The Electronic Piranha Can Jam

Ed. Note: In the Summer 1978 issue of TAC, we ran an article entitled "Jamming: Will It Be Tactically Effective?" by Mr. Lawrence E. Follis, technical director of the Concepts and Force Design Directorate of the US Army Combined Arms Combat Developments Activity. The article, which was not reflective of the US Army Signal Center philosphy of doctrine, has elicited a variety of comments from our readership. The following article is one such response. The TAC staff plans to run other reader responses in coming issues as space permits.

by LTC Don "Flash" Gordon
and CPT Bill Anton

Mr. Follis questioned the effectiveness of radio jamming (78 Summer Issue). His premise was that mathematical equations suggest that tactical jammers lack the power to overwhelm VHF/FM "push-to-talk" tactical communications. He questioned the generally held assumption that jamming may be highly effective on the outcome of the future battlefield.

Mr. Follis explains actions that could be taken by radio operators to eliminate jamming. The problem, of course, is that most radio operators are not as good at communicating as electronic warfare operators are at jamming. It isn't a case of mathematical formulae but one of defensive communication tactics and electronic counter-countermeasure (ECCM) training. We do neither very well in the US Army.

Our perspective is based on experience gained in the 313th Combat Electronic Warfare and Intelligence (CEWI) Battalion, 82d Airborne Division. We're the "electronic piranha" of the battlefield. Our battalion's 358th Electronic Warfare Company doesn't operate 9 to 18 kilometers from the enemy as in Mr. Follis's hypothetical model. We jam 2 to 5 kms from the forward edge of the battle area (FEBA). We train to survive there. We're mobile, camouflaged, and we fire a light antitank weapon if necessary. During Joint Readiness Exercise (JRX) BOLD EAGLE-77, we accompanied parachute infantry to jam behind the FEBA, in the enemy division support command area. During JRX GALLANT CREW-77, while supporting the 1st Cavalry Division with three other electronic warfare companies, we were at the FEBA and crossed it accompanying tanks. We drove our M151 mounted jammers inside M-548 tracked vehicles in order to maintain the tempo of the armor battlefield. The only electronic warfare company element operating 9 to 12 kms from the FEBA is the mess section!

Our battalion is also helping to test the steerable null antenna processor (SNAP) mentioned by Mr. Follis in his article. This is the antenna which is expected to eliminate interference caused by an enemy jammer. We think it was named SNAP because the electronic piranha got it! The steerable null antenna is an ECCM technique, but there is also a counter jamming technique—use two jammers. There simply is no magical or mystical ECCM technical device to protect against jamming. The electronic piranha will keep up with every innovation.

The electromagnetic spectrum is significantly different from either the chemical spectrum or the spectrum of mathematical formulae. It is dirty. When chemical element A is mixed with chemical element B in a clean test tube, chemical formula C is easily predicted. Mathematical formulae are also easily proven. Not so with electronics. The environment, the test tube so to speak, is dirty and propagation effects are unpredictable. The electronic piranha tries to make the communication environment as dirty as possible. We win more than we lose.

But Mr. Follis is correct to some extent. The use of jamming will not cause a huge black cloud of electronic interference to descend on the battlefield and totally disrupt all communications. Let us examine what it will do.

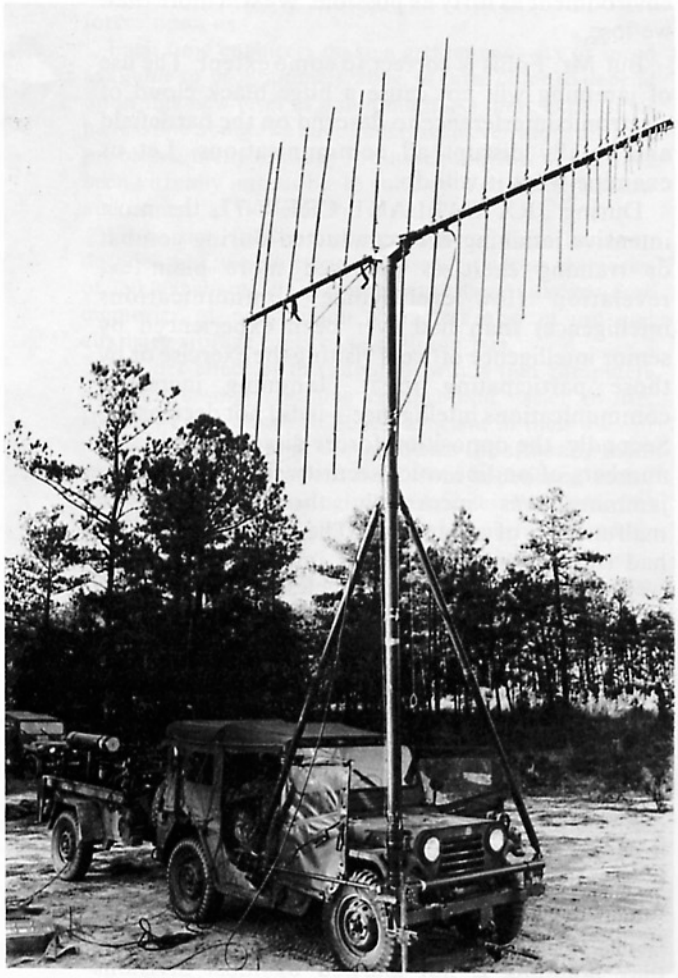
During JRX GALLANT CREW-77, the most intensive jamming ever conducted during combat or training exercises provided more plain-text revelation (low-level voice communications intelligence) than had ever been experienced by senior intelligence officers visiting the exercise or by those participating in it. Jamming increased communications intelligence—it did not decrease it. Secondly, the opposition forces disconnected large numbers of on-line voice security equipment when jamming was incorrectly thought to be a malfunction of equipment. The opposing division had trained well for this EW intensive exercise; it was not a novice unit. Nevertheless, the debilitating effects on them by our jamming were not uncommon.

