

PROJECT TOUCHDOWN:

HOW WE PAID THE PRICE FOR LACK OF COMSEC IN VIETNAM

DAVID FIEDLER

Editor's Note: *This article was previously published in Army Communicator magazine. The article details a glaring example of how non-secure radio communications can lead to the death of U.S. combat troops. In today's theaters of operations, the use of commercial radios without communications security (COMSEC) is still very dangerous.*

In late 1969, I and every other member of 1st Signal Brigade and 160th Signal Group's 44th Signal Battalion were searching for Viet Cong (VC) or North Vietnamese Army (NVA) spies within our local-hire signal workforce. (The Vietnamese locals were mostly base-camp telephone switchboard operators, installers, and repair personnel that 1st Signal Brigade employed in its base-camp facilities.) At that time, the G-2, U.S. Army Vietnam (USARV) – our command headquarters – was convinced that, because so much of our operational information was apparently in the enemy's hands and we were taking such high casualties, espionage on a large scale was the only possible explanation.

G-2 also felt that the most likely location for espionage was at major signal locations where operational information was concentrated and there was also a large local civilian workforce. In fact, in 44th Signal Battalion, we caught one of our cleaning women with a stolen manual for the AN/FRC-93 high frequency radio (also known commercially as the Collins KWM-2A) at a gate search. She was turned over to the Vietnamese National Police, which was probably determined to sentence the woman to death, and that bothers me even today because she was probably innocent. She probably wanted the manual for toilet paper, since such a use for publications was common among the Vietnamese.

Almost everyone was quite happy with this “spy capture” except myself and a few others. We failed to see how obtaining a manual that could be bought in any amateur radio store in America would be of much value as technical intelligence to the enemy. In addition, we thought our losses were clearly the result of operational, not technical, communications intelligence.

No spy ring, just arrogance

Thanks to our battalion S-2, 44th Signal Battalion Soldiers were aware as early as 1965 that the enemy was probably monitoring USARV tactical-radio nets. The Army Security Agency (ASA) tried to make everyone else a believer in this,

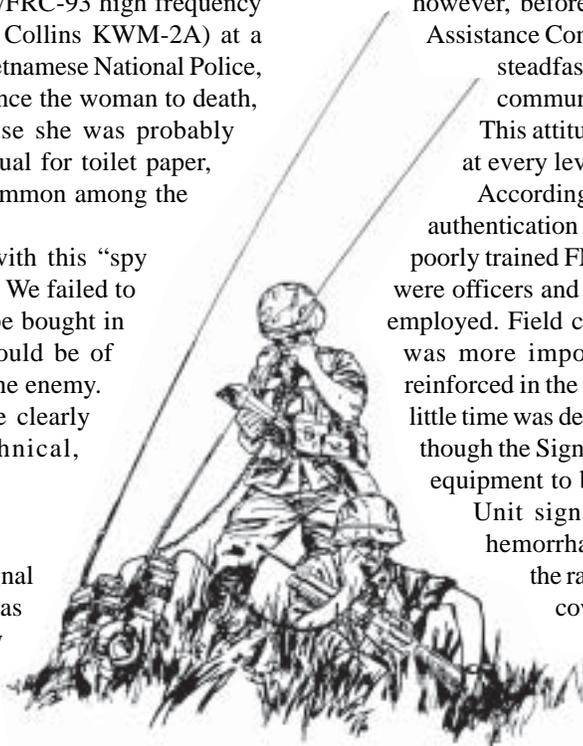
too. However, despite ASA's many warnings, it was USARV's official opinion that the NVA/VC had no equipment capable of monitoring U.S. tactical-radio nets, nor could they understand English well enough to use the information if they had the equipment. Most importantly, they believed our tactical forces moved so fast and our actions on the battlefield were so quick that even if the enemy managed to acquire some information from our tactical-radio nets, it would do them no good and us no harm. That arrogance was to cost us dearly.

At this point, it's important to know that by 1965 frequency modulation voice radio had been deployed to every level of command from squad to corps (and higher). It's also important to know that this radio equipment, AN/PRT-4 and AN/PRR-9 (handheld radios for squads or platoons), AN/PRC-25 (manpack and vehicular for platoon, company or battalion) and AN/VRC-46 (vehicular, platoon through corps and higher) did not have any communications security provisions at the Vietnam War's outset.

