Control the electromagnetic spectrum to win the unseen battle

by 1st Lt. Thomas W. Dworschak

Any device which emits electromagnetic radiation runs the risk of being located, neutralized or destroyed by the enemy. The United States Army, which stresses maximum use of existing terrain to avoid enemy observation, gives the enemy ample opportunity to locate American forces electronically. In addition to its communications instruments, a US mechanized division employs over 400 non-communicative emitters such as navigational beacons, radar and target acquisition systems. The activities performed by both types of equipment are of such importance that many future battles will be decided by how successful each side is in denying the enemy use of the electromagnetic spectrum.

Because modern weapons are so enormously lethal, the maxim "What can be seen can be destroyed" has become a familiar part of the military lexicon. A slight modification of this phrase, however, is even more accurate: "What can be seen electronically can be destroyed."

Although the many uses of the electromagnetic spectrum by contemporary armies (from voice communications to radar) give modern combatants the increased capabilities necessary to function on the battlefields of the 1980s, they also present the enemy with invaluable sources of readily accessible information. It is this paradox — the need to use the airwaves to disseminate vital intelligence, even though the very act of doing so seriously jeopardizes the security of both the units and the information involved — that has led to the critical but unseen battle known as electronic warfare (EW).

Any device which emits electromagnetic radiation runs the risk of being located, neutralized, or destroyed by the enemy. The United States Army, which stresses maximum use of existing terrain to avoid enemy observation, gives the Soviets ample opportunity to locate American forces electronically. A US mechanized division employs over 400 non-communicative emitters such as navigational beacons, radars and target acquisition systems,[1] and approximately 3000 communications instruments.[2] The activities performed by both types of equipment are of such importance that many future battles will be decided by how successful each side is in denying the enemy use of the electromagnetic spectrum.

The Soviet Union embraces this concept wholeheartedly. The Russian Army is the world's foremost proponent of EW, with an avowed goal of destroying or neutralizing 50% of any opponent's communications system. In pursuit of this objective, all fourteen Soviet armies in Eastern Europe have a Radio Electronic Combat (REC) battalion attached, which is equipped with 90 various types of interceptors, jammers and direction-finding equipment.[3] A Russian REC regiment is also assigned to each of the three Warsaw Pact Fronts, providing an extra 150 EW systems for use against NATO radio sets.[4] Just as the Soviets' numerical superiority in conventional and chemical armaments gives them the initiative in a ground war, the Russians' great preponderance in EW weaponry insures them of a decided advantage in any future struggle for the airwaves.

In Electronic Warfare, it is much easier to attack than to defend. To monitor enemy radio traffic, all that is needed is an antenna and a receiver, and short of physically destroying the listening station there is little the opposing side can

In Electronic Warfare, it is much easier to attack than to defend. To monitor enemy radio traffic, all that is needed is an antenna and a receiver, and short of physically destroying the listening station there is little the opposing side can do to make its transmissions immune to electronic surveillance.

do to make its transmissions immune to electronic surveillance. Radio signals travel far beyond the visible horizon, so a listening post set up behind enemy lines can monitor deep into American positions.[5] Every type of radio has a distinctive electronic signature. Therefore, from the instant even an encoded message is intercepted, the enemy will be able to discern the radio model which provides a vital clue to the type and size of the unit operating it. The frequency will also be apparent, and this information, combined with an analysis of call signs and traffic patterns, permits the enemy to rapidly form an impression of the dimensions of the US force opposing them.

Once an intercept is made, the monitoring station can increase the effectiveness of its EW measures in one or two ways. If the proper equipment is available, a jamming operation can be undertaken to disrupt enemy communications flow. Enemy jammers have the capability to seriously degrade US radio traffic, but there is one major factor which limits their use — jamming strength decreases with range. For this reason, REC units of opposing forces are expected to perform most of their jamming missions within short distances of the Forward Edge of the Battle Area (FEBA).[6]

If a US radio passes traffic for more than 25 continuous seconds, one or more enemy stations can collaborate to employ another form of EW: Direction-Finding (DF). Although a single station can attempt DF alone, only when three or more units work together can an accurate fix be obtained. A fix allows the enemy to ascertain the location of a transmitter within a Circular Error Probability (CEP). Even though the majority of CEPs will have a radius of 1500 meters or more, representing an area in excess of seven square kilometers,[7] the information they provide is crucial. Much of the land within the CEP would be unsuitable for deploying antennas and communications vans, so enemy forward observers would only have to identify the terrain where a signal platoon would likely set up — hilltops and woodlines — and bombard those areas. The Russians' massive concentrations of artillery are well suited for this purpose.

