

~~TOP SECRET NOFORN~~

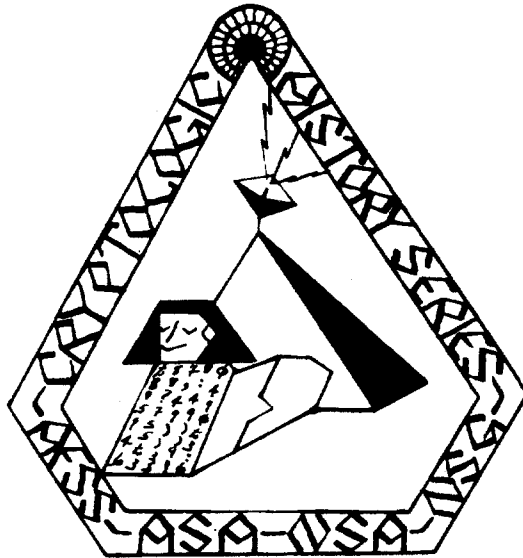
# 507

48/94

SOUTHEAST ASIA

*Working  
Against  
the Tide*

Part One



THIS DOCUMENT CONTAINS CODEWORD MATERIAL

~~TOP SECRET NOFORN~~

~~TOP SECRET UMBRA NOFORN~~

# *CRYPTOLOGIC HISTORY SERIES*

## SOUTHEAST ASIA

# Working Against the Tide

(COMSEC Monitoring and Analysis)

## PART ONE

(b) (3) - P.L. 86-36

Hiram M. Wolfe, III, ASA  
Raymond P. Schmidt, NAVSECGRU  
Thomas N. Thompson, AFSS

June 1970

~~TOP SECRET UMBRA NOFORN~~

## SECURITY NOTICE

Although the information contained in this journal ranges in security classification from *UNCLASSIFIED* to *TOP SECRET CODEWORD*, the overall security classification assigned to this issue is *TOP SECRET UMBRA*. The "No Foreign Nations" (NOFORN) caveat has been added to guard against inadvertent disclosure of portions of the text which discuss topics normally held to NOFORN channels.

While the TSCW NOFORN classification by itself requires careful handling, additional caution should be exercised with regard to the present journal and others in the series because of the comprehensive treatment and broad range of the subject matter.

## CRYPTOLOGIC HISTORY SERIES

### Southeast Asia

#### *Sponsors*

|                                   |                           |
|-----------------------------------|---------------------------|
| Vice Adm. Noel Gayler, USN        | Director, NSA             |
| Maj. Gen. Charles J. Denholm, USA | Commanding General, USASA |
| Rear Adm. Ralph E. Cook, USN      | Commander, NAVSECGRU      |
| Maj. Gen. Carl W. Stapleton, USAF | Commander, AFSS           |

#### *Joint Staff*

|                      |                |
|----------------------|----------------|
| Juanita M. Moody     | Chief          |
| William D. Gerhard   | General Editor |
| Lawton L. Sternbeck, | ASA            |
| Hiram M. Wolfe, III  | ASA            |
| Raymond P. Schmidt   | NAVSECGRU      |
| Bob W. Rush,         | AFSS           |
| Thomas N. Thompson   | AFSS           |
| Mary Ann Bacon       | Editor         |

## Foreword

Important as it is in peacetime, communications security becomes even more important in wartime. Ultimately, we must reckon wartime failure to secure communications against a background of U.S. casualties and of battles won and lost. As it did in World War II and the Korean War, the United States in Southeast Asia has failed to provide communications security of a sufficiently high degree to deny tactical advantages to the enemy. Once more the United States has lost men and materiel as a result.

*Working Against the Tide* is the story of the attempts of U.S. COMSEC monitors and analysts to bring security to the voluminous wartime communications. As the title suggests, it is not a success story. It outlines, instead, the problems confronting COMSEC specialists in dealing with communication-prone Americans at all levels of command. It gives insight into and documentation for the damage done to the United States and her allies as the enemy's SIGINT organization capitalized on American laxity in communications security. The story describes the technology applied in Southeast Asia to overcome COMSEC deficiencies and the manner in which that technology evolved during the war—particularly as monitoring adapted to a new methodology termed COMSEC surveillance. It further tells of U.S. attempts to apply monitoring knowledge in communications cover and deception operations against the enemy. The volume contains, finally, useful lessons for all who must communicate in wartime.

In addition to the present version of the COMSEC story, the joint NSA-SCA history staff is preparing a NOFORN SECRET-level, noncodeword edition. This will make possible a broad distribution of the material through normal military channels where study of the lessons learned will do the most good.

NOEL GAYLER  
Vice Admiral, U.S. Navy  
Director, NSA

## Preface

The authors of *Working Against the Tide* drew upon a wide variety of source materials in presenting their composite picture of monitoring and analysis in Southeast Asia. While the major part of these sources was for the years to 1968, the authors also used source documents from the 1968 and 1969 period when the materials were particularly germane to the topics under discussion. Important source materials included SCA monitoring reports, operational messages, reports issued by the military commands, briefings, special studies, SIGINT, and author interviews with commanders. One primary source of information was the SCA historical publications. The authors drew upon accounts provided by unit historians of components of the 509th ASA Group and the 6922d AFSS Security Wing. From these, the authors extracted sufficient information to treat in brief form the operations conducted by ASA and AFSS COMSEC units. Persons desiring information in greater detail on those operations may contact the historical offices of ASA and AFSS. Although NAVSECGRU has not published corresponding historical works, it did prepare for this publication papers that contained somewhat greater detail than that which appears in the present publication; these more detailed papers are also available for examination.

The authors have many debts to acknowledge. Within ASA, special thanks are due to Col. Julian W. Wells and Lt. Col. Robert H. Bye for advice and source materials. Maj. Andrew J. Allen, II, Mr. John Exum, Mr. Norman J. Foster, Mrs. Beverley K. Jordan, Mr. Robert C. Massey, Mr. Michael E. McIntire, and Mr. Paul R. Singleton all contributed in one way or another to the preparation of this publication. SP5 James A. Rambo and SP4 Frank K. Ayco of the historical division also made direct and valuable contributions. Within NAVSECGRU, Lt. Comdr. William E. Denton, Lt. William D. Kahl, CWO-2 Larry D. Poppe, CTCs Thomas E. Perry, CTC John O. Storti, Mr. Nicolas F. Davies, Mr. Richard J. Dennissen, and Mrs. Dorothy L. Prezis gave of their time and knowledge in preparing sections relating to NAVSECGRU COMSEC operations. At AFSS, Mr. Harry V. Hoechten, Lt. Col. Herbert R.

Morris, Jr., Mr. Glenn F. Clamp, CMsgt Melvin D. Porter, and Capt. John D. Dowdey deserve special mention for their help and comments. At NSA, Mr. Howard C. Barlow, [REDACTED]

[REDACTED] read the draft manuscript and provided comments. Finally, the authors wish to thank Mrs. Ida Ryder, who cheerfully typed the draft manuscript and countless changes many times before it reached final form.

A few source footnotes appear in text, mainly where the authors have used directly quoted material. A fully documented version of *Working Against the Tide* is available in P2, NSA. Requests for additional copies of this publication should be directed to P2, NSA.

The authors and associated members of the NSA/SCA history team assume sole responsibility for the use made of the comments and criticism offered and for any errors of fact or interpretation of the sources available to them.

May 1970

[REDACTED]  
Hiram M. Wolfe, III  
Raymond P. Schmidt  
Thomas N. Thompson

(b) (3) - P.L. 86-36

## Contents

| Chapter  | Page |
|--|------|
| <b>PART ONE</b>                                  |      |
| I. THE PROBLEM . . . . .                         | 1    |
| <i>Division of Responsibilities</i> . . . . .    | 2    |
| <i>Enemy SIGINT Threat</i> . . . . .             | 2    |
| <i>Major Problems</i> . . . . .                  | 11   |
| II. CONVENTIONAL COMSEC MONITORING . . . . .     | 19   |
| <i>Army Security Agency</i> . . . . .            | 21   |
| <i>Naval Security Group</i> . . . . .            | 54   |
| <i>Air Force Security Service</i> . . . . .      | 72   |
| <b>PART TWO</b>                                  |      |
| III. COMSEC SURVEILLANCE . . . . .               | 87   |
| <i>The Concept</i> . . . . .                     | 87   |
| <i>SILVER BAYONET</i> . . . . .                  | 90   |
| <i>Guam</i> . . . . .                            | 96   |
| <i>MARKET TIME</i> . . . . .                     | 109  |
| <i>GAME WARDEN</i> . . . . .                     | 116  |
| <i>ARC LIGHT</i> . . . . .                       | 119  |
| <i>PURPLE DRAGON</i> . . . . .                   | 128  |
| IV. COMMUNICATIONS COVER AND DECEPTION . . . . . | 139  |
| <i>Communications Cover</i> . . . . .            | 140  |
| <i>Communications Deception</i> . . . . .        | 141  |
| V. LESSONS LEARNED . . . . .                     | 155  |
| <i>COMSEC Education</i> . . . . .                | 155  |
| <i>The CC&amp;D Paradox</i> . . . . .            | 159  |
| <i>New Concepts for Old Problems</i> . . . . .   | 159  |
| <i>Full Treatment for the Patient</i> . . . . .  | 163  |
| <i>Better Systems, Better COMSEC</i> . . . . .   | 163  |
| <i>Command Emphasis</i> . . . . .                | 167  |




x

|                                 |     |
|---------------------------------|-----|
| LIST OF ABBREVIATIONS . . . . . | 169 |
| INDEX . . . . .                 | 173 |

## Maps

|  |     |
|--|-----|
| Major SCA Units Having COMSEC Missions . . . . . | 18  |
| Guam . . . . .                                   | 100 |

## Charts

|  |     |
|--|-----|
| Communications Circuits Monitored in Guam Survey . . . . .                                 | 99  |
|  . . . . . | 132 |
| . . . . .  | 133 |
| . . . . .  | 136 |

## Tables

|   |     |
|---|-----|
| COMSEC Personnel World-Wide, FY 1967 . . . . .                              | 21  |
| USASA COMSEC Resources in SEA, 1 January 1968 . . . . .                     | 28  |
| USASA COMSEC Positions in SEA, 1964-68 . . . . .                            | 31  |
| Transmissions Monitored by ASA, 1966-67 . . . . .                           | 35  |
| COMSEC Violations in the FFV II Area, November 1966-<br>June 1967 . . . . . | 39  |
| Reported Rates of Violations, 1966-67 . . . . .                             | 42  |
| Detachment 5 Mobile Operations, 1966 . . . . .                              | 76  |
| Seventh Air Force Classification of Information . . . . .                   | 81  |
| Warning Time Revealed in Teletype Transmissions . . . . .                   | 126 |

## Illustrations

|   |     |
|---|-----|
| The COMSEC Monitor at Work . . . . .                  | xii |
| Captured Enemy Communications Equipment . . . . .     | 4   |
| North Vietnamese Intercept Operator at Work . . . . . | 5   |
| Enemy SIGINT Personnel . . . . .                      | 9   |
| 404th ASA Detachment Operations Building . . . . .    | 26  |
| 404th ASA Detachment Officers' Billets . . . . .      | 27  |

(b) (1)

- (b) (3) -18 USC 798 -

(b) (3) -50 USC 403

(b) (3) -P.L. 86-36

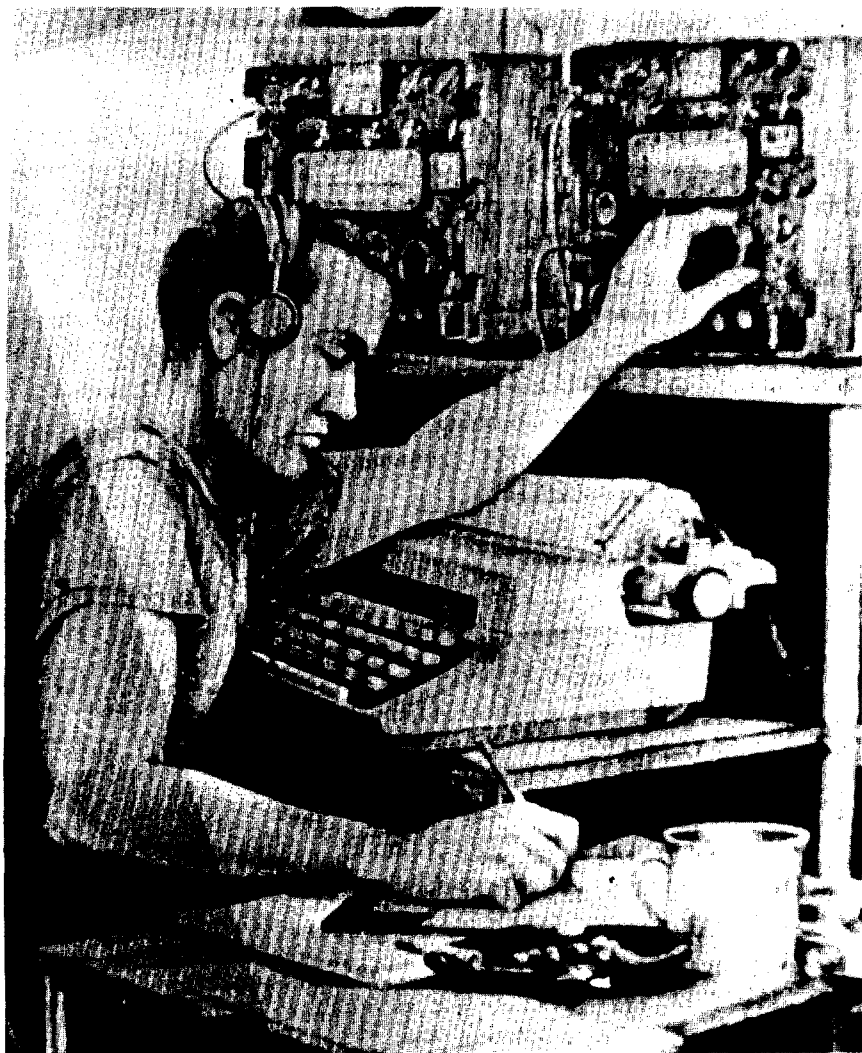
|  |     |
|--|-----|
| Conventional Radio Receivers . . . . .   | 32  |
| MRPZ-3 COMSEC Position . . . . .   | 33  |
| COMSEC Specialists of USASA Company, Saigon . . . . .  | 36  |
| Enemy Intercept of U.S. 1st Infantry Division  |     |
| Communications . . . . .   | 46  |
| Typescript of Intercept . . . . .  | 47  |
| Page From Enemy SIGINT Instruction Manual . . . . .  | 51  |
| Navy COMSEC Monitoring Position Ashore . . . . .   | 56  |
| Navy COMSEC Monitoring Position Ashore . . . . .   | 57  |
| USMC Sub Unit One COMSEC Monitor . . . . .   | 59  |
| COMSEC 705 Location . . . . .  | 60  |
| COMSEC Specialists Assembling an Antenna . . . . .   | 61  |
| <span style="border: 1px solid black; display: inline-block; width: 100px; height: 1.2em; vertical-align: middle;"></span> COMSEC Intercept Vans . . . . . | 66  |
| Operations Building . . . . .  | 67  |
| KW-26 and KW-37R, USS <i>Constellation</i> . . . . .   | 70  |
| KL-47, USS <i>Constellation</i> . . . . .  | 71  |
| Detachment 7, 6922d Security Wing, Buildings . . . . .   | 74  |
| Detachment 7, 6922d Security Wing, Positions . . . . .   | 75  |
| Detachment 5, 6922d Security Wing, Analysts at Work . . . . .  | 78  |
| Seventh Air Force KW-26 and KY-8 Equipment . . . . .   | 79  |
| The COMSEC Monitor at Work . . . . .   | 86  |
| Close Cooperation Between ASA COMSEC Personnel   |     |
| and Infantrymen . . . . .  | 89  |
| KL-7 Off-line Cryptographic Equipment . . . . .  | 92  |
| Soviet Trawler <i>Izmeritel</i> . . . . .  | 97  |
| Antenna Field, Barrigada, Guam . . . . .   | 101 |
| NSA's TEMPEST Shelter and Power Generator . . . . .  | 105 |
| COMSEC 705 Operations Area, Monkey Mountain . . . . .  | 111 |
| Jeep-mounted KY-8 Ciphony Device . . . . .   | 129 |
| BJU COMSEC Van . . . . .   | 140 |
| Truck-mounted ASA Reporting and Analysis Center . . . . .  | 143 |
| Vietnamese Communist Intercept . . . . .   | 156 |
| Typescript of Intercept . . . . .  | 157 |
| Vietnamese Communist Intercept . . . . .   | 160 |
| Typescript of Intercept . . . . .  | 161 |
| Vietnamese Communist Intercept . . . . .   | 164 |
| Typescript of Intercept . . . . .  | 165 |

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798



The COMSEC Monitor at Work (Charcoal by Specialist 5 Wayne A. Salge, a member of the ASA Combat Artists Program.)

## CHAPTER I

# The Problem

Without intelligence, one is vulnerable; without security,  
one is defenseless.

—Ancient military axiom

A nation's success in military operations often rises and falls on the basis of how well it communicates. When a nation does not secure its communications effectively, its enemies intercept and read its communications and win thereby military and diplomatic advantages.

In Southeast Asia, the United States and its Allies required electrical communications in great volume. The enemy controlled or had access to a large part of the disputed land area and could destroy or tap land lines. Therefore, radio was the most frequent vehicle for communications. If an accurate measure of the volume of these communications—those passed by the hundreds by U.S. Army, Navy, Air Force, and Allied units—were possible, that measure would suggest the sands of the sea itself. It was the responsibility of the communications security (COMSEC) community to keep the enemy from using these transmissions to the disadvantage of the United States and its Allies. The responsibility was an awesome one. The COMSEC community had to cope with an ocean tide of problems.

Providing communications security for U.S. forces in Southeast Asia entailed many diverse functions and required many cooperative actions on the part of the Armed Services and U.S. COMSEC agencies. Designing, manufacturing, and distributing cryptomaterials to satisfy U.S. needs and in some cases those of our Allies, testing U.S. communications facilities for conformity to physical and radiation standards (TEMPEST), training U.S. and Allied communicators in COMSEC practices, monitoring and analyzing U.S. communications in order to evaluate the effectiveness of COMSEC measures—these and other functions constituted the broad U.S. program to bring security to U.S. and Allied communications. As the heart of Service COMSEC activity, monitoring and analysis not only

required the greatest percentage of manpower but also provided the basis from which many COMSEC improvements stemmed.

### *Division of Responsibilities*

The Services had full responsibility for COMSEC monitoring and analysis, though NSA exerted some influence through its annual review of the Consolidated Cryptologic Program and other measures. In April 1967, Mr. Howard C. Barlow, chief of NSA's COMSEC organization, described the division of responsibilities in this manner: NSA's role was and should remain that of a *wholesaler* of COMSEC material—doctrine of use, cryptoprinciples, the operation of an integrated NSA-SCA R&D program, and production of crypto-equipment, keylists, codes, maintenance manuals, and all instructional and procedural documents that went along with the systems. The Service Cryptologic Agencies (SCA's), in contrast, were *retailers* of the cryptomaterials and had full responsibility for the security of the communications of their own Services—including monitoring and associated analytic functions. The Services also formulated their own requirements, both qualitative and quantitative, and determined for themselves the acceptability of NSA's products.

### *Enemy SIGINT Threat*

As in World War II and the Korean conflict, the U.S. and Allied communications in Southeast Asia were deficient in security, and an active enemy SIGINT organization was taking full advantage of this to acquire valuable intelligence. The purpose of U.S. COMSEC monitoring and analysis operations in Southeast Asia, simply, was to deny that advantage to the enemy by improving communications security practices. But COMSEC representatives often had difficulty convincing U.S. as well as Allied military commanders that the enemy had the ability to intercept and make tactical use of Allied communications. Unconvinced commanders did not always react positively to recommendations for COMSEC improvements.

The enemy SIGINT threat was real enough. According to the communists themselves, they collected almost all the Republic of

## THE PROBLEM

3

Vietnam Armed Forces (RVNAF) and U.S. traffic passed on selected Republic of Vietnam (RVN) traffic lanes, and they also monitored specific tactical RVN communications just before and during attacks. As early as September 1963, the Guidance Committee of the Vietnamese Communist's Central Office for South Vietnam transmitted a directive with instructions to intercept, country-wide, enemy (RVNAF) communications.

During 1964-65, the Vietnamese Communists conducted successful tactical SIGINT operations against the RVNAF. Often using U.S. equipment captured from Army of the Republic of Vietnam (ARVN) units, they intercepted RVNAF plain language communications, their most lucrative source of intelligence. They also were able to read the low-grade SLIDEX cryptosystem in which the RVNAF encrypted all or sensitive portions of many communications, as well as other low-grade systems. They gave, on the other hand, no known attention to RVN communications encrypted in the KL-7 or PYTHON (one-time tape) systems that the United States provided to South Vietnam.

The Viet Cong in this early period are not believed to have targeted English-language communications regularly. They did intercept U.S. Special Forces messages, but those collected at the time were transmitted through RVNAF communications channels. This apparent lack of SIGINT targeting of U.S. communications, it was believed, resulted from Viet Cong inexperience, lack of English linguists, and consideration of the Republic of Vietnam as the main enemy. It was even likely that they could gain all the intelligence they needed on the growing U.S. presence in Vietnam from RVNAF communications.

While the Viet Cong may have emphasized RVN communications during 1964 and 1965, the North Vietnamese were enjoying some success against U.S. Navy communications. In the very first week of regular bombing of North Vietnam, U.S. COMSEC revealed that naval communications were possibly giving flight information to the enemy. A Navy COMSEC unit intercepted a plain language transmission from the USS *Hancock* on 11 February 1965 indicating the imminent launch of aircraft and the carrier's intention of conducting recovery operations following an air strike against shore targets. The COMSEC unit immediately reported the possible compromise of this combat



Communications Equipment Captured From an Enemy SIGINT Unit. (Top, left to right: a homemade transmitter, a homemade receiver, two U.S. AN/PRC-25's, and a U.S. AN/PRC-77. Bottom, left to right: radio receiver parts, antenna parts, wire, headphone, and a CHICOM R-139 receiver with headphone.)

