SIGSEC and the Army of Excellence: "Who's listening now?"

by CWO 3(P) David E. Mann

All of us are constrained by the availability of sufficient soldiers to meet our mission...These constraints are now labeled "Army of Excellence."[1]

—Maj. Gen. Sidney J. Weinstein

Signal Security (SIGSEC) has been a U.S. Army program used to insure the security of radio and telephone communications. Monitoring, education, and inspections have been both help and hindrance to commanders. Recently, the commander of the U.S. Army Intelligence Center and School directed a complete reorganization of the U.S. Army's SIGSEC operations. Ordinarily, a smooth transition from the old dogma of SIGSEC into the new counter-Signals Intelligence (COUNTER-SIGINT) concept should be taking place. Army of Excellence (AOE) constraints, however, are causing considerable turbulence.

Until 1976, all COUNTER-SIGINT support, identified at that time as Signal Security (SIGSEC) support, for the Army field elements was provided by the U.S. Army Security Agency (USASA)....The USASA SIGSEC Operations Manual provided ... guidance and procedures for conducting SIGSEC support operations, and augmented the limited ... doctrinal publications ... Reorganization under the Intelligence Organization and Stationing Study (IOSS) in 1977 dispersed the technical SIGSEC expertise.[2]

After IOSS, the Army Intelligence community quickly dispersed SIGSEC capabilities and expertise. Tables of organization and equipment (TOE) and Army readiness training evaluation program (ARTEP) documents assigned SIGSEC personnel the sole mission of monitoring unsecured radio and telephone conversations.[3] But the hasty transformation did not allow adequate time for planning. IOSS resulted in a mismatch of SIGSEC requirements and training. Confusion began about relevance of the SIGSEC product. The SIGSEC mission devolved into a narrow, parochial field working at cross purposes to the supported commander and to the already existing Operations Security (OPSEC) community.

Gradually, SIGSEC employment evolved into limited support of OPSEC functions such as telephone and radio monitoring. Another evolution resulted from what commanders erroneously thought was a "pseudo-SIGINT" capability, the attempted replication of enemy SIGINT collection forces. Commanders perceived that in a

illustration by Mike Rodgers

pseudo-SIGINT role, SIGSEC specialists could receive and analyze communications as would the hostile intelligence services.

Echelons corps and below (ECB) and echelons above corps (EAC) were assigned integrated SIGSEC support as part of Military Intelligence companies, battalions, and groups (CEWI and I&S). SIGSEC tasks were performed by the signal security specialist, MOS 05G, a low-density MOS assigned to general support OPSEC missions at division level and above. These SIGSEC tasks continue today and include regular programs of communications monitoring and COMSEC inspections, services accepted by commanders as a required ordeal—like visits from the white-gloved command maintenance inspection teams of "the old brown shoe Army."[4]

The general support SIGSEC mission:

- To monitor telephones
- To monitor radios
- To produce communications/electronics operating instructions (CEOI)
- To present classes on SIGSEC practices
- To evaluate COMSEC status
- To template friendly emitter vulnerability
- To evaluate transmitter sites
- To make advice and assistance visits
- To identify weaknesses through survey techniques
- To examine adversary military force capabilities
- To recommend corrective actions

Currently, a typical SIGSEC team organized according to IOSS and operating at ECB spends much of its time listening to and analyzing the non-secure communications of the units which make up the parent unit. Tactical unit personnel monitor and analyze radio and telephone transmissions. Inspections of cryptographic account holders and training classes on SIGSEC topics fill the rest of the duty day for most personnel holding MOS 05G.

Telephone monitoring (nicknamed CT or conventional telephone) missions use standard military equipment attached to lines at the local telephone exchange. SIGSEC specialists listen to telephone calls, transcribe conversation, and analyze the information for intelligence value. If a security violation or a compromise of sensitive information is detected, the SIGSEC unit reports to the local commander, who could then take action against the offending caller if he so chooses.

