Is tactical LOS radio effective in nuclear or electronic warfare?

by Maj. Gary P. Clukey

LOS systems are clearly vulnerable to the enemy threat. The specific degree of vulnerability is determined by such variables as systems configuration, electronic technology, and designed protection. However, all communications facilities (especially LOS) are by their very nature susceptible to enemy detection.

To be survivable, communications cannot be totally destroyed and must remain either undamaged or capable of degraded operation. However, it is not enough for a particular LOS terminal to remain physically undamaged, the terminal must continue to provide a communications path to the outside world or to a distant headquarters.

Lt. Gen. William H. Hilsman, director of the Defense Communications Agency, recently wrote "All systems for command and control, intelligence, and logistics are ineffective without a communications system to support them." In other words, these sophisticated systems are only as effective as the communications links that interconnect them. Tactical line-of-sight multichannel radio (LOS) is often used to provide key links between major headquarters and between command elements. Specifically, LOS is used at the brigade, division, corps, and theater level, and it can be used to interconnect tactical elements to the Defense Communications System for communications to the National Command Authority. It provides user paths for high speed data and teletype, point-to-point and common-user telephone service, interswitch trunking, and access to commercial telephone facilities and the military's automatic voice network.

A question that concerns many communicators as well as commanders is whether or not LOS can be effectively used in a hostile electronic warfare (EW) environment. Sophisticated detection devices and accurate conventional and nuclear weapons make the physical survival of LOS systems doubtful. In the next major conflict, then, the tactical communicator's challenge will be to install, operate, and maintain LOS systems over varied distances and terrain under even more extremely adverse conditions than presently envisioned.

"Any system that depends on electromagnetic energy can be exploited by an enemy with the capability and opportunity to do so." This exploitation can be by jamming, firepower, or by intelligence gathering.

POSSIBLE SCENARIOS

There are three possible scenarios in which the next major conflict may be conducted: divisions-on-line battle situations, a mobile defense or tactical nuclear situation, or a combination of these two. The first scenario places the United States against a sophisticated enemy with near or equal parity in the air. The second envisions wide fronts and battle areas that range in depth from a few kilometers to as much as 150 kilometers against a sophisticated enemy with air parity or superiority. A combination of these two scenarios must be assumed for any discussion of the enemy (Soviet) threat. Movement of communications sites will undoubtedly be frequent, and contacts between opposing forces are perceived as vicious and of short duration. Only highly mobile and dispersed forces will be able to survive and fight; therefore, for effective command and control, communications systems must be flexible, responsive, and reliable.

LOS systems depend on electromagnetic energy, and the Soviets clearly have exploitation capabilities in this field. The primary threat to our LOS is their radio-electronic combat (REC), which would permit physical destruction of communication sites by conventional or nuclear weapons or disruption of systems/links by jammers.

THE EW THREAT

"Any system that depends on electromagnetic energy can be exploited by an enemy with the capability and opportunity to do so." This exploitation can be by jamming, firepower, or by intelligence gathering. LOS systems depend on electromagnetic energy, and the Soviets clearly have exploitation capabilities in this field. The primary threat to our LOS is their radio-electronic combat (REC), which would permit physical destruction of communication sites by conventional or nuclear weapons or disruption of systems/links by jammers. REC, which integrates electronic intercept and direction-finding (DF) with suppressive fires and electronic jamming, is designed to prevent us from coordinating the use of our weapons and from using our command and control systems. A direct link between collectors and fire support means is maintained. REC is not so powerful that we cannot defend against it, but it will disrupt control. We must expect that the enemy knows our strong and weak points; he will therefore make every effort to destroy key communications nodes. We can expect at least a fifty percent destruction or disruption of communications facilities and systems. Front line communications will be severely crippled, shut down for periods of time, or destroyed by weapons and EW.

In a recent article in THE ARMY COMMUNICATOR, Lt. Col. Don E. Gordon

There are three possible scenarios in which the next major conflict may be conducted: divisions-on-line battle situations, a mobile defense or tactical nuclear situation, and a combination of these two.