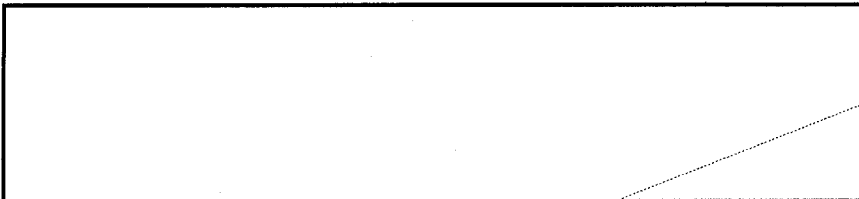
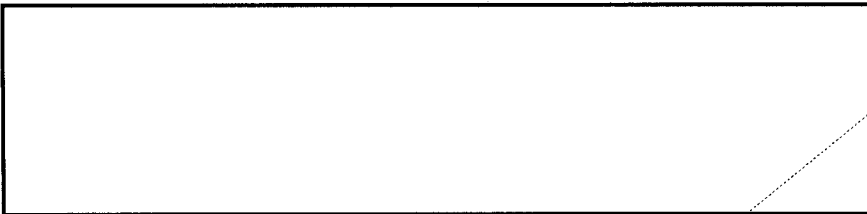
THE PROBLEM

5



North Vietnamese Intercept Operator at Work (Captured photograph)

information to the carrier strike force and to the Commander in Chief, Pacific Fleet (CINCPACFLT).

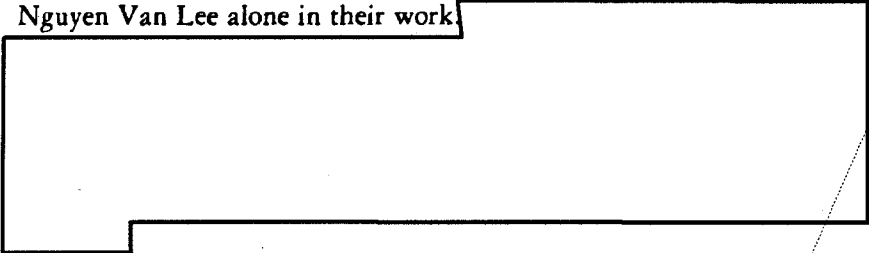


(b) (1)  
(b) (3) - P.L. 86-36  
(b) (3) - 50 USC 403  
(b) (3) - 18 USC 798



Ben Thuy directed North Vietnamese naval units to use camouflage and systematically disperse before the morning of 11 February.

In 1966 and 1967, as the dimension of the war grew and the enemy widened the scope of his SIGINT operations, he continued to rivet his attention on the plain language communications of the RVNAF and, increasingly, on those of the U.S. forces. Ralliers and defectors attested to the intelligence content and value of intercepted Vietnamese and English plain language messages. Interrogation of these men revealed that the enemy often did not have a sufficient number of English language specialists for the work at hand. One rallier, Nguyen Van Lee, who defected in 1967 after ten years with the Viet Cong, was very much impressed not only with the amount of information his unit was able to intercept but also with the accuracy of information from the North Vietnamese Central Research Directorate, which managed Vietnamese Communist SIGINT operations. He claimed that over a 10-year period his unit had never been taken by surprise. Nor were Viet Cong such as Nguyen Van Lee alone in their work.



Since the Vietnamese Communists did not differentiate SIGINT from other intelligence, it was often difficult to label examples of known enemy-obtained intelligence as being of strictly SIGINT derivation. There were, nevertheless, many cases in which SIGINT was beyond doubt the source of the intelligence.

U.S. forward air controllers (FAC's) were certain, for example, that the enemy often had prior warning of incoming U.S. aircraft flights and that the forewarnings must have come from his intercept of U.S. voice communications. This was true particularly of night operations. FAC's reported that enemy ground vehicles had been observed to move off roads and turn off their lights following U.S. air-to-air or air-to-ground-to-air voice communications. For low-flying aircraft, noise could have provided the tip-off. However, the controllers found it hard to believe that noise of their aircraft could be detected when aircraft were operating in a "loiter"

## THE PROBLEM

7

configuration. Further, FAC and strike crews working at night observed that after they discussed the geographical direction of an imminent strike, enemy defensive weapons often were oriented in the direction of the coming attack. Occasional voice spoofing by the FAC and strike force communicators confirmed the observation.

Communist foreknowledge of U.S. air strikes, including the B-52 bomber operations, also came from ARVN and U.S. ground-to-ground voice communications. Enemy SIGINT operators often intercepted ARVN warnings to pro-ARVN province chiefs of forthcoming air strikes in their areas. Of many examples showing how poor U.S. COMSEC practices limited the effectiveness of the B-52 program, the one below is perhaps typical. The Americans were discussing "heavy artillery" (B-52 strikes) in plain English over a radio one day at 0855:

1st American: You know heavy artillery warning yet?

2d American: Negative.

1st American: At coord XT 550 600 315/31 until 1130 hours.

The document recording this conversation, which gives up to two hours and thirty-five minutes advance knowledge of a B-52 strike at unenciphered geographic coordinates, is not from a U.S. monitoring report from an early period in the war, but from enemy SIGINT material captured by the 1st U.S. Infantry Division only a few months before this journal went to press.

While the enemy was exploiting to the maximum Allied plain language communications, he was not entirely ignoring encrypted messages. Captured documents showed that communications encrypted in widely used "homemade" codes and the U.S.-produced AN series operations code were under cryptanalytic study. There was no evidence, as of January 1968, that the enemy was able to exploit messages encrypted in the AN-series code. There was, for that matter, no evidence that enemy SIGINT agencies were reading any messages enciphered in cryptosystems approved by U.S. cryptologic agencies beyond the occasional solving of misused manual systems. There was considerable evidence, on the other hand, that the enemy was exploiting U.S. communications encrypted in home-grown tactical codes through cryptanalysis, and off-line systems through traffic analysis.

Besides working on U.S. communications passively for intelligence of value to his operations, the enemy's experience with these communications was such that he could imitate them when it suited his purpose. To win tactical advantage, the enemy intruded actively on U.S. nets either to deceive the U.S. operators with false information or to obtain accurate tactical information from them. These ruses often worked because U.S. operators usually failed to apply proper authentication procedures.

As valuable as tactical and strategic intelligence was, imitative communications deception (ICD) was the capstone of the enemy's SIGINT operations. Through the successful use of ICD, the enemy revealed the success of his own SIGINT operations against U.S. communications. One example involved an attack against the U.S. air base at Da Nang. After killing a U.S. base guard without being detected, the Viet Cong used the guard's unsecured telephone and, speaking English, briefly announced that the far end of the base was being attacked. No authentication was demanded. When the guards rushed off to the far end of the field, the Viet Cong attacked according to plan with little resistance. The damage to the base and its planes was estimated to be around \$15,000,000. In another instance, the Viet Cong, with good English and good communications procedures, lured heliborne troops into a trap by using designated call signs on proper frequencies and then guiding the aircraft into a properly marked landing zone—but not the right one. The deception was not recognized as such until the helicopters were fired upon during their landing approach.

At Pleiku, by tapping a field telephone circuit supporting the perimeter defenses of a large storage area, the Viet Cong on another occasion expertly imitated the Spanish accent of a guard sergeant. Stating that he was preparing hot food, the imitator asked for a count of the number of troops in each of the operating bunkers. Fortunately, this time the deception was recognized as such.

The 509th Army Security Agency (ASA) Group in Vietnam made a list of known Vietnamese Communist attempts at deception against U.S. Army units for the period 1 January 1964 through July 1967. The list gave 73 incidents of ICD, of which 23 were at least partly successful, most of them in the 1966–67 period. There were examples of misdirection of friendly air and artillery strikes, which on six occasions

## THE PROBLEM

9



Captured Photograph, Believed to Represent a SIGINT Analyst  
Passing Material to Couriers.

diverted the fire on to friendly positions. In other instances, the enemy gained advantage by giving false cease-fire orders. The United States lost at least 8 helicopters during this period as a result of the enemy's successful communications deception. In addition, the survey detailed over 100 cases of Viet Cong and North Vietnamese Army (NVA) jamming of U.S. communications. In the first four months of 1967, III Marine Amphibious Force (MAF) units experienced over 40 attempts at communications deception. These had the objective of misdirecting air strikes and artillery missions.

The incidence of enemy ICD efforts against U.S. forces, especially in I and II Corps Tactical Zones, increased several fold in 1968. For example, on 6 January 1968 in northern Tay Ninh Province there occurred what became known as the "Australian ICD Incident." It is one of the most sustained and better-documented examples during the war of an enemy attempt—fortunately unsuccessful—at imitative communications

deception. While a battalion of the 2d Brigade, U.S. 25th Infantry Division, was conducting a search and destroy mission, an intruder entered the battalion command net and for nearly ten hours was engaged in a running tactical exchange of information. The intruder, purporting to be of an Australian unit operating near the 2d Brigade battalion, declared that he wanted to establish liaison so as not to interfere with the U.S. battalion's operations. The intruder gave his position as "about 23 meters" to the north of the battalion, and stated he was from the "Australian 173d Unit" on a separated search and destroy mission.

Although the intruder's accent seemed to be Australian, although he had entered the battalion net using the battalion's call sign, and although his methods conformed to normal Allied operational transmissions procedures, his responses to challenges and authentications were evasive. Lt. Col. John M. Henschman, the U.S. battalion commander, suspected an enemy ICD ruse. The "Australian" could not be as close as 23 meters to the battalion, did not know the authentication code, and could not or would not give his exact location and direction of movement, first pleading a different set of maps from those used by Colonel Henschman's battalion, then stating that his unit was lost.

Instructing his radioman to keep the exchange with the "Australian" going, Colonel Henschman, using other communications, checked and found that there were no Australian units in Tay Ninh Province and no unit called the Australian 173d existed. He thereupon plotted several locations from which the intruder could be transmitting and called down artillery fire on the areas. Finally reflecting in his transmissions that Henschman had had a near miss, the intruder asked that the artillery cease firing on "friendly forces." A few more rounds of "friendly fire" and the "Australian" suddenly broke off and presumably left the scene. A subsequent examination of the area of the enemy's operation brought moderate contacts with Viet Cong and uncovered some empty enemy base camp installations, but no "Australian."

The result of this enemy ICD attempt was negligible. Incoming traffic that would have used the battalion command net was interrupted for about ten hours while the "Australian" was kept on the net at Colonel

## THE PROBLEM

11

Henchman's pleasure, but battalion operations continued to be directed on alternate company nets.\*

The enemy's success in posing as a valid U.S. net subscriber was in direct proportion to his intimate knowledge of U.S. communications procedures, frequencies, and the personalities of those who communicated. The only way the enemy had of acquiring such deep familiarity with U.S. communications was through his own successful SIGINT operations.

*Major Problems*

A wide variety of COMSEC problems were related to monitoring and analysis. While some affected one Service more than another, most were general in nature. There were also problems not specifically related to COMSEC but that nonetheless posed major constraints on the conduct of a monitoring and analysis program.

*The Short-Tour Dilemma*

The 1-year tour policy prevailing in Vietnam presented a major challenge to communications security. With a change in communicators every twelve months, COMSEC units each year saw their modest gains dissipate. COMSEC specialists themselves rotated in and out of Vietnam annually, and suitably trained personnel often were not available to man the positions, write the reports, and give the educational briefings. During most of the war years to the end of 1967, the Army Security Agency and Air Force Security Service (AFSS) had no field expertise for executing or even planning communications cover and deception (CC&D) projects. The MARKET TIME CC&D operation\*\* showed


\*ASA monitors recorded the complete exchange of communications in this incident, 16 pages in all. Colonel Henchman presented a special report of the episode at the Headquarters, USASA, Annual SIGSEC Work Shop, 3 December 1969. Coincidentally, ABC newsmen and TV crews were at the battalion CP at the time of the ICD, and they filmed and taped the incident, later released, in part, as an ABC 45-minute special on the Vietnam War about March 1968. Interview with Maj. Andrew J. Allen, II, SIGSEC Br., ODCSOPS, Hq USASA.

\*\*See below, pp. 144-48.

that the Navy Beach Jumpers needed additional training. The 1-year tour worked against high standards for U.S. communicators and COMSEC specialists alike.

### *Working With Allies*

Another problem with which COMSEC analysts had to deal seemed to have no real solution. Early in the war, monitoring revealed the problem of achieving operational security at the tactical level when the COMSEC of our Allies was poor.



In the early 1960's, the United States rejected several South Vietnamese requests for COMSEC support. The United States first had to decide on the extent of its involvement in Southeast Asia, what South Vietnamese and other Allied officials it could trust, and to what extent it ought to give COMSEC assistance to Allies having limited COMSEC sophistication and lax physical and personnel security practices. The United States also needed assurance that, once cryptomaterials were given to an Ally, the Americans would have full cooperation of the Ally in the secure use of those materials.

In mid-1964 the United States supplied M-209 cryptomachines to RVN and ROK forces for use at battalion level, and in January 1965 it distributed the AN-series operations code for encryption at any echelon (replacing the SLIDEX). Although RVNAF and ROK COMSEC malpractices did decrease noticeably after the South Vietnamese and Korean forces began using U.S.-produced cryptomaterials, U.S. authorities in the 1964-68 period never achieved an effective means of convincing the South Vietnamese that cryptosystems of their own design and production were insecure. The Americans could not share cryptologic techniques with the South Vietnamese as they could with a second party country such as Australia, and this limitation made U.S. COMSEC advice somewhat less convincing than it might otherwise have been. While overcoming the problems of timely and effective release of U.S. cryptomaterials to an Ally was not the responsibility of field monitoring

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798

## THE PROBLEM

13

and analysis personnel, it was their monitoring and analysis operations that most effectively documented Allied deficiencies and set the stage for that assistance.

*Vague Guidelines*

U.S. and Allied commanders varied in their use of classification procedures and employed diverse criteria in categorizing information for encryption and electrical transmission. Without specific guidance, a COMSEC analyst supporting a commander had no fixed scale on which to evaluate monitored communications. Despite the issuance from time to time of specific essential elements of friendly information (EEFI), the analyst frequently could not tell if existing regulations required secure transmission and encryption of the monitored information—usually plain language—that he had in hand. The monitor and analyst accordingly had to rely extensively upon their own judgment. Since the average communicator tended to believe that he had erred only when Service regulations prohibited his action, the monitor and analyst often found themselves without a convincing arguing point. The extent of this problem varied during the period 1964—67, but it was never resolved.

*The Preference for Plain Language Communication*

By tradition, the military depended upon communicating in plain language—especially in the voice mode—and the tradition was hard to change, especially when change normally required additional time, trouble, and expense. Thus any recommendations to secure communications met rebuff after rebuff. On many occasions COMSEC units recommended use of voice ciphony at a time when the equipment was not available in sufficient supply for issue in Vietnam. In the absence of equipment, they had to recommend manual systems, the only other encryption possibility.

In Vietnam, especially during the early years, the U.S. stocked warehouses with manual systems generally suitable for securing U.S. communications in the war zone. COMSEC monitors quickly showed that, instead of using these materials, U.S. communicators continued to pass altogether too much sensitive material in plain language. While

~~TOP SECRET UMBRA NOFORN~~

(b) (1)

(b) (3) -P.L. 86-36

(b) (3) -50 USC 403

(b) (3) -18 USC 798



COMSEC analysts on occasion achieved limited improvement, the problem remained. At times, COMSEC analysts singled out unprotected lanes over which unusual volumes of sensitive information passed in plain language and recommended allocation of crypto-equipment to stem the flow. At other times, COMSEC analysts tried to attain reasonable security along with continued use of plain language communications by creating an awareness of what was and what was not sensitive information. Unfortunately, there was no blotter large enough to dry up sensitive, exploitable plain language communications in Vietnam.

### *The Amateur Cryptographer*

Many a U.S. serviceman became an amateur cryptographer, producing his own codes designed to serve a particular need. His intention was not to obtain personal privacy in communication but to achieve easy-to-use systems for his unit's communications. In working with the easy-to-use homemade codes, communicators avoided the more complex and time-consuming cryptographic procedures sometimes inherent in approved systems. Not realizing that their systems afforded at best only marginal security, the communicators regularly encrypted sensitive information in them. Commanders failed to prevent the use of the unapproved cryptographic systems over their communications links, and COMSEC specialists often were unable to persuade commanders to discontinue their use.

SCA specialists demonstrated over and over the cryptanalytic vulnerability of the home-grown variety of cryptographic systems, but to little avail—their continued appearance on the scene has constituted one of the major COMSEC headaches of the war. Even as late as the spring of 1969, the U.S. Air attache in Laos, who was coordinating semicovert U.S. air and other operations in that country, was sending most of his messages in a code he had made up for himself. Air Force Security Service COMSEC analysts monitoring the attache's transmissions found that they could completely reconstruct his code within 8 to 10 hours after each change. Since the attache changed codes only every five weeks, most of his messages were susceptible to immediate enemy SIGINT exploitation. The appearance and reappearance of codes of this type demanded constant COMSEC alertness.

## THE PROBLEM

15

*Lack of Command Emphasis*

A commander's attitude toward COMSEC obviously had its effect upon the COMSEC status of his unit. Not all commanders placed the emphasis on COMSEC required to deny advantages to the enemy. Col. Tom M. Nicholson, Signal Officer, 1st Cavalry Division (Air Mobile), from September 1965 to January 1966, having a good understanding of COMSEC matters, elaborated on some of the attitudes and problems then confronting a U.S. commander:

With regard to COMSEC, it was not good in Vietnam. But, until we can resolve the problem of sufficient frequencies and multiple allocations for tactical units, we won't be able to do much toward the basis of COMSEC application. If there were enough frequencies, with alternates allocated to various commands, then we might be able to change frequencies. Until this is possible it is useless, from a COMSEC viewpoint, to change SOI-SSI and call-signs without changing frequencies. In Vietnam, there were not enough available . . . ; therefore, the frequencies never changed, the call-signs were not practicably changeable, and the first basic principle of COMSEC was defeated. Further, any attempt to preserve the loss of OB information through COMSEC applications in any foreign area in which USF operates, where part of the people are hostile or unsympathetically motivated, would be an exercise in futility.

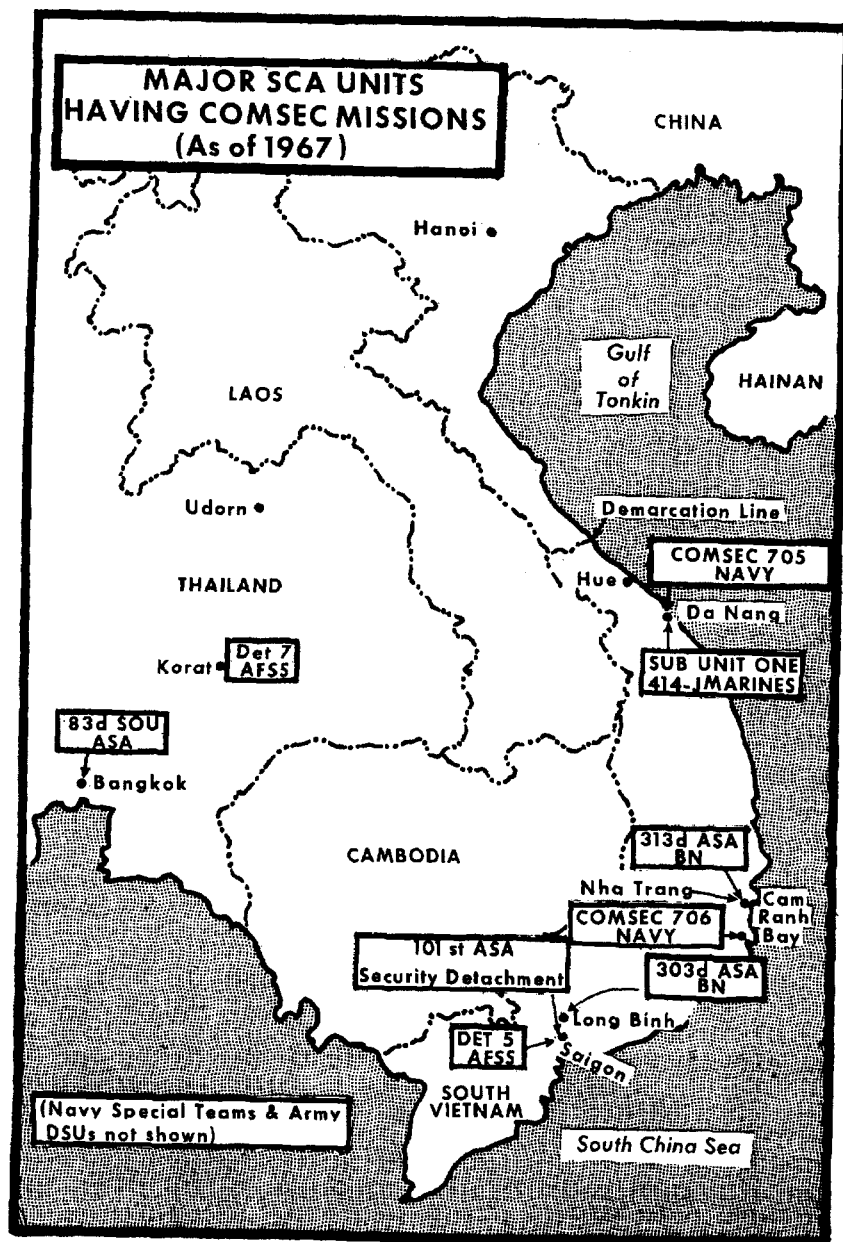
The extent of communications usage and reliance in SVN, with multinetts—for example, MEDIVAC and troop transport helicopter companies operating within hourly time-frames, hundreds of miles apart, in support of many international units they did not even know, for which they could not possibly carry or use all the SOI's involved—compelled the use of non-changing call-signs. For example, we changed all call-signs in the 1st Cavalry Division where there were many air/ground, artillery, transport, logistic, administrative and command nets involved. The resulting confusion hampered our operations. We ordered a change back to the known call-signs to regain operational effectiveness. Further COMSEC problems were derived from the aviators of air support elements where rapid reaction operational capability was a necessity. For example, a GI could get MEDIVAC immediately in certain areas in SVN by calling "DUSTOFF" on a frequency known by all. We couldn't afford to change that, for the soldier-officer-user could not, in emergency, keep up with or look up a new frequency and call-sign when the choppers were needed. It is possible that "DUSTOFF" was monitored by the enemy; however, its use saved many lives.

