
	Monitoring		Direction Finding		Deception		Jamming		
	OFF	DEF	OFF	DEF	OFF	DEF	OFF	DEF	
METHODS ECCM									
Brevity Codes	X	X	X	X	X	X	X	X	X
Short Burst Transmissions	X	X	X	X	X	X	X	X	X
Alternate Frequencies	X	X	X	X	X	X	X	X	X
Higher than MUF	X	X	X	X	X	X	X	X	X
Authentication Codes					X	X			
Alternate means of Communication		X		X		X		X	
Terrain Masking		X		X		X		X	
HARDWARE ECCM									
Secure Voice	X	X			X	X			
Directional Antennas		X		X		X		X	
Horizontal Antennas									X

Table 1. AN/PRC-104 (HF) ECCM Techniques.

activity by changing frequencies. This technique is essentially a *crude method of manual frequency hopping*. It should be noted, however, that extensive prior coordination is required among all members of any radio net using this technique to ensure a *smooth changeover in frequencies*.

Higher-than-MUF frequencies. This technique applies only to HF communications in general and to the AN/PRC-104 in particular. It limits *monitoring by enemy receivers* that rely on skywave propagation. By using a groundwave antenna and by operating on frequencies that are higher than the maximum usable frequency for skywave propagation, the AN/PRC-104 operator can effectively keep the entire skywave class of enemy receivers from monitoring his transmissions. To use this technique, the AN/PRC-104 must be within groundwave range of the opposite end of the radio link.

It is appropriate here to clear up a common misinterpretation of when to use ECCM during offensive operations.

Specifically, many inexperienced radio operators fail to realize that the need for radio silence or reduced radio communications at the *outset of an operation* changes dramatically once enemy contact is made. Before contact, the objective is to hide the company's frequencies from the enemy. Once engaged, though, the enemy knows where the company is. At that point, radio operators should talk freely and let the company commander, the battalion CP, and the supporting arms know what they need. In short, radios should be used to their maximum advantage at this point so that the enemy can be destroyed before he can react fully.

In defensive operations, the operator has more flexibility in the techniques available for "methods ECCM" than he has in offensive operations. This flexibility stems primarily from the variety of alternate communication means available in the defense. The radio operator can use not only the same four "methods ECCM" used in offensive situations but also the following additional techniques:

Alternate means of communication. In the defense the reliability, speed, and number of alternatives to radio wave

transmission increase. The specific methods available to the company in the defense are field phone wire links and courier service. (Both of these are also possible in the offense, of course, but dragging wire in a footmobile offense will prove highly unreliable; and using runners is not nearly as reliable as in the defense. In the defense a courier knows where the company position is and therefore where he is going; in a mobile offense he must hunt around to find a unit that is moving.)

As in other ECCM techniques, there are some common misunderstandings about the use of alternate means of communication within a company. In particular, platoon leaders may interpret a company commander's actions as inconsistent if they (the platoon leaders) are required to maintain radio silence and use couriers or wire while the forward observers from the supporting arms are allowed to use their radios. They should understand, though, that the distances between the forward units and the actual fire support batteries, combined with operational demands, frequently make it impossible for the supporting arms forward observers to use alternate means of communication.

The necessity for the supporting arms to use their radios in no way nullifies the platoons' efforts at radio silence; in fact, this makes these efforts even more critical. For example, an enemy's radio monitors maintain logbooks and chart the company's radio usage. From this, they can determine when the company is likely to change from defensive to offensive operations if its overall radio usage increases dramatically. Consequently, if distance demands that our supporting arms observers use radio links, the platoon links within the company must use alternate means of communication to reduce overall company radio usage.

Terrain masking. In a defensive situation, the company has time to put prominent pieces of terrain between itself and the enemy receivers. The company's critical nets (supporting arms and the link to the battalion CP) are trying to talk back from the FEBA to the rear area while the enemy receivers are in the opposite direction on the other side of the FEBA. Mountains or hills between the company's radios and the FEBA, therefore, will not affect the company's communications but

Overall Company Ops ECCM Technique	ENEMY EW CAPABILITIES							
	Monitoring		Direction Finding		Deception		Jamming	
	OFF	DEF	OFF	DEF	OFF	DEF	OFF	DEF
METHODS ECCM								
Brevity Codes	X	X	X	X	X	X	X	X
Short Burst Transmissions	X	X	X	X	X	X	X	X
Alternate Frequencies	X	X	X	X	X	X	X	X
Authentication Codes					X	X		
Alternate Means of Communication		X		X		X		X
Terrain Masking		X		X		X		X
HARDWARE ECCM								
Directional Antennas		X		X		X		X
Horizontal Antennas								X

Table 3. AN/PRC-75 (UHF) ECCM Techniques.

will hinder an enemy's monitoring capability. It should be noted, though, that the operators cannot remote their antennas any great distances from their radios because of equipment limitations. Consequently, the use of terrain masking may be limited in situations where a terrain feature could diminish the ability of the supporting arms observers to see and control air, mortar, or artillery strikes along the FEBA.

As for "hardware ECCM," both standard issue and field expedient devices can be used to counter monitoring:

Secure Voice. In the mobile offense, an operator will have little time to construct field expedient ECCM devices. Therefore, he must rely on standard issue devices. The only real standard issue device available to a radio operator, though, is a secure voice crypto device such as those in the Parkhill and Seville family of equipment, and secure voice devices are presently available only with the AN/PRC-104 and the AN/PRC-77. Secure voice methods do not apply to the AN/PRC-74, but they will with its replacement, the AN/PRC-113. (Within a decade, in fact, all transmissions will be encoded.)