Since there was no COMSEC device, either internal or external, provided to this equipment until late in the conflict, the only solution was to constantly stress the vulnerability of FM voice radio intercept and analysis and to carefully use signal operating instructions, off-line (paper) operations codes and authentication tables (challenge and reply) to provide net security. As I said, however, before late 1969, the USARV and Military Assistance Command Vietnam (MACV) commanders steadfastly refused to believe there was a real communication intelligence (COMINT) threat. This attitude was reflected across the entire force at every level.

Accordingly, since existing operations codes and authentication tables were cumbersome for the typical poorly trained FM voice radio operators (most of whom were officers and senior NCOs) to use, they were rarely employed. Field commanders clearly believed that time was more important than security. This view was reinforced in the combat-arms training base, where very little time was devoted to communications subjects, even though the Signal Corps had declared combat-net radio equipment to be “user-owned and operated.”

Unit signal officers (S-6/G-6) magnified the hemorrhage of vital tactical information over the radio because many of these officers were cowed by higher headquarters and tactical commanders into also believing there was no COMINT threat. By direction, signal officers rarely, if ever, took even the minimal action



of just simply changing net call signs and frequencies.

Taken together, our COMSEC laxness – created by our arrogant assessment of the enemy’s capabilities and intelligence – led to a massive opportunity to intercept and exploit our tactical FM communications nets, which our astute enemy used to an extreme advantage.

While we in the Signal Corps tout good communications as a combat multiplier, we rarely mention that Vietnam proved enemy exploitation of our communications is deadly.

No one to my knowledge has ever been able to calculate the number of names on the Vietnam Wall due to poor COMSEC, but all indications are that the number is considerable. The number of Americans killed and wounded in action due to lack of radio security certainly must, in my opinion, far exceed the much-publicized losses due to friendly fire or noncombat related deaths due to accidents, for example.

The blame for this unfortunately lies squarely with the major U.S. field commands (MACV and USARV), the Signal Corps leadership, and the Signal Corps’ schools at Fort Gordon, Georgia, and Fort Monmouth, New Jersey. Compounding the “user-owned and operated” COMSEC disaster was the concept that tactical-unit signal officers (S-6s) could be trained in nine weeks at Fort Gordon in the Signal Officer Basic Course. These basic signal officers were then assigned to tactical units in the United States or Europe for periods as short as eight months where, according to the Signal Corps, they would learn their job on the job, be promoted to first lieutenant and then deployed to Vietnam.

The result of this concept speaks for itself, since most signal officers when assigned to tactical units did very little signal work, had no formal training while in these assignments and no signal standards to meet while in these assignments.

Embarrassed by Alpha-3

Fortunately, in late December 1969 – almost four years after the U.S. Army deployed major units to Vietnam and after four years of exposing our combat radio nets to exploitation – the situation changed dramatically. On the morning of December 20, 1969, a scout from 1st Brigade, 1st Infantry Division, discovered a long wire antenna on the ground at the old Michelin rubber plantation in the area northwest of Saigon. The antenna wire led to a carefully concealed underground bunker complex that was packed with enemy radio-communications intercept equipment. This complex was the operations center for an NVA/VC platoon-sized radio “technical reconnaissance unit” known as Alpha-3 that was part of the NVA’s 47th Technical Reconnaissance Battalion.

After a short fight, 12 members of Alpha-3 were taken prisoner. Even more significant, however, was the fact that U.S. infantry also captured all of Alpha-3’s equipment and its logbooks. These logbooks proved without doubt that the enemy had been intercepting U.S. voice radio traffic over an extended period of time, understood the exact meaning of the traffic and were able to easily decrypt and understand traffic covered by unauthorized

The most shocking thing about Alpha-3 platoon’s capture by far, however, wasn’t its intercept equipment or its ability as antenna engineers, but rather its station log books, training materials and knowledge of U.S. operational CNR doctrine and procedures.

(locally made) codes and infrequent SOI changes.

Alpha-3’s actual intercept equipment wasn’t the product of some super-secret Soviet or Chinese version of Fort Monmouth or the Massachusetts Institute of Technology labs. Alpha-3’s stuff consisted mostly of captured AN/PRC-25 or AN/PRC-77 radios and others bought from our South Vietnam allies or through third parties.