To a great extent, however, clear voice was employed with a reasonable degree of security consciousness or awareness. Voice communications were used primarily by officer-communicators from platoon to division levels. They had an awareness of the probability of enemy intercept and, generally, spoke in the clear only within an operational time-frame—a few hours or that day—from which the enemy could not gain sufficient information to react against our speed and mobility. When discussing forthcoming operations or events of the future more than 24 hours away, they used secure means, courier, or codes. All of our primary operational communications were passed on KW-7-secured (LLTT-RATT) circuits from battalion to FFV levels, and between Operations Centers at superior, subordinate or lateral battalions, brigades and divisions. Thus, for the more important traffic, we had good security. I know of no instances where COMSEC weaknesses contributed to enemy exploitation of USF, or changes of USF operations/plans.\*

COMSEC monitors and analysts had an advisory role only and no power themselves to effect changes. For a variety of reasons commanders frequently ignored, or read sympathetically without action, the findings of the COMSEC units. When the commanders did not appreciate the significance of COMSEC—and many of them had not learned of the importance of COMSEC in tactical operations before being assigned to Vietnam—they did not adequately support monitoring and analysis operations. A forceful Intelligence or Signal staff officer fully sold on communications security could partially compensate when the commander failed to be involved personally, but barring the presence of a COMSEC-oriented staff officer, disinterest on the part of the commander could obviously have only an unfavorable effect on the COMSEC status of his command and an adverse psychological effect upon the monitors. Under these circumstances, attempts to introduce sound COMSEC practices seemed a thankless task.

---

\*Interviews conducted by H. M. Wolfe, III, 1967-68, with various officers who had held commands in Vietnam. Hereafter cited as Wolfe, Interviews. This and later quotations are used simply to reflect prevailing attitudes of the period and should in no way be taken as criticism of those concerned.



## CHAPTER II

### Conventional COMSEC Monitoring

In conventional COMSEC operations the monitor places himself in the role of the enemy. Selectively, he intercepts the communications of his own Service and then reports on the intelligence he has—and the enemy could have—gleaned from them. When all goes well—when the U.S. command takes the action implicit in or recommended by the monitor's report—the monitor has earned his keep.

Maj. Jerry L. Brown, COMSEC officer at the ASA Field Station, Phu Bai [redacted] during the first part of 1968 recalled one instance when a compromise was reported in time to perhaps save the life of the Deputy Chief, Military Assistance Command, Vietnam, Lt. Gen. Creighton W. Abrams.

During the formation of MACV FWD, Gen. Abrams made a helicopter trip from Saigon to Hue-Phu Bai. The details of the flight, including time, altitude, route and passengers, were transmitted in the clear on an RTP link. Our COMSEC monitors picked it up and reported it immediately. As a result, the flight plan was changed. However, an accompanying craft was not notified of the change, and it was shot at the whole way from Saigon to Phu Bai—an unusual effort by the VC, who did not usually shoot at helicopters on such flights. This I believe was a certain example of enemy SIGINT use.\*

Here several important aspects of a successful monitoring operation come into play. Having only limited coverage of U.S. communications (2 percent to 6 percent at best), the monitor had heard and recognized a COMSEC violation, reported it without delay, and realized success when the U.S. command changed General Abrams' flight plan. Dramatically, the command's failure to warn the accompanying aircraft led to a demonstration of the enemy's use of SIGINT.

---

\*Wolfe, Interviews.

(b) (1)

(b) (3) -P.L. 86-36

(b) (3) -50 USC 403

(b) (3) -18 USC 798

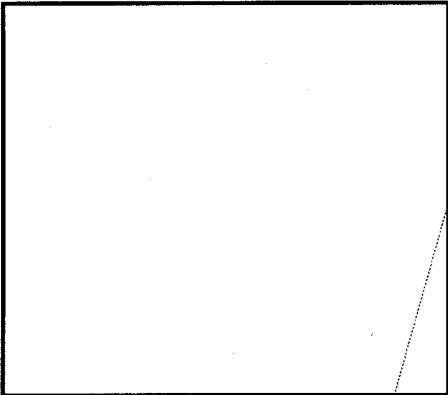
As early as 1959, questions arose concerning the communications security status of the U.S. Military Assistance Advisory Group's (MAAG) communications nets in South Vietnam. During an annual inspection of the MAAG cryptocenter at Saigon in 1960, the ASA Pacific inspecting officer discussed COMSEC with the Signal Officer, MAAG Vietnam. Later, at the prompting of his Signal officer, the Chief, MAAG Vietnam, Maj. Gen. Charles J. Timmes, asked ASA Pacific to send a COMSEC monitoring team to South Vietnam to sample MAAG communications. Late in 1960 a 6-man team arrived on TDY from Okinawa. The team's monitoring revealed that there was practically no application of COMSEC within South Vietnam on the uncovered U.S.-RVN radio nets operated in support of MAAG. The team learned that some advisors had not once used their one-time encryption pads during their entire tour. In other instances where the pads were used, the volume of "unclassified" clear-text transmissions was sufficient to provide much usable intelligence to a hostile SIGINT organization. Investigation revealed that no SCA had been tasked to provide COMSEC assistance in Southeast Asia. The monitoring team then reported its findings to General Timmes and the Chief of USASAPAC, Col. Robert T. Walker. To improve the situation, Colonel Walker issued crypto-equipment to MAAG teams, stressed the use of one-time pads, recommended the encrypted for transmission only (EFTO) policy, and established control for continuing call sign and frequency assignments in Vietnam.

In the early 1960's, each SCA developed in Southeast Asia a COMSEC organization scaled to the need for monitoring the communications of its own Service, the Army Security Agency in addition guarding for the joint communications of MAAG and MACV. Responsibility for COMSEC at the COMUSMACV level rested at first in the J-6 staff, and in mid-1965 shifted to the J-2 staff section, which in 1967 added a position for a COMSEC officer (MOS 9630). While SCA specialists often had other COMSEC functions to perform, by and large monitors and analysts predominated in the Southeast Asian as well as world-wide COMSEC organization. (See table, p. 21.)

CONVENTIONAL COMSEC MONITORING

21

COMSEC Personnel World-Wide  
(FY 1967)

|                              | <i>Army</i>   |          | <i>Navy</i> |          | <i>Air Force</i> |          |
|------------------------------|---|----------|-------------|----------|------------------|----------|
|                              | <i>Pers</i>   | <i>%</i> | <i>Pers</i> | <i>%</i> | <i>Pers</i>      | <i>%</i> |
| Monitoring                   |  |          |             |          |                  |          |
| Analysis and transcribing    |   |          |             |          |                  |          |
| Doctrine (Hq)                |   |          |             |          |                  |          |
| Technical guidance           |   |          |             |          |                  |          |
| CC&D                         |   |          |             |          |                  |          |
| ELSEC                        |   |          |             |          |                  |          |
| Maintenance                  |   |          |             |          |                  |          |
| Administration and logistics |   |          |             |          |                  |          |
| Total personnel              |   |          |             |          |                  |          |

*Army Security Agency*

*Organization*

Of the Service Cryptologic Agencies, ASA developed the largest and most complex COMSEC organization in Vietnam, over the years evolving from one stage to another, each more complex than the last, as U.S. troop levels increased. After the 1960 TDY visit of the ASA COMSEC team to Vietnam, the 400th USASA Special Operations Unit (SOU) (Provisional) (covername, 3d Radio Research Unit) was the first ASA organization assigned SIGINT functions in South Vietnam. Arriving in May 1961 and at first staffed with only  the 400th SOU in the early days of its existence had no formal COMSEC section but did perform COMSEC operations in the Saigon area, monitoring telephone circuits on the RVNAF-MAAG switchboard and recommending COMSEC improvements to the MAAG Vietnam J-6 staff. It also had responsibility for the security of CRITICOMM circuits in Southeast Asia. In September 1961 the ASA unit was redesignated the 82d Special Operations Unit.

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

On 12 October 1961 six enlisted COMSEC specialists from the 104th USASA Security Detachment on Okinawa arrived in Saigon on TDY. After a short stay in the MAAG headquarters compound, the men moved into 82d SOU facilities at Tan Son Nhut Air Base. With three positions that they brought with them, the men monitored the telephone, radiotelephone, teletype, and manual Morse communications of MAAG Vietnam. The men formed the nucleus for the 82d SOU's COMSEC section. Headquarters, USASA, formalized the 82d's COMSEC mission by an operations plan in December 1961 under which the commanding officer of the 82d SOU assumed responsibility for the full scope of COMSEC support to both the Chief, MAAG Vietnam, and the Republic of Vietnam Armed Forces.

With this modest beginning, the 82d SOU's COMSEC section gradually expanded its monitoring of MAAG and MACV military communications. By the summer of 1962, the section had monitored approximately 60,000 radiotelephone and teletype messages and reported numerous transmission security (TRANSEC) violations and dangerous practices to MACV. After the introduction into Vietnam of the POLLUX off-line cryptosystem for general use by U.S. military units in the spring of 1962, it began the task of examining encrypted communications and reporting on practices found dangerous to security.

Soon, the COMSEC section of necessity began operations with mobile equipment to cover the widely dispersed communications of U.S. advisory personnel. The first mobile operation, in November 1961 by a 2-man team with a TPHZ-3 position, monitored the ARVN I Corps MAAG Advisory Team I (Da Nang) communications. In later months, similar operations supported other advisory teams at other locations. By the end of 1962, COMUSMACV had levied further requirements on the 82d SOU to provide COMSEC coverage of the JUSMAAG in Thailand.

Activation on 1 March 1963 of the 101st USASA Security Detachment (SD) (covername, 7th Radio Research Unit) represented a second stage in the developing ASA COMSEC organization in Southeast Asia. Assigned to the 82d SOU and having a strength of [REDACTED]

[REDACTED] the 101st was organized initially into three sections—headquarters, security monitoring, and control and analysis. The 101st exercised technical control over all U.S. Army COMSEC operations in Southeast Asia until about mid-1966, when the arriving ASA battalions

(b) (1)

(b) (3) -50 USC 403

(b) (3) -18 USC 798

(b) (3) -P.L. 86-36



## CONVENTIONAL COMSEC MONITORING

23

assumed control of the tactical COMSEC functions of the ASA direct support units (DSU's). Headquarters of the 101st SD was at the site of the Joint General Staff Compound (Camp Tran Hung Dao, Saigon). Functioning as a subordinate of the 82d SOU and assuming all COMSEC functions of the latter's COMSEC section, the 101st Security Detachment coped with an expanding mission that by then included COMSEC responsibility for MACV, MACTHAI, and the Joint U.S. Military Assistance Advisory Group in Thailand, as well as advisory and training support to the RVN Army.

With the establishment of the 101st Security Detachment, ASA also expanded its mobile operations. By the end of 1963, as many as [ ] mobile teams were operating in such locations as Da Nang, My Tho, Ban Me Thuot, Nha Trang, Can Tho, Pleiku, Qui Nhon, and Kontum. Dispersal of the teams to the various combat tactical zones (CTZ's) permitted the COMSEC specialists to cover, on a recurring basis, the communications passed by ARVN corps MAAG advisor teams and by users of the MACV country-wide wire, teletype, and radio circuits.

Many problems attended the deployment of the mobile units. Road transportation was difficult even when armed convoys were not necessary. Air travel was hard to schedule. Although mobile monitoring team operations represented a major portion of the 101st SD's COMSEC operations during fiscal year 1965, the various problems in fielding the teams caused a loss of much effective monitoring time. By July 1964 the 101st SD strength stood at [ ] officers and men, and more equipment became available. Later, teams established "permanent" detachments in each CTZ, reducing the need for short-term mobile operations. MACV generally provided air transport, albeit at low priority, to move teams to bases near their monitoring locations.

In 1965 tasks assigned the 101st Security Detachment nearly exceeded its capabilities, despite the long hours the men of the unit worked. At that time the 101st was supporting MACV and four major commands with communications complexes serving division-sized units in addition to nearly 30 other switchboards. By mid-1965 at least [ ] more men were assigned and another [ ] came on TDY from the 104th Security Detachment, Okinawa, to help satisfy the growing requirements. In this manner, the 101st Security Detachment was gradually acquiring both additional specialists and more equipment to cope with an expanding

(b) (1)

(b) (3) -50 USC 403

(b) (3) -18 USC 798

(b) (3) -P.L. 86-36

mission. By early summer of 1966 manpower and positions were double [redacted] those of 1963.

*509th ASA Group* In view of the burgeoning commitment of U.S. Army forces to Vietnam, USASA undertook a major upgrading of its organization in Vietnam in mid-1966. It discontinued the 82d SOU and organized the 509th ASA Group, a level of ASA organization needed to support a field army. The 509th Group had COMINT, ELINT, ELSEC,\* and electronic warfare (EW) as well as COMSEC functions. The group-level of organization called for a strength of [redacted]

[redacted] COMSEC spaces with tasks directed toward minimizing order of battle information divulged; determining the approximate amount of intelligence information available to the enemy through insecure communications practices and procedures; determining communications security violations that might compromise planned operations, thereby permitting the enemy to take counteraction; making recommendations to help evaluate and remedy deficiencies in communications security; assessing the physical security status of cryptographic facilities and distribution points; and developing communications data to support manipulative communications deception operations.

Components of the 509th working on the expanding COMSEC requirements were the 101st Security Detachment and the COMSEC elements of the 303d and 313th ASA Battalions and their direct support units.

*101st Security Detachment* Headquarters, 101st Security Detachment, and the 1st Platoon were with the 509th Group at Tan Son Nhut. The 101st headquarters operational personnel were divided into the 509th Group COMSEC Section and the 101st SD Operations Section with two advisors attached to J-2 MACV. The 101st controlled 14 to 18 COMSEC positions.

The 2d Platoon was colocated with the 330th ASA Operations Company (330th RRC) near Pleiku. The 3d Platoon was near the headquarters of the 303d ASA Battalion (Corps) at Long Binh. The 4th

\*Army uses the expression Signal Security (SIGSEC) to include COMSEC and electronic security (ELSEC), the security of noncommunications signals.

(b) (1)

(b) (3) -50 USC 403

(b) (3) -18 USC 798

(b) (3) -P.L. 86-36

## CONVENTIONAL COMSEC MONITORING

25

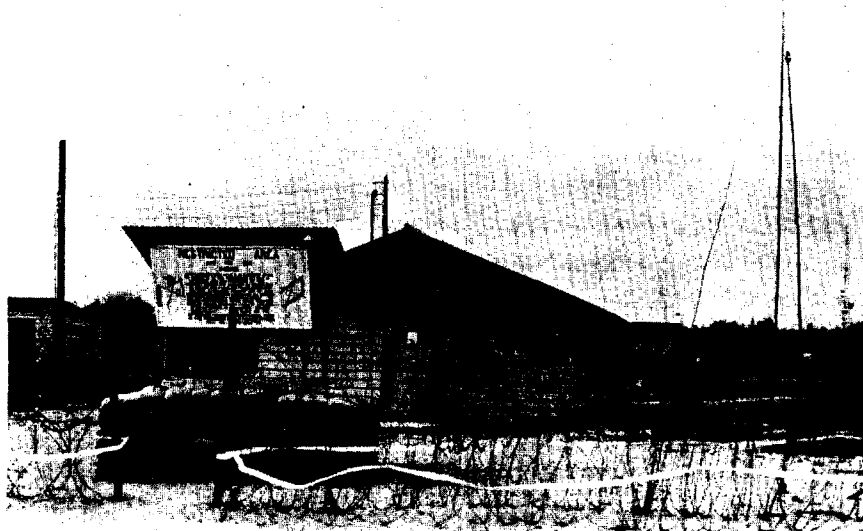
Platoon was in Can Tho. Detachment 1 of the 101st SD worked in the MACTHAI-JUSMAAG compound in Bangkok, Thailand, and an *ad hoc* Capital Monitoring Team of two positions and six men, formed by direction of MACV, covered switchboards in the Saigon-Cholon headquarters complex.

The 101st had responsibility for all aspects of COMSEC for MACV, including monitoring and analysis; review of all locally generated cryptosignal publications; inspection and approval of all cryptofacilities; COMSEC briefings, lectures, training, and command visits; investigation of cryptosecurity violations and deficiencies; passive ELSEC support; and specialized training for and assistance to the RVNAF on the U.S. cryptosystems loaned to them.

*313th and 303d ASA Battalions and the Direct Support Units* ASA organization provided for the attachment of direct support units to Army tactical commands for direct SIGINT and COMSEC support to the unit commanders. COMSEC specialists comprised 10 to 20 percent of the DSU strength, though frequently ASA commanders, under pressure to provide more SIGINT coverage, temporarily had to divert COMSEC specialists to SIGINT tasks.

ASA DSU's began arriving in Southeast Asia during the latter half of 1965, either with or shortly after the tactical units to which they were attached. From 4 DSU's operating in 1965, the number expanded to 16 by 1968. The 101st Security Detachment (on 15 December 1967 redesignated the USASA Company, Saigon) directed and helped the DSU's in their work with Field Force Vietnam (FFV) headquarters and the divisions and brigades that they supported. The DSU's issued monitoring reports both to the supported commands and to higher ASA and command authorities.

In February 1966 the 313th ASA Battalion (13th RRU), with about 60 percent of its authorized strength, began COMSEC support to Headquarters, I Field Force Vietnam (FFV I). It established liaison channels within FFV I and began coordinating the work of its subordinate DSU's at the division and brigade level, gradually relieving the 101st Security Detachment of this responsibility. The 313th also concentrated on FFV I headquarters telephone switchboards and radio circuits. After May 1966, the 303d ASA Battalion (17th RRU) began parallel COMSEC support to Headquarters, FFV II at Long Binh. The

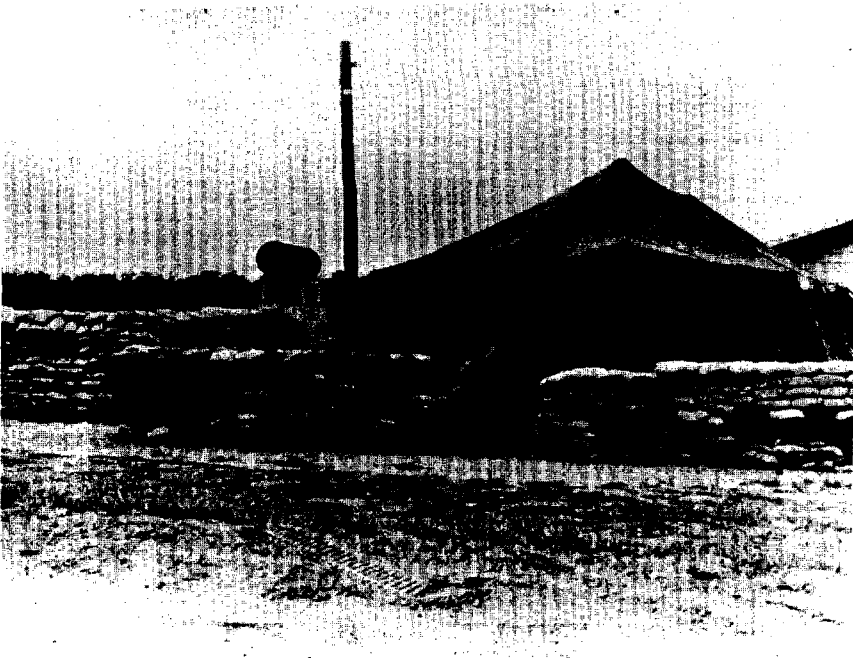


404th ASA Detachment (Airborne) Operations Building, Bien Hoa, 1967

headquarters companies of the 303d and 313th ASA Battalions each had authorization for a Security Platoon (SIGSEC) of [ ] [ ] men and operated from [ ] positions, in addition to performing a wider scope of COMSEC analysis and advisory functions.

Subordinated to the 303d and 313th Battalions were the DSU companies and detachments. The companies gave COMSEC support to division commands, usually had an officer and about [ ] men for COMSEC functions, and operated from [ ] positions. The DSU detachments and platoons gave COMSEC assistance at brigade and battalion levels. Generally, platoons had about [ ] COMSEC specialists [ ]. As an exception, heavy separate detachments served the Armored Cavalry regiment and mechanized brigades. Each heavy separate detachment had a COMSEC officer, [ ].

In fiscal year 1967 large-scale COMSEC operations in support of field commanders took place for the first time since the 1950's in Korea. The 303d and 313th ASA Battalions were operating with 12 DSU's by April



404th ASA Detachment (Airborne) Officers' Billets, Bien Hoa, 1967

1967. In June of that year, authorized COMSEC spaces in the 509th Group totaled [ ] by October 1967 the total had increased to [ ] of which about [ ] were present. The COMSEC element of the 509th, reaching full strength in 1968, was the largest organization of its type ever to support a U.S. field army.