REC, which integrates electronic intercept and direction-finding (DF) with suppressive fires and electronic jamming, is designed to prevent us from coordinating the use of our weapons and from using our command and control systems. A direct link between collectors and fire support means is maintained. REC is not so powerful that we cannot defend against it, but it will disrupt control.

contrasted the Soviet EW concept with ours by discussing a possible scenario:

> *The enemy depends on barrage jamming (covers a major portion of the radio band) to keep numerically inferior allied forces from coordinating their technologically superior weapons and command and control systems. Key communication centers at battalion, brigade, and division levels are disrupted with spot jamming (specific channels).*
>
> *- TAC Vol. 5 (Summer 1980) 11-15.*

US forces, he says, are more apt to attempt to develop communications intelligence than to make a hasty decision to disrupt or destroy enemy facilities. US jamming, primarily spot, is much more selective. Soviet jammers are not assigned to intelligence units as in the US Army, but rather are assigned to special EW or signal units.

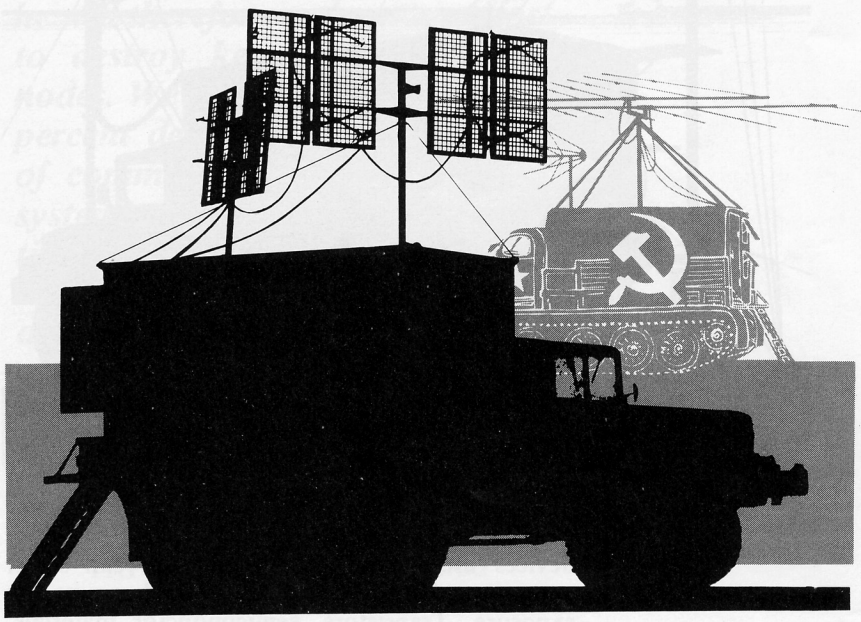
The Soviets, through a combination of airborne direction-finding (DF) and ground DF stations, are capable of providing sufficiently accurate "fixing" to permit effective targeting by conventional weapons (artillery or multiple rocket launchers for example). After detection priorities are established for jamming and/or destruction, command and control systems receive first priority, and command posts, communications centers, and radar stations receive second priority. The threat to LOS communications facilities is obvious.

Those who doubt that the Soviets now have a sophisticated detection capability are reminded that in 1974, during a European Microwave Conference, Western nations openly demonstrated their latest "threat" electronics equipment touting its rugged modular design and publicizing its capabilities for digitally controlled microwave receiving and analysis (even disclosing its effective spectrum characteristics). Since then, the Soviets have made tremendous progress towards achieving technological parity in all areas with the United States and other Western nations, as evidenced by their recent success in space exploration. Can there by any remaining doubts that they have adequately responded to the 1974 display?

Only highly mobile and dispersed forces will be able to survive and fight; therefore, for effective command and control, communications systems must be flexible, responsive, and reliable.

THE NUCLEAR THREAT

The nuclear threat adds still another dimension to the "usability" problem. Destruction of site facilities, degradation of the propagation qualities of the atmosphere, and injury to site personnel are some of the obvious adversities that can result when nuclear weapons are employed. Direct and near