Obviously, this equipment was 100-percent interoperable with the radios in our units since it was identical to our equipment. Supplementing the captured or acquired U.S. standard very-high-frequency equipment, Alpha-3 had several Chinese R-139 HF receivers and a good number of Sony and Panasonic commercial radios they had simply modified to work in the U.S. tactical-frequency bands.

Alpha-3’s hardware engineering wasn’t without some imagination, though. At the time, all U.S. units were suffering from a critical shortage of BA-4386 magnesium batteries. Alpha-3 soldiers discovered they could solder together eight BA-30 D-cell flashlight batteries (no shortage of these) and produce the 12 volts of direct-current power the AN/PRC-25 needed to receive signals.

In addition, unlike U.S. forces, the NVA signal establishment was able to impart to Alpha-3 an appreciation of the critical role antenna engineering plays in any radio system. Compared to Fort Gordon graduates of both then and now, Alpha-3 personnel were antenna geniuses. With this knowledge, Alpha-3 was able to produce antennas that extended the normal operating distances of their radio intercept receivers far beyond their expected range.

This lesson needs to be remembered today as the Army adopts more non-COMSEC-protected radios, radio/intercoms and wireless local-area network equipment with the expectation that their low radiated-signal levels will protect them from enemy interception and exploitation. The Alpha-3 experience teaches us that nothing could be further from the truth. Supposedly ignorant third world Alpha-3 soldiers were expert enough to actually build radio receivers in the field from new and used parts obtained or manufactured locally. Very few U.S. Army Signal Corps personnel either then or now could duplicate this capability.

The most shocking thing about Alpha-3 platoon’s capture by far, however, wasn’t its intercept equipment or its ability as antenna engineers, but rather its station logbooks, training materials and knowledge of U.S. operational combat net radio (CNR) doctrine and procedures. In short, Alpha-3 was reading our mail and knew exactly what it meant and what to do about it. U.S. infantrymen found handwritten logs containing the texts of American voice conversations transcribed verbatim in English and then analyzed by excellent English linguists.

The 47th Technical Reconnaissance Battalion was primarily interested in plain-language and brevity-coded voice communications its intercept operators had no problem understanding. Of particular interest were forward air controller, forward observer, command and control, and civilian press communications. The civilian press, in fact, proved to be a great

source of immediate operational information throughout the war. Present day commanders should take a lesson from this when considering allowing the civilian press and its normally uncovered communications (satellite phone, cell phone, etc.) into their operations area. A better approach may be to let the press use COMSEC-protected military communications to avoid immediate disclosure of critical operational information.

The Alpha-3 logs showed us that back in 1965 we were passing this operations-security information over the air in the clear because we underestimated the enemy's COMINT capabilities:

- Artillery target information (in time for the enemy to take cover);
- Artillery harassment and interdiction fire schedules (in time for the enemy to stay clear of targeted locations);
- Ambush site locations (bringing up the question of who ambushed who);
- Casualty reports;
- Air strike (B-52) warnings;
- Friendly troop positions;
- Radio-net call sign and frequency changes;
- Unit status reports;
- Plans and orders; and
- Idle operator chitchat containing all sorts of operational information.

More examination of captured enemy material also revealed the enemy had deduced from their COMINT operations the following general characteristics about our CNR operations and could exploit them:

■ U.S. units made extensive use of locally produced unauthorized codes, many of the "point of origin" or Sardot type, which the NVA/VC had no difficulty cracking. Alpha-3's logs clearly show many locally invented coded transmissions transcribed verbatim and then the plain English meaning of the transmission written next to it. The seriousness of this action was magnified many times because U.S. operators were convinced their transmissions sounded great over the radio, were fully secure, and could only be understood by friendly forces. The amount of tactical advantage given to the enemy because of this false sense of security can only be imagined.

■ Captured 47th Technical Reconnaissance Battalion training material stated that U.S. units didn't change call

signs or frequencies very often, but when they did, some frequencies or other components were often retained from the previous net structure. The material went on to explain how to recover unit identity after an SOI change. An example was shown of operator chitchat where one operator told another the details of an SOI change (old call sign to new call sign, old frequency to new frequency) many hours before the actual change. In this case, 47th Technical Reconnaissance Battalion made the change faster than the U.S. unit, who had coordination problems. The 47th Technical Reconnaissance Battalion's interceptors had already been waiting for several hours on the new frequencies by the time the U.S. unit got its problems sorted out.