### *Operations*

ASA's COMSEC units, particularly COMSEC elements of the direct support units, usually operated in or near the command posts of the forces they supported. Close association of the COMSEC unit with the military commander and his staff, usually the G-2 or S-2 and the Signal officer, had, of course, many advantages. Not the least among them, it kept the military commander apprised of the COMSEC status of communications under his control, facilitated procedural changes urged by the COMSEC

~~TOP SECRET UMBRA NOFORN~~

(b) (1)

(b) (3) -50 USC 403

(b) (3) -18 USC 798

(b) (3) -P.L. 86-36

## USASA COMSEC Resources in SEA, 1 January 1968

| <i>Unit Designation<sup>a</sup></i>     | <i>Unit Cover Name<sup>a</sup></i> | <i>Arrived SEA</i> | <i>Supported Command</i>      |
|---|------------------------------------|--------------------|-------------------------------|
| USASA Company, Saigon<br>(101st SD)     | 101st RRC (7th RRU)                | Mar 63             | COMUSMACV & USARV             |
| 313th ASA Bn (Corps)                    | 313th RR Bn (13th RRU)             | Apr 66             | I FFV                         |
| 371st ASA Co (AM Div)                   | 371st RRC (10th RRU)               | Sep 65             | 1st Air Cav Div               |
| 374th ASA Co (Inf Div)                  | 374th RRC (Det; 14th RRU)          | Aug 66             | 4th Inf Div                   |
| 404th ASA Det (Abn)                     | 404th RRD (Det 1, 3d RRU)          | Jun 65             | 173d Abn Bde (Sep)            |
| 406th ASA Det (Abn)                     | 406th RRD (Det 3, 3d RRU)          | Jul 65             | 1st Bde, 101st Abn Div        |
| 408th ASA Det (Inf Bde)                 | Americal DSC (Prov)<br>408th RRD   | Aug 66             | Americal Div<br>196th Inf Bde |
| 415th ASA Det (Inf Bde)                 | 415th RR Det                       | Dec 67             | 11th Inf Bde (Sep)            |
| 601st ASA Det (Inf Bde)                 | 601st RR Det                       | Oct 67             | 198th Inf Bde (Sep)           |
| 303d ASA Bn (Corps)                     | 303d RR Bn (17th RRU)              | May 66             | II FFV                        |
| 265th ASA Co (Abn Div)                  | 265th RRC                          | Dec 67             | 101st Abn Inf Div             |
| 335th Div Support Co (Inf)              | 335th RRC                          | Jan 67             | 9th Inf Div                   |
| 337th ASA Co (Inf Div)                  | 337th RRC (11th RRU)               | Aug 65             | 1st Inf Div                   |
| 372d ASA Co (Inf Div)                   | 372d RRC (16th RRU)                | Jan 66             | 25th Inf Div                  |
| 409th ASA Det (Armd)                    | 409th RR Det                       | Sep 66             | 11th Arm Cav Regt             |
| 856th ASA Det (Inf Bde)                 | 856th RR Det                       | Dec 66             | 199th Inf Bde (Sep)           |
| ASA Field Station, Bangkok<br>(83d SOU) | U.S. Field Station, Bangkok        | Sep 59             | COMUSMACTHAI                  |

<sup>a</sup> Earlier names shown parenthetically.<sup>b</sup> Actual strength; authorized strength in parentheses.<sup>c</sup> All officer personnel and 6 enlisted men of 101st SD were COMSEC surveillance specialists.<sup>d</sup> Positions and personnel from ASA Company, Saigon; the Bangkok field station's authorizations for COMSEC was never filled.

specialists, and permitted immediate command reaction to any major compromises reported. Further, the continual person-to-person relationship was indispensable in promoting COMSEC awareness and personnel and unit education and training.

Platoons of the 101st Security Detachment dispatched COMSEC teams to cover COMUSMACV and ARVN advisors' communications,

CONVENTIONAL COMSEC MONITORING

29

-Continued

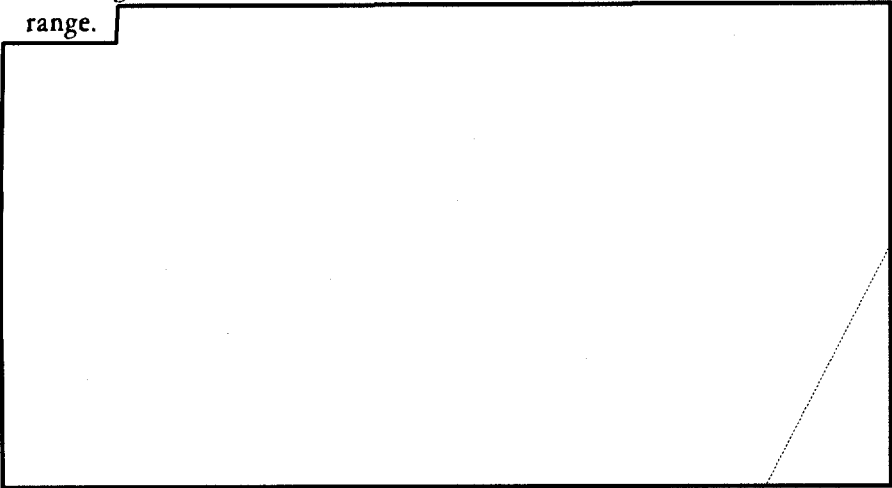
*Total COMSEC Personnel<sup>b</sup>*

| <i>Base<br/>Location</i> | <i>COMSEC</i>    |                             |           |                 |  | <i>Analysts</i> |
|--------------------------|------------------|-----------------------------|-----------|-----------------|--|-----------------|
|                          | <i>Positions</i> | <i>Officers<sup>c</sup></i> | <i>EM</i> | <i>Monitors</i> |  |                 |
| Saigon<br>(Tan Son Nhut) |                  |                             |           |                 |  |                 |
| Nha Trang                |                  |                             |           |                 |  |                 |
| An Khe                   |                  |                             |           |                 |  |                 |
| Pleiku                   |                  |                             |           |                 |  |                 |
| Phu Hiep                 |                  |                             |           |                 |  |                 |
| Phan Rang                |                  |                             |           |                 |  |                 |
|                          |                  |                             |           |                 |  |                 |
| Chu Lai                  |                  |                             |           |                 |  |                 |
| Chu Lai                  |                  |                             |           |                 |  |                 |
| Chu Lai                  |                  |                             |           |                 |  |                 |
| Long Binh                |                  |                             |           |                 |  |                 |
| Bien Hoa                 |                  |                             |           |                 |  |                 |
| Bear Cat                 |                  |                             |           |                 |  |                 |
| Lai Khe                  |                  |                             |           |                 |  |                 |
| Cu Chi                   |                  |                             |           |                 |  |                 |
| Xuan Loc                 |                  |                             |           |                 |  |                 |
| Cat Lai                  |                  |                             |           |                 |  |                 |
| Bangkok                  |                  |                             |           |                 |  |                 |
| Totals                   |                  |                             |           |                 |  |                 |

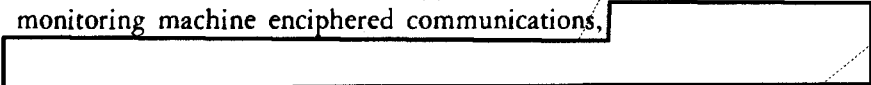
often deploying them from their platoon bases for extended periods of time. A team of the 2d Platoon, Pleiku, for example, was in Nha Trang in January 1967, in Da Lat in February, in Phan Thiet in March, and at Cam Ranh Bay in April, without returning to the base camp. Although the platoon base sites normally had access to ASA CRITICOMM circuits, communications with detached teams often were delayed.

(b) (1)  
(b) (3) -18 USC 798  
(b) (3) -50 USC 403  
(b) (3) -P.L. 86-36

*Collection* Although ASA monitors used many types of equipment, there were four basic types of positions: MRPZ-3, MJRZ-3, TPHZ-3, and MRQZ-3.\* With this equipment, the monitors could copy MM, radiotelephone, radioteletype, multichannel, conventional telephone, FM single sideband, and other communications in the .5-2,000 MHz range.



*Coverage* ASA specialists spot-monitored encrypted communications to check cryptographic systems and transmission practices for conformity to prescribed procedures. Although machine-enciphered communications (KW-7, KW-26, KY-8 ciphony family, and so forth) did not receive cryptanalytic or traffic analytic attention, COMSEC specialists through liaison with cryptocenters were able to demonstrate cryptonetting vulnerabilities. Brought to the attention of appropriate authorities, this resulted in recurrent major cryptonet realignments. Rather than monitoring machine enciphered communications,



\*MRPZ-3 is a 3/4-ton, truck-mounted, manual Morse and radiotelephone position, covering frequencies .5-100 MHz; MJRZ-3 is a 3/4-ton, truck-mounted, multichannel monitor position capable of covering 12 channels—4 channels simultaneously—in frequencies 30-2,000 MHz; TPHZ-3 is a 3/4-ton, truck-mounted, conventional telephone monitor position, with a 30-line capacity, recording one line at a time; and MRQZ-3 is a 3/4-ton, truck-mounted, manual Morse and radiotelephone FM single sideband, air-to-ground communications monitor position, operating in frequencies .5-400 MHz.

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798



CONVENTIONAL COMSEC MONITORING

31

USASA COMSEC Positions in SEA, FY 1964-68

*Unit\**

USASA Security Co, Saigon

USASA FS Bangkok

404th ASA Det

405th ASA Det

303d ASA Bn, HHC

313th ASA Bn, HHC

337th ASA Co

371st ASA Co

372d ASA Co

403d ASA SOD

406th ASA Det

335th ASA Co

374th ASA Co

408th ASA Det

409th ASA Det

856th ASA Det

265th ASA Det

415th ASA Det

601st ASA Det

Totals

<sup>a</sup> Only units of 509th ASA Group with COMSEC elements listed. List does not reflect subordination, but is generally chronological. Where units have had several designations, the latest designation is used.

<sup>b</sup> Does not reflect the withdrawal of COMSEC positions from DSU's later in CY 68, as realigned under the COMSEC surveillance concept.

<sup>c</sup> Read figures as "Authorized/Actual (Employed)." Actual varied with availability and mission requirements during annual periods.

<sup>d</sup> Inactivated in FY 1966.

<sup>e</sup> Reactivated in support of a different unit in FY 1968.

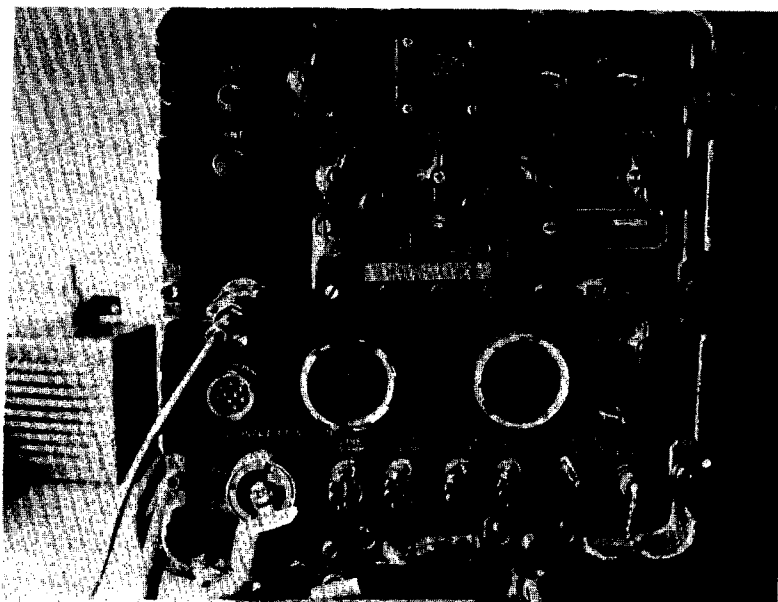
<sup>f</sup> Eliminated in 1967.

(b) (1)

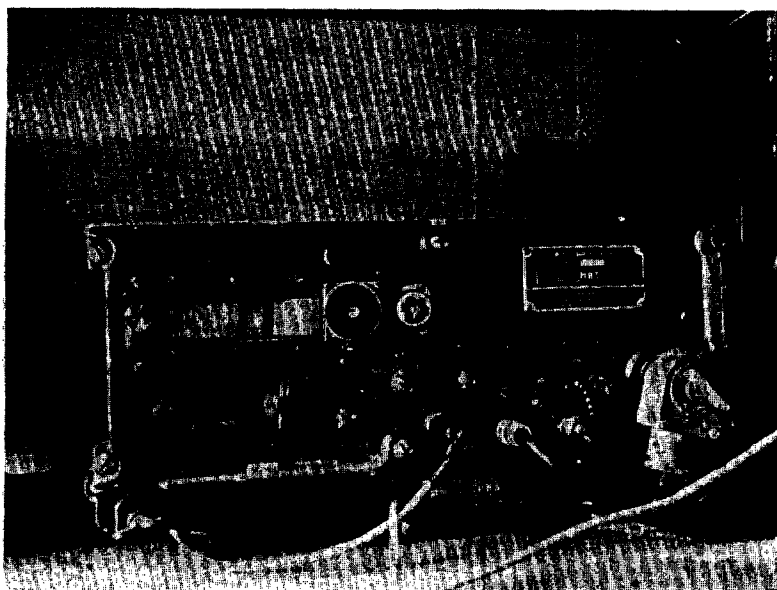
(b) (3) -50 USC 403

(b) (3) -18 USC 798

(b) (3) -P.L. 86-36



Conventional Radio Receivers (R-392 above, R-744 below)  
used with four basic Army equipment configurations.



CONVENTIONAL COMSEC MONITORING

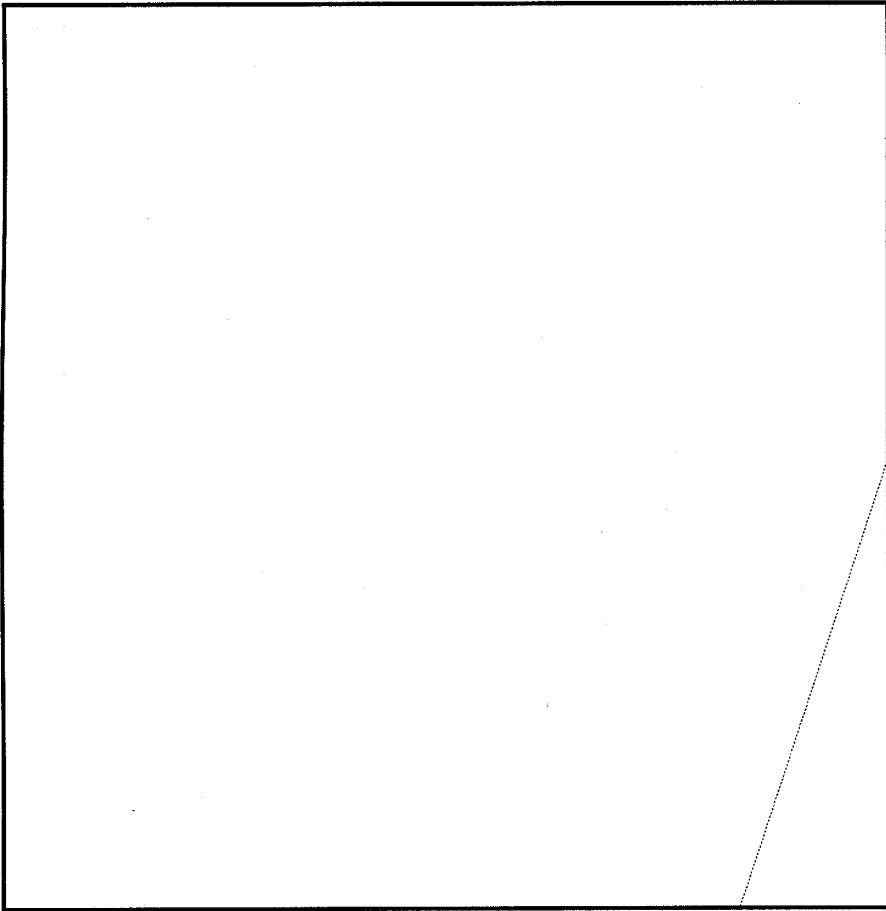
33



MRPZ-3 COMSEC Position at Diep Hoa, with sandbagged shelter at right and generator trailer at left. Such positions are connected with field analysis centers.

ASA COMSEC elements routinely monitored single-channel, non-multiplexed radio (AM and FM), radiotelephone and landline (wire) telephone, and multiplexed telephone and radiotelephone transmissions. They monitored wire communications by patch-in at communications terminals, single-channel radio communications by radio reception methods, and multiplexed communications by both methods.

- (b) (1)
- (b) (3) -P.L. 86-36
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798

*Against the Tide*

The direct support units gave an account of COMSEC weaknesses and status in written reports and in briefings to commanders and their staffs. If a specific commander's communications compromised a planned operation, ASA personnel were at hand to convey the necessary warning. Face-to-face presentation of the evidence, even replaying monitored tapes, at times was not only the quickest but also the most effective means to convey the warning. While commanders did not always heed the warnings, most of them, when convinced, appreciated the support.

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798

## CONVENTIONAL COMSEC MONITORING

35

## Transmissions Monitored by ASA

|                        | 1966             | 1967             |
|------------------------|------------------|------------------|
| Radio telephone        | 1,430,059        | 6,606,539        |
| Conventional telephone | 228,605          | 559,214          |
| Radio teletype         | 6,404            | 17,810           |
| Totals                 | <u>1,665,068</u> | <u>7,183,563</u> |

Lt. Col. Grail L. Brookshire, S-2 of the 11th Armored Cavalry from September 1966 through June 1967, recalled one instance in which his regiment revised its plans when monitoring showed that transmitting over insecure communications, an attached ARVN unit had given the time and place of the attack.

The commander of the 303d ASA Battalion from April 1967 to April 1968, Lt. Col. Norman J. Campbell, reported an incident when a COMSEC warning went unheeded. While discussing operational matters with a subordinate unit over a VHF-linked desk phone at Headquarters, 1st Infantry Division, one of the staff officers remarked—aside, but audibly enough for the COMSEC monitor to hear—that a specific operation was to take place in a location “35 kilometers north of here tomorrow.” Although this likely compromise was brought to the staff officer’s attention, the plans were not changed since the landing zone and the area were suitable for the operation. On landing, the assault force met unexpectedly heavy resistance; U.S. losses were approximately 58 men killed and 82 wounded. Colonel Campbell regarded the outcome as the results of an enemy reaction to a security breach.

Other incidents continued to reinforce the knowledge that, given a chance, the enemy would use U.S. communications to plan his tactical moves. For example, a heliborne senior commander contacted a ground patrol and, on FM in the clear, ordered a rendezvous at a specific crossroad location. Thirty minutes after the patrol arrived there, it was hit by Viet Cong, who had not been known previously to be in that area. While the encounter may have been a coincidence, Lt. Col. Richard B. Blauvelt of the 303d ASA Battalion, which covered the incident in support of Field Forces Vietnam II, stated that the “COMSEC breach possibly caused /those/ U.S. casualties.” He told of many similar



USASA Company, Saigon, COMSEC Specialists analyzing, transcribing, and reporting on U.S. communications, Tan Son Nhut.

instances happening shortly after detected COMSEC violations, not all of which could have been tactical coincidence, [REDACTED]

[REDACTED] PWI of VC captured in the DELTA area, . . . indicated that the VC usually were tipped-off from 3-4 days in advance of any operation, [REDACTED]

*Reporting* While direct channels were open to disclose compromises endangering U.S. tactical operations, COMSEC specialists also used various types of reports to convey the COMSEC lesson to the military commands they served. At the direct support unit level, analysts at first prepared draft reports and forwarded them to higher authority for

\*Wolfe, Interviews.

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798

## CONVENTIONAL COMSEC MONITORING

37

publication, but after March 1967, as did other echelons of ASA's COMSEC organization, the DSU's issued their own publications.

In contrast to lower echelon DSU's, the battalions served as major control points for field analysis of monitored communications and for preparation of individual and summarized field COMSEC reports based on items from subordinate units. The battalions forwarded their reports, in turn, to the 101st Security Detachment, which reported to MACV and others.

ASA specialists classified COMSEC malpractices, using two basic kinds of reports: the Transmission Security Violation Report (TSVR) for actual security violations, and the Practice Dangerous to Security Report (PDSR) for a broader category of procedural violations that might lead to enemy exploitation. These they issued as "spot reports" or periodically as required at successive command levels. A third report form, the Transmission Security Analysis Report (TSAR), was published on an aperiodic basis, usually on completion of a task period, mission, or operation.

At the end of each month, the ASA Company, Saigon (and its predecessor) consolidated all monitoring reports of its subelements into the special Transmission Security Summary Report (TSSR) for J-2 MACV. The 303d and 313th ASA Battalions sent their reports to the Field Forces Vietnam and each quarter consolidated all analysis and reports into a quarterly summation for COMUSMACV. The quarterly report was especially useful at other levels of command and provided input to the Headquarters, USASA, annual report to the Department of the Army. ASA personnel did not assess intelligence losses. They reported only the information of possible intelligence value to the enemy that they had observed in monitoring. "The primary mission of COMSEC monitoring is to evaluate the effectiveness of measures taken to maintain and improve COMSEC and to identify or define security weaknesses or malpractices."\*

The reporting system produced literally thousands of examples of deficiencies. In 1965-68 the instances noted in these many warnings to

---

\*CGUSASA Msg to DIRNSA, IAOPS-E (M) 7132835, sub: Status of COMSEC Surveillance Activities (U) AGI Nr. 35364 DTG 122210Z May 67, CONFIDENTIAL.

the commands, and the thousands more that undoubtedly were undetected, represented a veritable flood of intelligence for enemy SIGINT exploitation and tactical application, a flood that spelled defeat or losses during many U.S. combat operations.

In that flood are examples from the period before large-scale U.S. commitment to Vietnam began, from the later periods, and from all levels of the U.S. military command. Like the perennial Asian flu, poor COMSEC practices affected without discrimination all echelons; like the flu, it also attacked every wave of Americans arriving in Vietnam.

In 1964 a 101st Security Detachment mobile team monitored MAAG Advisory Team 75. It also monitored the ARVN 7th Division operations and intelligence (O&I) net, the BLUEBIRD Advisor Group switchboard, and the FM air-to-ground net used by the advisory team. Team specialists identified nine COMSEC violations. COMSEC reports outlined the violations and noted the intelligence compromised. Monitoring revealed in this case the location of an artillery battery, expected time of attack by friendly aircraft 30 minutes before the strike, the imminence and objectives of an air reconnaissance mission, the expected time of arrival of Chief MAAG in the My Tho area and the mode of travel to be used by him and his party, the compromise of the grid coordinate encryption system contained in the MAAG-ARVN 7th Division standing operating instructions, and the disclosure of operating frequencies and call signs. The monitors recommended increased use of the encrypted for transmission only policy, better COMSEC education for BLUEBIRD switchboard users, use of the grid coordinate encryption system, employment of prescribed authentication procedures, and reduction of unnecessary chatter during transmissions.

Compromise of tactical information occurred at every echelon, even at the highest levels. In late summer of 1965, ASA monitors, for example, recorded a conversation that passed over an unsecured conventional telephone line between Saigon and Da Nang and revealed information on troop movements of value to the enemy. The offenders were a general and a colonel. (See illustration, p. 40.) ASA monitors prepared a TSVR on the violation just as they would have for compromises occurring at lower echelons. (See illustration, p. 41.) Correlating information showed that other communications had also compromised the operation. About ninety minutes before the conversation between the general and the



## CONVENTIONAL COMSEC MONITORING

39

COMSEC Violations in the FFV II Area, November 1966-June 1967

| <i>Category</i>   | <i>Number</i> |
|---|---------------|
| Use of unauthorized codes                               | 312           |
| Linkage of call signs to frequency or unit              | 32            |
| Compromises of authorized codes                         | 21            |
| Types of disclosures of classified information          |               |
| Unit locations and coordinates in clear                 | 104           |
| Communications and general matters                      | 120           |
| Reports (ops, intel, after-action, etc.)                | 73            |
| Plans and operations (OPLANS, OPREPS, objectives, etc.) | 71            |
| Movements (units, convoys, equipment, etc.)             | 51            |
| Results of enemy action                                 | 20            |
| Personnel matters and unit strengths                    | 17            |
| VIP itineraries   | 16            |
| Logistical information and critical shortages           | 11            |
| Unit capabilities                                       | 7             |
| Unit identifications                                    | 2             |
| Experimental equipment                                  | 1             |
| Cryptoviolations  | 1             |

Number of transmissions monitored:

Radio telephone 1,847,852

Conventional telephone 182,418

colonel, monitors had recorded a conversation between a J-3 MACV representative and another colonel. This too had disclosed information on classified movements and plans for the same military operation and was the subject of a separate violation report.