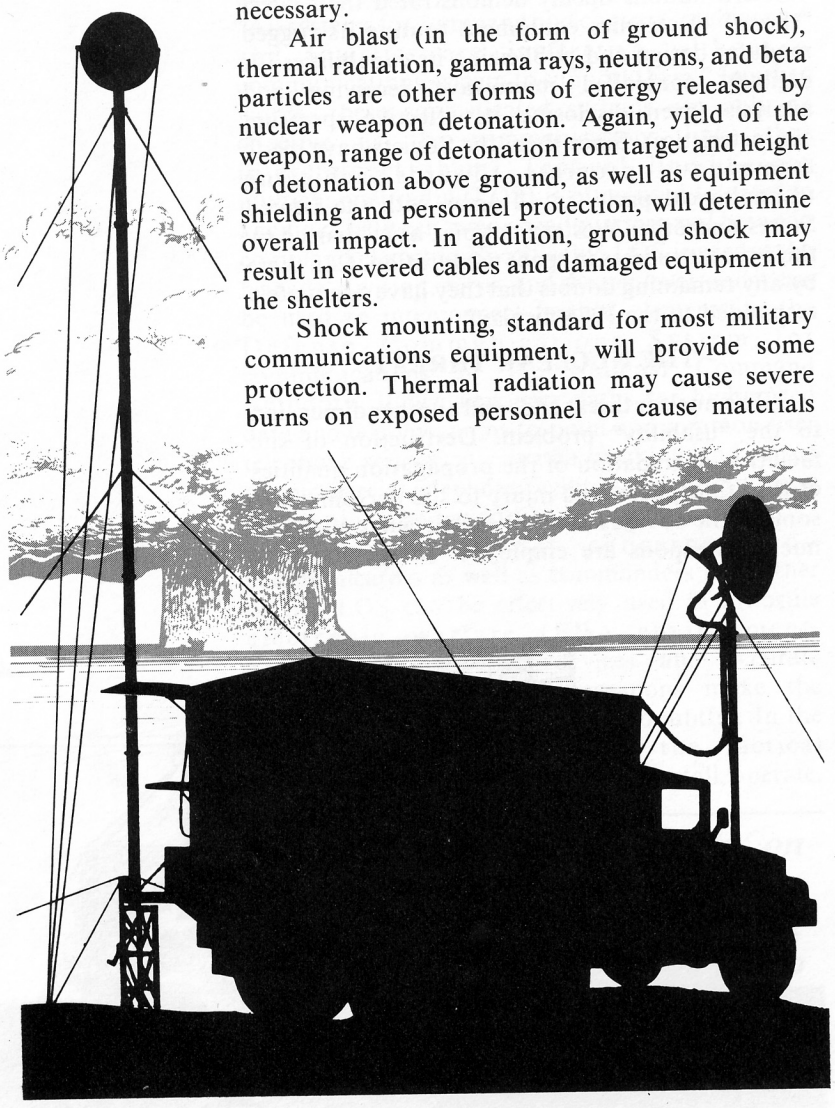


hits, and even distant nuclear explosions, can be lethal to tactically deployed radio teams. The yield of the nuclear weapon, height-of-burst, and distance to target when the weapon is activated are some of the variables which will determine actual damage to personnel and equipment. For example, a one-megaton weapon detonated below two kilometers will cause an above-ground reinforced concrete structure to suffer severe damage (wall and roof collapse). Tactical LOS facilities with parabolic dish antennas (often raised to heights of fifty feet using antenna mast sections and anchored with only guy lines), signal equipment shelters covered only with camouflage netting, and wave guide sections extended from the radio receiver and transmitter to the antenna dish can be damaged much more easily than reinforced concrete structures. In other words, direct targeting for

destruction by nuclear weapons is simply not necessary.

Air blast (in the form of ground shock), thermal radiation, gamma rays, neutrons, and beta particles are other forms of energy released by nuclear weapon detonation. Again, yield of the weapon, range of detonation from target and height of detonation above ground, as well as equipment shielding and personnel protection, will determine overall impact. In addition, ground shock may result in severed cables and damaged equipment in the shelters.

Shock mounting, standard for most military communications equipment, will provide some protection. Thermal radiation may cause severe burns on exposed personnel or cause materials



(especially paper) to ignite at distances up to one hundred miles from the impact point. Solid state devices used in all LOS equipment can suffer permanent damage from neutron and gamma ray exposure. Transistors, semiconductor materials, and other electronic components may be damaged. The necessary grounding systems, wave guide and cable runs, and antenna leads provide numerous external electrical paths thus making LOS radios expecially susceptible to damage by a nuclear phenomenon known as electromagnetic pulse (EMP), which is produced by emitted gamma rays. EMP can penetrate a facility through any conducting path and cause burnout of electrical components. Surprisingly, modern solid state circuitry is more susceptible to EMP damage than older technology circuitry.