In every exercise in which the 313th CEWI Battalion is *allowed* to use free play jamming, we invariably derive significant intelligence and cause important delays in calls for fire. We frequently cause confusion when using jamming in conjunction with imitative or manipulative deception, either rerouting "enemy" units to ineffective locations or capturing them. The unfortunate aspect is that jamming is so successful that, except for JRX GALLANT CREW-77, free-play jamming is not allowed by most divisions because of concern that it will ruin their exercise or ARTEP. Wait until enemy jamming really ruins the

first battle of a next war because we lack good experience in fighting on an electronic warfare battlefield.

The purpose of jamming in the US Army is the development of communications intelligence, and to confuse and to delay. In that regard, jamming is a weapon system. There are few valid missions which require us to block communications with overwhelming noise, though we can frequently do this. If we do, however, turn on the noise for a long time to overwhelm the enemy, we endanger the jammer by increasing its vulnerability to direction-finding followed by suppressive fires.

In contrast, the doctrinal purpose of jamming by our most likely enemy (and some allies) is to prevent communications by overwhelming noise. Jammers are usually assigned to Signal or electronic warfare units, not intelligence units as is the case in the US Army. The purpose of barrage jamming commonly used by a potential enemy is to keep a numerically inferior force—the US Army—from controlling its technologically superior weapons. The enemy has a large number of rugged, dependable, high power (1,500 watt) jammers to do this. They, too, deploy near the FEBA. Unless the US Army pays more attention to training its radio operators than to mathematical models, the enemy will easily succeed during those first critical minutes of the first battle.



The AN-TLQ 17 jammer is pictured in foreground, with the companion radio jeep in the rear.

In too many cases, US Army units jam themselves by a lack of net control. The net control station simply does not direct the net. Instead, the senior officer, with little training, directs the net rather than a well-trained NCS operator. Frequently, net discipline is all but nonexistent. There are too many outstations on VHF/FM nets; would you believe 56 stations on a brigade command net? In too many instances, command nets are explanatory rather than directive in nature. The electronic warfare unit thrives on this mismanagement. Our jamming, usually only a few seconds in duration during key parts of a message, adds dignity to what is already self-imposed electronic chaos. Oh, how we love armor units; their nets are similar to TV without the video. They explain every facet of the battle.

We can create a real circus by jamming secure VHF/FM voice. Half the stations will predictably go to the plain-text mode while the remaining stations stay secure. Do this during a CEOI frequency/call sign change and watch the havoc. Then insert imitative communication deception and a voice intercept operator can become a brigade or battalion commander but without privilege of rank or pay. Tactical unit commanders work their way out of this. They yell for controllers to initiate "stop-buzz," the Army-wide procedure to stop jamming for safety reasons. There will be no "stop buzz" on the modern battlefield. That's why the 82d Airborne Division uses relatively free-play electronic warfare in ARTEPs and field training exercises. We train to win.

Mr. Follis questioned the value of the low-power expendable jammer (its range is a radius of about 500 meters). Expect a real surprise if you find it fired (by artillery) around river crossing points, brigades or command posts shortly before an air assault. Expendable jammers are designed for effectively jamming enemy communications at a critical time and place of our choosing and although battery powered, they can be remotely activated at the most opportune time.

Mr. Follis dismisses the potential for effective jamming by a remotely piloted vehicle. Effective use of a lightweight linear amplifier could increase the power output to 500 watts. It would then be a weapon to contend with.

A broad-band jammer mounted in a remotely piloted vehicle could enable the system to jam a great many frequencies.

The electronic piranha is a real threat. The piranha uses aggressive tactics, not formulae. It can be avoided only by not swimming in the electronic spectrum or by very good communication training for all radio (and radar) operators. The US Army can't afford not to swim in (use) the electronic spectrum. You can beat jamming only with well-trained radio operators who understand the basics of radio-wave propagation and ECCM.