The earlier conversation revealed that the 173d Airborne Brigade had been alerted to move as reserve in support of RVNAF forces engaging a regiment of the NVA 320th Division. While the specific coordinates of the planned move were not revealed, the enemy would have been able to determine the approximate location since he knew where his own unit was fighting. What remedial action, if any, resulted from the two monitoring reports cannot be ascertained from available records.

*Management Data* As did the other SCA's, ASA specialists worked hard to get at the basic causes of the thousands of compromises they detected in monitoring. COMSEC specialists needed more than an isolated incident here and there to convince some military commanders that they had a problem. Accordingly, the specialists studied violations

Enclosure (Monitored Telephone Conversation)

J-3 SPECIALIST . . .

COLONEL / . . ./ PLEASE.

ONE MOMENT SIR.

COLONEL . . .

GO AHEAD SIR.

HELLO.

THIS IS GENERAL / . . ./

THIS IS / . . ./ SIR.

YEH.

I'M CALLING WITH RESPECT TO THE SITUATION IN 2 CORPS.

YES.

GENERAL THROCKMORTON HAS ORDERED AH BUTCH TO MOVE A.S.A.P. NOW THIS WAS BASED ON SEVERAL CONSIDERATIONS. IT WAS THE STRONG RECOMMENDATION OF COLONEL MATAXIS, IT WAS A STRONG RECOMMENDATION OF GENERAL TONG, WAS BASED ON A GOOD TENTATIVE IDENTIFICATION OF A NEW PAVN UNIT IN THE AREA.

I SEE.

AND IT WAS BASED ON A FACT THAT ARVN ALREADY HAS SIX GENERAL RESERVE BATTALIONS COMMITTED UP THERE . . . .

YES.

SO GENERAL DEPUY RECOMMENDED THIS COURSE OF ACTION . . . .

OKAY.

TO GENERAL THROCKMORTON AND THEY WILL MOVE WITH TWO BATTALIONS AS SOON AS POSSIBLE AND A DECISION ON THE THIRD TO BE MADE LATER ON AS THE SITUATION DEVELOPES.

YES.

AND THEIR MISSION WILL BE TO CONDUCT OPERATIONS WEST OF PLEIKU IN SUPPORT OF THE CG OF 2 CORPS.

WELL AH I THINK, WELL I THINK YOU'VE TOLD ME AH ENOUGH IF NOT TOO MUCH.

RIGHT.

AH WHAT IS THE GENERAL SITUATION UP THERE NOW, ARE THEY STILL IN CONTACT?

YES SIR, AH, THEY'VE HAD ABOUT A HUNDRED AND FIFTY CASUALTIES! THIS IS THE LAST WORD WE RECEIVED.

I SEE, ARE THEY GETTING PLENTY OF AIRSTRIKES THERE?

SIR?

ARE THEY GETTING PLENTY OF AIRSTRIKES?

AH THE WEATHER RIGHT NOW IS BAD, SO THEY'RE JUST NOT GETTING MUCH.

CONVENTIONAL COMSEC MONITORING

41

YES.

GENERAL DEPUY IS ON HIS WAY UP THERE AND GENERAL TONG IS ON HIS WAY UP THERE AND THEY WILL MEET AND THEY'LL PROBABLY BE SOME MORE FALL OUT OF IT AS SOON AS THEY GET UP THERE.

RIGHT, WHAT ABOUT VC AH CASUALTIES?

AH WE HAVE NO WORD ON THAT.

/END OF CONVERSATION/

IAPVCS

SUBJECT: Transmission Security Violation Report (U)

TO: Commander

US Military Assistance Command, Vietnam

ATTN: MACJ2, CI & S Branch

APO US Forces 96243

1. (C) The following violation was committed by a member of your command at the time and date indicated below. This report is submitted for your information and any action deemed necessary.

- a. Monitored Circuit: Trunk Circuit between DaNang and Saigon.
- b. Parties Involved: General . . . and Colonel . . . .
- c. Time and Date of Violation: 1036H - 1038H, 10 August 1965.
- d. Type of Transmission: Conventional Telephone Conversation.
- e. Type of Violation: Disclosure of Classified Movements and Plans.
- f. Violation of: APPENDIX III, AR 380-5.
- g. Monitored Conversation: See Inclosure.

2. (C) The information disclosed in this conversation can be linked with the information disclosed during the conversation monitored between 0905H and 0908H, 10 August which was previously reported. The information disclosed indicates that the 173d Airborne Brigade will deploy to Pleiku and will operate as a reserve to RVNAF Forces engaged with a Regiment of the 320th PAVN Division west of Pleiku.

FOR THE COMMANDER:

1 Incl

as

JAMES J. SINGSANK

Captain, AGC

Adjutant

| Year | Reported Rates of Violations<br>(Per 1,000 transmissions) |     |                |                  |     |     |                  |     |         |                              |
|------|---|-----|----------------|------------------|-----|-----|------------------|-----|---------|------------------------------|
|      | R/T   |     | Conv Telephone |                  |     |     | RTTY             |     | Average |                              |
|      | Nr. <sup>a</sup>  | TSV | PDS            | Nr. <sup>a</sup> | TSV | PDS | Nr. <sup>a</sup> | TSV | PDS     | Violation Rates<br>Per 1,000 |
| 1965 | —   |     |                |                  |     |     |                  |     |         | 2.93 <sup>b</sup>            |
| 1966 | 1,430   | .7  | .8             | 229              | 14. | .5  | 6                | 5.5 | 4.9     | 3.3                          |
| 1967 | 6,607   | .3  | .2             | 559              | 1.9 | 1.1 | 18               | .7  | .7      | .65                          |

<sup>a</sup> Expressed in thousands.

<sup>b</sup> Average violation rate (incompletely reported) for the last half of 1965.

NB. Above figures based on total monitoring, which reflected less than 6 percent of the total communications passed. These statistics are not a valid indicator of COMSEC status, but provide only an indication of likely trends and averages.

and classified them by type. They then were able to give the commanders involved information in depth with respect to the COMSEC status of their units so that the commanders would have at hand management data on which to take corrective actions.

ASA analysts had specific guidelines for identifying violations—AR 380-5 among them—and from such guidelines classified the violations. The table on page 39, for example, shows the number of violations so classified for FFV II transmissions between November 1966 and June 1967. From this, it is easy to see that use of unauthorized codes was a major problem.

In another study ASA specialists, also working within FFV II, reviewed 18,000 conventional telephone and 285,000 RTP transmissions for the first six months of 1967. From these they identified 83 transmission security violations and 35 practices dangerous to security. The percentage rates of violations against total transmissions monitored ranged from a low of .053 in February to a high of 1.57 in April. ASA was able to evaluate this violation rate as "fairly good," based on its larger framework of experience.

Any comparison of violations for different periods of time always, of course, involves certain limitations. Nevertheless, ASA did find it instructive to show observed rates of violations—transmission security violations (TSV) and practices dangerous to security (PDS)—per 1,000 transmissions in the several communications modes ASA monitors

## CONVENTIONAL COMSEC MONITORING

43

emphasized. The table on page 42 gives the results of the ASA quarterly monitoring summary reports for all communications monitored in Vietnam during 1966-67. Over-all rates of violations showed a significant and welcome drop between 1966 and 1967. At this time a violation rate above 2 violations per 10,000 transmissions (.2 per 1,000) was considered excessive.

*An Example of Cause and Effect* In 1967 COMSEC analysts did a year-long study of the 25th Division's voice radio communications, correlated COMSEC actions with the COMSEC status of the division, and showed that communications could be made secure in relation to the cryptomaterials' availability, quality, and employment, and to command emphasis. The study showed that the violation rate per 10,000 voice radio transmissions was: January, 1.6; February, not reported; March, 2.1; April, 1.5; May, .5; June .4; July 9.8; August, 22.3; September, 8.0; October, 3.4; November, 1.4; and December, 1.3.

The drop in April-June period corresponded to the issuance of the KAC-P/Q, NSA-produced operations codes, which were an improvement over those previously used. When the new codes were issued, ASA conducted classes in their use, and subsequent monitoring showed that the communicators were at first using them for encoding communications. However, the division communicators complained that the system was too complicated, and monitoring in June-August revealed that homemade codes—SHACKLE, point-of-origin, and an unnamed code, all of which offered little resistance to cryptanalysis—were once again being used.

COMSEC analysts alerted the 25th Division's commanding general, Maj. Gen. F. K. Mearns, to the significant rise in communications security malpractices. General Mearns informed the DSU and his staff that he would personally review all transmission security violations and that disciplinary action would be in order for offenders. This positive command emphasis had immediate results—in September the rate of violations declined. During the decline, monitoring showed an increased use of the KAC-P/Q codes and a reduction in the use of unauthorized codes. A contributing factor to this decline was the publication and distribution, throughout the division, of a J-6 MACV pamphlet

~~TOP SECRET UMBRA NOFORN~~

(b) (1)

(b) (3) -P.L. 86-36

(b) (3) -50 USC 403

(b) (3) -18 USC 798

[ ] findings. In October, the division began to use KY-8 ciphony equipment, and this too improved security. In November and December, monitoring revealed extensive use of the KAC-P/Q codes and increasing use of the KY-8.

While no record of violation rates for the 25th Division's conventional telephone conversations are available for 1967, a graph of them would appear almost identical to that of monitored radiotelephone and FM communications. A physical inspection of the telephone lines in October of that year revealed, incidentally, evidence of unauthorized wiretapping. Following that revelation, use of the telephone dropped to a very low rate and almost no violations came to the attention of monitors. For the benefit of the 25th Division, ASA listed the most frequent violations: the use of unauthorized codes; disclosure of locations in the clear; disclosure of future plans for operations (not found after October); and the most frequent practice dangerous to security, complete failure to authenticate combined with extremely long, rambling, conventional telephone conversations and lengthy radiotelephone transmissions.

The monitoring during 1967 reflected the communications of a very active division—the 25th was involved in ten major operations. The microwave and troposcatter systems serving the division (over which much tactical clear text was transmitted) included 50-kilowatt transmitters whose main beam extended 640 miles, with side lobes of 410 miles and a back lobe of 300 miles. Thus, the Pleiku-Da Nang pattern extended into mainland China, while transmissions from 1, 10, and 50-kilowatt transmitters at other sites could be heard in Laos, Cambodia, North Vietnam, and other hostile areas.

There were from time to time concerted actions to demonstrate the need for COMSEC safeguards against a particular source of COMSEC weakness. For example, to correct the ever-present COMSEC problem of securing call signs General Denholm, CGUSASA, directed that the fixed suffix, one-callword principle be field tested in Vietnam so that ASA could evaluate its worth. In the experiment, the 25th Division used a periodically changing suffix call word, the 1st Cavalry Division (Airmobile) used a similar fixed suffix call word but without periodic change, and the 1st Infantry Division employed a periodically changing net call word with a periodically changing suffix call word. Within three

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798

## CONVENTIONAL COMSEC MONITORING

45

23 July 1966

IAPV77

SUBJECT: Callword Study (U)

4. (C) RECOMMENDATIONS: The following recommendations are based on the conclusion of this study that no reliance should be placed on radical callword allocation systems as a means to prevent interception, analysis, or intrusion of friendly radio voice communications. Adherence to standard, historical solutions to callsign security are the best means to impede the actual initial net reconstruction and subsequent derivation of order-of-battle from detailed traffic analysis—regardless of the callword allocation systems employed.

- a. Assign callwords and expanders to nets and within nets in a random manner.
- b. Change callwords and expanders within tactical commands as frequently as operational conditions permit, daily if possible, at the start of each new operation as a minimum.
- c. Change callwords simultaneously with each change of frequency.
- d. Maintain uniformity of appearance of callwords and expanders within major tactical commands by using authorized callword allocations and manners of callword expansion.
- e. Insure that callwords are not compromised by use in conjunction with superseded calls, telephone switching designators, aircraft tail numbers, or with corresponding plain-text unit designations.

FREDERICK B. LOTHROP

Captain, AIS

Commanding

days, ASA analysts reconstructed the nets of all three divisions. Despite the popularity enjoyed by the one-callword principle, ASA analysts warned against its use. The 101st Security Detachment report on the results of the experiment (see above) went to J-2 MACV, G-2 and SIGO USARV, and the 303d and 313th ASA Battalions.

One of the most serious COMSEC weaknesses was the ever-present homemade code. The point-of-origin code, used to hide true map coordinates, was one of the continual offenders. In many cases ASA COMSEC analysts, to persuade commanders that such codes were indeed insecure, broke them, often in less than 30 minutes, using only monitored operational traffic. In one instance, when ASA COMSEC analysts broke a division's complete point-of-origin code from normal traffic in less than





## CONVENTIONAL COMSEC MONITORING

47

| <u>TIME OF INTERCEPT</u> | <u>U.S. COMMUNICATORS</u> |                    | <u>DATE</u>   | <u>VOICE NET</u><br>D2/2<br>2 |
|--------------------------|---------------------------|--------------------|---|-------------------------------|
| 0745                     | Stroy 91                  | Stroy A66          | You have new CH+<br>+Affirmative+<br>We found 2 mines at 665320 and 664322+<br>My 26 element return my location about 02 minutes+<br>Pres my location is from ATN (U1.1 L1.2) +<br>Inbound your location, eta 10 minutes, your 66 available?+<br>+Roger, my 66 is standing by+<br>My lead element move into operation+<br>Pres my location is from ARM (Lo.5 D1.9) ((585341))<br>CV is at CPT 35+<br>Pres my location is from ARM (R1.0 D1.1) ((590349)) now moving to N+<br>Pres my location is from ARM (R1.1 on line) ((591360))+<br>My 16, 46 element location is from ATN (L2.0 U0.3) ((620323)) my 36 element is moving to N+ |                               |
| 0850                     | C66                       | 80                 |   |                               |
| 0848                     | C80                       | 80                 |   |                               |
|                          | A66                       | "                  |   |                               |
| 0920                     | Expoider 77F              | "                  |   |                               |
| 0930                     | Stroy A66                 | "                  |   |                               |
| 0955                     | B66                       | "                  |   |                               |
| 1000                     | B66                       | "                  |   |                               |
| 1015                     | B66                       | "                  |   |                               |
|                          | C66                       | "                  |   |                               |
|                          |                           |                    |   | D2/28<br>2                    |
| 1135                     | Sluch 11<br>Fire 53       | Fire 3<br>Sluch 11 | We have mission for you, give me location+<br>At coord XT 517367, having appo 100VC in the area+<br>+You have friendly near area+<br>We have friendly at 3 clicks to the E area+<br>+The area is west or east side Blue+<br>That area is at western side of Blue+<br>My 16 element sp at this time+<br>My 16 and Fire B80 is at location from COUTINE (R1.0 U1.0) ((590360)) also my 26 and 36 is at Fire 94 location+<br>Give me pres your location+<br>+Pres my location is from CPT DARLEY (R2.0 U0.5)+<br>You give me your friendly location+<br>+Wait+   |                               |
| 1215                     | Stroy B29                 | Fire 3             |   |                               |
| 1300                     | Stroy B96                 | "                  |   |                               |
|                          | Fire 3                    | Fire B94           |   |                               |
| 1405                     | Sluch 17                  | Fire 3             |   |                               |
|                          |                           |                    |   | D2/28<br>5                    |
|                          | Stroy B96                 | Fire 3             | Coordinate I gave you 597351+<br>You pass smoke location your site+<br>Pres location 500 for last site now moving to Tenixi for Fire D extraction+<br>We will put A/S at 575399, you have friendly near area+<br>+At 1 half KM NW area+<br>Contact on the ground+<br>+Fire D94<br>Pres my location is from CPT COUTINE (R1.6 U0.3) ((896333))<br>Fire of hold and moving shortly+   |                               |
|                          | "                         | Bandit 41          |   |                               |
| 1400                     | Sluch 15                  | Fire 3             |   |                               |
|                          |                           |                    |   |                               |
| 1405                     | Stroy B96                 | "                  |   |                               |

Partial Transcript of Intercept

three hours, the shaken commander acknowledged the obvious and applied, at least for a time, greater COMSEC emphasis and enforcement. Although ASA specialists always emphasized that such codes were insecure, an on-the-spot demonstration was often necessary to convince the "doubting Thomas." Unfortunately, the doubting Thomases are still in evidence. In December 1969 a captured enemy SIGINT soldier stated that Vietnamese Communist analysts not only learned U.S. troop locations through exploitation of locally produced U.S. point-of-origin grid codes but that, at least within his team, they were able to convert instantly the intercepted coded equivalents to the true 6-digit coordinates.

*Education and Training* In addition to producing COMSEC reports and management data to bring about positive COMSEC actions, ASA units attempted to educate commanders and communicators. Following the transfer of COMSEC responsibility from J-6 to the J-2 MACV in mid-1965, a Headquarters, USASA, 2-man SIGSEC advisor team—Maj. George D. Reichard and Maj. George V. Jarrett—spent three months TDY with J-2 MACV to help develop a COMSEC program for MACV. Using the results of local COMSEC monitoring and reporting, Majors Reichard and Jarrett drafted COMSEC regulations and directives, which MACV and USARV then issued. During their 1965 TDY and another one in the following year, the two men visited all major commands in South Vietnam and, through interviews with commanders and staffs, gained a better knowledge of attitudes toward COMSEC and explored the need for COMSEC education. They also studied status reports to determine which deficiencies required priority attention in COMSEC education. J-2 MACV itself advocated a vigorous educational program as a means of eliminating the malpractices being brought to light by such studies as that made of the SILVER BAYONET operation in 1965.\*

From early 1966 on, ASA COMSEC units emphasized COMSEC education. COMSEC teams visited all levels of command from battalion upward, providing guidance, training lectures, and educational classes. In their presentations, the teams made effective use of translated documents, interrogation reports, and other materials received from ASA's SIGINT

\*See below pp. 90-95.

## CONVENTIONAL COMSEC MONITORING

49

and target exploitation (TAREX) organization in Vietnam. With these, ASA instructors illuminated the increasing enemy SIGINT threat and gave concrete examples of the enemy's tactical use of U.S. COMSEC weaknesses. At times the teams played taped recordings of U.S. communications breaches to illustrate the danger to U.S. lives. They also trained officers, troops, and communicators in the proper use of the KAC series of codes and demonstrated methods of employing KY-8 ciphony in secure nets, always encouraging maximum use of the KY-8's.

General William C. Westmoreland, COMUSMACV, backed the ASA COMSEC program, issuing directives that ordered COMSEC improvements and gave the basis for moving through progressive educational steps toward stated COMSEC goals. Helped by a gradually increasing command interest, ASA COMSEC specialists educated thousands of persons, from generals to radiotelephone operators, in communications security.

The 509th ASA Group's COMSEC elements over the years established close contacts and working relationships with commanders, Signal officers, intelligence staff officers, and tactical communicators at all levels. In spite of the hectic combat environment, which was thus not conducive to formal education programs, they continued to instruct in the application of ciphony, cryptonetting, and other subjects. They also helped commanders prepare for secure communications as one aspect of planning military operations. In addition, COMSEC advisors drafted for the commanders command letters, directives, and guidance materials for use in standing operating procedures.

By 1968 the 509th ASA Group had given organizational status to its educational teams, calling them COMSEC Assistance and Advisory Teams (CAAT). The teams, each made up of at least six experienced COMSEC NCO's, visited the divisions, in turn, spending from 7 to 14 days with each, conducting with staff officers a thorough review of all COMSEC matters, and applying preplanning or surveillance techniques to improve communications in forthcoming military actions.

In 1968 and thereafter, improvement over the COMSEC status of 1965-66 was evident. COMSEC surveillance and CAAT operations were meeting the continuing COMSEC challenges and bringing about some measure of relief.

*Convincing the Commanders* The Army Security Agency found a wide variety of responses to their efforts to obtain communications security in Vietnam. Some understanding commanders applied COMSEC safeguards conscientiously; other commanders did not. Until SILVER BAYONET in October 1965, most U.S. Commanders in Vietnam showed only a marginal interest in COMSEC, since they doubted that the enemy could conduct successful SIGINT operations. These commanders reasoned that U.S. superiority in training, firepower, and mobility made COMSEC of little importance.

Commanders during the early months of combat were often frustrated in their efforts even to find the elusive enemy, and at least one officer said that he hoped that the enemy *would* use intelligence gained from insecure U.S. communications—at least then he might attack and thus show himself. Lt. Gen. Harry W. O. Kinnard, commander the 1st Cavalry Division (AM) from September 1965 to May 1966, exemplified the thinking at the time:

The DSU and my Signal Officer offered much advice and guidance in this /COMSEC/ area. But, I'm afraid I didn't let them help me much. It was impracticable to change SOI-SSI and codes often in the division, because there were so many nets involved, and normal tactical employment required rapid changing of control of battalions, even companies, from one subordinate command to another, at any time in operations. Our communications gave us the capability to react and adjust rapidly and flexibly, and I could not afford to risk communications (hence tactical) confusion by using changing codes and calls in different subordinate commands. I am convinced that, even though the enemy may have gained some OB information from our communications . . . they were not able to glean sufficient usable information from monitoring our nets to react to their advantage, for our deployments and tactical reactions were too rapid for them to apply what they may have gleaned. This was the choice I had to make, and I decided that tactical speed and mobility from stable communications was more important than possible tactical voice COMSEC loss.\*

Others, including Maj. Gen. Richard T. Knowles of the 1st Cavalry Division (1965-66) and Maj. Gen. William E. DePuy, commander of

---

\*Wolfe, Interviews.