Propagation (transmission of radio waves through free space) will almost certainly be affected by a nuclear detonation. Radio signals at all frequencies propagated through the nuclear fireball (which usually lasts a few minutes) will be absorbed. The fireball rises and expands as it cools and may

The Soviets, through a combination of airborne direction-finding (DF) and ground DF stations, are capable of providing sufficiently accurate "fixing" to permit effective targeting by conventional weapons (artillery or multiple rocket launchers for example).

intercept a LOS signal for varying periods of time. The nuclear radiation effects on personnel, which can range from no impact to immediate incapacitation or death within thirty minutes (depending on the level of exposure), are equally important.

LOS MULTICHANNEL IMPROVEMENT

An elaborate and expensive program to improve LOS equipment is currently underway. It is a part of the TRI-TAC effort, a joint Army, Navy, Marine Corps and Air Force program, designed to achieve interoperability among tactical communications systems. One of the basic equipment items being developed includes a digital group multiplexer for use with LOS systems. The major goal of the TRI-TAC program is gradual transition from analog, manual, non-secure communications to all digital, automatic, fully compatible systems. During this transition, digital capabilities will be established while still retaining analog operations as necessary. Some units based in Europe and others in CONUS, designated as joint task force elements, already possess a secure capability for LOS through use of the KG-27 bulk encryption device. This device permits quick, secure exchanges of information and thus significantly reduces an enemy's capability to collect and gain intelligence. Other research, testing, and

The nuclear threat adds still another dimension to the "usability" problem. Destruction of site facilities, degradation of the propagation qualities of the atmosphere, and injury to site personnel are some of the adversities that can result when nuclear weapons are employed. Direct and near hits, and even distant nuclear explosions, can be lethal to tactically deployed radio teams.

After deception priorities are established for jamming and/or destruction, command and control systems receive first priority, and command posts, communications centers, and radar stations receive second priority. The threat to LOS communications facilities is obvious.

development aimed at improving the survivability of materiel and improving the reliability of electronic systems are being conducted by various agencies such as the Electronic Research and Development Command. Nevertheless, what some tactical communicators have now, and *all* should have by 1992, is essentially the same LOS radios modified only by the addition of a secure bulk encryption device.

SOME LOS DIFFICULTIES IN A NON-THREAT ENVIRONMENT

During the past several years, I observed various LOS radio sets during numerous joint service exercises. These exercises, directed by the Joint Chiefs of Staff and sponsored by either the United States Readiness or Atlantic Command, involved Army, Air Force, Marine Corps, and Navy elements. Not once did I see LOS fail catastrophically. In fact, the reliability of LOS was always high. However, these LOS systems were not being used in a hostile threat environment, and time and budgeting constraints did not allow major commanders to relocate major headquarters frequently. The establishment of LOS communications in this kind of environment, however, is not an easy task.

Often, in the planning phase, a usable system path is difficult to identify, or it is discovered that a particular system installation is not feasible since it will require an excessive number of intermediate relay sites. During the site survey (when time permits one to be conducted), it may be discovered that a site selected by map study is inaccessible or is completely surrounded by two-hundred foot trees—conditions that simply do not permit LOS communications. Finally, when the execution phase is reached, adverse weather conditions, radio frequency interference from unknown sources (maybe the friendlies), or improper grounding techniques can be problems. On the whole, conditions such as ground electrical characteristics (two-thirds of the world has what is considered poor ground), ambient noise levels, terrain profiles, and vegetation are always potential problems.

In addition, training of personnel is not normally complete or up to desired standards, and all equipment is not always fully operationally ready or complete. Obviously, these problems are not insurmountable nor unique to LOS multichannel radio; otherwise, the military would not have it in the inventory.

Thermal radiation may cause severe burns on exposed personnel or cause materials (especially paper) to ignite at distances up to one hundred miles from the impact point. Solid state devices used in all LOS equipment can suffer permanent damage from neutron and gamma ray exposure. Transistors, semiconductor materials, and other electronic components may be damaged.