A defensive situation, on the other hand, gives an operator a chance to construct field expedient devices to improve his ECCM capabilities.

What kind of such devices can an operator construct in the field? Since he wants to make it harder for an enemy monitor to pick up his signal, he can reduce his radio wave power output. But how does he reduce the power of the signal reaching the enemy while maintaining or increasing the power of the signal reaching his CP? The answer is directional antennas.

Directional antennas. Considering the position of enemy and friendly units with respect to the FEBA (Figure 2), and remembering the omnidirectional field patterns of the standard whip antenna, the operator can achieve his ECCM objective by reducing the lobes of the field patterns pointing in the direction of the enemy while maintaining or increasing the lobes pointing in the direction of the friendly receivers. He can build field expedient directional antennas from material normally at hand in the field, such as communication wire.

It would be ideal if a directional antenna's nulls could be pointed directly at the enemy receivers, but a radio operator will probably not know the enemy's exact locations. Nonethe-

Overall Company Ops ECCM Technique	ENEMY EW CAPABILITIES							
	Monitoring		Direction Finding		Deception		Jamming	
	OFF	DEF	OFF	DEF	OFF	DEF	OFF	DEF
METHODS ECCM								
Brevity Codes	X	X	X	X	X	X	X	X
Short Burst Transmissions	X	X	X	X	X	X	X	X
Alternate Frequencies	X	X	X	X	X	X	X	X
Authentication Codes					X	X		
Alternate Means of Communication		X		X		X		X
Terrain Masking		X		X		X		X
HARDWARE ECCM								
Secure Voice	X	X			X	X		
Directional Antennas		X		X		X		X
Horizontal Antennas								X

Table 2. AN/PRC-77 (VHF) ECCM Techniques.

less, he will know their general direction (that is, the opposite side of the FEBA) and can present the enemy receivers with at least the directional antenna's reduced sidelobes if not (with luck) the nulls themselves. (Many publications describe specific directional antennas or precise construction methods.) It should be noted, however, that the use of directional antennas with the AN/PRC-75 would be rare since that radio most often requires omnidirectional patterns to talk to friendly aircraft moving rapidly about the battlefield.

Direction Finding

Aside from these enemy monitoring ESMs, one that is potentially much more dangerous to a rifle company is direction finding (DF). While the objective of measures taken against monitoring is to deny the enemy the content of the company's transmissions, for direction finding it is to deny him the knowledge that the company is even transmitting.

In practical terms, most of the ECCM techniques that can be used against monitoring can also be used with confidence against direction finding. The secure voice technique is an exception. For direction-finding purposes, secure voice transmissions are just as good to the enemy as transmissions sent in the clear. (ECCM techniques that are applicable in combatting DF are summarized in the DF column of Tables 1, 2, and 3.)

Imitative Deception

Imitative deception, a type of enemy ECM, requires that the enemy be able to do two things: monitor us on our frequencies and employ a skilled linguist to deceive our radio operators or to elicit information from them.

Since the enemy's success depends directly on his monitoring capability, all of the previously developed ECCM techniques for use against monitoring also apply in this case, along with an additional technique — authentication.

Authentication codes are pseudo-randomly generated codes an operator can use to verify the authenticity of any suspicious station on his net. The codes are disseminated daily and can be employed even when no suspicious messages have been received, just to make sure a highly skilled linguist is not operating against the unit. (The appropriate techniques to use against imitative deception are summarized in the tables.)

Jamming

Jamming — the intentional introduction of noise power to a receiver so that the operator cannot understand the signals

transmitted — is, for purposes of this discussion, the most dangerous type of ECM. The point to remember is that this is a reception problem for the radio operator and not a transmission problem.

The ECCM techniques to be used against enemy jamming can be summed up in two steps: First, "methods ECCM" can be used to keep him from knowing our operating frequencies. This means practicing the same techniques used against direction finding. Second, "hardware ECCM" techniques can be used to shield our radios from the jammer's power:

Directional antennas. Just as a radio operator can use directional antennas to prevent the enemy from monitoring his transmissions, he can also use directional antennas to reduce or eliminate the jamming power a friendly receiver gets. He does this by pointing the antenna's nulls in the direction of the enemy.

Horizontal antennas. He can also use field expedient antennas constructed to be horizontally polarized. Since most Soviet groundwave tactical jammers are vertically polarized, a radio receiver with a horizontally polarized antenna would be largely unaffected by the jamming.

(The principle behind this can be demonstrated with two pairs of polarized sunglasses. If both pairs are put on, one over the other, the sun can be seen through them. But when one pair is removed and rotated 90 degrees with respect to the other, the sun is completely blocked out.)

When we rotate our antennas to a horizontal polarization, we are doing the same thing to the jammer's power that the rotated sunglasses do to the sunlight. Of course, both ends of the friendly radio link must have the same polarization.

Additionally, horizontal polarization will diminish the groundwave distance that the radio wave can travel, so it cannot be used to great effect when opposite ends of the friendly line are on either end of the horizon. In other words, operators must plan carefully and be selective when using horizontally polarized antennas.

In summary, there are electronic counter-countermeasures that can be effectively used at company level against an enemy's electronic warfare capabilities. All a company commander and his radio operators need to keep their ECCM shield raised is a little knowledge and a lot of confidence. The guidelines offered here can serve as a starting point from which they can build that knowledge and confidence.

Major Patrick J. Dullin, USMC, is a communications engineer assigned to the Marine Corps Development and Education Command at Quantico, Virginia. A 1973 graduate of the United States Air Force Academy, he holds master's degrees from the University of Southern California and the Naval Postgraduate School. He has served as a Marine infantry commander at platoon and company level and as a battalion S-3 and S-4

