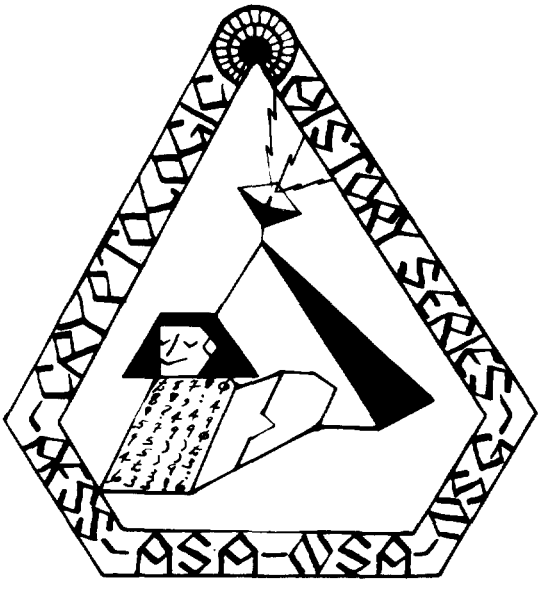
~~TOP SECRET NOFORN~~ #507

48/94

SOUTHEAST ASIA

Working Against the Tide

Part One



THIS DOCUMENT CONTAINS CODEWORD MATERIAL

~~TOP SECRET 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

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] 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

PART ONE

I. THE PROBLEM 1
Division of Responsibilities 2
Enemy SIGINT Threat 2
Major Problems 11

II. CONVENTIONAL COMSEC MONITORING . . . 19
Army Security Agency 21
Naval Security Group 54
Air Force Security Service 72

PART TWO

III. COMSEC SURVEILLANCE 87
The Concept 87
SILVER BAYONET 90
Guam 96
MARKET TIME 109
GAME WARDEN 116
ARC LIGHT 119
PURPLE DRAGON 128

IV. COMMUNICATIONS COVER AND DECEPTION . . 139
Communications Cover 140
Communications Deception 141

V. LESSONS LEARNED 155
COMSEC Education 155
The CC&D Paradox 159
New Concepts for Old Problems 159
Full Treatment for the Patient 163
Better Systems, Better COMSEC 163
Command Emphasis 167

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–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

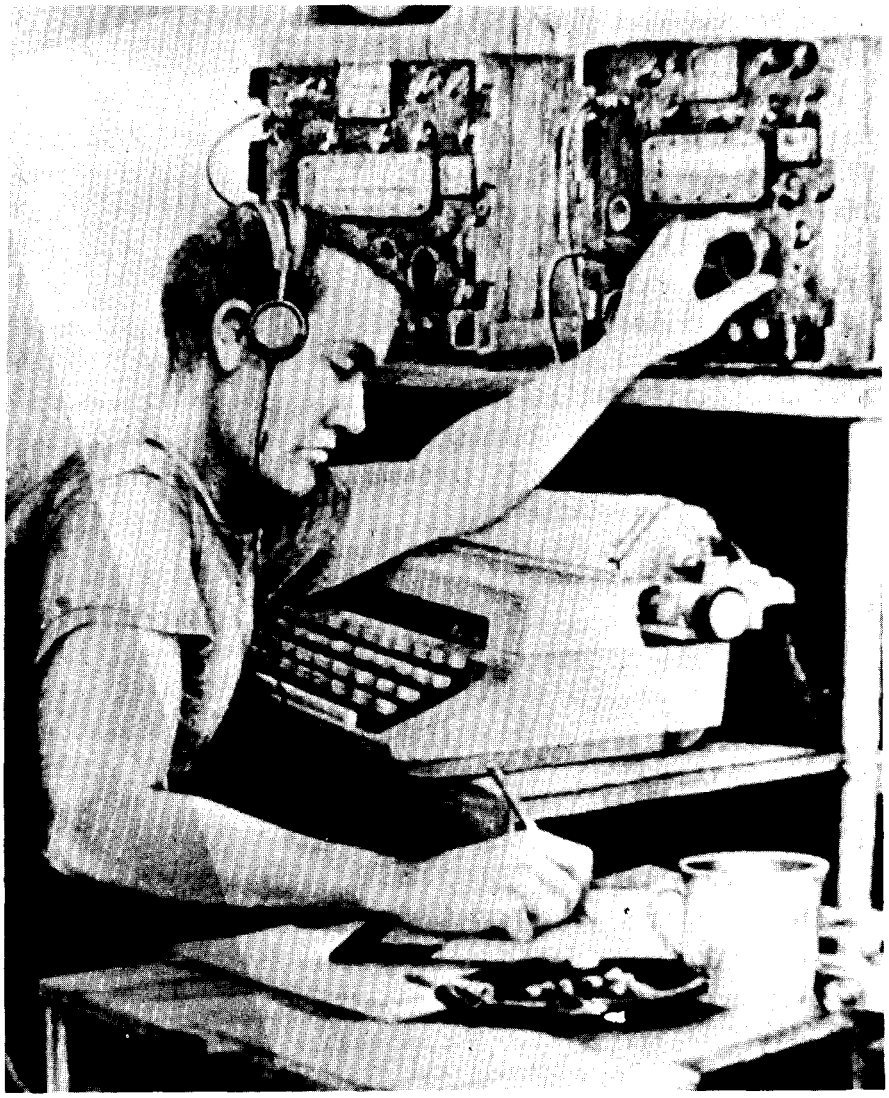
Illustrations

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
[redacted] COMSEC Intercept Vans 66
[redacted] Operations Building 67
KW–26 and KW–37R, USS *Constellation* 70
KL–47, USS *Constellation* 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 *Izmeritel* 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 prupose 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

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.)

North Vietnamese Intercept Operator at Work (Captured photograph)

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

[redacted]

[redacted]

(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"

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

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

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. Henchman, 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 Henchman's battalion, then stating that his unit was lost.

Instructing his radioman to keep the exchange with the "Australian" going, Colonel Henchman, 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 Henchman 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

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

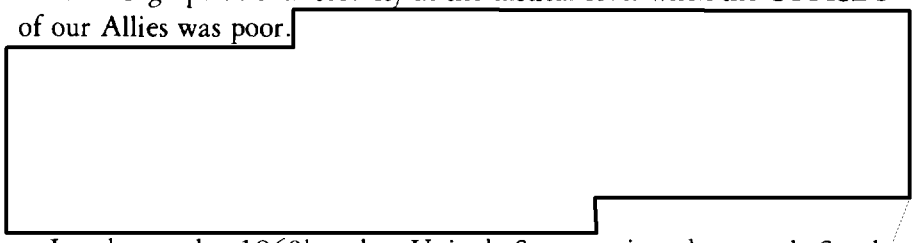
*ASA monitors recorded the complete exchange of communications in this incident, 16 pages in all. Colonel Henchman presented a special report of the episode at the Headquarters, USASA, Annual SIGSEC Work Shop, 3 December 1969. Coincidentally, ABC newsmen and TV crews were at the battalion CP at the time 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

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

(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.

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:

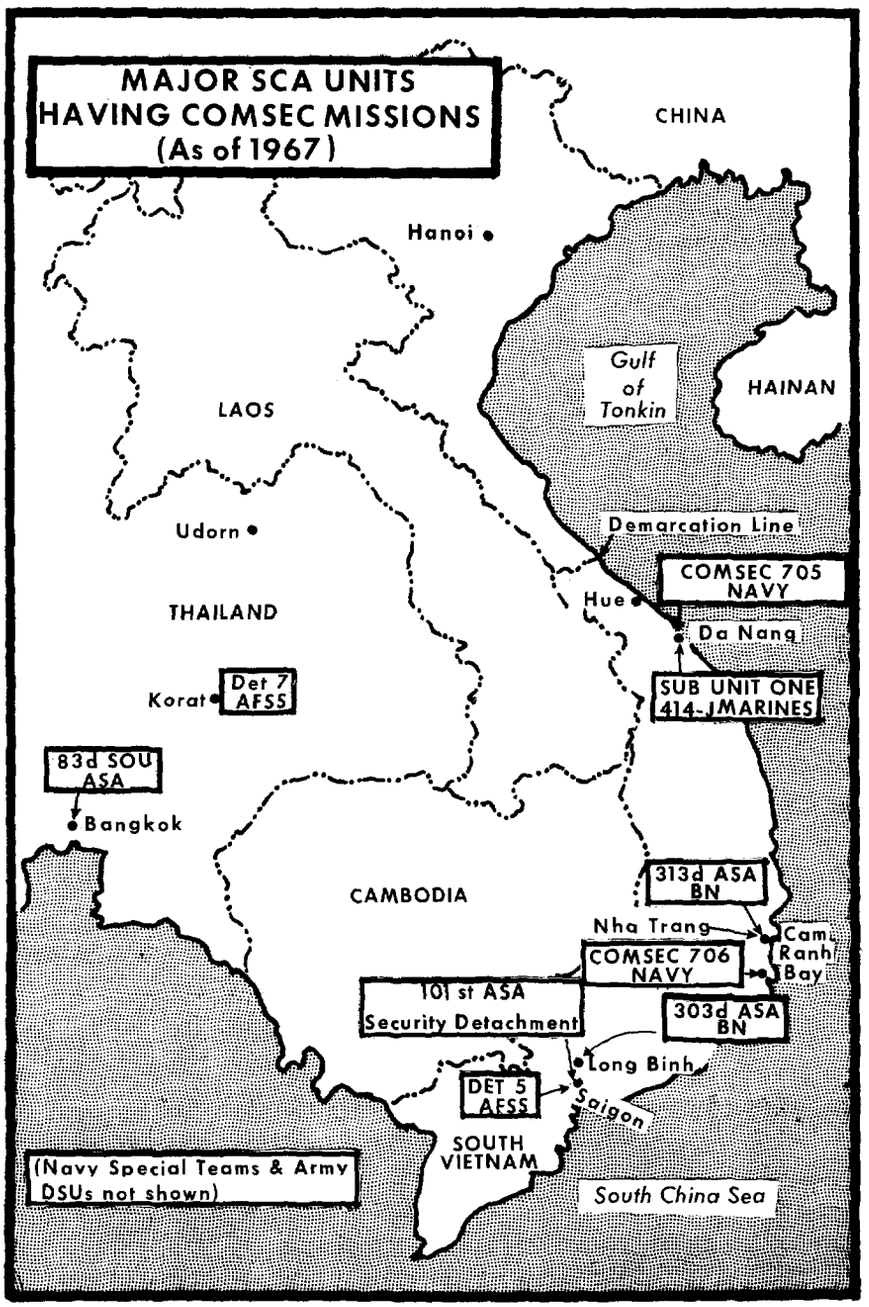
> With regard to COMSEC, it was not good in Vietnam. But, until we can resolve the problem of sufficient frequencies and multiple allocations for tactical units, we won't be able to do much toward the basis of COMSEC application. If there were enough frequencies, with alternates allocated to various 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 multinets—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.