Radio telephone or RT missions are conducted much like CT missions, except that non-secure VHF FM tactical nets are the only communications monitored. Radioteleprinter, facsimile, manual morse, and data communications are not monitored, since SIGSEC personnel have neither the training nor equipment to do so. There has been no planning for or procurement of equipment capable of monitoring new generation frequency hopping tactical FM radios.

With the VINSON family of speech security devices installed and operated, transmissions made by tactical radios can be intercepted, but clear voice or data cannot be understood. Receivers must have an identically keyed piece of crypto gear to allow reception of clear text voice transmissions. Of course, the fact that radio transmissions are encrypted does not reduce the vulnerability to

radio direction finding (RDF) at all. The encrypted status of a radio signal often is a factor which in itself is an "OPSEC indicator" pointing to a higher echelon of command or a unit with a sensitive mission.

Communications users are often dangerously uninformed about the security of equipment. During one survey conducted at an Infantry division headquarters, some radio operators stated that use of the "BINTSUM" (sic) would prevent the enemy from locating them through RDF because it was secure.[5] Other radio operators had high confidence in communications security because they used cyphers which their units had developed at company and battalion level.[6] One battalion commander said that because he sent traffic by RTTY it was secure, even though the cryptographic equipment was not working.

There are very few managers who would view the results of a CT or RT mission as anything other than career threatening. Commanders at all levels are naturally intimidated by what they perceive to be an "outside agency" monitoring their radios and telephones. They are particularly unhappy when their security problems become a high visibility item at the daily staff meeting. Hindsight reveals that after IOSS SIGSEC has become a less than perfect partner to the local G2 and is now seen as the "radio police," its reports universally dreaded by commanders.[7] RT and CT missions do not produce a meaningful product or even recommendations for approval—only security violation statistics.

In January 1983, the assistant chief of staff, Intelligence, HQDA, appointed a "CI task force" to study CI problems and prioritize the actions required to resolve them. One very high priority item was revision of outdated SIGSEC concepts. Guidance was that "evolving CI ... doctrine was to be considered but [was] not to hamper development of the [SIGSEC] concept."[10]

The COUNTER-SIGINT concept is compatible with the goals and objectives of the CI concept ... [which] emphasizes the need for an analytical approach to CI support for the Army. This COUNTER-SIGINT concept restates the need for a strong analytical approach. It further redirects the primary focus of COUNTER-SIGINT efforts from the **traditional compliance inspections, surveys, and communications discrepancy monitoring** *to a focus of assisting the supported commander in maintaining combat effectiveness by helping to preserve security and retain the element of surprise.*[11]