CONVENTIONAL COMSEC MONITORING

51

" B) SAMPLE MESSAGES AND METHOD OF COMPOSITION  
COMMONLY USED:

IN GENERAL THE 11th ARMORED CAV REGT DOES NOT  
HAVE SET MESSAGE FORMATS WITH THE EXCEPTION OF A FEW  
MESSAGES THAT REPORT B-52 STRIKES AND ARTILLERY FIRE.

EXAMPLE: REPORT OF B-52 STRIKE (AS IN THE TEXT -  
IN ENGLISH))

- BADMAN 96 - ALL STATIONS - HEAVY ARTILLERY  
WARNING AT COORDINATES 1408800 ON THE 345/44  
BIEN-HOA TACONS ARE AVOID BY 10 NAUTICAL MILES  
FROM NOW UNTIL 1200H. ALL STATIONS ACKNOWLEDGE, IN  
RETURN."

"REPORT OF ARTILLERY FIRE (AS IN TEXT - IN ENGLISH)

- BADMAN 96 - ALL STATIONS ARTILLERY WARNING.  
FIRING FROM LEAR TO GRID XU723415 MIGHT SHOT 200 FEET  
1900 DEGREES. MIGHT RANGE 12-5 12M."

Page From Enemy SIGINT Instruction Manual

1st Infantry Division (1966-67), expressed similar views on COMSEC, sharing in the belief that the enemy could not acquire much help from unsecured U.S. tactical voice communications. Each also thought the U.S. battlefield maneuverability demanded rapid communications and a nonchanging SOI.

[REDACTED] COMSEC officials at the time  
were also placing unwarranted reliance on the availability (and assumed proper use) of manual codes that were not yet tailored for Vietnam.

The situation changed slowly as COMSEC agencies and Army commanders gained experience in Vietnam. NSA began production of manual codes tailored to Vietnam field requirements. ASA TAREX collection helped reveal the hostile SIGINT threat, providing a steady stream of examples of enemy SIGINT successes against the United States and its Allies. ASA in-country monitoring highlighted for the

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798

commanders the danger of communications deficiencies, and COMSEC personnel at the DSU level worked directly with the commands. Capt. Leo M. Melanson, commander of the 371st ASA Company, in 1968 spoke of the way in which the DSU's operated to bring about COMSEC changes within the commands:

/In/ the field of COMSEC, its . . . varying degrees of success among the Divisions in Vietnam can be, and are, directly attributable to the Company's relationship, /not only with the command and the G2 but/ with the Division Signal Officer /DSO/. Once /he is/ aware that part of the Radio Research Company's mission is to assist the Division in /COMSEC/ . . . and actually believes it, then a successful program can be achieved. . . . the 1st Cavalry Division /had/ continually and blantly used the point of origin code. It was not until the DSO was won over to the COMSEC side that the practice was stopped completely. Extensive education of . . . operators at all levels in the use of the KAC-Q/P codes, terminating with a command message, finished the point of origin code's use in the Division.\*

As a result of similar COMSEC operations, it eventually became easier to influence most U.S. ground commanders. For example, in early 1967 the 325th ASA Company, with the help of the 303d ASA Battalion, monitored for five days the 9th U.S. Infantry Division's nets in the Mekong Delta area. Without using any of the available operational information, the 325th analysts reconstructed from the normal tactical voice nets about 95 percent of the division's total operation—organization, units, personalities, nets, call signs, frequencies, plans and intentions, movements, and objectives. As a result, Maj. Gen. George G. O'Connor became a firm believer and a stringent enforcer of COMSEC practices. His 9th Division became one of the most secure divisions in Vietnam during that period.

Referring to the value of COMSEC indoctrination, Maj. Gen. John R. Deane, Jr., commander of the 173d Airborne Brigade (Separate) from December 1966 through August 1967, stated:

I believe that the U.S. COMSEC posture in general in SVN was very poor. I am a firm believer in good COMSEC practices and applications. However, I was not aware of any drastic actions against COMSEC violators . . . the DSU regularly reported on COMSEC violations and advised me concerning the

\*Wolfe, Interviews.

## CONVENTIONAL COMSEC MONITORING

53

picture of friendly operations that had been gleaned from COMSEC analysis, and the dangers thereof if similarly gleaned by enemy COMINT. I used their educational capabilities to the maximum practicable in the command.

He then spoke of problems in the Army COMSEC program:

Directives to enforce COMSEC by stringent penalties on individual violators will encourage people to absorb the regulations and training afforded, and given by ASA all the time. If we had better security motivation and if COMSEC had more teeth in it, then there would not be so much loss of tactical information from clear voice traffic. However, there is a practical and economic limit to which we can afford to give every radio an accompanying piece of COMSEC equipment. . . . In general, I've seen no great development in COMSEC status since WW II. Although there have been improvements in COMSEC equipment, there is a practical limit to the amount of COMSEC equipment that we need, or which can be carried by the combat soldier. In SVN, the use of even the KY-38 was not practicable for manpack on the soldier in active combat. . . . There are still major problems that need to be resolved.\*

Lt. Col. John L. Heiss, III, SSO J-2 MACV (1966-67), revealed unusual sensitivity to the need for COMSEC:

In most operations USF did not want to get ARVN forces involved, for this was a definite weak link. Our worst weakness was the tendency to talk too much, or talk around classified matters on telephones. Our telephone . . . system was a weakness and, although I have no hard evidence, I can't help but believe that the VC attempted to exploit this weakness. I suspect that a study of the background of some of the ambushes we suffered may represent enemy exploitation of U.S. COMSEC weaknesses.\*

However, despite better education in COMSEC procedures, the availability of some secure voice equipment, issuance of better codes to fill requirements, a sizable U.S. monitoring program, and a more general acceptance by many commanders of the existence of a viable hostile SIGINT threat, significant security malpractices continued, although diminished in volume. These were especially the unnecessary or incautious use of unsecured voice communications, use of unauthorized and insecure home-grown codes, improper use of call signs, and lack of

---

\*Wolfe, Interviews.

authentication. The weaknesses continued largely because too many commanders and their communicators still did not know about or were unwilling to follow operationally acceptable COMSEC practices. To these commanders and communicators the fastest possible communications, unencumbered by security practices and equipment, were a necessity of war. Education of commanders in COMSEC remained, therefore, as a major problem.

### *Naval Security Group*

#### *Organization*

At the time of the Gulf of Tonkin incidents in August 1964, the Navy COMSEC organization in the Western Pacific (WESTPAC) was already well established. Permanent COMSEC components were at the Naval Communications Station Guam (COMSEC 701), the NAVSECGRU Activity Kamiseya, Japan (COMSEC 702), and the Naval Communications Station Philippines (COMSEC 703), and were manned by [ ] of which a team of an officer and [ ] enlisted men were on temporary additional duty afloat with the Seventh Fleet. The afloat team had begun in January 1963 to assist the Commander, Seventh Fleet, embarking on assigned ships. At first the team was designated COMSEC Team ALFA, later COMSEC Team One.

In July 1963 the Navy was planning for the establishment of a COMSEC component (COMSEC 704) at the NAVSECGRU Activity Hanza, Okinawa, in order to have a permanent COMSEC listening post more responsive to Seventh Fleet requirements. Okinawa lay close to the Communist Bloc countries near which Seventh Fleet ships operated. COMSEC 704 began operations in June 1965 and was fully operational by the end of the following month.

To cope with a rapidly changing communications situation in Southeast Asia, the Navy rearranged its COMSEC organization in the Pacific during the winter and spring of 1965. The new organization emphasized traffic analysis of monitored communications and centralized reporting on a broad geographical basis. Under the reorganization, COMSEC components called collection and reporting centers performed



## CONVENTIONAL COMSEC MONITORING

55

monitoring and first echelon reporting, then forwarded raw traffic immediately to a processing and reporting center (PRC), where detailed analysis took place. NAVSECGRU Activity Kamiseya served as the processing and reporting center for the Western Pacific.

*COMSEC Team Vietnam* ~~(C)~~ The Western Pacific COMSEC reorganization came simultaneously with the establishment of a temporary Navy COMSEC team at Da Nang. In early March 1965 a NAVSECGRU officer inspected alternative locations in the Da Nang area to determine the best site for COMSEC operations, investigating the availability of working areas and equipment for a COMSEC unit that would be known as COMSEC Team Vietnam ~~(C)~~ and have one officer and four enlisted men. COMSEC Team Vietnam ~~(C)~~ began operations on 31 March 1965 in support of Brig. Gen. Frederic Karch, Commanding General, Ninth Marine Expeditionary Brigade (MEB) and Navy and Marine Corps units in SVN.

The team was to operate for a 90-day period. After it became operational, however, the Naval Communications Station Philippines recommended that it be continued beyond 30 June 1965 if General Karch still needed COMSEC monitoring. Vice Adm. Roy L. Johnson, Commander, Seventh Fleet, supported the recommendation, provided the COMSEC status of Marine and naval communications warranted it. With the accelerating tempo of military operations at the time, no one doubted that the team was needed. The team had already identified a number of COMSEC deficiencies, in particular: permanent assignment of code names or nicknames to specific locations for landing zones, thereby increasing the likelihood of their recovery by the enemy; failure to utilize authentication at any time; shortage of operations codes and improper use of those available; and use of nonapproved, locally generated codes.

On 29 May 1965 Commanding General, Fleet Marine Force, Pacific (FMFPAC), Lt. Gen. Victor H. Krulak, noted that the COMSEC team at Da Nang had done an outstanding job in helping to tighten security on radio nets of deployed Marine units. The COMSEC support provided to Navy and Marine Corps units at Da Nang amply demonstrated the value of continuing an active COMSEC program after 30 June. General Krulak stated further that the Marine Corps First Radio Battalion would continue that COMSEC assistance. Therefore, effective 5 July 1965, the

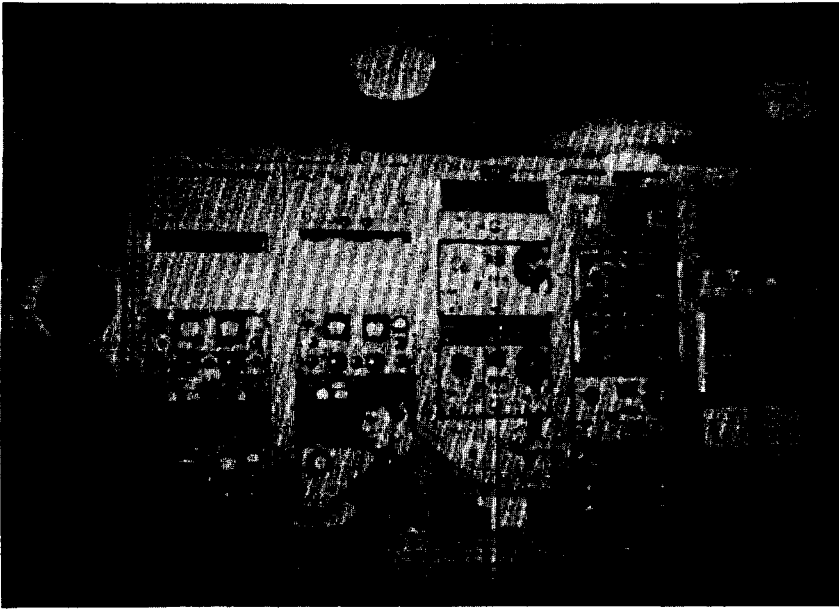


Navy COMSEC Monitoring Position Ashore

Navy COMSEC Team Vietnam (C) was deactivated and its tasks were assumed by a recently formed Marine COMSEC team of the First Radio Battalion, Fleet Marine Force, Pacific.

*Sub Unit One, First Radio Battalion* Elements of the First Radio Battalion had operated in South Vietnam as early as 1962, giving emphasis to SIGINT. In March 1965 Detachment J of the First Radio Battalion was established in support of the Ninth MEB, and included [ ] COMSEC positions among its resources. This detachment carried on the COMSEC functions that had been performed by COMSEC Team Vietnam (C). The [ ] positions were increased to [ ] in January 1966 when Detachment J was deactivated and its men and equipment became part of Sub Unit One, First Radio Battalion [ ]

[ ] While the original Detachment J had reported to its parent command in Hawaii, the new subunit came under the direct operational control of General Krulak. The direct support role of Sub Unit One



Navy COMSEC Monitoring Position Ashore

corresponded somewhat to that of ASA direct support units then being administered by senior-level ASA echelons but under the operational control of the Army commanders to whom they gave assistance.

*COMSEC 705* The need for communications security in Southeast Asia continued to grow with the expansion of communications. In September 1965 Admiral Johnson, by then Commander in Chief, Pacific Fleet, expressed a need for continuous COMSEC monitoring of new naval circuits then being activated at Da Nang. Accordingly, an officer and six enlisted men formed a unit, designated COMSEC Team, Naval Support Activity Da Nang, that went into operation in October 1965 with  monitoring positions and an indefinite tenure. Its mission was to provide COMSEC support to local naval elements and to determine possible intelligence losses through communications. Specific tasks were to provide COMSEC support to Naval Support Activity Da Nang and to naval units in the South China Sea and to monitor and evaluate naval

~~TOP SECRET UMBRA NOFORN~~

(b) (1)

(b) (3)-50 USC 403

(b) (3)-18 USC 798

(b) (3)-P.L. 86-36

communications. By December 1965, [ ] additional enlisted billets had been approved and action taken to fill them. In June 1966 the team was redesignated Detachment Delta, Naval Communications Station Philippines, and assigned the Navy title COMSEC 705.

Thus, by December 1965 Navy COMSEC personnel in the Western Pacific numbered [ ] officers and [ ] enlisted men; COMSEC elements totaled 5 COMSEC components plus a team afloat.

*COMSEC Team Saigon* In 1966 naval operations extended southward from Da Nang. COMSEC Survey Team Saigon (one officer and one enlisted man) was formed in the spring of 1966 to conduct a survey of MARKET TIME communications.\* Using the men and facilities of another specialist team aboard the USS *Jamestown* for monitoring and other Navy COMSEC units, the survey team had access to a total of [ ] positions. The results were startling. The COMSEC deficiencies uncovered not only stimulated COMSEC improvement through the distribution of more suitable operations codes but also emphasized the need for Navy COMSEC teams in the area. While there was a concentrated special survey to improve MARKET TIME communications security in the first three months of 1966, MARKET TIME operations themselves continued throughout the war, and monitoring of U.S. MARKET TIME communications continued to be a significant part of Navy COMSEC operations.

*COMSEC Team Three (Delta)* In February 1966 [ ] enlisted men were ordered on temporary additional duty (TAD) at Vung Tau in South Vietnam to establish COMSEC Team Delta. Headed by a chief petty officer, the team was activated, initially for 45 days, at the Coastal Surveillance Center, Vung Tau, its mission being to provide COMSEC support to the commander of Task Force 115 and his units in Southeast Asia, and to naval elements involved in the MARKET TIME operations. The team also was charged with reporting on the advisability of establishing a permanent COMSEC unit at the mouth of the Mekong

---

\*MARKET TIME was a covername given to operations taking place in the offshore waters of South Vietnam. For the survey, see below, pp. 109-16.

(b) (1)

(b) (3) -50 USC 403

(b) (3) -18 USC 798

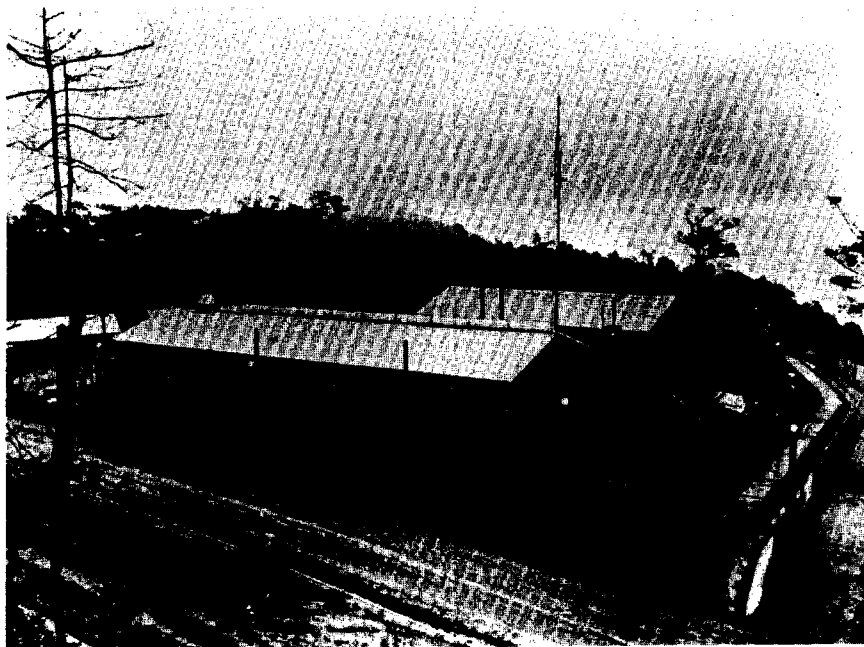
(b) (3) -P.L. 86-36



USMC Sub Unit One COMSEC Monitor

River Delta. The work of the team was of value to the chief of the Naval Advisory Group in Saigon who, in March, took special note of the assistance provided by Team Delta in the MARKET TIME survey. He confirmed that the requirement for a COMSEC unit to monitor southern MARKET TIME and Mekong River Delta area communications continued to exist. He stated further that the COMSEC Team Delta would be invaluable in helping Task Forces 115 and 116 to maintain an accurate picture of their communications security. Therefore, in April of 1966, the team shifted operations from a temporary structure to a specially configured COMSEC van at Vung Tau, and in July was redesignated COMSEC Team Three.

In January 1967 Admiral Johnson noted that the COMSEC Team Three had been especially effective in maintaining secure communications for Navy tactical commanders. Information received from COMSEC 705 and NAVSECGRU Activity Kamiseya substantiated

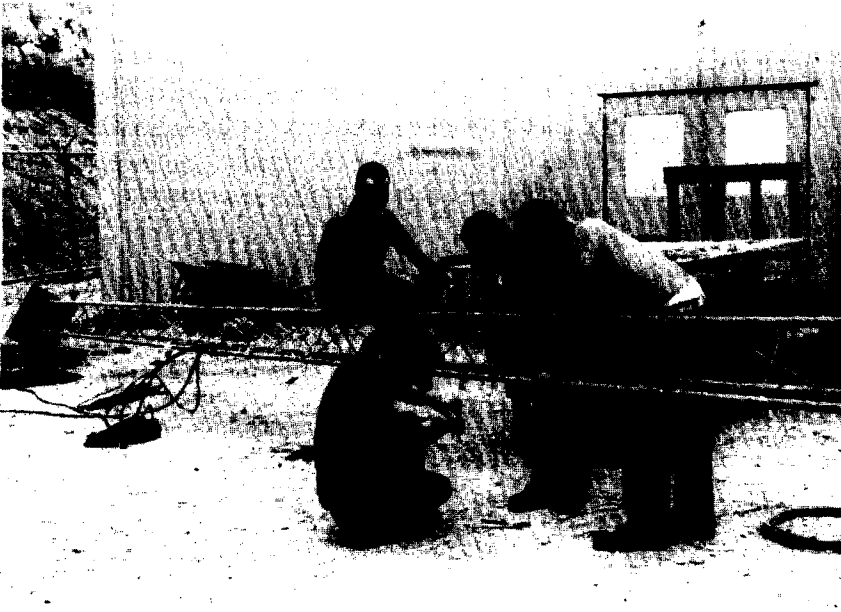


COMSEC 705 Location at Foot of Monkey Mountain

the fact that termination of operations at Vung Tau would seriously curtail naval COMSEC control in the delta area.

Although several attempts were made to establish COMSEC Team Three as a permanent component, each request for additional billets met with Defense Department disapproval. Because the team had proven itself to be a valuable COMSEC asset to in-country forces, however, it continued its existence with personnel on temporary duty from COMSEC 705's sparse allowance of ☐ enlisted men.

*COMSEC Team Two (Bravo)* In January 1966 Vice Adm. John T. Hyland, Commander, Seventh Fleet, pointed out the desirability of embarking a COMSEC team with naval amphibious forces in Southeast Asia. Admiral Johnson agreed that a full time COMSEC team would help maintain communications security and could give technical assistance as needed for manipulative cover and deception in amphibious operations. First designated COMSEC Team Bravo and shortly thereafter



COMSEC Specialists Assembling an Antenna, Monkey Mountain

as COMSEC Team Two, the unit began operations in June 1966 with one officer and [ ] men, monitoring and evaluating amphibious force communications. Although it was initially planned that the team be assigned to Task Force 76, for transfer with the staff as it rotated among flagships, COMSEC Team Two was in practice used in support of Task Group 76.5 (Group Bravo) and occasionally Task Group 76.4 (Group Alpha).

*COMSEC Team Five* COMSEC Team Five was organized on 24 March 1967 and assigned to Beach Jumper Unit (BJU) One. This team of an officer and [ ] enlisted men had an assigned mission to exchange techniques, knowledge, and experience with the beach jumper unit through an exchange in personnel. As a result of this venture, both COMSEC and BJU personnel gained a keener awareness of the complexities inherent in the communications deception operations in which the beach jumper units were involved. Although the team was deacti-

(b) (1)

(b) (3)-50 USC 403

(b) (3)-18 USC 798

(b) (3)-P.L. 86-36

vated on 22 May 1967, permanent COMSEC components continued to provide COMSEC technical assistance for BJU operations and served as points of contact for mutual exchange of information. Another result of Team Five's exchange of personnel was the establishment of two permanent COMSEC billets in the BJU personnel allowance, both of which were filled in the fourth quarter of fiscal year 1969.

*COMSEC Team Four* COMSEC Team Four, with a chief petty officer and [ ] enlisted men, commenced limited COMSEC operations on 25 April 1967 and became fully operational during May. Personnel for the team were provided TAD from various permanent Pacific COMSEC components. The team operated from a truck-mounted van—supplied by the Naval Communications Station Philippines—that contained [ ] monitoring positions and was based at Vinh Long in the Mekong Delta area. Team Four's mission was to provide COMSEC support in the Mekong River Delta to Riverine Task Force 117 and to extend service also to GAME WARDEN, Task Force 116. In February 1968, during the Tet offensive, a mortar shell demolished the van and, although there were no casualties, operations had to be suspended until March 1969, when a new van was installed on a barge in the Mekong River.