MAJOR SCA UNITS
HAVING COMSEC MISSIONS
(As of 1967)
CHINA
Hanoi
Gulf of Tonkin
HAINAN
LAOS
Udorn
Demarcation Line
COMSEC 705 NAVY
THAILAND
Hue
Da Nang
Det 7 AFSS
Korat
SUB UNIT ONE 414-J MARINES
83d SOU ASA
Bangkok
313d ASA BN
CAMBODIA
Nha Trang
Cam Ranh Bay
COMSEC 706 NAVY
101 st ASA Security Detachment
303d ASA BN
Long Binh
DET 5 AFSS
Saigon
SOUTH VIETNAM
(Navy Special Teams & Army DSUs not shown)
South China Sea

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 callsign 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.)

COMSEC Personnel World-Wide
(FY 1967)

	Army		Navy		*Air Force*	
	Pers	%	Pers	%	*Pers*	%
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 [redacted] 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] 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

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 [redacted] 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 [redacted] 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 [redacted] more men were assigned and another [redacted] 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] 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

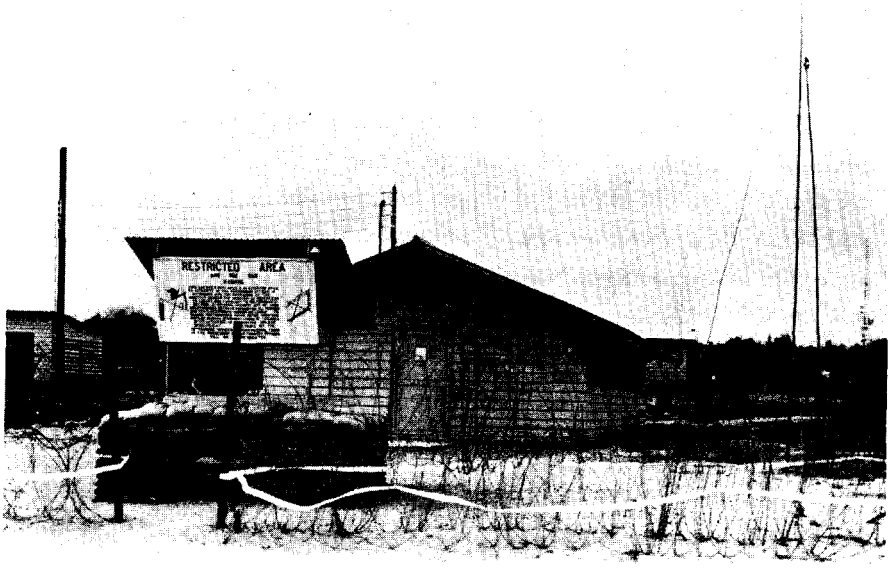
Platoon was in Can Tho. Detachment 1 of the 101st SD worked in the MACTHAI-JUSMAAG compound in Bangkok, Thailand, and an *ad hoc* Capital Monitoring Team of two positions and six men, formed by direction of MACV, covered switchboards in the Saigon-Cholon headquarters complex.

The 101st had responsiblity 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 [redacted] men and operated from [redacted] 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 [redacted] men for COMSEC functions, and operated from [redacted] positions. The DSU detachments and platoons gave COMSEC assistance at brigade and battalion levels. Generally, platoons had about [redacted] COMSEC specialists [redacted] As an exception, heavy separate detachments served the Armored Cavalry regiment and mechanized brigades. Each heavy separate detachment had a COMSEC officer, [redacted]

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

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

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

1967. In June of that year, authorized COMSEC spaces in the 509th Group totaled [redacted] by October 1967 the total had increased to [redacted] of which about [redacted] 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

(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

Unit Designation[a]	*Unit Cover Name*[a]	*Arrived SEA*	*Supported Command*
USASA Company, Saigon (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) 408th RRD	Aug 66	Americal Div 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 (83d SOU)	U.S. Field Station, Bangkok	Sep 59	COMUSMACTHAI

[a] Earlier names shown parenthetically.
[b] Actual strength; authorized strength in parentheses.
[c] All officer personnel and 6 enlisted men of 101st SD were COMSEC surveillance specialists.
[d] 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,

-Continued

Base Location	*COMSEC Positions*	*Total COMSEC Personnel*[b] *Officers*[c]	*EM*	*Monitors*	*Analysts*
Saigon (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

USASA COMSEC Positions in SEA, FY 1964–68

Unit[a]	
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	

[a] 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.

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

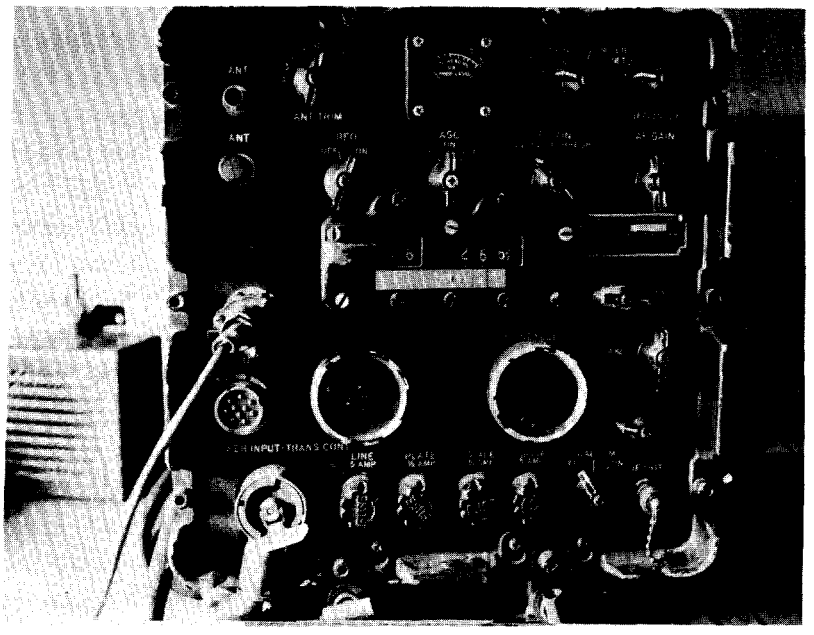
[c] Read figures as "Authorized/Actual (Employed)." Actual varied with availability and mission requirements during annual periods.

[d] Inactivated in FY 1966.

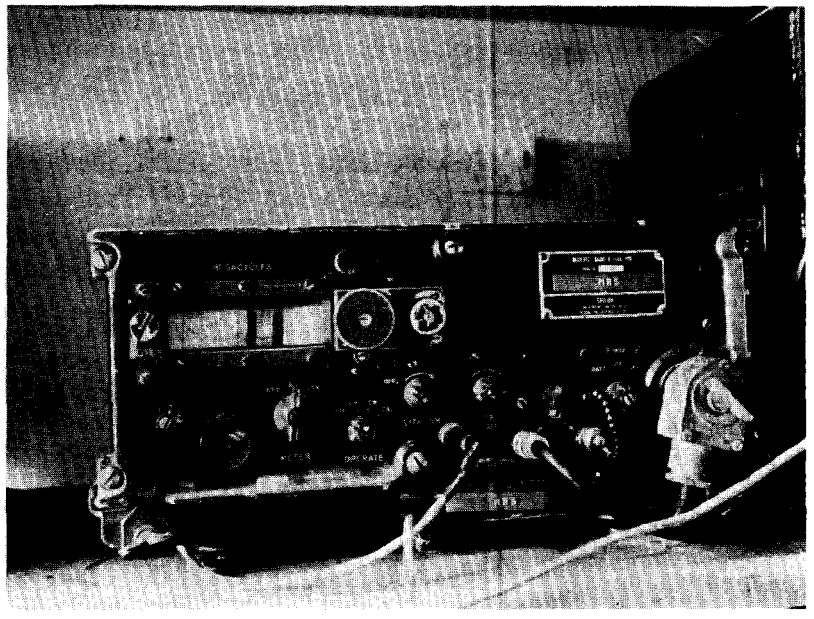
[e] Reactivated in support of a different unit in FY 1968.