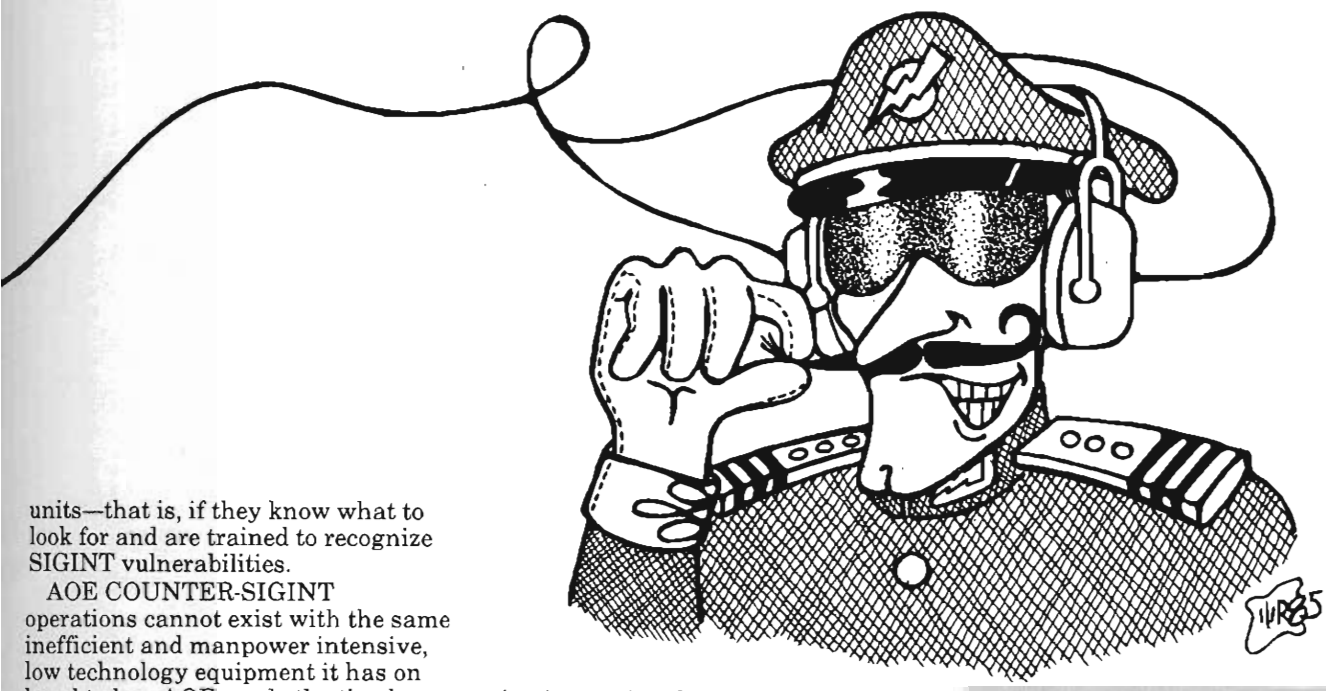
In the face of the CI task force report, the issue of SIGSEC support is still not clearly addressed in descriptions of Military Intelligence (MI) support to the AOE. There is a lack of clarity as to what functions, missions, or assets have been removed from ECB and transferred to EAC MI units. Establishment of the AOE also requires that MI undergo deep personnel and TO&E space reductions in order to trim down AOE units. Supposedly, MI functions lost at ECB will be carried out by EAC Regular and Reserve augmentation forces.[12]

AOE force reductions which MI must undergo necessitate the reduction of a function that is perceived by some to be superfluous at ECB: the COUNTER-SIGINT mission. COUNTER-SIGINT activities conducted by ECB MI battalions and companies are planned now as the "bill payer"[13] when it comes time for personnel cuts.

Plans are to provide "some" COUNTER-SIGINT support at the corps MI group level; both active and USAR mobilization units are being considered. Personnel cuts mandated by AOE MI mean COUNTER-SIGINT personnel will not be able to provide real-time support to ECB small unit commanders. However, lack of support anxieties have been somewhat quieted by assurances that "what will be provided will be better and more realistic support than before."[14]

Commanders can begin preparing today for attrition of 05G personnel by instituting an in-house training program for communicators. Unit personnel can be trained to carry out basic COUNTER-SIGINT analysis prior to and during garrison and field communications activities. Any type of in-depth analysis can be done by unit personnel assigned OPSEC duties as a "second hat." (This and any other "second hat" duties presume that the commander has enough people assigned to perform primary missions first.)

AOE COUNTER-SIGINT support planning shows evidence of a movement toward modernization of equipment and doctrine. COUNTER-SIGINT concepts have been written to remove the "gigs and violations mentality." Assuming that innovative planning will continue, new COUNTER-SIGINT operators will be able to give the supported unit an OPSEC capability which has not yet been seen. One does not need specialized equipment and people in order to conduct OPSEC; any ordinary U.S. Army unit can conduct its own COUNTER-SIGINT operations by using personnel within the unit who know its various communications systems. These soldiers *can* provide OPSEC for their own



units—that is, if they know what to look for and are trained to recognize SIGINT vulnerabilities.