*COMSEC 706* As a result of a preliminary study conducted in December 1965, NAVSECGRU Activity Kamiseya recommended that a COMSEC component be established at the Naval Communications Station Cam Ranh Bay. Planning for a permanent component there with [ ] billets received approval of the Secretary of Defense in November 1966, but difficulties in procuring and installing equipment delayed activation of the unit for over a year. As COMSEC 706, the unit finally became operational on 5 January 1968, with the mission of providing COMSEC close support to Pacific Fleet naval commanders in Southeast Asia.

At the end of 1967, Navy COMSEC personnel authorized for the Western Pacific were [ ] officers and [ ] enlisted men, of which [ ] officers and [ ] enlisted men were actually on board.

(b) (1)

(b) (3) -50 USC 403

(b) (3) -18 USC 798

(b) (3) -P.L. 86-36



## CONVENTIONAL COMSEC MONITORING

63

*Operations*

NAVSECGRU's COMSEC organization monitored and analyzed long-haul naval communications passed between shore stations and ships at sea and air squadrons. Marine Corps direct support units monitored and reviewed the communications passed by Marine units operating in northern South Vietnam.

Monitoring and analysis were the major aspects of NAVSECGRU's COMSEC operations in the war zone and, as in the case of Army, by far the greater number of Navy personnel assigned to COMSEC duties spent their time largely on these functions. Navy COMSEC personnel were thus working on such tasks as: conducting COMSEC surveys; monitoring and analyzing naval communications and preparing Communications Improvement Memoranda; measuring frequencies and preparing off-frequency reports; training personnel in cryptographic and communications procedures, in message drafting, and in physical security with emphasis on intelligence losses from unprotected circuits; and helping communicators to prepare and revise operations plans, operations orders, and communications plans and to identify and solve communications problems as they arose.

The Navy increased its COMSEC organization to keep pace with the growing volume of communications during the period 1964 to 1968. From a force of [ ] men and [ ] positions, the Navy's Western Pacific COMSEC organization expanded during this period to [ ] men and [ ] positions—[ ] monitoring, [ ] frequency measuring, and [ ] radio fingerprinting positions.

The afloat COMSEC Teams One and Two continued to monitor by patching from the host ship a minimum of two CW and/or voice radio circuits to the operating space being occupied by the teams. The COMSEC monitoring equipment used by Navy and Marine COMSEC elements included:

*Equipment*

R-390A  
SP-600  
R-274B  
R-1279 with CV-1750  
range extender  
R-389

*Use*

shore facilities for HF communications  
shore facilities for HF communications  
shore facilities for HF communications  
VHF communications  
low frequency communications

(b) (1)

(b) (3)-50 USC 403

(b) (3)-18 USC 798

(b) (3)-P.L. 86-36

Initially, NAVSECGRU had problems with the equipment it placed ashore in Vietnam. Navy receivers were more suitable for use on ships or in permanent installations than they were for use in tents and small vans where dust, mud, rain, and heat affected their operation. Dust, for example, penetrated the equipment and caused malfunctions. During the time that the Navy's COMSEC Team Vietnam (C) was operating at Da Nang, it was without maintenance personnel, and malfunctioning equipment was shelved, awaiting assignment of repair personnel who came later.

For the most part, the Navy kept its COMSEC monitoring elements that were stationed in the Vietnam area fully manned at authorized strength. Personnel to man the positions came from the more permanent Naval COMSEC establishments in Hawaii, Japan, and Guam, and as a result these components farther from the war zone continuously had to operate below authorized strength. Despite the full manning of the elements ashore in Vietnam, personnel very frequently worked 16-hour shifts.

The Navy's COMSEC organization concentrated on communications passed during Seventh Fleet naval and naval air, MARKET TIME coastal surveillance, naval gunfire support, special mission positive identification radar advisory zone (PIRAZ) and search and rescue (SAR), GAME WARDEN, and amphibious operations. While the volume of traffic collected changed from time to time, the Navy monitored, according to estimates, a relatively high percentage of the communications passed. One estimate made in the summer of 1966, for example, gave these figures:

| <i>Type of Communications</i>   | <i>Estimated Percentage of<br/>Total Traffic Monitored</i> |
|---------------------------------|--|
| TF 77                           | 18   |
| TF 76                           | 5  |
| TF 73 (underway replenishment)  | 25   |
| TF 115                          | 30   |
| TF 116                          | 20   |
| TG 70.8 (naval gunfire support) | 25   |
| TF 72 (patrol aircraft)         | 10   |
| Ship-to-shore                   | 40   |
| Air-to-ground                   | 23   |
| Harbor common                   | 50   |

## CONVENTIONAL COMSEC MONITORING

65

The geographic location of NAVSECGRU COMSEC components permitted reasonably good coverage of high frequency transmissions of forces operating in Southeast Asia. The afloat COMSEC Teams One and Two randomly sampled VHF and UHF communications employed by units of the Seventh Fleet, patching into these communications through lines leading to their COMSEC space. Shore-based COMSEC components monitored VHF and UHF naval communications in their immediate areas and long-haul communications of ships moving into and out of the war zone.

*Sub Unit One, First Radio Battalion* Sub Unit One had COMSEC positions at the various locations of its detachments during the years 1964-68. In early 1966 it had 2 positions at Chu Lai, 2 at Da Nang, and 1 at Phu Bai. In the fall of 1968 it had 2 at Camp Carroll, 2 at Dong Ha, 1 at Hill 327 near Da Nang, and 1 at Vandergrift Fire Support Base. While the subunit usually had [ ] COMSEC positions in operation, at times it became necessary to task these positions with SIGINT missions.

Sub Unit One detachment commanders worked closely with G-2 and S-2 officers in the supported USMC units to arrange for tasking of the COMSEC monitors. By and large, Marine COMSEC specialists monitored low-level tactical FM radio nets, which they regarded as those most likely to compromise U.S. tactical intentions. They also monitored radio relay circuits, using a Rycom selective voltmeter on loan from the NSAPAC Representative [ ]. Whenever possible, communications of units engaged in combat or active patrol had priority. In static situations, monitors sampled radio transmissions at combat bases. Marine units kept their positions engaged 16 hours a day, and from about 1966 on they copied and analyzed approximately 4,000 transmissions each week.

*Against the Tide*

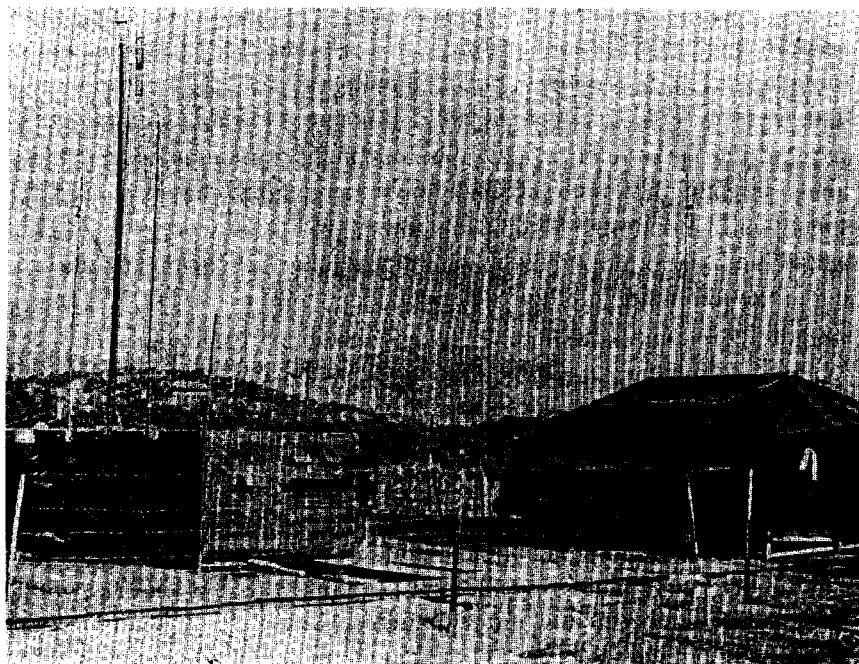
Navy and Marine COMSEC specialists employed much the same procedures as did those of the Army and Air Force in alerting commanders and communicators to dangerous practices and in pointing the way to improved COMSEC. They conveyed their message in face-to-face presentations, briefings, and spot and general reports.

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798



COMSEC Intercept Vans and Operations Tent,  
Chu Lai

Person-to-person presentations seemed, for the most part, to be the most effective means of settling many of the problems that arose. Before its functions were assumed by Sub Unit One, Navy's COMSEC Team Vietnam had established procedures to deal directly with in-country Marine communicators. The team participated in weekly communications officers' conferences conducted by the III Marine Amphibious Force communications electronics officer, in this way dealing directly with both the communications officers and their senior NCO's. The NCO's took measures to prevent recurrence of violations in their unit communications and, when time permitted, trained their own operators in the field.

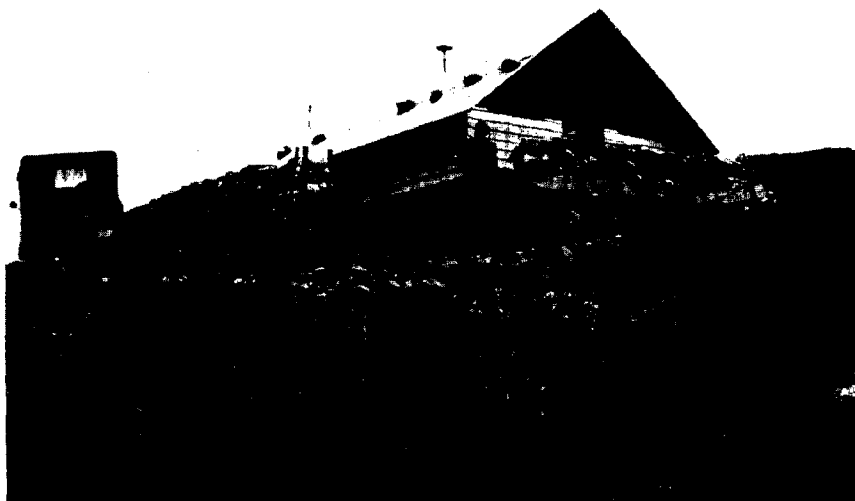
Sub Unit One continued the practice of person-to-person presentations. The unit made regular use of live examples in briefings to communicators and Signal officers of Marine field units, giving about 200 a year. The

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798



Operations Building at Hill 327, Da Nang

unit's briefing program did much to overcome the "electronic spy" stigma often borne by a COMSEC organization. Briefers generally overlooked minor procedural errors and emphasized combat-associated security lapses that endangered the lives of the Marines. As a result of person-to-person COMSEC service, better rapport resulted. Unit commanders at times even requested orientation lectures for their units. Sub Unit One COMSEC reports, when these were made, also had a better reception.

Navy COMSEC specialists were also at work on a person-to-person basis. They, too, used actual examples of operational communications deficiencies in their educational briefings for naval personnel ashore and afloat.

Both Marine and Navy COMSEC specialists spot-reported significant violations affecting the tactical posture of friendly units. Navy specialists informed the Commander, Carrier Striking Force, Seventh Fleet, for

~~TOP SECRET UMBRA NOFORN~~

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798

example, of information they had monitored from the Navy's air traffic coordination circuits that revealed strike plans and other intelligence. Marine Corps spot reports reaching the Special Security Officer, III MAF, often were in time to cancel or postpone Marine tactical operations.

Besides the spot reports, there were periodic COMSEC status reports that went to Navy and Marine Corps commanders. Marine specialists at the platoon level at first reported violations monthly through the Marine chain of command; later reports were made twice monthly. The reports went to the 1st and 3d Marine Divisions and the 1st Marine Air Wing. Sub Unit One also issued a monthly report to MACV describing the emphasis placed on communications security during the month, the number of transmissions monitored, and the number of violations found.

While only a rough measure of actual violations occurred, these Sub Unit One reports provided an indication of COMSEC status reliable enough for value judgments. During the last three months of 1968, the average number of monitored transmissions for each month remained approximately the same, yet the detected violations in October were 519, while for December only 216 violations were detected. Marine COMSEC analysts attributed this reduction in violations to increased emphasis during the period on the lecture method to improve security and to the establishment of closer working relationships between the platoons providing the COMSEC support and the supported G-2 and S-2 officers. When he was in command of III Marine Amphibious Force, Lt. Gen. Lewis W. Walt kept abreast of reports on the COMSEC status of Marine units and took note when he could of progress made by the subunit. In a letter of 28 November 1966 to the commanding general of the Fleet Marine Force Pacific, General Krulak, and others, he wrote:

It has been noted with pleasure that the communications security posture of the III Marine Amphibious Force has shown marked improvement during the past 11 months. This is apparent in the fact that the number of significant communication security violations committed each week by III Marine Amphibious Force units, air and ground, has decreased by 75 percent since January 1966. This improvement can only be attributed to extensive command interest and concern shown at all echelons of command, increased use of available cryptographic aids, and to the efforts of Sub Unit One, First Radio Battalion in presenting over 200 periods of instruction on this subject to III Marine Amphibious Force Units.

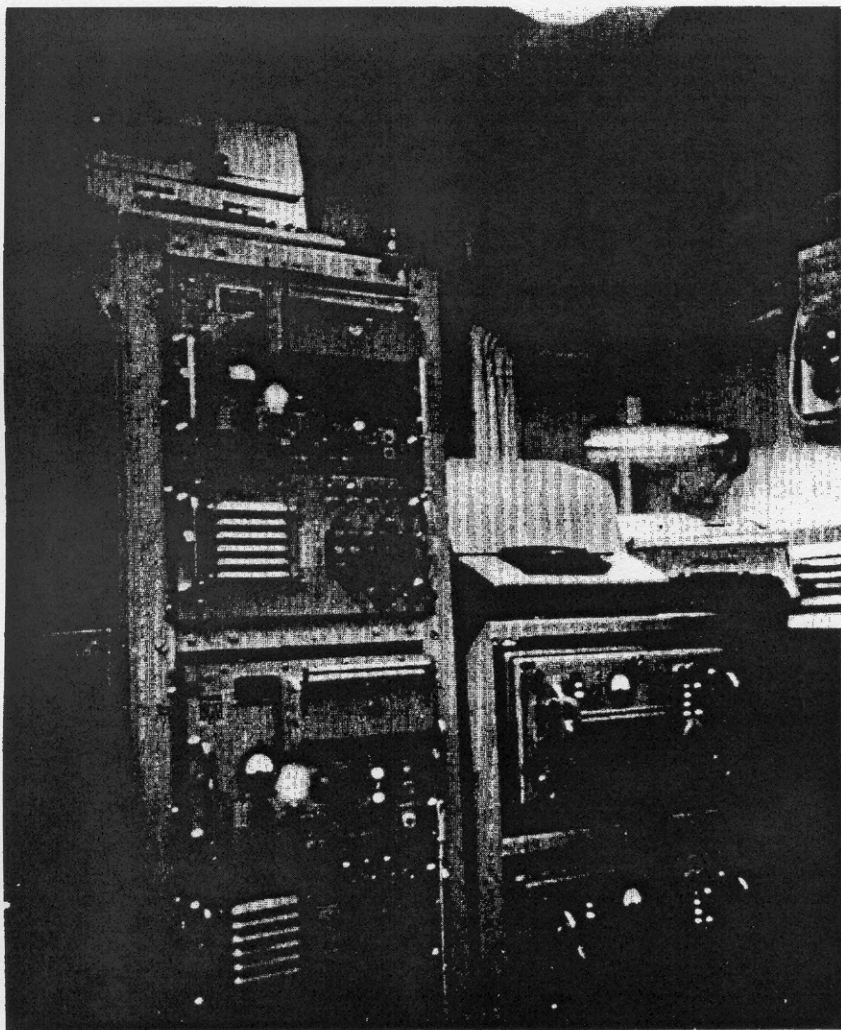
## CONVENTIONAL COMSEC MONITORING

69

Navy COMSEC reports also prompted command actions of one kind or another. A major report, the quarterly COMSEC Traffic Analysis Report, not restricted to but incorporating the Southeast Asia naval COMSEC reports, gave wide circulation to the COMSEC problems in Southeast Asia and the Western Pacific in general and provided the basis for initiating corrective COMSEC actions. Within WESTPAC the reports helped in a variety of COMSEC management steps. The analysis of monitored circuits, as reported, helped managers to determine priorities in the assignment to voice nets of short-supply secure ciphony equipment. Monitored findings helped also in the assignment of nonvoice crypto-equipment to provide cryptocover. For example, in January 1967 COMSEC 702, at Kamiseya, issued a traffic analysis report that resulted in authorization for on-line cryptocover of one of the communications links of the Naval Tactical Data System serving many of the Navy's ships in the war area. When reports on a MARKET TIME communications survey revealed a major netting problem and limited code vocabularies, COMSEC managers were able to press for improvements in operations codes and to recommend the use of improved codes in particular cases, such as communications giving naval gunfire shore targets.

Most important, the many reports prompted command actions directed toward WESTPAC communications discipline. For example, the commander of the Seventh Fleet issued a general message reiterating and explaining encrypt-for-transmission-only requirements. At the next higher level, the commander in chief of the Pacific Fleet advised subordinate commanders that unclassified messages originated by shore establishments concerning WESTPAC ships often disclosed movements or indicated impending arrival of ships in Western Pacific ports.

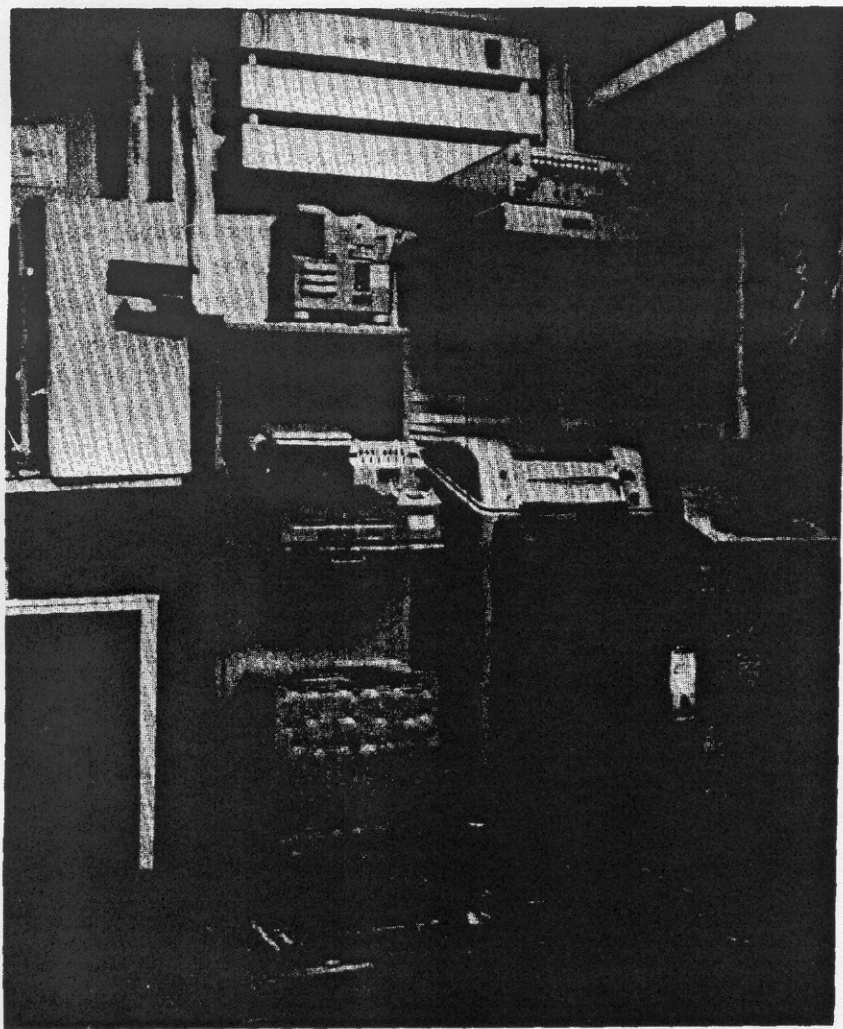
Generally, commanders reacted to spot monitoring reports and recommendations in a spirit of cooperation. But, as in the case of Army, NAVSECGRU COMSEC specialists found that not all commanders appreciated the support. Some high-ranking officers resented reports concerning their commands' errors appearing in electrical messages with multiple addresses. The resentment was more pronounced when the monitoring reports called attention over and over to the same malpractices. Marine and Navy commanders often felt that good COMSEC practices alone could not protect their military operations since the enemy did not need to intercept U.S. communications to obtain



KW-26 and KW-37R in Detachment 5 Cryptocenter, USS *Constellation*, Gulf of Tonkin

intelligence on naval and Marine components—the location of an aircraft carrier standing offshore was obvious, and the presence of fighter aircraft in support of ground operations told the enemy where the U.S. forces were. Application of strict COMSEC techniques therefore seemed to have no real purpose.





KL-47 in Detachment 5 Cryptocenter, USS *Constellation*, Gulf of Tonkin

To develop better rapport with commanders, monitors did not always follow strictly the basic instructions to report significant COMSEC malpractices electrically and with multiaddresses. The monitors preferred, instead, to report repetitive errors in weekly newsletters or in written monthly reports, which were less offensive.

*Air Force Security Service**Organization*

Headquarters, AFSS, at Kelly Air Base in Texas, controlled the Air Force COMSEC programs. Its Pacific headquarters, the Pacific Security Region (PACSCITYRGN) at Wheeler Air Base, Hawaii, operated a number of security wings (SW) in various parts of the Pacific. Of these, the 6922d Security Wing at Clark Air Base, Philippines, together with its several detachments, was the one principally involved in the Vietnam War in the years to 1968.

PACSCITYRGN also controlled other resources not administratively committed to a particular operating security wing, including a mobile TRANSEC\* team equipped with an HF position (AG-2761), a UHF/VHF position (AG-88711), a radiotelephone position (AG-274), and a COMSEC hut. PACSCITYRGN's Detachment 2 at Hickam Air Base, Hawaii, performed second echelon analysis and reporting and had direct operational control over the 6922d's detachments in Saigon, and in Korat, Thailand. After November 1967, Detachment 2 moved from Hickam to the PACSCITYRGN headquarters location at Wheeler.

