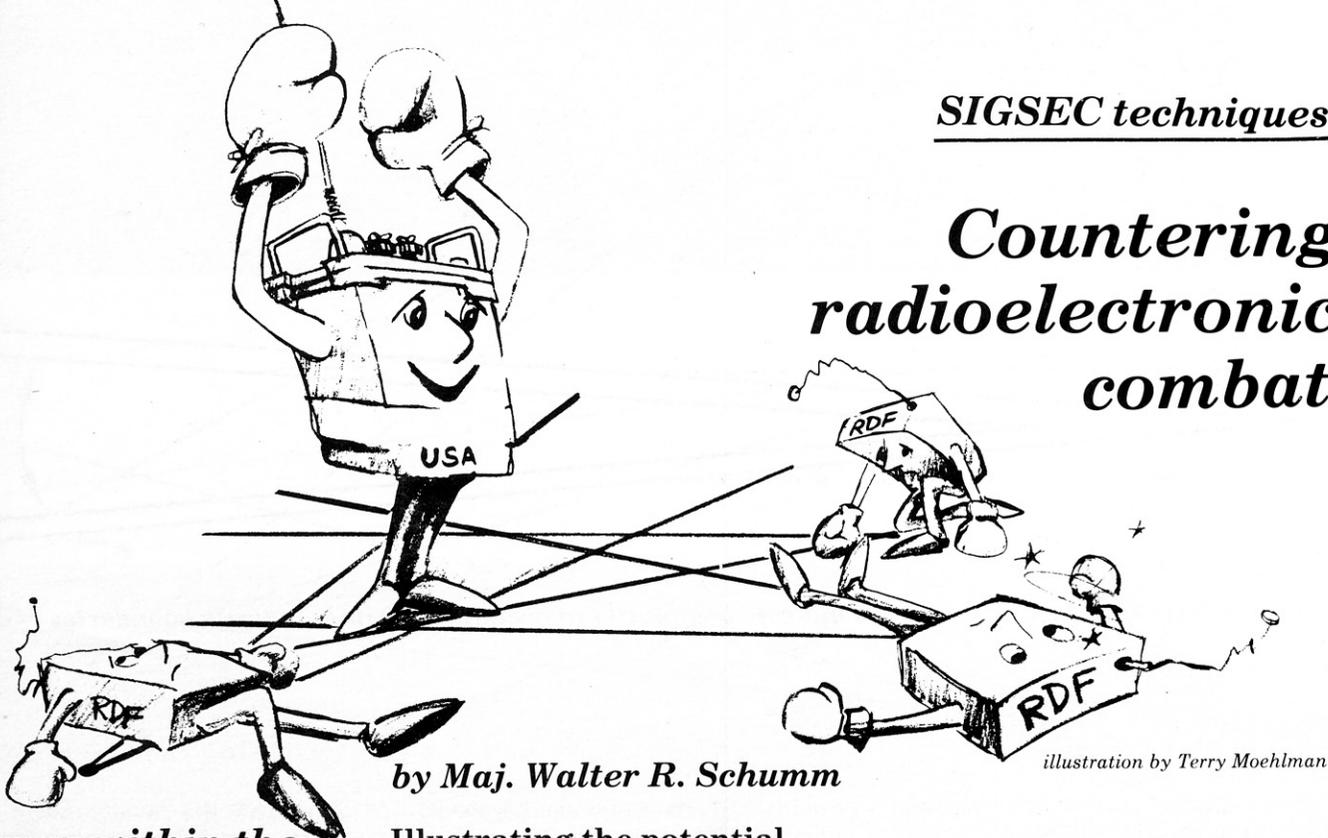


Countering radioelectronic combat



by Maj. Walter R. Schumm

illustration by Terry Moehlman

Illustrating the potential effectiveness of RDF in radioelectronic combat

FM 102-2-1 (Chapter 15) makes it clear that Soviet forces place a high priority on the physical destruction of Allied units that have been located through radio/radar direction finding (RDF). Furthermore, if an RDF fix is not accurate enough by itself to permit firing on an important target, Soviet analysts may refine the fix through terrain analysis and the use of other intelligence. In general, Soviet forces may place a unit under fire if its location can be pinned down, or at least estimated to be, within a kilometer grid square, the area that a BM-27 battalion can place under fire with one salvo.