We must expect that the enemy knows our strong and weak points; he will therefore make every effort to destroy key communications nodes. We can expect at least fifty percent destruction or disruption of communications facilities and systems. Front line communications will be severely crippled, shut down for periods of time, or destroyed by weapons and EW.

THE VULNERABILITY OF LOS COMMUNICATIONS

LOS systems are clearly vulnerable to the enemy threat. The specific degree of vulnerability is determined by such variables as systems configuration, electronic technology and designed protection. However, all communications facilities (especially LOS) are by their very nature susceptible to enemy detection. Terminal and relay sites often require a relatively large area for site set-up (50 by 100 feet), may be powered by noisy generators, and may be surrounded by protruding antenna dishes. Most LOS equipment, although mounted in shelters on wheeled vehicles to provide increased mobility, is physically too large to move constantly. LOS systems, designed for use where difficult terrain or other considerations prevent the use of multipair cable, generally require use of high ground locations for best transmission and reception. Operators often use high frequency (HF) or very high frequency (VHF) radios with omni-

The necessary grounding systems, wave guide and cable runs, and antenna leads provide numerous external electrical paths thus making LOS radios especially susceptible to damage by a nuclear phenomenon known as electro-magnetic pulse (EMP).

EMP can penetrate a facility through any conducting path and cause burnout of electrical components. Surprisingly, modern solid state circuitry is more susceptible to EMP damage than older technology circuitry.

directional antennas (radiating, in all directions, signals which are generally easy to detect) to communicate from one microwave link to another, particularly during initial site set-up. Further, operators often talk in a casual or unsecure mode on the "engineering" channel of the LOS system thus compromising key information (unit locations or strengths for example). Improved operational procedures and use of electronic counter-counter measure (ECCM) tactics can reduce LOS vulnerability, but there are no convincing arguments that the skillful use of existing doctrine and equipment will ensure survivability.

METHODS FOR SURVIVABILITY

According to *Command and Control for Survival*, survivability is "the ability of a system to continue performing its essential function after an enemy attack." To be survivable, communications cannot be totally destroyed and must remain either undamaged or capable of degraded operation. However, it is not enough for a particular LOS terminal to remain physically undamaged, the terminal must continue to provide a communications path to the outside world or to a distant headquarters.

Lt. Gen. Thomas M. Rienzi, the Army's preeminent communicator of the 70's, prescribes four-step defensive planning as the key to survival in a hostile EW environment. First, he says, identify the problem and determine/estimate your vulnerability; this evaluation must be made at the outset. Second, develop a solution and formulate a defense; specify ECCM tactics that can be employed; include these tactics in operational plans. Third, train personnel for implementation or employment. Fourth, test and revise the plan during individual and unit/collective training, maneuvers and exercises. This four-step cycle must then be forever repeated since a defense can become obsolete as the threat changes.

Unfortunately, the training and testing steps under totally realistic conditions are virtually impossible. Area and safety limitations, such as frequency spectrum use and weapons detonation, restrict our capability to provide a hostile EW environment. In contrast, equipment specifications can be tested fairly accurately through computer simulation techniques. Despite limitations, all techniques and facilities that will increase training and/or testing realism should be used to the maximum feasible extent.

ELECTRONIC COUNTER-COUNTER MEASURE (ECCM) TACTICS

There are numerous ECCM tactics outlined in various training circulars, field manuals, and technical periodicals. These tactics, combined with prior planning, effective and realistic training, and technical improvement of equipment seem to be the major points advocated to insure survivability. On the whole, ECCM tactics, categorized as deployment, employment, replacement, and concealment, will help to improve the chances for LOS system survivability. Planning must make provisions for alternate routes for circuits, redundant facilities, and component interface (interoperability). Employment techniques (such as frequency selection and use), signal security, and control of transmit power are equally important. Survivability can also be improved by using other means of communications including wire and cable, tactical satellite, HF and VHF radio, messenger, and visual and sound techniques, and by using concealment tactics including emission control, antenna masking, camouflage, simulating

An elaborate and expensive program to improve LOS equipment is currently underway. It is a part of the TRI-TAC effort, a joint Army, Navy, Marine Corps, and Air Force program, designed to achieve interoperability among tactical communications systems.