■ U.S. units often failed to use authentication procedures in a deception environment. This was particularly evident under a higher stress situation such as medical evacuation, search-and-rescue, quick-fire artillery targets and units in contact with the enemy. The NVA's imitative communications deception could exploit this U.S. characteristic to lure evacuation and SAR aircraft into preplanned "kill boxes," misdirect artillery fire to harmless locations or on to U.S. forces and disrupt, confuse and expose maneuvering U.S. troops. I personally saw this at work in 1969, when an unauthenticated transmission caused 69th Signal Battalion's base camp at Ben Hua to be shelled, producing produced several casualties.

■ U.S. radio operators, many of whom were field grade commissioned officers and senior NCOs, lacked proper circuit discipline. These operators were prone to long chats over the air that invariably led to the disclosure of important operational information.

■ Prior to major operations, COMSEC levels didn't increase. This led to disclosure of some useful information before almost every U.S. operation.

■ Secure communications equipment, if available, was almost never used between 1965 and 1969, since the equipment (Nestor) was bulky and the S-6 staff had problems structuring mixed COMSEC and non-COMSEC radio nets. This changed after the capture of Alpha-3, when a crash program began immediately to install COMSEC equipment in vehicles and aircraft.

Equipment bulk was not a problem on these platforms but was for manpack operations, so equipping the light infantry lagged. Unfortunately, the bulk of U.S. combat forces were light infantry.

■ Radio operators in tactical units generally failed to acknowledge radio communications' vulnerability to COMINT. After Alpha-3's capture, great pressure was brought upon the Signal Corps to improve operator training. This was done in many maneuver units, but since most equipment was "user-owned and operated," operator training was considered out of Signal's control and thus improvements were difficult, spotty and depended on the unit's S-6 and staff's quality and training. Mindsets were also very hard to change in maneuver units, where signal officers weren't particularly well regarded as communications experts, sometimes with good reason.

If these revelations weren't shocking enough, the Alpha-3 treasure trove of training documents also showed how extracted information from radio transmissions was used against specific units such as 11th Armored Cavalry Regiment, 1st Infantry Division, 25th Infantry Division, and 1st Cavalry Division.

The 47th Technical Reconnaissance Battalion actually profiled these major U.S. units based on CNR intercepts. Some typical examples of unit profiling were:

• Normal modes of transportation, down to identifying vehicle types and characteristics. The VC/ NVA, according to Alpha-3, had a healthy respect for the M-113 family of armored personnel carriers and the UH-1 helicopter. The M-151 jeep didn't particularly impress them, neither did the Stryker-like V-100 armored car U.S. military policemen used.

• Unit areas of operation. The enemy usually knew which U.S. unit was opposing them and within what areas the unit operated.

• Methods of navigation. The enemy knew which units were using landmarks to determine position and what the landmarks were.

• Unit message formats and radio procedures.

• Unit composition, weapons and capabilities.

• Radio-net traffic volume and what it meant.

Also, 47th Technical Reconnaissance

Battalion was sophisticated enough to actually analyze the tone and content of unit radio traffic and used the analysis to predict unit actions. There is considerable information that 47th knew much of this type of data before the Tet 1968 enemy offensive and used it against us extensively during that action.

After Alpha-3 was captured in 1969, a new emphasis was placed on COMSEC in U.S. combat units.

Long-dormant signal staff officers began to enforce long-disregarded COMSEC directives, such as station authentication and encryption of coordinates, due to pressure from their combat-arms commanders.

Project Touchdown

The information that Alpha-3's logs contained astounded the USARV commander, General Creighton Abrams. A surviving audio record of Abrams' reaction to this (I've personally listened to it) reveals an obviously shaken commander completely floored by proof that our enemy had been intercepting and exploiting our tactical voice radio communications on a grand scale and that there was no spy organization to be busted.

After this, Abrams' hostility to Signal Corps officers, our training, doctrine and tactics as taught and conceived at Fort Gordon – and particularly Signal officers in S-6/G-6 assignments battalion through corps – is legendary. Led by the MACV high command, the Signal Corps quickly became the target for an unmerciful attack by our combat arms brethren, who at the time needed a blood sacrifice and something to blame for why the ground war was not going particularly well.