FM 102-2-1 indicates that Soviet RDF assets can obtain bearings on Allied transmitters with an accuracy of $\pm 3\frac{1}{2}$ degrees. However, in accordance with the principle of "never underestimating your enemy," it may be safer to estimate their capability, under optimum conditions, at approximately half that figure—perhaps ± 2 degrees. With improvements expected to occur in equipment that is commercially available, figures that may be valid today are likely to be underestimates of performance data tomorrow. In any case, it is safer to err on the side of future trends, although more specific data may be available in classified form depending on the status of Allied intelligence at the time.

However, such data may mean little to the unit commander or his Signal officer. Given the distance of one's unit from the forward edge of the battle line (FEBA), exactly how accurately could RDF locate one's unit (or the transmitter's antenna, if the antenna were remoted from the CP location)? One technique that this author has found helpful involves the use of a locally fabricated "RDF template," which can be made from the cardboard backing of a pad of paper, acetate, and the help of a protractor, scissors, and scotch tape.

This device has been used successfully with students at the Sixth U.S. Army Intelligence Training Army Area School to illustrate the potential and the limitations of RDF as part of Soviet radioelectronic combat (REC). The template is made by drawing and cutting out a four degree sector in cardboard, then removing the interior of the sector to form a "V." (See Figure 1.)

The space between the edges is strengthened by attaching clear acetate with transparent scotch tape, a feature that also allows one to see the area within any particular bearing. To strengthen the device, the acetate is squared off at the base of the "V" as shown in Figure 1.

The area within the lines that have been drawn will be that area most likely targeted by the Soviets. Within that area, it is especially important to avoid placing one's unit on key terrain features that Soviet analysts would identify as ideal unit locations and, hence, as ideal locations for combat missions.

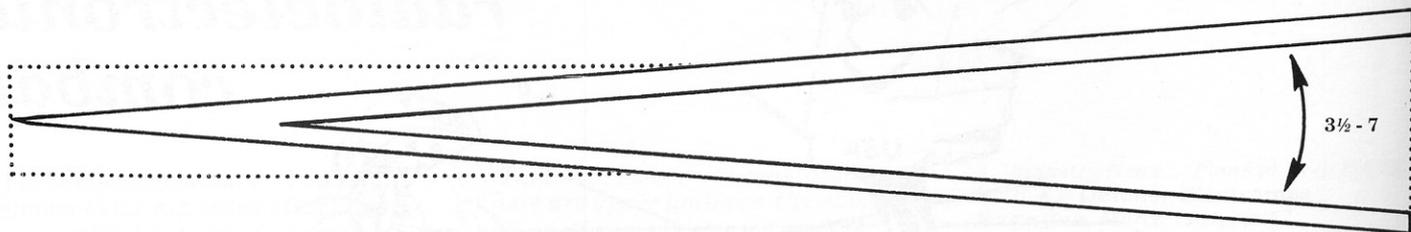


Figure 1. RDF template. Dotted lines indicate boundaries of acetate; solid lines indicate boundaries of cardboard.

To use the template with a map, one first must select an Allied unit location, then determine the possible or known locations of enemy RDF sites, keeping in mind that standard FM tactical radio sites are likely to be two to ten kilometers behind the FEBA, with the most likely area probably being four to six kilometers behind the FEBA. RDF sites are also likely to be on high ground, with adequate camouflage, and separated by several kilometers. FM 100-2-3 suggests that a typical Soviet division will have three RDF sites along its front, although army and front units might contribute additional sites, perhaps slightly to the rear. After identifying the known and potential RDF sites, place the small end of the "V" at each site and place the centerline of the "V" through the actual location of one's unit. Then draw pencil lines along the outside edges of the "V" to determine the limits of each RDF bearing, assuming it was perfectly centered. (In practice, it is unlikely that all RDF bearings will be perfectly centered, and their overlap probably will be larger than what is obtained by the method presented here.) The area within the lines that have been drawn will be that area most likely targeted by the Soviets. Within that area, it is especially important to avoid placing one's unit on key terrain features that