Air superiority, which has been an invaluable ally for any army since 1939, will assume even greater significance in any US-Soviet conflict in the 1980s. In many ways, an aircraft is the ideal platform for EW equipment. An enemy plane or helicopter flying 30 kilometers behind its own lines

In many ways, an aircraft is the ideal platform for EW equipment. An enemy plane or helicopter flying 30 kilometers behind its own lines at an altitude of 3000 feet could monitor American signals along a front 300 kilometers wide and 50 kilometers deep and still be able to discern individual transmitters.

at an altitude of 3000 feet could monitor American signals along a front 300 kilometers wide and 50 kilometers deep and still be able to discern individual transmitters.[8] If US air resistance was weak enough, an enemy EW aircraft would be able to harass American brigade, division, and corps headquarters situated far behind the FEBA. By remaining close to these command posts, an enemy EW plane could jam American receivers from extremely short ranges, as well as employ DF to identify targets for ground attack aircraft. The potential for airborne EW elements is not lost upon the Soviets, who attach eight MI-8 Hip helicopters and two AN-24 Coke aircraft to every REC battalion, plus an additional five Hips and eight Cokes to each REC regiment.[9]

Every type of radio has a distinctive electronic signature. Therefore, from the instant even an encoded message is intercepted, the enemy will be able to discern the radio model which provides a vital clue to the type and size of the unit operating it. The frequency will also be apparent, and this information, combined with an analysis of call signs and traffic patterns, permits the enemy to rapidly form an impression of the dimensions of the US force opposing them.

The standard configuration for most antennas is vertical. This decreases interference from terrain, but radiates a signal in a 360 degree pattern, facilitating enemy interception. By simply mounting the antenna horizontally it becomes bidirectional, since the signal now radiates only off the two ends. This permits the user to control the path of this transmission and keep it oriented towards friendly receivers and away from hostile ones. When combined with low power usage, horizontal polarity greatly enhances signal security.

If nuclear weapons are employed, an extra dimension of EW opens up. Besides their obvious thermal and blast effects, all atomic detonations give off a short (8 - 10 seconds) but intense burst of energy known as an Electromagnetic Pulse (EMP). Although it is harmless to individuals, EMP is destructive to most communications gear. For example, the energy produced by a one kiloton explosion will permanently burn out the components of almost every operational radio and erase computer memories within a radius of 1570 meters. The EMP destruction radius is still fairly small for even a 100 kiloton explosion (3890 meters), which is ideal for the attacker. These limited EMP ranges will result in devastated enemy signal sites, yet friendly stations will be far enough away from ground zero to allow them to continue normal operations. They would not have to shut down out of self-preservation and thereby reveal an impending attack. Only if advance warning is given by other means can the targeted transmitters take the necessary precautions against EMP: disconnect the radios from their antennas, wrap the radios in foil, and place them inside of AFVs. Few units, however, can afford to have all their radios in this configuration for extended periods of time.[10]

The combat power of Soviet EW can scarcely be overrated. The Russians have developed their REC capabilities to such an extent that the standard American tactical platoon radio, the AN/PRC-77, has a 61% chance of being intercepted every time it transmits within ten kilometers of an enemy listening station; the AN/VRC-12, which is used all the way up to division level, will be intercepted 99% of the time.[11] In an environment where what can be intercepted can often be located, jammed, or destroyed, in a future conflict the US Army might well be faced with the dilemma of either not communicating or not surviving.

American forces employ several Electronic Counter-Countermeasures (ECCM) to decrease the effectiveness of enemy REC. The best ECCM is to reduce the number of friendly transmissions; the enemy cannot intercept what does not exist. By keeping messages short (less than 30 seconds) and as infrequent as possible, unfriendly listening posts will be deprived of the information they need to mount an effective EW operation.[12]

Even if unnecessary radio use is eliminated, there are a certain number of transmissions that have to be made, and the US Army has developed techniques to insure their receipt. One method is to use the minimum amount of power required to send the message. Many American radios have the ability to operate in either high or low power; for the AN/VRC-12, the strengths are 35 and 8 watts, respectively. Transmitting at low power reduces the AN/VRC-12's range from 41 to 8 kilometers, and the probability of interception drops to 83%. The AN/PRC-77 operating at low power will only be intercepted 19% of the time.[13]

The possibility of a message being intercepted is further reduced when the transmitting antenna's polarity is modified. The standard configuration for most antennas is vertical. This decreases interference from terrain, but radiates a signal in a 360 degree pattern, facilitating enemy interception. By simply mounting the antenna horizontally it becomes bidirectional, since the signal now radiates only off the two ends. This permits the user to control the path of this transmission and keep it oriented towards friendly receivers and away from hostile ones. When combined with low power usage, horizontal polarity greatly enhances signal security; transmissions by the AN/VRC-12 now have only a 15% chance of interception, and 85% of those interceptions will be too weak to allow the enemy to employ DF. For the AN/PRC-77, 92% of all messages will be undetectable by the enemy, and the source of transmission for the 8% that are picked up by the enemy will be impossible to locate.[14] Horizontal polarity does have its drawbacks, however. The most significant is the difficulties that arise when transporting awkward horizontal antennas, and the requirement that both the transmitting and receiving stations use the same polarization.