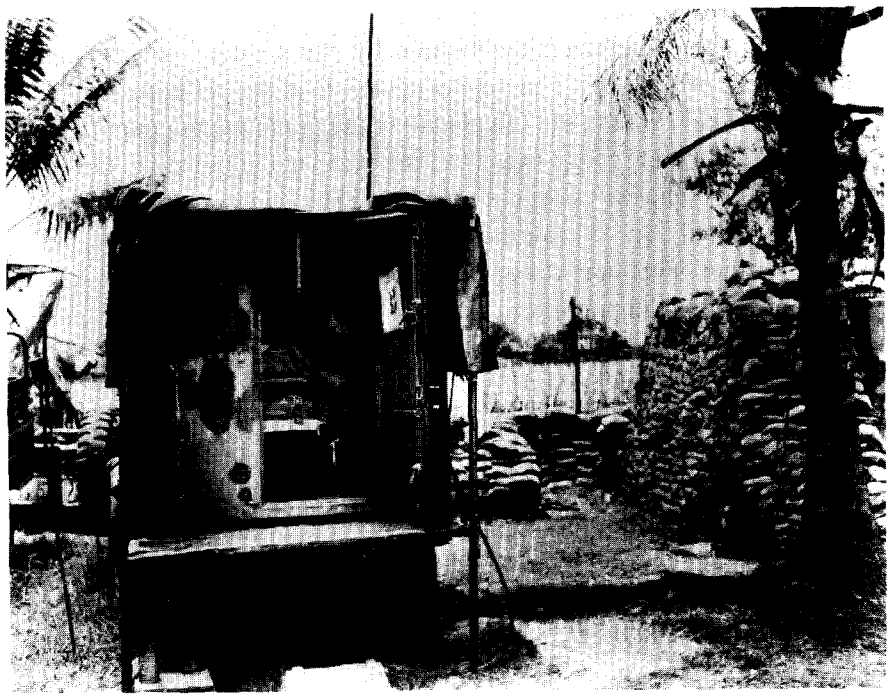
[f] Eliminated in 1967.

(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.





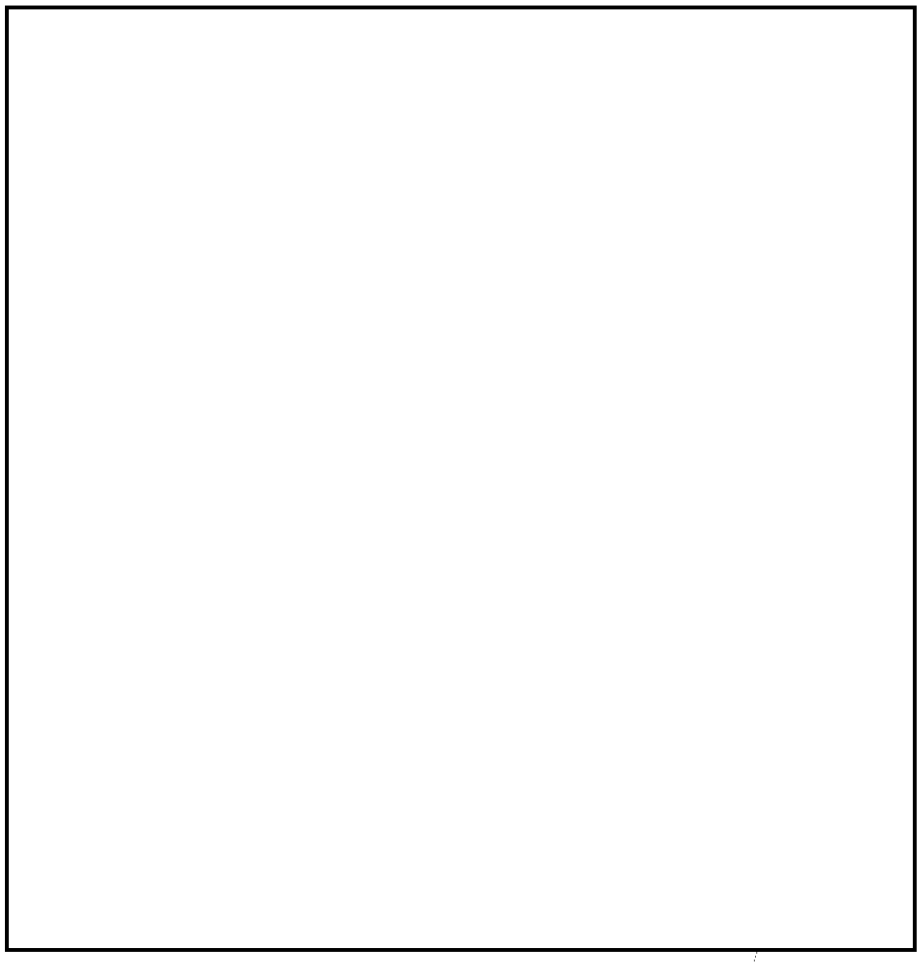
MRPZ-3 COMSEC Position at Diep Hoa, with sandbagged shelter at right and generator trailer at left. Such positions are connected with field analysis centers.

[redacted]

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.

[redacted]

(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

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	1,665,068	7,183,563

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] 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

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 went 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 conversion between the general and the

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

Category	*Number*
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.

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

	Reported Rates of Violations (Per 1,000 transmissions)									
Year	*R/T*			*Conv Telephone*			*RTTY*			*Average Violation Rates*
	Nr.[a]	*TSV*	*PDS*	*Nr.*[a]	*TSV*	*PDS*	*Nr.*[a]	*TSV*	*PDS*	*Per 1,000*
1965	—									2.93[b]
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

[a] Expressed in thousands.

[b] 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

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

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

[redacted] 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

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. Adherance 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.

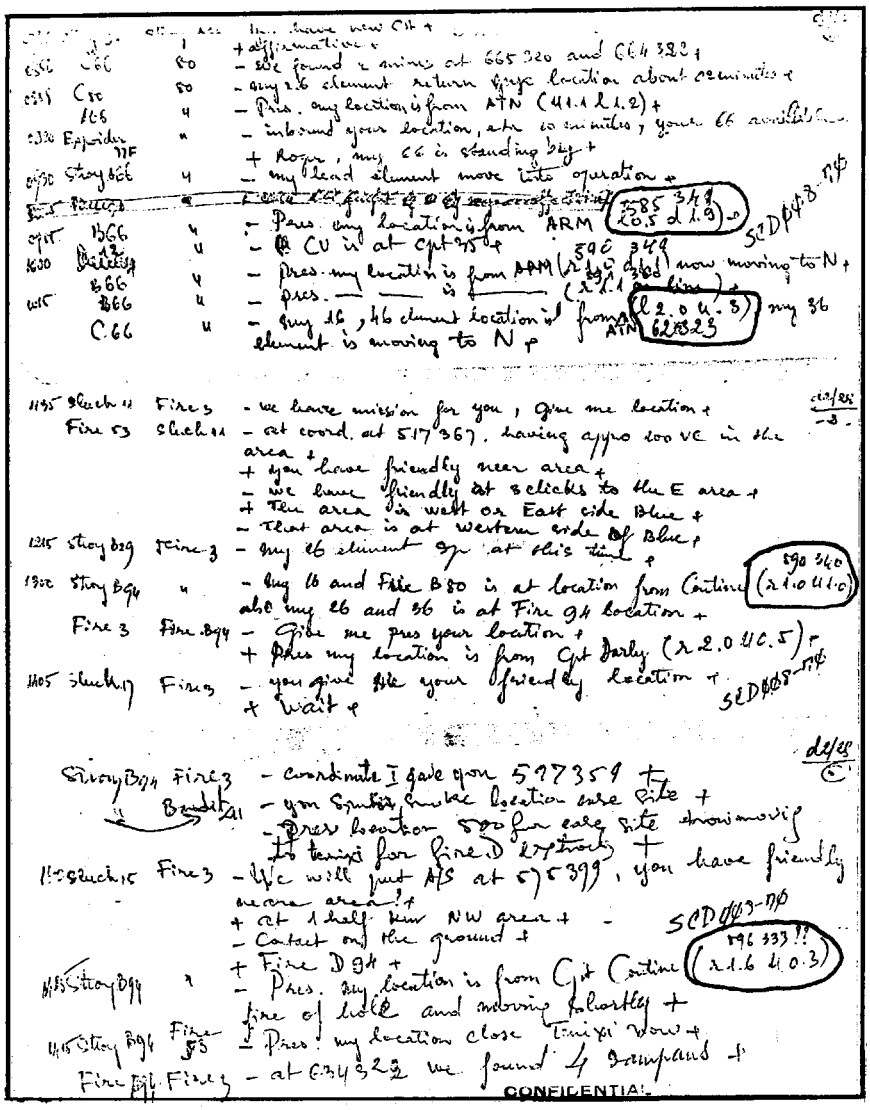
d. Maintain uniformity of appearance of callwords and expanders within major tactical commands by using authorized callword allocations and manners of callword expansion.

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



Enemy Intercept of U.S. 1st Infantry Division Communications. (Note that the intercept operator has converted and penned in the actual coordinates beside the copied point-of-origin code. Source: ASA TAREX unit.)

TIME OF INTERCEPT	U.S. COMMUNICATORS		DATE	VOICE NET
				D2/2 2
0745	Stroy 91	Stroy A66	You have new CH+ +Affirmative+	
0850	C66	80	We found 2 mines at 665320 and 664322+	
0848	C80	80	My 26 element return my location about 02 minutes+	
	A66	"	Pres my location is from ATN (U1.1 L1.2) +	
0920	Expoider 77F	"	Inbound your location, eta 10 minutes, your 66 available?+ +Roger, my 66 is standing by+	
0930	Stroy A66	"	My lead element move into operation+	
0955	B66	"	Pres my location is from ARM (Lo.5 D1.9) ((585341))	
1000	B66	"	CV is at CPT 35+ Pres my location is from ARM (R1.0 D1.1) ((590349)) now moving to N+	
1015	B66	"	Pres my location is from ARM (R1.1 on line) ((591360))+	
	C66	"	My 16, 46 element location is from ATN (L2.0 U0.3) ((620323)) my 36 element is moving to N+	
				D2/28 2
1135	Sluch 11	Fire 3	We have mission for you, give me location+	
	Fire 53	Sluch 11	At coord XT 517367, having appo 100VC in the area+ +You have friendly near area+ We have friendly at 3 clicks to the E area+ +The area is west or east side Blue+ That area is at western side of Blue+	
1215	Stroy B29	Fire 3	My 16 element sp at this time+	
1300	Stroy B96	"	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+	
	Fire 3	Fire B94	Give me pres your location+ +Pres my location is from CPT DARLEY (R2.0 U0.5)+	
1405	Sluch 17	Fire 3	You give me your friendly location+ +Wait+	
				D2/28 5
	Stroy B96	Fire 3	Coordinate I gave you 597354+	
	"	Bandit 41	You pass smoke location your site+ Pres location 500 for last site now moving to Temixi for Fire D extraction+	
1400	Sluch 15	Fire 3	We will put A/S at 575399, you have friendly near area+ +At 1 half KM NW area+ Contact on the ground+ +Fire D94	
1405	Stroy B96	"	Pres my location is from CPT COUTINE (R1.6 U0.3) ((896333)) Fire of hold and moving shortly+	

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.