Soviet analysts would identify as ideal unit locations and, hence, as ideal locations for combat missions. It is also important to consider the electromagnetic profile of one's unit, keeping radio and radar signals (among any others) dispersed and minimized so as not to present the expected pattern of frequencies, locations, and antenna polarizations to enemy SIGINT sites. Spreading one's antennas outside the target area will assist in making identification of one's profile more difficult. In general, this method provides a rough idea of the potential effectiveness of Soviet RDF for locating one's unit. Hopefully, such knowledge will encourage the practice of COMSEC measures that will make accurate RDF more difficult.¹

Expediting the destruction of jammers

As discussed above, Soviet doctrine for radioelectronic combat gives priority to RDF and destruction of command and control/communications centers so located. However, a secondary priority for Soviet REC is the use of jamming to disrupt our control processes. It is also quite

likely that the Soviets recognize the advantages of jamming for supporting attempts at imitative communications deception (ICD) and RDF. The practice of jamming his own stations "attempts" at authentication is one way for the enemy to make us "forgive" the station for not being able to authenticate properly, and thus to accept a phony message as valid. But while jamming may cause frustrated radio operators to relax proper authentication procedures, it may also cause them to transmit for longer periods of time, setting up their stations for effective enemy RDF. FM 102-2-1 points out that Soviet RDF units can target locations within 3 minutes if they can catch a radio station broadcasting for more than 20-25 seconds. If a radio operator tends to keep his transmissions to only 10-15 seconds, it is not improbable that he might increase his transmissions to 20-30 seconds under certain types of jamming. The operator might think that the use of words twice, spelling out words, and using full callsigns will defeat jamming, without realizing that he is making his station and unit dangerously vulnerable to more effective RDF and the combat/fire missions which might ensue. In summary, jamming can serve other purposes than simple disruption of a particular radio message.

However, jamming stations themselves present lucrative targets.

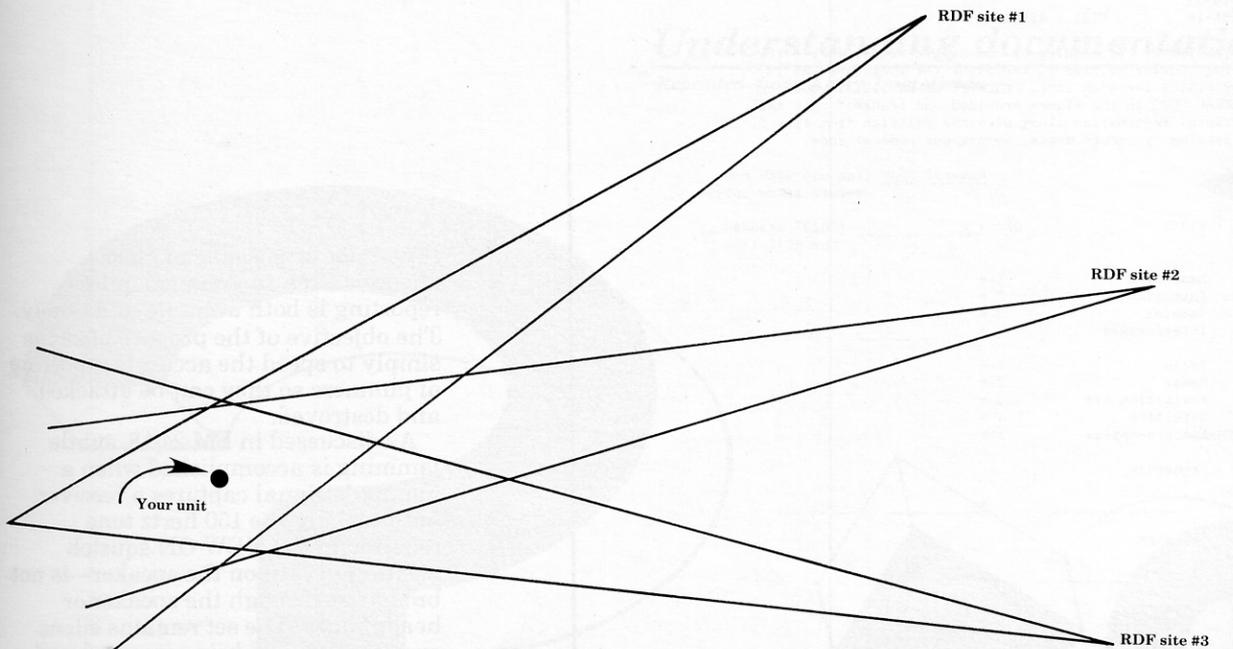


Figure 2. Application of RDF templates on a map.