One of the basic equipment items being developed includes a digital group multiplexer for use with LOS systems. The major goal of the TRI-TAC program is gradual transition from analog, manual, non-secure communications to all digital, automatic, fully compatible systems.

communications radiations at a dummy site, and/or altering the sequence of events at a particular site to deceive the enemy. Obviously, my intent is not to discuss all possible ECCM tactics but to point out that there are many to choose from.

Various assumptions about LOS are contained in volumes of EW literature; these assumptions are important since they help to emphasize that a Soviet threat does exist and that our LOS systems are vulnerable. First, even the most advanced systems are doomed to eventual obsolescence which can result from an improvement in the enemy's capabilities or our own state-of-the-art equipment advances. Second, no LOS node is safe from conventional or nuclear attack. Third, the enemy knows our strong and weak points and will make every effort to hit us in our critical areas. Fourth, our systems can be jammed and the enemy has this capability. Fifth, in the future, our superiority in technology cannot be trusted to offset our lack of planning.

There are numerous ECCM tactics outlined in various training circulars, field manuals, and technical periodicals. These tactics, combined with prior planning, effective and realistic training, and technical improvement of equipment seem to be the major points advocated to insure survivability. On the whole, ECCM tactics, categorized as deployment, employment, replacement, and concealment, will help to improve the chances for LOS system survivability.

I endorse these assumptions and agree that continuous defensive measures (preplanned operational tactics and technical improvements) are necessary to minimize the threat. However, when I contemplate the question of whether or not we will be able to communicate, I must respond negatively. When I examine redundance, which on the surface appears to insure that some facilities will survive for use, I see that first it is too costly to implement, and second, it does not guarantee that communications to the outside world will remain intact. Maintenance of a varied equipment inventory implies that somehow (regardless of the threat) we will be able to communicate using one system or a combination of systems; a full equipment "menu" is no failsafe guarantee.

The alternate means of communications that we could effectively use as substitutes for LOS are extremely limited. Cable is just not sufficiently responsive to mobility and range requirements on the modern battlefield where flexibility and mobility are the keys to survival. HF equipment has small channel capacity, and its use is often impaired by adverse propagation characteristics which may or may not be overcome by antenna adjustment. Tactical satellite equipment, which is probably the best LOS substitute that we currently have, is limited by some of the same conditions that limit LOS (for example, locating a site that permits an unobstructed signal take-off angle needed to insure high quality circuits can be difficult).

Improved operational procedures and use of electronic counter-counter measure (ECCM) tactics can reduce LOS vulnerability, but there are no convincing arguments that the skillful use of existing doctrine and equipment will ensure survivability.

CONCLUSION

Will LOS be usable? Obviously there is no definite answer to this question. Chances for survivability can be improved. Nevertheless, once a terminal or relay site is detected by the enemy, it will most likely be destroyed or jammed, thus rendering it ineffective. Undetected sites are susceptible to incidental destruction by mass conventional indirect fire and/or nuclear weapons. ECCM tactics are limited by available personnel and equipment assets. Even if assets were unlimited, it would not be feasible to saturate a particular area since one carefully detonated nuclear weapon could still destroy them all. Consequently, the communicator cannot guarantee the usability of LOS in the threat environment described here. Moreover, it is important for all planners and commanders to recognize now that LOS communication (as we know it today) will probably not be usable during a major conflict with the Soviets.

ECCM tactics are limited by available personnel and equipment assets. Even if assets were unlimited, it would not be feasible to saturate a particular area since one carefully detonated nuclear weapon could still destroy them all. Consequently, the communicator cannot guarantee the usability of LOS in the threat environment described here.

It is important for all planners and commanders to recognize now that LOS communication (as we know it today) will probably not be usable during a major conflict with the Soviets. We are in this tenuous position because our technical design and sophistication of LOS equipment has not kept pace with current operational doctrine...

We are in this tenuous position because our technical design and sophistication of LOS equipment has not kept pace with current operational doctrine calling for a highly active and mobile defense in which our engaged forces will be heavily outnumbered and our reserve forces small. A shortened procurement cycle (to prevent obsolescence before deployment), early funding, anticipation of requirements, and participation of ECCM experts in the planning and conceptual development stages are necessary. A major technological breakthrough that leads to the design and timely fielding of a viable substitute for current LOS equipment would surely help.