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.

" 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 XT400800 ON THE 345/44 BIEN-HOA TACON, ALL A/C 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 blantantly 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.

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 [redacted] of which a team of an officer and [redacted] 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

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

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.

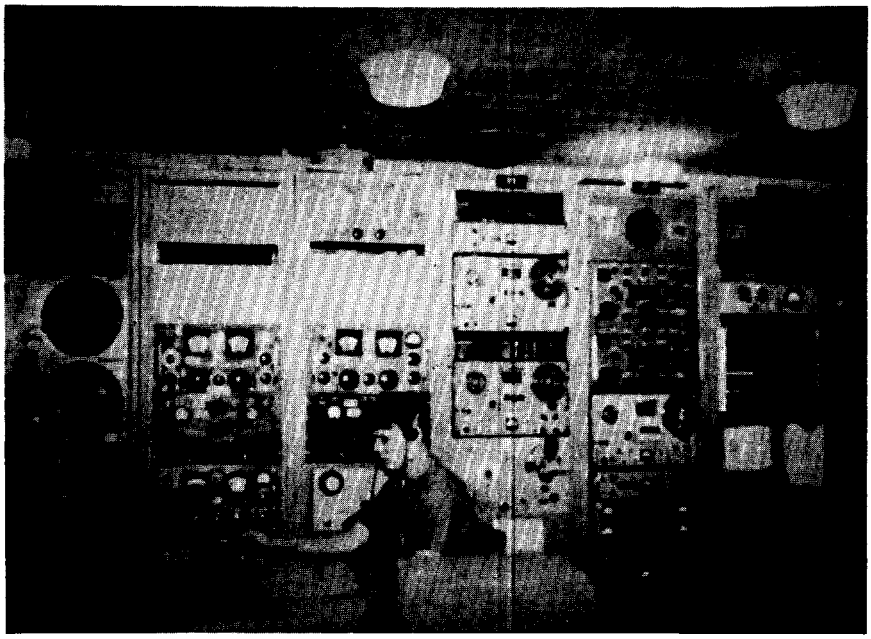
On 29 May 1965 Commanding General, Fleet Marine Force, Pacific (FMFPAC), Lt. Gen. Victor H. Krulak, noted that the COMSEC team at Da Nang had done an outstanding job in helping to tighten security on radio nets of deployed Marine units. The COMSEC support provided to Navy and Marine Corps units at Da 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 [redacted] COMSEC positions among its resources. This detachment carried on the COMSEC functions that had been performed by COMSEC Team Vietnam (C). The [redacted] positions were increased to [redacted] in January 1966 when Detachment J was deactivated and its men and equipment became part of Sub Unit One, First Radio Battalion [redacted] 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

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



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 [redacted] 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

(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.

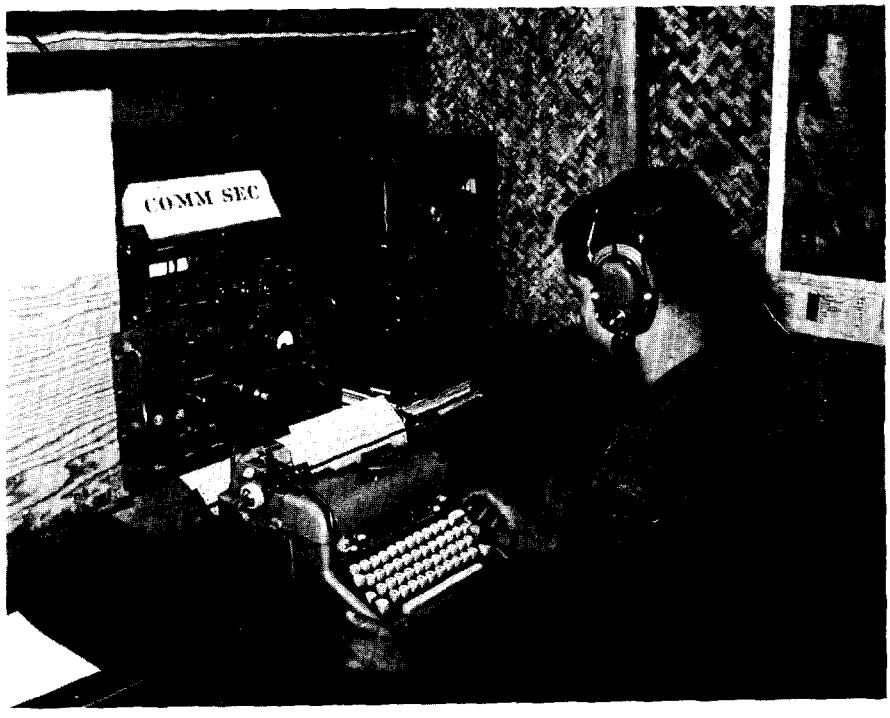
Thus, by December 1965 Navy COMSEC personnel in the Western Pacific numbered [ ] officers and [ ] enlisted men; COMSEC elements totaled 5 COMSEC components plus a team afloat.

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.

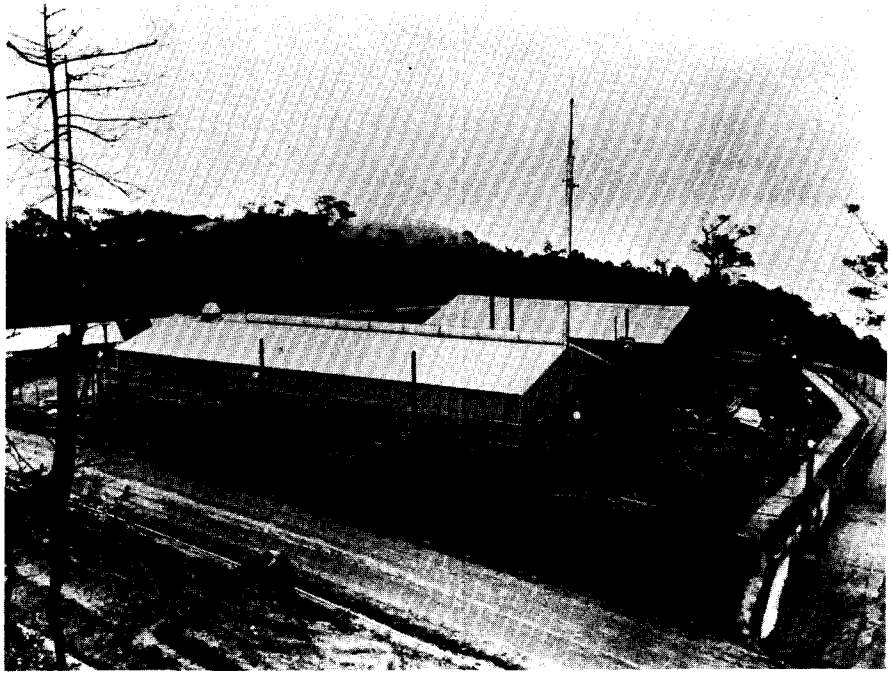
(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36



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



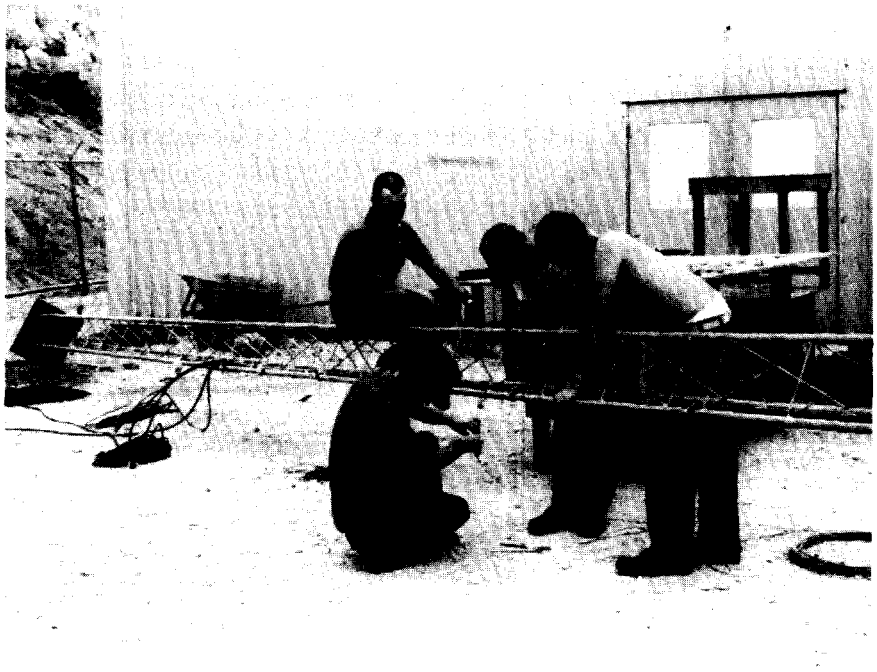
COMSEC 705 Location at Foot of Monkey Mountain

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 [redacted] 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

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



COMSEC Specialists Assembling an Antenna, Monkey Mountain

as COMSEC Team Two, the unit began operations in June 1966 with one officer and [redacted] 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 [redacted] 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 perseonnel 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

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 [redacted] men and [redacted] positions, the Navy's Western Pacific COMSEC organization expanded during this period to [redacted] men and [redacted] positions—[redacted] monitoring, [redacted] frequency measuring, and [redacted] 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	*Use*
R-390A	shore facilities for HF communications
SP-600	shore facilities for HF communications
R-274B	shore facilities for HF communications
R-1279 with CV-1750 range extender	VHF communications
R-389	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:

Type of Communications	*Estimated Percentage of Total Traffic Monitored*
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

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.