Their relatively high levels of power make them even easier to RDF than regular radio stations. The destruction of even a few jamming stations would certainly make their operators more nervous about jamming for long periods of time, a factor that might be particularly important if they were using subtle jamming, the “white whisper” discussed in FM 24-18 (December 1984). Jammers often exchange missions in order to make RDF more difficult, but the more pressure placed on them to do this often, the more likely they are to make mistakes in coordination, with the end result being a less effective job of disrupting our control.

In practice, however, units often have a difficult time responding to jamming quickly enough to make RDF on jammers a feasible procedure, the jammers having traded missions or left the area before artillery fire can be brought to bear on their estimated positions. Operators who must dig out the correct format for a jamming report from their CEOI, reproduce it on plain paper, and then figure out how to code it, may be inclined to simply overlook the matter. Even with the best of command emphasis and operator intentions, such an involved procedure may not lead to rapid reporting of jamming attempts. Under the pressure of jamming, operators may forget the proper jamming response procedures.

In order to solve such problems, I wanted to create a jamming report form that would meet several criteria. Its format must correspond to current doctrine, in which MIJI 1 reports are to be submitted immediately through channels, with longer follow-up MIJI 2 reports submitted later; it should provide for easy encryption of its contents, in case it should have to be sent over nonsecure means; it should allow some space for information needed on a MIJI2 report; and it should provide information on how to respond to jamming. If the form met the above criteria, it would allow for on-the-spot “hip pocket” training, as a section NCO could use the form for guidance either in instituting anti-jamming procedures or in completing MIJI 1 reports. Additionally, the form should be small enough so that it could be folded once or twice to fit inside a fatigue jacket pocket, from which it could be retrieved more easily than from a CEOI (whose contents are usually not removed).

As with any new form, it might work only as well as the practice given to it. It is unlikely that any jamming report could be self-explanatory to an operator not familiar with the requirements of a MIJI 1 report. However, use of the form proposed here is better than having to look up the correct format in a CEOI or field manual and then creating one’s own form on-the-spot in nonstandard format.

The proposed jamming form is presented in Figure 3, with its reverse in Figure 4. The operator circles the

appropriate answers for lines 2 and 3 while filling in the appropriate blanks for lines 4, 5, and 6. Each line may be encrypted with numeral code, if needed. The bottom of the form reminds the operator of items to be noted for a follow-up MIJI 2 report. The appropriate classification may be stamped at the top and bottom of the form. The reverse of the form provides instructions for ways in which to respond to jamming. The instructions should serve to remind a trained operator of the steps to use when being jammed, but untrained radio operators would need further explanation. For purposes of training, NCOs might evaluate their operators’ skills by asking them to describe, explain, and justify each of the 17 numbered procedures as well as the unnumbered preliminary procedures. That would be a hard test for many operators, but it would permit a thorough analysis of how well they understood their job. Of course, both sides of the form can be adapted to the particular requirements of any unit, especially the details associated with the channels through which jamming is to be reported.

The goal of reporting jamming must not be forgotten, however. While it is nice to study types and effects of jamming for intelligence purposes, the physical destruction of enemy jammers must remain a high priority.

INSTRUCTIONS: If sending by non-secure means, circle the correct answer or fill in the blank for that line, as is appropriate for each line. ENCRYPT LINES 1,2,3,4,6 using NUMERAL CODE in the blanks provided and transmit only the encrypted information along with the callsign from line 5. If sending by secure means, do not use numeral code.

LINE		Numeral Code	(for use with non-secure means only)
1	MIJ 1	022 =	_____ ("022" stands for MIJI 1)
2	Meaconing	1 =	
	Intrusion	2 =	
	Jamming	3 =	
	Interference	4 =	_____
3	Radio	1 =	
	Radar	2 =	
	Navigation Aid	3 =	
	Satellite	4 =	
	Electro-optics	5 =	
4	Frequency		_____ = _____
5	Callsign		_____
6	Location		_____ = _____

MAKE A COPY FOR YOURSELF BEFORE SENDING ORIGINAL TO:

NOTE times, effectiveness, type of incident, weather, bandwidth of EMI, operator/POC name, RDF bearings, purpose of station, how it began/ended, ECCM used and results, all other details for MIJI 2 report:

CLASSIFICATION

It will not be possible to place effective fires on jammers unless reporting is both accurate and timely. The objective of the proposed form is simply to speed the accurate reporting of jammers so they can be attacked and destroyed.