The Air Force organization for COMSEC monitoring and analysis in Southeast Asia grew slowly in the early period of U.S. involvement. After some token monitoring of Air Force communications at Tan Son Nhut in September 1962, not much was done until two AFSS COMSEC specialists monitored VHF, UHF, and HF single sideband communications at Bien Hoa in November and December 1964. Their monitoring showed that a significant amount of intelligence was being passed unprotected [REDACTED]

[REDACTED] on the type of aircraft operating out of Bien Hoa Air Base, and on the command and control system used in operations.

\*Air Force personnel use TRANSEC in a manner to be more inclusive than the definition, "measures designed to protect the intentionally transmitted signal from intercept and exploitation by means other than cryptanalysis." Air Force use frequently equates to the broader term communications security (COMSEC). To avoid confusion in this volume, COMSEC will be used throughout this section except, of course, where TRANSEC appears in quotes.

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798

## CONVENTIONAL COMSEC MONITORING

73

Before the end of 1964, the Pacific Air Force (PACAF) authorized an additional COMSEC study, and Detachment 2, PACSCTYRGN, undertook the work. Although at first only a test was scheduled in order to establish the need for improvements, so flagrant were the many violations observed during the test period that Detachment 2 concluded the 2d Air Division (forerunner of the Seventh Air Force) tactical communications were receiving only marginal security protection. Air Force COMSEC analysts in Hawaii processed the intercepted tapes and almost immediately broke the PALMER JOHN operational code produced by the 2d Air Division and used by it to pass strike coordinates, times over target, aircraft call signs, and so forth. The analysts also noted insecure transmission of two messages relating to projected air strikes, as well as the itinerary of a forthcoming field trip by the 2d Air Division commander, Maj. Gen. Joseph H. Moore. As a result of the test, USAFSS recommended the establishment of a permanent COMSEC element in Southeast Asia. As an interim solution, the Air Force approved use of a mobile COMSEC H-1 van for the area.

*Detachment 5, 6922d Security Wing* As outgrowth of these early actions, on 8 April 1965 PACSCTYRGN deployed a [ ] COMSEC team and a mobile H-1 van to the Tan Son Nhut Air Base near Saigon. The deployment was on a TDY basis pending a request to General John P. McConnell, the Chief of Staff, USAF, for a personnel ceiling increase in South Vietnam permitting a [ ] COMSEC team.

Obtaining the ceiling increase, AFSS activated Detachment 5, 6922d Security Wing, at Tan Son Nhut in July 1965 to provide close tactical transmission security support to the 2d Air Division. Initial strength was one officer and [ ] airmen. Equipment approved for the detachment included [ ] HF positions (AG-2761), one UHF/VHF position (AG-88711), one radiotelephone position (AG-274), and one transcribe position (AG-4).

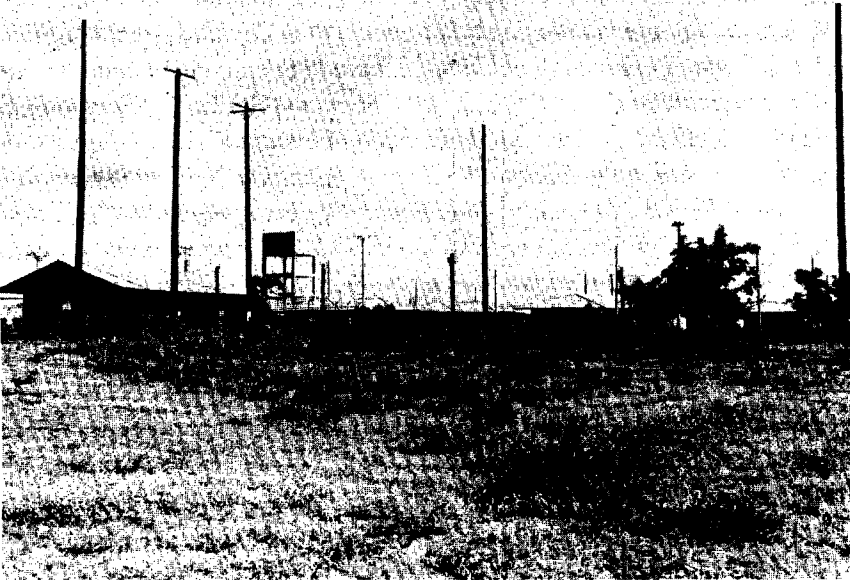
Completion of a semipermanent facility for the unit enabled the detachment to expand monitoring to the extent of doubling of telecom monitoring lines and adding multichannel monitoring equipment. Initially the new building contained [ ] HF (8761), [ ] VHF/UHF (887-EII), [ ] telephone (AG-275), and [ ] transcribe positions (AG-4). One more telephone position came at the end of 1967.

(b) (1)

(b) (3) -50 USC 403

(b) (3) -18 USC 798

(b) (3) -P.L. 86-36



Detachment 7, 6922d Security Wing, Buildings, Korat

*Detachment 7, 6922d Security Wing* In preparation for a visit to Saigon in July 1965 by Secretary of Defense Robert S. McNamara, MACV proposed to ask for an increase in COMSEC resources for all three Services. For this, the recently activated Detachment 5, 6922d Security Wing, supplied the following assessment of additional Air Force requirements: "We need [ ] more R/T (radiotelephone) positions and one more HF position plus [ ] more personnel. To cover South Vietnam adequately at least [ ] more TRANSEC units of [ ] personnel, each with 1 HF and one R/T position, would be necessary." The Secretary reacted favorably.

In specific reply to a 1 September 1965 CINCPAC request for Service and SCA review of monitoring requirements, the Thirteenth Air Force recommended establishing monitors in Korat, Thailand, using mobile vans. The plan called for a team not to exceed [ ] men with equipment for monitoring troposcatter, HF, and UHF/VHF communications.



Detachment 7, 6922d Security Wing, Positions, Korat

Among locations considered—Takhli, Udorn, and Korat—Korat was the best location for collection of radiotelephone communications. AFSS would use mobile vans to collect UHF and VHF singals in the immediate areas of Takhli and Udorn.

Detachment 7, 6922d Security Wing, began operations at Korat Air Base on 1 April 1966 supporting, through tactical COMSEC monitoring, the Deputy Commander, 7/13 Air Force,\* in operations conducted in and from Thailand. On 4 May the unit had only one officer and

\*Senior U.S. Air Force commander in Thailand. The title denotes his administrative and logistic relationship to Thirteenth Air Force, based in the Philippines, and his operational relationship to the Seventh Air Force, which had headquarters at Tan Son Nhut Air Base, South Vietnam.

(b) (1)

(b) (3) -P.L. 86-36

(b) (3) -50 USC 403

(b) (3) -18 USC 798

## Detachment 5 Mobile Operations, 1966

| <i>Date</i>   | <i>Place</i>                    | <i>Communications Targeted</i>          |
|---------------|---------------------------------|---|
| 21 Feb-6 Mar  | Da Nang AB                      | nontactical VHF frequencies of air base |
| 2 Apr-15 Apr  | Bien Hoa AB                     | nontactical VHF frequencies of air base |
| 1 Jun-10 Jun  | Da Nang AB                      | USAF VHF/UHF tactical frequencies       |
| 29 Aug-7 Sep  | Monkey Mt. site of<br>6924th SS | USAF VHF/UHF frequencies                |
| 17 Nov-26 Nov | Monkey Mt. site of<br>6924th SS | VHF/UHF frequencies                     |
| 17 Nov-26 Nov | 6924th SS main site             | HF frequencies                          |
| 17 Nov-26 Nov | Da Nang AB                      | telephone exchange                      |

airmen, but by 30 June the number of airmen had increased to [ ] This was still below the authorized strength of one officer and [ ] airmen.

By the end of 1967, [ ] AFSS men were monitoring and analyzing communications in Vietnam and Thailand. Other Air Force COMSEC elements in Japan, on Okinawa, in the Philippines, in Hawaii, and at Kelly Air Base helped monitor and analyze SEA communications.

AFSS considered its monitoring resources as of 1967 to be basically adequate for Southeast Asia requirements. Nevertheless, during much of the time personnel and equipment strengths were less than authorized. Many Air Force circuits were not checked, even periodically, during the entire 1964-67 period. The effect of personnel shortages is illustrated by a Detachment 7 report in 1967:

One common problem Det wide, and one which adversely affected the operations, was the untimely replacement of personnel. On 21 April 1967, [ ] personnel (NCOs and airmen) were relieved of duty to effect a 24 April 1967 port-call. Consequently, on 22 April 1967, trick operations were frozen to a two shift concept of 12 hours on, and 12 hours off. The 6922 SCTY WG responded to the situation with TDY assistance from Det 4, 6922 SCTY WG, and Det 7 was able to return to a three shift concept on 26 April 1967. Although this assistance lasted for 59 days, losses continued to exceed replacements, and additional assistance was received from Det 2, PACSCTYRGN in the form of authorization to close one wideband position. . . . This loss/gain problem continued throughout the period.

(b) (1)

(b) (3) -50 USC 403

(b) (3) -18 USC 798

(b) (3) -P.L. 86-36

## CONVENTIONAL COMSEC MONITORING

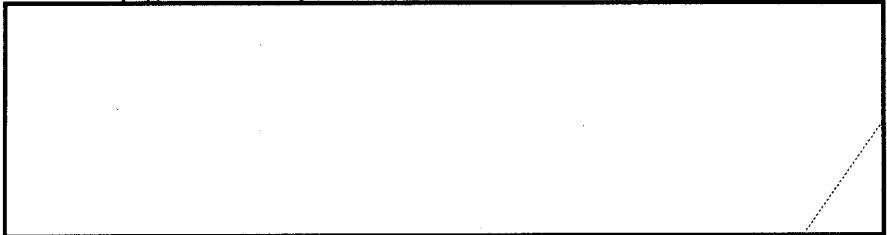
77

*Operations*

As in the case of Army and Navy operations, AFSS monitors selected circuits that they regarded the most profitable sources of intelligence to the enemy SIGINT organizations. They gave little attention to on-line encryption. Detachment 5 and 7 specialists concentrated, instead, on close-range monitoring of unsecured radio circuits used by ground crews to service aircraft. These circuits and the communications of unit protocol officers normally revealed intelligence useful to an enemy.

The Seventh Air Force established essential elements of information (EEI's) to guide the monitoring and reporting of the COMSEC detachments. The EEI's called for reports on violations whenever monitored communications revealed information on prestrike arrangements, logistics, communications disruption (jamming or saturation of secure circuits), tactical methods, aircraft performance, pilot and unit capabilities, or other sensitive data.

Both Detachment 5 and Detachment 7 had mobile monitor teams. Detachment 5's 1966 record of its mobile operations, as reflected in the table on page 76, was representative.



In December 1965 PACSCTYRGN directed the 6988th to provide a COMSEC monitor for a COMSEC test [redacted]

[redacted] Detachment 2, PACSCTYRGN, in its April 1966 evaluation of the results of this [redacted] monitoring recommended continual employment of a COMSEC monitor [redacted] Headquarters, AFSS, agreed to the continual operation [redacted]



[redacted] COMSEC monitors collected plain language communications passing over VHF/UHF guard and tactical voice channels, which carried information on strikes, MIG and SAM alerts, bomb damage assessments,

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798



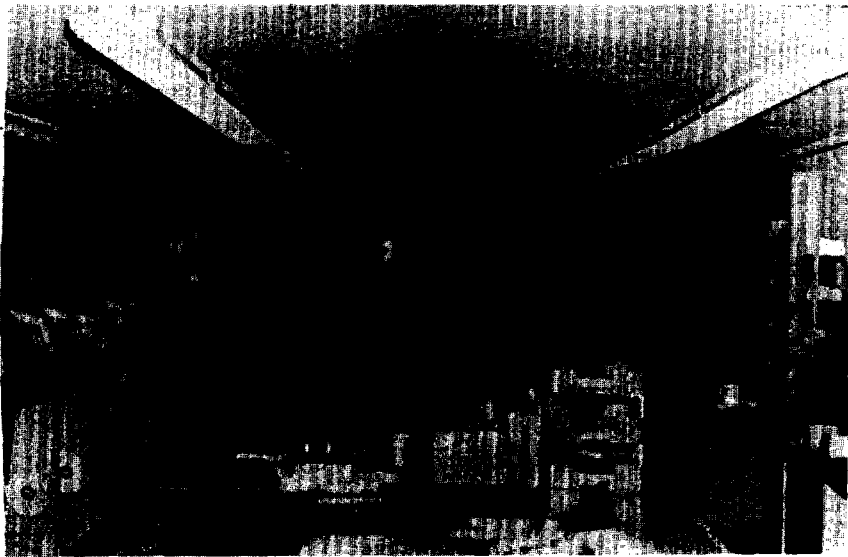
Detachment 5, 6922d Security Wing, Analysts at Work, Tan Son Nhut

targets, air refueling, and air-to-air coordination. After some experience with these communications, the monitors focused on frequencies used during air-to-air refueling operations as communications on these appeared to be continually revealing the general direction of outgoing fighter-bombers.

By September 1966 Detachment 2, PACSCTYRGN, called the [redacted] COMSEC monitoring the primary source of its "most lucrative findings."

[redacted] The COMSEC collection brought attention to communications weaknesses concerning alert systems, special navigation techniques, tactics, and command and control communications—all of which were of high interest to enemy SIGINT units. [redacted] COMSEC, providing information on forward area air communications that





KW-26 and KY-8 Crypto-equipment in Seventh Air Force Operations Area, Tan Son Nhut

controlled strikes in northern South Vietnam and the demilitarized zone (DMZ) and information on search and rescue communications.

When the AFSS began its COMSEC support of the 2d Air Division, the command had asked for reports directly from the monitoring detachments within 6 to 14 hours of intercept. In 1964 and 1965, AFSS COMSEC units were not capable of real-time reporting of monitored COMSEC weaknesses—reports that would have permitted the Air Force to change plans when strike operations, target areas, and so forth had been compromised. However, during those years some elements of the 2d Air Division did not feel that real-time reporting of COMSEC violations was necessary since they did not believe that operational plans should be altered on the basis of reported COMSEC violations. In July 1966 Detachment 5 listed some 25 monitored events that perhaps should have caused a change in plans if an immediate reporting system had been employed. Minimum required reporting time was then 4 hours, and regular reporting was possible only during normal duty hours. Under these conditions, reports often were received too late to affect operations.

In mid-1966 Detachment 5 recommended that the reports of monitored activity, both in-country and out-of-country, be reported "immediately" to appropriate tactical commands and that officials be authorized to alter plans on the basis of these reports. The Air Force accepted these recommendations. In February 1967 AFSS accordingly began sending "immediate" reports of detected violations to all levels of Air Force command down to air division. AFSS also began to include the names of communications violators when they were so requested by the command element involved.

AFSS employed various types of reports for notifying commands of COMSEC breakdown and for the COMSEC units' own use. Perhaps the most basic of the reports going to the commands was the Transmission Security Message Report (TSMR), the vehicle for immediate reporting. Detachment 7 issued 77 of these in 1967 alone. A variation of the TSMR, the Prestrike Report, came into use for situations in which information on a forthcoming air strike had been divulged 1 hour and 45 minutes or more before the strike. When voice ciphony circuits were available, AFSS units used them in communicating the COMSEC message to the military command concerned. Such reporting made it possible to change plans and thus offset possible enemy action predicated on the compromised information. Once a month, AFSS units forwarded a TSMR recap electrically to commanders and senior AFSS echelons, noting any actions taken by Air Force operational commands as a result of the monitors' reports.

Another report going to Air Force operational commands was the Transmission Security Monthly Summary (TSMS), a report giving the state of COMSEC, noting infractions of procedures by specified elements. In addition to its wide dissemination to Air Force operating elements, this report went to PACSCTYRGN, which also used it in dealing with command personnel.

While these various reports were for use primarily by operational personnel, another category of reports had the objective of aiding the monitoring effort itself. This category included a Daily Activity Summary (DASUM), a report forwarded electrically to PACSCTYRGN. For more immediate reporting, a TRANSEC Item of Interest (TIOI) went from detachment elements to higher authority when an observed practice

## CONVENTIONAL COMSEC MONITORING

81

## Seventh Air Force Classification of Information

| <i>Planned or Completed Missions (In-Country)</i> | <i>Classified</i> | <i>Declassify</i> |
|---|-------------------|-------------------|
| Sorties scheduled                                 | Yes               | after strike      |
| Target coordination                               | Yes               | 1 hour prior      |
| Target description                                | Yes               | 1 hour prior      |
| Time over target                                  | Yes               | 1 hour prior      |
| Number of aircraft in flight                      | Yes               | 1 hour prior      |
| Type of mission                                   | Yes               | after strike      |
| Special type missions                             | Yes               | indefinite        |
| Ordnance being carried                            | Yes               | 1 hour prior      |
| Request for strikes                               | Yes               | 1 hour prior      |
| Request for reconnaissance                        | Yes               | 1 hour prior      |
| Strike results                                    | No                | —                 |
| Reconnaissance results                            | Yes               | indefinite        |

appeared dangerous but not sufficiently alarming to warrant notification of operating forces. Similar to the TIOI was the TRANSEC Interim Summary (TSIS), which provided higher headquarters with a preliminary evaluation of a particular observed communication practice. TRANSEC Analysis Notes (TAN's) also documented COMSEC findings useful for those working within the COMSEC speciality.

Although PACAF and subordinate organizations down to division level had authority to determine whether a monitored transmission was or was not a security violation, the lack of guidelines for monitors caused many problems. Issued EEI's should have helped resolve this problem, but they could not do so completely. The Seventh Air Force guides to the proper classification of information show the complexity of decision making in this regard. (See table above.) Obviously, a one-hour-prior-to-strike criterion was arbitrary rather than truly denotative of operational sensitivity. Since most strike requests were made within the one-hour period, the classification guide for the most part permitted such information to be sent as unclassified.

*Against the Tide*

AFSS monitors acquired sensitive information on a number of actions and very often operational commanders were able to take corrective measures on the basis of monitoring reports. One subject of especial concern was VIP movements. When President Lyndon B. Johnson in the fall of 1966 went to the Pacific and made an unannounced visit to Southeast Asia, Air Force monitoring uncovered many indications that his movements were being passed in unprotected communications. Reports containing this evidence went to General McConnell, USAF Chief of Staff, who ordered the passing of such information only over secured lines.

At other times monitors reported vital operational information revealed in Air Force communications. Through monitoring and analysis, Detachment 5 reconstructed the entire geographic grid system being used for area target identification along with the code names assigned to identify the grid blocks. The code names were not changed until all targets in a particular geographical area had been hit—often a matter of months. Since MACV and operations personnel used the code names in unsecured communications as much as a month before actual air strikes, enemy foreknowledge was obviously possible. In each strike the MACV air operations personnel, using unsecured communications, called the SAC liaison officer in Saigon about 36 hours before a strike and in approximately one-third of the conversations used the target code name. The top RVN command used unsecured communications when calling the U.S. and Allied field forces to alert them to forthcoming RVN air strikes and also included target identifications through use of the code name approximately one-third of the time. Detachment 5's report to MACV and SAC in September 1966 outlined the dangers of using code names in this fashion.

From mid-1966 through January 1967, monitored U.S. communications disclosed U.S. involvement in the Thai counterinsurgency operations (COIN). Unsecured communications disclosed the types of U.S. aircraft involved and an increased participation. At the time there was no public acknowledgment that U.S. forces were engaged in COIN operations in Thailand.

## CONVENTIONAL COMSEC MONITORING

83

In the spring of 1967, AFSS monitored VHF/UHF unsecured communications at the Nakhon Phanom Air Base in Thailand and found frequent references to TACAN azimuth and range positioning, thus disclosing the orbits and operational areas of flareships, FAC's, and strike and other aircraft. Unsecured HF communications contained information revealing details on special force and air commando components operating within Laos—including air strike activity in support of Laotian Government troops. Six specific recommendations for COMSEC improvement were forwarded with the report of findings.

In the fall of 1967, AFSS teams prepared eleven separate reports setting forth evidence of the misuse or possible compromise of KAC-J, a digital authentication code used for encrypting coordinates and other numerals in direct support operations. AFSS headquarters sent three of these reports to General McConnell to support the need for a replacement code. In March 1968, General John D. Ryan, the commander in chief of PACAF also expressed his concern over the situation to Seventh Air Force and others:

TRANSEC message reports (TSMRS) submitted by Det 5, 6922 SW, during Jan and Feb 68 indicate KAC-J code being compromised when encoded coordinates passed in air strike are later given in plain text in BDA report. PACSCTYRGN cryptanalysts confirm that KAC-J code can be recovered because of this ops procedure. Further, complete compromise occurs when previously encrypted coordinates and TOTS are confirmed by FAC in the clear just prior to air strike to eliminate possibility of errors in target locations.\*

In November 1967, following a Detachment 7 semiannual briefing at Korat Air Base, monitors studied two 388th Tactical Fighter Wing telephone circuits. The monitors were able to recover a substantial part of the daily F-105 and support aircraft status reports and a fair amount of the sorties-flown portion of the reports.

While the list of examples is extensive, there were extenuating circumstances. Lack of sufficient cryptosecurity equipment to encrypt voice communications during the years 1964-67 made impossible the

---

\*CINCPACAF Msg to 7th Air Force and others, sub: 7AF FAC Code, DTG 210243Z Mar 68, SECRET.

securing by crypto-equipment of every voice link over which sensitive information was being passed. Corrective action for voice communications tended to be in the nature of advising the operators as to what should and what should not be transmitted in the clear, of suggesting alternate means of communications that would be secure, and of assuring that appropriate manual cryptosystems were available and procedures for their use were understood. As of September 1967, 1,733 voice channels were in use in the all-Service Southeast Asia Wideband System (SEAWBS). This system, with a 2,775-voice-channel capability consisted of the Vietnam BACK PORCH and the Thailand "Philco Tropo" systems. At least 660 channels of the system were clearly vulnerable to intercept from fixed SIGINT sites within North Vietnam.

General McConnell and commanders at lower levels often took strong action to reduce COMSEC violations. In September 1965 General McConnell approved the releasing of the names of COMSEC violators to their commands (down to the division level), a new procedure that helped to curb violations. At a lower command level, the Seventh Air Force in 1966 established a TRANSEC Review Board, which made regular use of monitor reports to improve various aspects of COMSEC.

Despite these and other Air Force actions, there were far too many instances where the Vietnamese Communists temporarily evacuated their personnel from a target area just before aircraft arrived over the target. Not all of these evacuations were directly attributable to a lack of COMSEC, but enough instances came to light during monitoring and analysis of Air Force communications to suggest that poor COMSEC was a major factor.