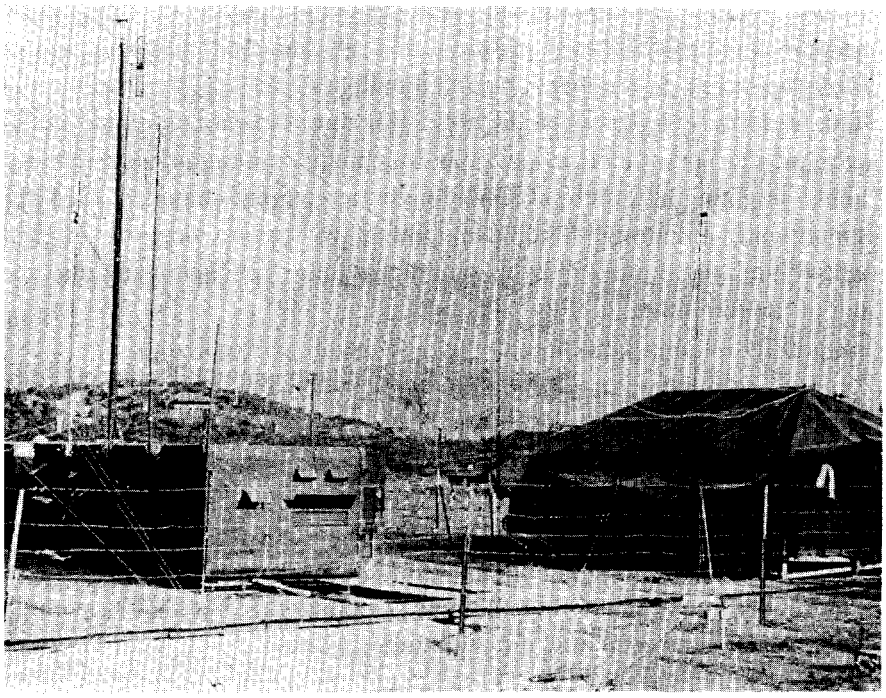
Sub Unit One, First Radio Battalion Sub Unit One had COMSEC positions at the various locations of its detachments during the years 1964–68. In early 1966 it had 2 positions at Chu Lai, 2 at Da Nang, and 1 at Phu Bai. In the fall of 1968 it had 2 at Camp Carroll, 2 at Dong Ha, 1 at Hill 327 near Da Nang, and 1 at Vandergrift Fire Support Base. While the subunit usually had [redacted] 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 [redacted] 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

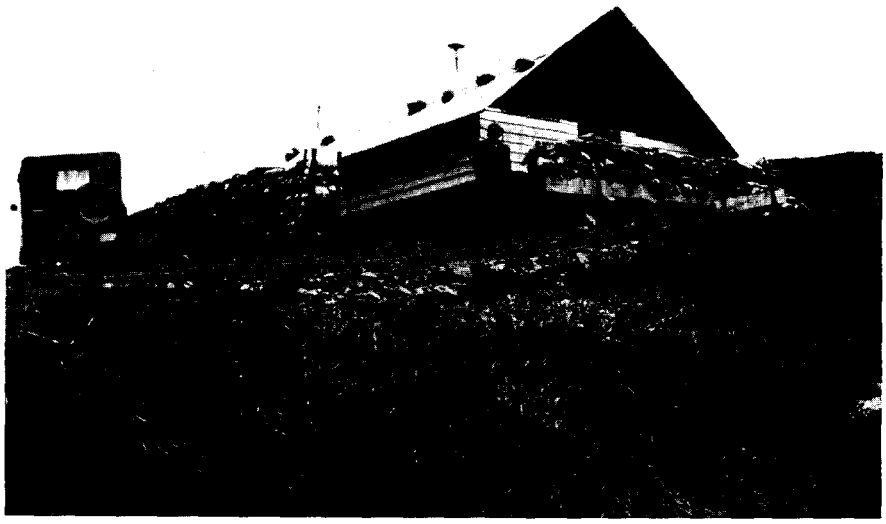


[redacted] COMSEC Intercept Vans and Operations Tent, Chu Lai

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



[redacted] 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

(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.

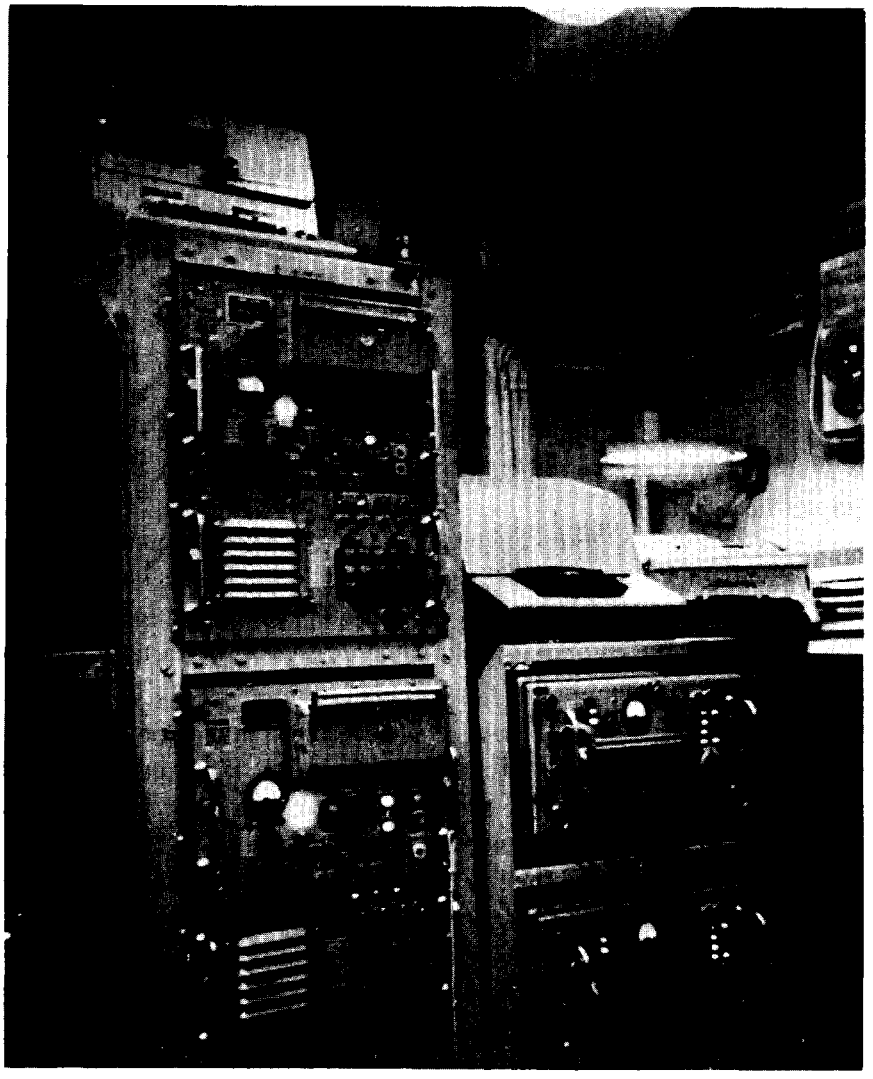
While only a rough measure of actual violations occurred, these Sub Unit One reports provided an indication of COMSEC status reliable enough for value judgments. During the last three months of 1968, the average number of monitored transmissions for each month remained approximately the same, yet the 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.

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.

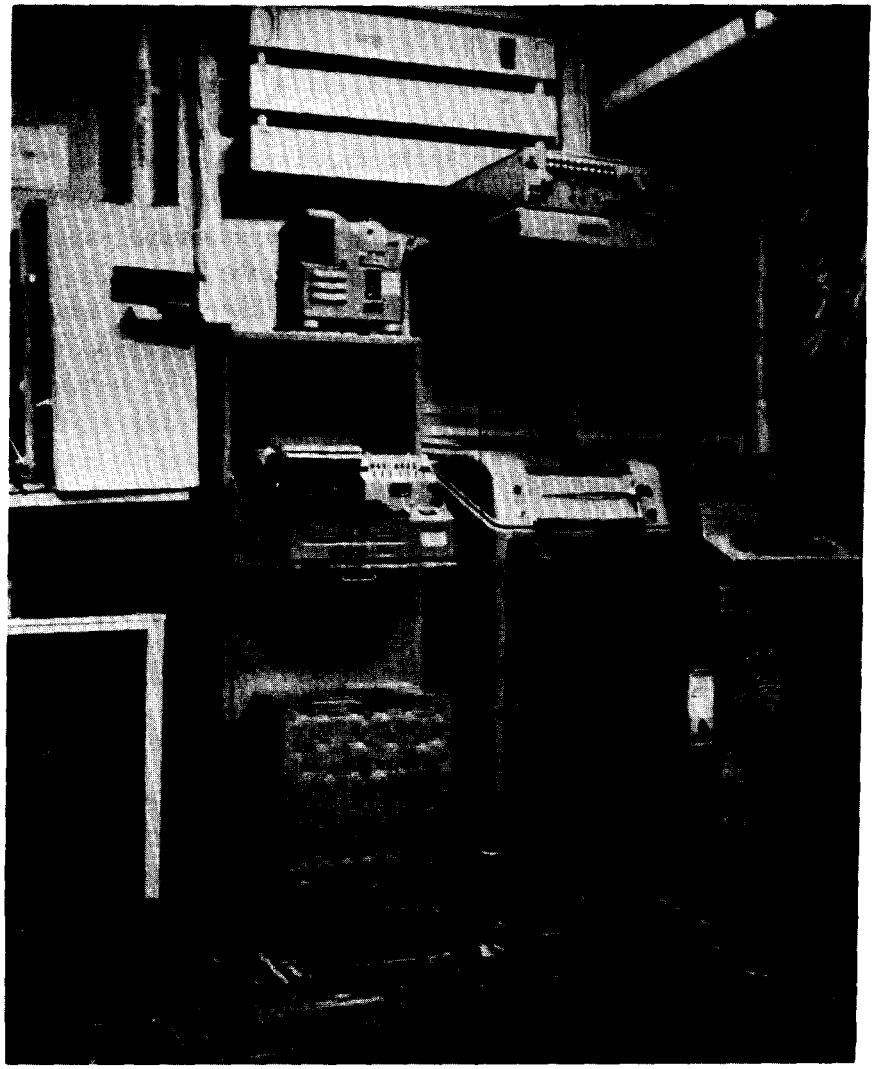
Most important, the many reports prompted command actions directed toward WESTPAC communications discipline. For example, the commander of the Seventh Fleet issued a general message reiterating and explaining encrypt-for-transmission-only requirements. At the next higher level, the commander in chief 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 (PACSCTYRGN) 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.