As discussed in FM 24-18, subtle jamming is accomplished when a jammer's signal captures a receiver, but—lacking the 150 hertz tone required in the NEW ON squelch position to turn on the speaker—is not broadcast through the speaker or headphones. The set remains silent even though it is being jammed and other stations are trying to make contact. Subtle jamming is especially dangerous because it is not easily recognized as jamming. On the other hand, once it is recognized, it may be possible to take advantage of overconfidence on the part of jammers. Jammers who believe they have not been detected offer better targets for RDF and fire missions.

Figure 3.

REMEDIAL ELECTRONIC COUNTER-COUNTER MEASURES
 RADIO JAMMING

By disconnecting your antenna, determine if EMI is internal or external to your radio set. If noise continues without your antenna, then check for dirty, loose, bad cable connections or grounds. If all connections seem OK but the noise continues without the antenna, then check the radio for possible maintenance. If the noise stops after you disconnect the antenna, check for natural or local manmade sources of EMI -- lightning, generators, sparks, malfunctioning equipment; if the EMI is natural or local, try to correct it. If it appears to be other people on your frequency (mutual interference) try to contact them and obtain a valid authentication. If a valid authentication is not obtained, the EMI may be jamming. (NOTE: if your best hunch is that the problem is jamming, you may want to skip the previous steps in order to react more rapidly.) NOW:

1. Continue to operate (your mission).
2. Inform your supervisor.
3. Check adjacent frequencies for bandwidth of EMI.
4. Prepare an initial MIJI report (see reverse).
5. If possible, start recording the EMI on a tape recorder for your follow-up MIJI 2 report.
6. Keep the same operator on the radio; do NOT discuss jamming or its effectiveness on the air or near a keyed handset.
7. Apply CP-1380/VRC (SNAP) if available.
8. Adjust receiver controls for best signal to noise ratio: gain, volume, squelch, fine tune, AGC, BFO, filters, etc.
9. Slow down and keep transmissions brief.
10. Use phonetic alphabet, brevity codes, words twice.
11. Adjust your antenna (height, direction, polarization, location, terrain masking).
12. Do NOT go into plain text from cipher mode (secure gear).
13. Prepare to displace rapidly.
14. Keep operating on the same frequency even if another radio is used in order to tie up the jammer for RDF and to keep deceiving the enemy about the effectiveness of his jamming.
15. Secure assistance in RDF from the FCC or higher HQ.
16. As a last resort, change frequency along with callsigns, operator, background noise, antenna pattern, and location. Wait a few minutes before coming up "on the air" on the new frequency.
17. Start working on your MIJI 2 report.
 Remember that jamming may be a prelude to an attack or be used as a cover for ICD in your own or another net. Don't let the enemy know his effect on you; use as few measures as you can. Keep calm. USE SIGSEC techniques to prevent jamming. Report jammers to get them destroyed! Be mentally ready for various nerve wracking types of jamming signals, as well as subtle jamming (NEW ON squelch).

ENDNOTE

1. Schumm, W.R., "New perspectives on electronic warfare defense," **ARMY COMMUNICATOR**, Volume 10, No. 1 (winter), 1985, pgs. 50-54.

Major Schumm is an assistant special movements transportation officer with the 425th Transportation Agency of the 89th Army Reserve Command. He is a graduate of Signal Officers Basic Course, C-E Staff Officers Course, and the Signal Officers Advanced Course (correspondence) and is an associate professor of family studies at Kansas State University, Manhattan, Kansas. During the summer, he serves as OIC of the Electronic Warfare Committee of the Sixth U.S. Army Intelligence Training Army Area School at Los Alamitos, California. He has served as assistant battalion C-E staff officer with the 1/5th Field Artillery, 1st Infantry Division, Fort Riley, Kansas; state Signal officer, HHD, Kansas Army National Guard; commander, 135th Signal Platoon, 69th Infantry Brigade; commander, "B" Company, 138th Signal Battalion; and division radio officer, 38th Infantry Division, Indiana Army National Guard.

Figure 4.