AOE COUNTER-SIGINT operations cannot exist with the same inefficient and manpower intensive, low technology equipment it has on hand today. AOE needs the timely reporting of relevant COUNTER-SIGINT information. This means there has to be a *real time data flow* between COUNTER-SIGINT and G3 battle operators so that information can be given to the G3 as it develops in time for them to react. A developmental real time system was used during Reforger '81 at one ECB unit; however, it was only partially successful because of concern over conforming to the "gigs and violations" standards then existent rather than with providing information about OPSEC "fixes."[15]

COMSEC gaps can be exploited by COUNTER-SIGINT personnel just as they can by enemy analysts. MPs directing traffic of a convoy and supporting vehicle recovery teams are not usually equipped with secure radios. The actual units participating in the movement may have all of their communications secured. However, listeners need only tune to the non-secure traffic control net to recover rates of travel, quantities of vehicles, stopping points, recovery operations, and accident reports. With the introduction of extensive COMSEC protection over maneuver units, non-secure nets decrease in number, and interception is easier.

Determining the future signal vulnerability of a unit is more complex. Identification and templating of emitters used by the brigade and support units, even if secure, produce some vulnerability to hostile interception. Frequency management systems are fragmented, with no centralized data base of radio equipment. Frequency ranges, equipment densities, COMSEC status, directivity of antennas for microwave systems, and adjoining unit communications pointed toward the unit under survey are key template elements currently not examined by SIGSEC teams.

All of these important items can be obtained without relying on conventional SIGSEC RT and CT missions. In fact, collection and analysis of such information by non-MI personnel of ECB units can form the basis for a revitalized COUNTER-SIGINT effort.[16]

MOS 05G (to be redesignated as MOS 97G), Signal Security specialist, is viewed as the AOE "bill payer": by chopping the number of 05G personnel, other MI MOS strength levels can benefit. The COMSEC mission is to be moved to EAC to reduce 05G strength at ECB, thereby providing plus-ups for other MOSs. Also, some planned mission transfer to Reserve units will supposedly provide additional bodies.[17]

A request of the DCSPER, resulting from personnel issues identified in the MI functional area assessment, caused the Intelligence Center and School to host a structure review conference in September 1984; its goal was to achieve a grade feasible MI force structure considering AOE requirements, CMF restructuring, and emerging EAC architecture.[18] The results of that conference suggest significant downward adjustments in the top five grades in order to achieve an expansion of the accession base.[19]

Job concerns

Losing the mission and jobs continues as an issue among career SIGSEC personnel. Concerns are:

If Army communications become secure, is there a need for the COUNTER-SIGINT mission?

A unit with encrypted communications, using frequency hopping and spread spectrum communications technology, would appear to have a greatly lessened SIGINT vulnerability, eliminating the RT mission requirement.[8]

Telephone systems with bulk-encrypted, microwave backbones, local fiber optic cables, and analog voice to digital conversion telephone instruments would eliminate CT missions and, presumably, 05G personnel.[9]

MOS 05G personnel believe that implementation of high technology COMSEC measures will put them out of work. The emotional response has even caused some mid-level 05G personnel to request retraining in other military occupational career fields.

However, no matter how optimistic the program managers are, the U.S. Army continues to have an unsatisfactory record of fielding COMSEC equipment. (Consider the availability of modern Cyphony equipment.) Equipment density restrictions mandated by TOE and TDA, budget constraints, lack of planning when updating authorization documents, and fragmented authority probably will continue to create a lack of effective COMSEC protection for our communications.

COMSEC engineers who believe their own pronouncements have stated that voice and message traffic of the U.S. Army will be secure before the year 2000. But past performances in fielding COMSEC equipment to the Army demonstrate that monetary and bureaucratic restrictions will prevent attainment of that security goal. Thus, 05G personnel should have many years of meaningful work ahead of them even if the majority of communications go secure.