PACSCTYRGN 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. PACSCTYRGN'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 PACSCTYRGN 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] 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

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.

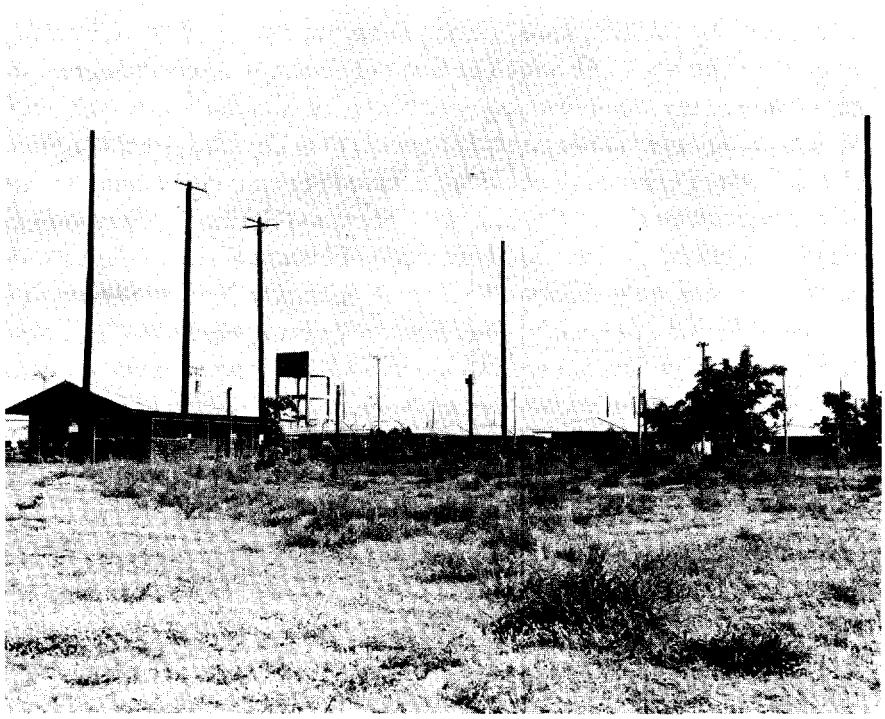
Detachment 5, 6922d Security Wing As outgrowth of these early actions, on 8 April 1965 PACSCTYRGN deployed a [redacted] COMSEC team and a mobile H–1 van to the Tan Son Nhut Air Base near Saigon. The deployment was on a TDY basis pending a request to General John P. McConnell, the Chief of Staff, USAF, for a personnel ceiling increase in South Vietnam permitting a [redacted] 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 [redacted] airmen. Equipment approved for the detachment included [redacted] 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 [redacted] HF (8761), [redacted] VHF/UHF (887–EII), [redacted] telephone (AG–275), and [redacted] transcribe positions (AG–4). One more telephone position came at the end of 1967.

Government Note

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

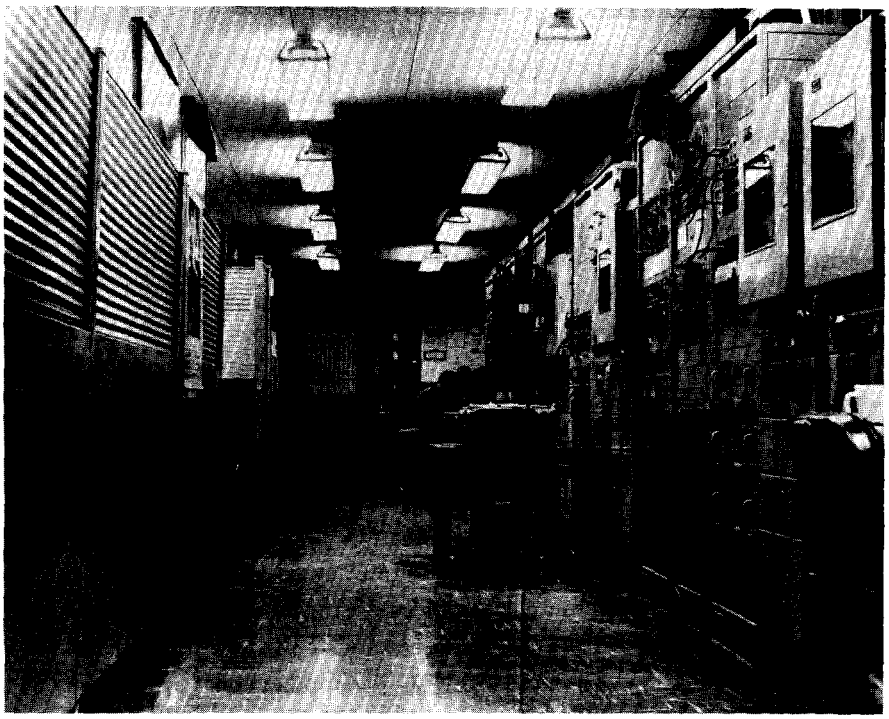


Detachment 7, 6922d Security Wing, Buildings, Korat

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 [redacted] more R/T (radiotelephone) positions and one more HF position plus [redacted] more personnel. To cover South Vietnam adequately at least [redacted] more TRANSEC units of [redacted] 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 [redacted] men with equipment for monitoring troposcatter, HF, and UHF/VHF communications.

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



Detachment 7, 6922d Security Wing, Positions, Korat

[redacted]

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 [redacted]

*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

Date	*Place*	*Communications Targeted*
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 6924th SS	USAF VHF/UHF frequencies
17 Nov–26 Nov	Monkey Mt. site of 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 [redacted] This was still below the authorized strength of one officer and [redacted] airmen.

By the end of 1967, [redacted] 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, [redacted] 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

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

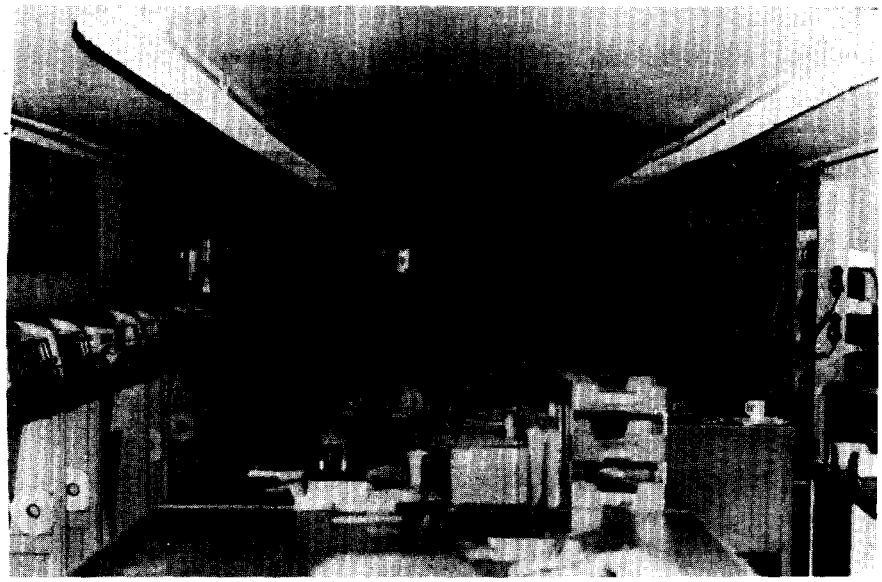
(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 403
(b)(3)-18 USC 798

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

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



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

Seventh Air Force Classification of Information

Planned or Completed Missions (In-Country)	*Classified*	*Declassify*
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.

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.