Another effective ECCM technique is to position the transmitter and the operator in separate places. The Army's AN/GRA-39 permits units to remote a radio away from its operator; if the enemy uses DF to find the station, any incoming fire will be directed against the antenna and the transmitter, not the radio operator.[15] When used in conjunction with decoy antennas — non-functioning antennas which are easily observed by the enemy — a substantial portion of enemy artillery can be kept occupied shelling these less vital targets.

Just as existing cover should be used to

camouflage communications equipment, terrain can be used to mask radio waves. If antennas are deployed behind hills, buildings or trees, the part of the transmission that radiates towards enemy lines will be dissipated by the obstruction, sharply reducing the probability of enemy interception. Even if a portion of the weakened signal is picked up by the enemy, it will be of reduced value since the terrain will deflect the radio waves, making it difficult to take an accurate fix.[16]

One more key to survival is to keep moving, especially for stations which transmit very powerful signals, such as jammers. Frequent displacement of headquarters, regardless of the tactical situation, is also essential; present US doctrine states that every 24 hours a Division Command Post must relocate one to three times, a Brigade CP three to five times, and a Battalion CP six to eight times.[17]

Proper radio procedure will also reduce enemy REC capabilities. Soviet tactics dictate that if an opposing station cannot be destroyed or jammed, deception will be employed to enter enemy radio nets so that information can be acquired and false traffic passed. Correct transmission techniques are designed to prevent unwanted intrusion into friendly radio nets. These techniques consist of challenging any new station attempting to gain admission to the net; changing call signs every 24 hours in accordance with a prearranged schedule; sending messages in clear text only when absolutely necessary; and ensuring that all numerical information — map coordinates, times, dates and distances — is always encoded.[18]

These ECCM tactics are the US Army's best weapons against the enemy's EW threat. And these are tactics which must be employed, for victory in any future war will belong to the side which can best control the electromagnetic spectrum.

American forces employ several Electronic Counter-Countermeasures (ECCM) to decrease the effectiveness of enemy REC. The best ECCM is to reduce the number of friendly transmissions; the enemy cannot intercept what does not exist. By keeping messages short (less than 30 seconds) and infrequent as possible, unfriendly listening posts will be deprived of the information they need to mount an effective EW operation.

One more key to survival is to keep moving, especially for stations which transmit very powerful signals, such as jammers. Frequent displacement of headquarters, regardless of the tactical situation, is also essential.

Proper radio procedure will also reduce enemy REC capabilities. Correct transmission techniques are designed to prevent unfriendly intrusion into friendly radio nets.

ENDNOTES

[1] *Battlefield Survival and Radioelectronic Combat* TC 30-22 (July 1978), p. 10.

[2] *Combat Communications* FM 24-1 (Sep 76), p. 1-6.

[3] *Opposing Forces Europe* FM 30-102 (Nov 1977), p. A-42.

[4] FM 30-102, p. A-40.

[5] *Threat Handbook: Battlefield Survival and Radioelectronic Combat* (The Radio Direction Find Threat) (Jan 1977), p. 46.

[6] *US Army Electronic Warfare Concept* (March 1978), p. 2-2.

[7] *Threat Handbook,* p. 49.

[8] TC 30-22, p. 15.

[9] FM 30-102, p. A-46.

[10] *Combat Communications within the Division,* FM 11-50 (March 1977), pp. 4-15 through 4-22.

[11] *Threat Handbook,* p. 77.

[12] TC 30-22, p. 44.

[13] *Threat Handbook,* p. 77.

[14] *Threat Handbook,* p. 77.

[15] TC 30-22, pp. 52-53.

[16] TC 30-22, p. 57.

[17] FM 24-1, p. 6-4.

[18] TC 30-22, p. 61.

After earning two bachelor's degrees, one in history and one in political science, from the University of Illinois, 1st Lt. Dworschak received his RA commission through that school's ROTC program in 1979. Dworschak completed the Signal Officers Basic Course in August 1979 and was assigned to 333d Signal Company at Ft. Gordon where he served as a platoon leader for one year. He currently works for the Fort Gordon Public Affairs Office as Editor of The Semaphore, the post newspaper.