Unfortunately, much of the attack was well deserved. The Army got so serious about placing the blame mostly on the Signal Corps that the National Security Agency – the folks responsible for producing codes, ciphers and COMSEC equipment, not the Signal Corps (whom Army headquarters assumed would lack objectivity) – was directed to produce detailed briefings, training materials and movies exposing how Army combat communications were being exploited in Vietnam. In their effort to expunge themselves from blame, top commanders declassified this information and used it to justify procuring new, less vulnerable CNR equipment (Nestor, Vinson, the Single-Channel Ground and Airborne Radio System) as well as establishing larger field COMSEC organizations controlled by G-2, not the Signal Corps. The name for this exposure effort was Project Touchdown, and the Army distributed its highly embarrassing training materials under that name for many years.

Relevance for today

Many today will ask what relevance this almost 40-year-old information is to today's Army? I say:

- Never underestimate the capabilities of your "electronic enemy." Technology needs to be applied with a good dose of common military sense today more than ever. Even a technologically unsophisticated enemy like 47th Technical Reconnaissance Battalion can find a flaw in something we do and exploit it. Command, control, communications, computers, intelligence, surveillance and reconnaissance systems are often the most vulnerable to exploitation – the Signal Corps is the heart of C4ISR, so be alert.

- The trained S-6 is key to protecting combat units from

COMINT and other forms of communications and automation exploitation. Assignment of junior, inexperienced, minimally trained officers to S-6 positions in maneuver units leads directly to defeat on the battlefield, as the Vietnam experience proved.

- COMSEC and OPSEC procedures properly applied in Vietnam would have kept many names off that famous wall in Washington. In the most glaring cases of Tet 1968 and 7th Cavalry/1st Cavalry Division at Ia Drang 1969, we'll never know how many lives could have been saved by a few well-trained signal officers aggressively doing their jobs in spite of what others may have thought. In my opinion, the number would have been considerable.

Over the years since Vietnam, the temptation to relax COMSEC and OPSEC requirements for the sake of convenience, ease of operation, cost, time, or just plain laziness continues to rear its ugly head.

While all CNRs in tactical units now have either embedded or external COMSEC devices, the temptation not to use them or not to change the COMSEC keys, for instance, has triumphed too often. The devices and proper net-operations procedures do no good if you don't use them.

Also, to satisfy their commander's perceived need for more communications, some S-6s have sanctioned the use of unprotected radio equipment to supplement organic protected CNRs.

Initially, modified amateur (ham) radios were used, followed by citizen-band radios (particularly during the CB craze of the 1970s) and, most recently, by Family Radio Service radios – which can be easily obtained, don't even require a Federal Communications Commission license and have been seen in some units, even outside the continental United States. Sometimes this equipment is disguised with names like wireless LAN, soldier intercom, brand-name brick, wireless orderwire, cellular telephone and cellular telephone walkie-talkie – and now even voice-over-Internet protocol and others.

Users invariably treat these devices as if they were secure U.S. Type I COMSEC protected CNRs. If you don't believe me, the next time you're in an operational situation, see if anyone on a cell phone is authenticating the station on the other end, using operations codes or encrypting location coordinates.

If we learned nothing else from Vietnam and Alpha-3, it's that this sort of thing gets people killed and must be stopped. Only the competent, well-trained and aggressive S-6/G-6 is able to do this, so let's get on with it!

David Fiedler, a retired Signal Corps lieutenant colonel, is an engineer and project director at the Project Manager for Tactical-Radio Communications Systems, Fort Monmouth. Past assignments include service with Army avionics, electronic warfare, combat surveillance and target-acquisition laboratories, Army Communications Systems Agency, PM for mobile-subscriber equipment, PM-SINCGARS and PM for All-Source Analysis System. He's also served as assistant PM, field-office chief and director of integration for the Joint Tactical Fusion Program, a field-operating agency of the deputy chief of staff for operations.

Fiedler has served in Army, Army Reserve and Army National Guard signal, infantry, and armor units and as a DA civilian engineer since 1971. He holds degrees in both physics and engineering and a master's degree in industrial management. He is the author of many articles in the fields of combat communications and electronic warfare.