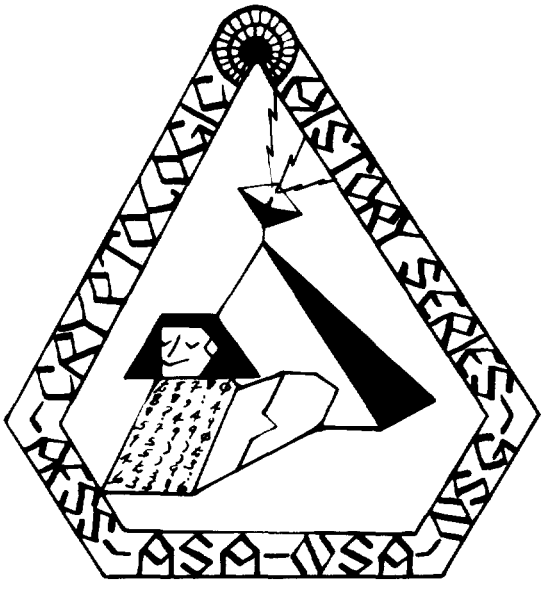
Despite these and other Air Force actions, there were far too many instances where the Vietnamese Communists temporarily evacuated their personnel from a target area just before aircraft arrived over the target. Not all of these evacuations were directly attributable to a lack of COMSEC, but enough instances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

~~TOP SECRET NOFORN~~

SOUTHEAST ASIA

Working Against the Tide

Part Two



THIS DOCUMENT CONTAINS CODEWORD MATERIAL

~~TOP SECRET NOFORN~~

CRYPTOLOGIC HISTORY SERIES

SOUTHEAST ASIA

Working Against the Tide

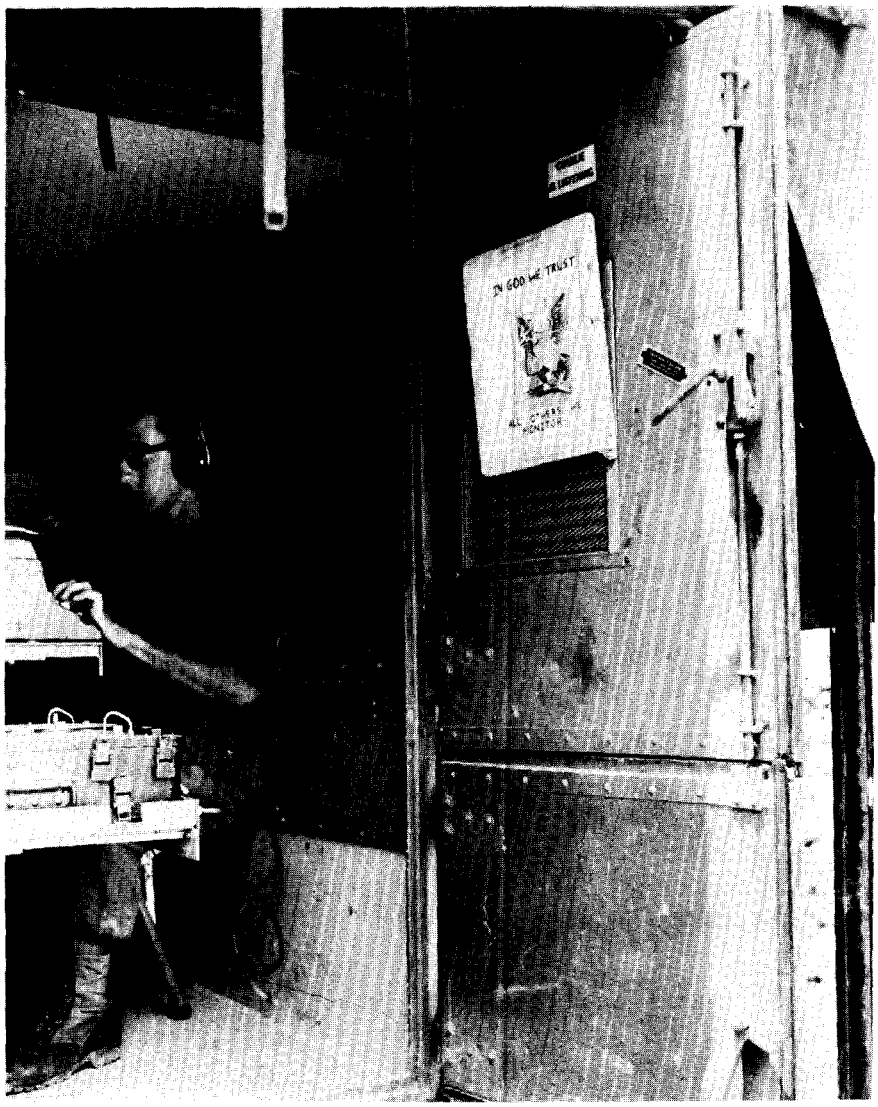
(COMSEC Monitoring and Analysis)

PART TWO

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.


IN GOD WE TRUST

CHAPTER III

COMSEC Surveillance

The Concept

In the mid-1960's, COMSEC specialists began to encourage a new approach to the problem of insecure communications, one in which the rules of the game in monitoring were considerably altered. The new approach, termed *surveillance*, called for the inclusion of COMSEC safeguards in planning military operations, thus averting, except for operator error or other unforeseen circumstances, most security malpractices. COMSEC analysts worked with the communications planners and others fully knowledgeable in operations. Most important, they had access to information that would assist them. As normally practiced under conventional monitoring procedures, monitors and analysts worked in relative isolation from operational planners and had little access to information about frequencies, call signs, and schedules employed by U.S. units unless it had been acquired from previous monitoring.

Initiated in part as a result of a visit by NSA COMSEC specialist Mr. (b)(3)-P.L. 86-36 to CINCPAC in the summer of 1965 and outlined in an NSA letter of 23 December 1965 to the three Services, COMSEC surveillance had as its immediate objective the correction of communications malpractices in the Pacific war area, with world-wide application as its longer range goal. In December 1965 Admiral Sharp, CINCPAC, issued to his commanders a directive on surveillance that outlined the role of the COMSEC surveillance specialist.

Coordinate with commanders' staffs to determine what traffic must flow during planning and implementation phases;

Amalgamate information derived with that available through previous COMSEC monitoring and analysis;

Determine the participating communications facilities and the relative speed and security of all communications involved;

Prepare recommendations for handling operational traffic (e.g., communications procedures and use of cryptomaterials);

Conduct selective monitoring during the operation to test the effectiveness of previous actions;

Advise participants of results with recommendations for change.*

As the first NSA COMSEC representative to be permanently stationed in the Pacific and serving as a member of the Headquarters, NSA Pacific (NSAPAC) staff, [(b)(3)-P.L. 86-36] helped introduce and promote COMSEC surveillance. Changing over to the new approach was, however, a slow process, in part because of the shortage of qualified COMSEC specialists. Most of the COMSEC monitors in Southeast Asia, in fact, were still using the traditional approach at the end of 1967.

While improvement of COMSEC was the goal of both conventional monitoring and surveillance, the new approach was more *preventative,* and conventional monitoring more *curative.* Under the new concept, COMSEC units de-emphasized broad monitoring coverage and intensified selective monitoring to achieve specific goals. COMSEC personnel served more frequently as advisors and preplanners. By the end of 1967, SCA's began to identify some COMSEC personnel as surveillance specialists, distinguishing them from others working strictly as monitors and analysts. In conventional monitoring the COMSEC analyst, working in isolation from the communications operator, often had an "electronic spy" or policeman's image. As a surveillance specialist, he became a member of the team who helped prevent and overcome communications security problems. The COMSEC surveillance concept reached its best application to that date in the PURPLE DRAGON operational security survey of 1966–67.** The cutting edge of COMSEC surveillance was that it represented command recognition of the importance of COMSEC and, in so doing, facilitated change in procedures when COMSEC considerations demanded them.

In the years to 1968 the SCA's, NSA, and the military commands undertook six major COMSEC monitoring or surveillance operations to attain specific objectives. One dealt with Army communications in

*CINCPAC 040354Z Dec 65.

**See pp. 128–38.

Close Cooperation Between ASA COMSEC Personnel and Infantrymen

Vietnam, two concerned Navy communications in the offshore waters and riverways of South Vietnam, and three examined the communications of all three Services.

The six studies, here presented in rough chronological order, show to some degree the increasing trend toward the use of COMSEC surveillance as opposed to conventional monitoring, although it is not always possible to distinguish one from the other. The Guam study, the second in the series, was a Navy-Air Force-NSA operation employing the NIGHTSTICK concept—inspecting all communications in a given area simultaneously for over-all COMSEC evaluation. This represented, of course, a departure from the isolated, single-Service study normal in conventional monitoring. Although CINCPAC and NSA were developing the surveillance concept during these years, the key element of precommunications COMSEC planning was largely absent from the Guam study and from the SILVER BAYONET, MARKET TIME, and

GAME WARDEN studies undertaken in 1965 and the first part of 1966.

For the mid-1966 ARC LIGHT study, Admiral Sharp, CINCPAC, specifically requested the application of the surveillance concept, and at the end of that study expressed his dissatisfaction with the methods as applied. In CINCPAC's PURPLE DRAGON operation, the Services successfully employed the surveillance concept, involving the COMSEC specialists in the preplanning stages of the operation and giving them access to all necessary information. PURPLE DRAGON demonstrated fully the merit of the surveillance concept.

SILVER BAYONET

The first special COMSEC study involved the Army's SILVER BAYONET operation of late 1965. In the fall of that year the North Vietnamese 325th Division entered South Vietnam and attacked the U.S. Special Forces Camp at Plei Me on 19–20 October. The 1st Cavalry Division, launching a relief and pursuit operation called SILVER BAYONET against two regiments of the 325th Division, engaged the enemy in the Ia Drang river valley near the Chu Pong Massif, very close to the Cambodian border. As the engagement developed, the North Vietnamese Army forces turned out to be larger than anticipated and, in contrast to the Viet Cong's normal casual attire, were wearing military uniforms. The enemy fought tenaciously and, in contrast to most Viet Cong actions, held its ground. Between 16 and 24 November, the North Vietnamese forces introduced a third regiment and succeeded in drawing a task force from the 1st Cavalry Division's 3d Brigade into a hammer-and-anvil ambush. U.S. losses were heavy. Were it not for U.S. air support, including tactical employment of B–52 aircraft from Guam, and for the 1st Cavalry's air mobility, the outcome might well have been a U.S. disaster. The majority of the U.S. losses during the operation—326 killed and 602 wounded in action—were inflicted in the 2-day period of the ambush. Postoperations studies showed that the North Vietnamese were prepared for the battle with supply dumps, a hospital, and a rest, recuperation, and replacement camp just across the border in Cambodia.

During SILVER BAYONET the 371st ASA Company and additional ASA COMSEC units gave the 1st Cavalry Division limited monitoring support, but the 371st was unable to deploy its COMSEC personnel and equipment with the division when it originally moved out because the company could not get air transportation. On 23 November, when SILVER BAYONET was almost over, one COMSEC position did deploy to the forward Division Tactical Operations Center (DTOC) at Pleiku, where it monitored 18 to 24 hours a day for two days. The position then moved back as the DTOC returned to its base camp at An Khe in Binh Dinh Province. Thus the volume of traffic from close-in monitoring was small in comparison with the material actually sent. In addition to the two days at the divisional center, for the entire period of the engagement other COMSEC personnel monitored the division's radiotelephone communications from the base camp at An Khe, from which the ASA specialists could hear only one side of the conversation because of the two-channel send-receive techniques the division employed.