BIBLIOGRAPHY

Backus, Paul H. "An Overview of the Army's EW and C³CM." *Journal of Electronic Defense,* Vol. 3 (January/February 1980), 21-26.

Bowers, Jack L. "Active Countermeasures." *Journal of Electronic Defense,* July/August 1980, pp. 10-12.

Connoly, John J. *Command and Control For Survival.* Report by Litton Systems, Inc., 13 June 1962.

Donohue, Carol L. "ECCM Training: Reducing the REC Threat." *Army Communicator,* Vol. 5 (Summer 1980), 48-49.

Eustace, Harry F. "Soviets Deploy New Jamming Gear." *Electronic Warfare/Defense Electronics,* Vol. 10 (May 1978), 26.

Fitts, Richard E. *Fundamentals of Electronic Warfare.* Colorado: USAF Academy, 1972.

Fossum, Robert R., and Vinton G. Cerf. "Communications Challenges for the 80s." *Signal,* Vol. 34 (October 1979), 17-20.

Gordon, Don E. "Target: The Spoken Word." *Army Communicator,* Vol. 5 (Summer 1980), 11-15.

Heverly, Ross J. and James E. Russel. *Range Mobility and Transmission Reliability Factors for Division Communications.* Technical Memorandum by Research Analysis Corporation, June 1962.

Hilsman, William J. "Communications in Support of Automated Battlefield Systems." *Journal of Electronic Defense.* Vol. 3 (July/August 1980), 39-40.

Hoover, John E. "TRI-TAC—Tactical Communications for the 1980s." *Signal,* Vol. 31 (August 1977), 92-103.

The International Countermeasures Handbook 1977-1978. Ed. Harry F. Eustace. Palo Alto, California: EW Communications Inc., 1978.

International Defense Review. *Electronic Warfare.* Geneva: Interavia, 1978.

King, Michael A., and Paul B. Fleming. "An Overview of the Effects of Nuclear Weapons on Communications Capabilities." *Signal,* Vol. 34 (January 1980), 59-66.

Lampos, Nicholas T. "Electronic Warfare Defense Planning and Tactics." *Electronic Warfare,* Vol. 6 (November/December 1979), 44-47.

Lampos, Nicholas T. and Thomas M. Rienze. "Electronic Warfare Defense For Communicators." *Signal,* Vol. 31 (July 1977), 21-22.

Marcus, Michael J. "Communications ECCM: A Spectrum of Techniques." *Signal,* Vol. 32 (March 1978), 47-51.

Mentry, Louis C. and A. R. McCahan. "Communications in the 4th Infantry Division (MECH)." *Army Communicator,* Vol. 5 (Summer 1980), 52-54.

Raggett, Ronald J. "C³—the Key to Future Survival?" *Military Technology and Economics,* Vol. 3 (May/June 1979), 53-58.

Raggett, Ronald J. "Field Communication—To Sophistication and on to the ECCM." *Military Technology and Economics,* No. 5, 1978, pp. 49-50.

Slay, Alton D. "Electronic Warfare Integration and Planning." *Signal,* Vol. 33 (March 1979), 16.

Thurbon, M. T. "The Nature of Electronic Warfare." *Journal of Electronic Defense,* Vol. 3 (May/June 1980), 31-34.

US Army Command and General Staff College. *Reference Book 100-33: Electronic Warfare Operations,* Fort Leavenworth, Kansas, August 1978.

US Army Southeastern Signal School. *Special Text 11-54-2: Signal Reference Data—Radio and Radar Communications Equipment,* Fort Gordon, Georgia, 1974.

US Department of the Army. *Field Manual 32-30: Electronic Warfare—Tactics of Defense.* Washington, 31 August 1976.

US Department of the Army. *Training Circular 30-22: Battlefield Survival and Radioelectronic Combat.* Washington, 7 July 1978.

US Department of the Army. *Training Circular 100-33: Division Electronic Warfare Operations.* Washington, September 1979.

Maj. Clukey has a B.S. from Norwich University and an M.B.A. from New York Institute of Technology. He is a graduate of the Radio Systems Course, the Signal Officers Advanced Course, the C-E Systems Engineer Course and the Armed Forces Staff College. He is assigned as a staff officer in Canberra, Australia, with the Australian Directorate of Communications.