For its communications, the 1st Cavalry Division had the on-line KW–7 with AN/MRC–95 radios to secure teletype communications between battalion, brigade, and division tactical operations centers. Off-line KL–7 equipment* was at the division and lower echelons down to company. The division had AN/VRC–47 and AN/PRC–25 radios for radiotelephone communications. On these, all traffic went out in plain text unless encrypted in the manual systems available. The division did make some use of an operations code, a numerical code, a map coordinate code, and an authentication system of KAG–24.

Monitoring of 1st Cavalry Division communications showed that the division did not make full use of the cryptomaterials it had at hand, nor did it exercise discretion in what it sent out in clear language. Although the division had secure KL–7 equipment, records show that the cavalrymen did not use it during this period, nor did they use manual systems to good effect. Commenting on SILVER BAYONET, one ASA officer unofficially stated that he did not think any codes were used after

*The KL–7 equipment provides much faster encryption and decryption of normal text than do manual codes. Normally, if a communicator were going to encrypt at all, he would select the KL–7 rather than a manual code.

KL–7 Off-line Cryptographic Equipment (center), which Cavalrymen did not use in SILVER BAYONET.

the first shot was fired.* ASA noted in a later official assessment, however, that the KW–7 on-line equipment was used to full advantage. But, even here, study of the KW–7 traffic for the period did not reveal the significant traffic volume peaks to be expected in an operation of the scope of SILVER BAYONET. Thus some question arises as to whether or not the on-line equipment was used to maximum advantage.

Since KL–7's were not used for intrabattalion and lower echelon communications, these had to be encrypted by manual systems, many of which were cryptographically insecure, being of local construction and not authorized by ASA or NSA.

*Maj. Gen. John R. Deane, Jr., who held command positions in South Vietnam in 1966 and 1967, made the following related statement on the use of manual systems: "We made use of the codes and COMSEC equipment available to encode operational messages, plans and preparation in advance of forthcoming operations, although, once in action, we used voice radio largely without formal codes to gain reaction time. We used convenience codes and coded location references, but generally, the use of the KAC pencil-and-paper OPCODES took too long for tactical requirements."

A 101st Security Detachment COMSEC study of communications monitored just before, during, and just after SILVER BAYONET gave a large number of instances in which sensitive information passed in the clear and in which other insecure practices abounded. The study analyzed SILVER BAYONET communications for three periods. During the first period, 1–23 October, ASA units monitored 10,902 transmissions in three types of communication: radiotelephone, radioteletype, and CW. These revealed a high rate of disclosures of classified information such as U.S. identifications of enemy locations, frequency allocations, plans, operations, logistical information, and classified equipment capabilities. Communicators did not use authentication even though such systems were available. There were many incidents, for example, of operators accepting plain language cancellations of spot reports and of establishing initial communications contact without offering or presenting a challenge for station or message authentication. 1st Cavalry Division units did not change frequencies and call words, and communicators at all echelons appeared to have little knowledge of which types of information would aid the enemy.

During the second period, 24 October–20 November, the ASA specialists monitored 28,023 radiotelephone transmissions and observed again many disclosures of classified information, including troop movements and friendly locations, compromises of call words and frequencies, and failure to use prescribed authentication procedures. In one very serious case, a U.S. operator was requested to transmit the locations of all his units and to make contact with his South Vietnamese counterpart and ask him to do the same. The exact location of that command and three subordinate units went out in an unauthorized, insecure map coordinate code commonly used throughout the division. The operator had given the requested information without a challenge for authentication. Within 20 minutes the ASA COMSEC element, without the use of collateral information, deciphered the coordinates. In general, the COMSEC weaknesses in the second period of monitoring were much the same as those of the first period. COMSEC reports for the first period had no significant effect on communications practices.

In the third period of monitoring, 21 November–20 December, ASA units collected 35,000 radiotelephone transmissions. Analysis of these showed only a marginal improvement, though the division units were no

longer in heavy combat. Authentication was used more frequently, and communicators and commanders appeared to be more aware of the need for COMSEC but, as in the first two periods, classified information on friendly locations, plans, and operations still appeared in unsecured communications. During this period it was pointed out to the division that there were insufficient callword assignments to the division's radio stations, which resulted in the compromise or linking of the call words, nets, and frequencies in use. Also during the period, an unauthorized operations code appeared, as did an unauthorized version of a map coordinate code. As an interim corrective measure, ASA advised the division to use KAG–21 codes for map coordinates until such time as the KAC-J, an NSA-produced code for encrypting numerals and for authentication, became available to the division.

The Ia Drang battle received wide attention in the U.S. press. Within the cryptologic community—at ASA's Washington headquarters especially—SILVER BAYONET brought about a searching review of the status of COMSEC in Army tactical units. Generally, COMSEC analysts recognized that deficiencies observed in SILVER BAYONET were not unique to the 1st Cavalry Division but were, with variations, prevalent throughout Army tactical units.

SILVER BAYONET dramatically underscored the dangers inherent in unsecured voice communications and the already recognized need for getting the KY–8 ciphony equipment distributed. SILVER BAYONET monitoring undoubtedly contributed to the JCS decision that all available KY–8 equipment would be sent to Vietnam.

In addition to those improvements in 1st Cavalry Division communications noted, actions were taken some weeks later to achieve long-range improvement. On 31 December ASA reviewed the cryptoholdings of the 1st Cavalry Division to determine if any shortage of crypto-equipment or keying material existed. ASA did not find any shortages for the period of SILVER BAYONET itself, except that one KW–7 was not operational. The division held 90 KW–7's and 31 KL–7's. By March 1966 ASA Headquarters was able to report to NSA that the division no longer used the "very insecure alphabetical grid reference code." ASA also reported that the division was using

authentication more frequently, although still not to the extent desired. About the same time, ASA began producing, in coordination with the 1st Cavalry Division, a new numeral and authentication system combining System 3 of KAC–24 and System VIII of KAC–21. The 1st Cavalry Division put the new system, KAC-Q, into use after NSA approved it. ASA also sent the division a number of authorized codes. These included 400 copies of the KAC-F segmented tactical operations code (96 editions of the code shipped on 12 January 1966 and later shipsments made to allow an 8-month supply) and 1,000 copies of the KAC-J series combination numerical code and authentication system (shipped for the division requirements on 6 December 1965 with a total of 32 editions per month, allowing for daily supersession). ASA also sent a total of 36 KY–8 ciphony sets (for arrival by 15 January 1966). ASA recognized a requirement from the division for a total of 82 ciphony sets. Being assigned priority, the 1st Cavalry Division was the first tactical command in South Vietnam to receive these. On 3 March 1966, the ASA Headquarters SIGSEC Division, in a briefing to NSA COMSEC personnel on the status of Army tactical COMSEC in Vietnam, reviewed many of the corrective steps taken, centering attention on the 1st Cavalry Division and SILVER BAYONET. Documenting its facts with monitored findings, the SIGSEC Division ended with the statement that the COMSEC status of U.S. Army units in Vietnam was "pitifully poor."

Thus, the monitoring and analysis during SILVER BAYONET revealed many deficiencies. The analytic findings were a significant, praiseworthy achievement but, for those acquainted with then prevailing Army communications practices, the findings should not have been surprising. Nevertheless, partially as a result of timing and the U.S. reaction to this major engagement, the monitored results were very useful at the tactical level and at all echelons of the cryptologic community. Within COMSEC circles, the Army's COMSEC practices received wide publicity. Although major improvement in the reduction of insecurities was to await arrival of KY–8 equipment, SILVER BAYONET aroused a general feeling in those controlling U.S. COMSEC that something must be done. It was obvious to the COMSEC community that poor U.S. COMSEC practices were one of the causes for the enemy success at Ia Drang.

Guam

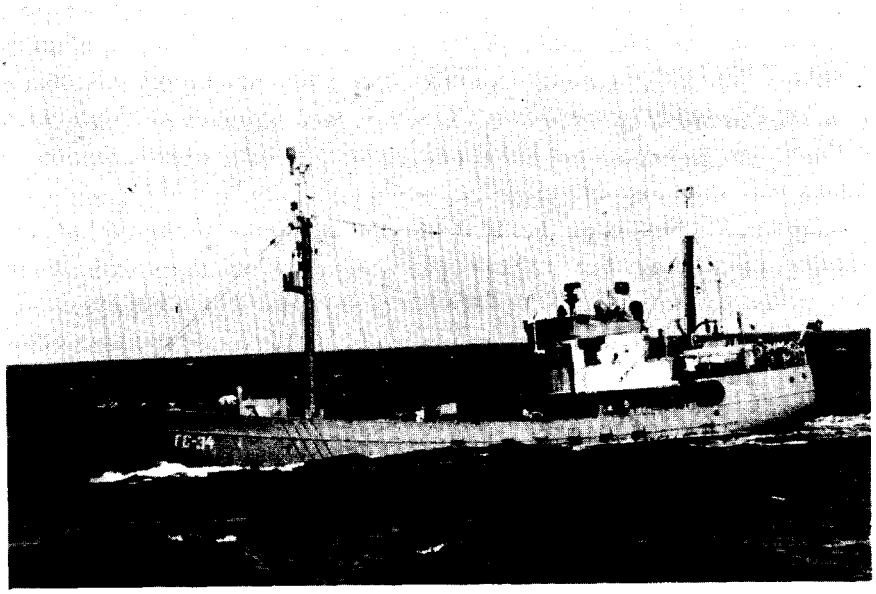
In the fall of 1965 and in early 1966, the Navy and Air Force undertook a major COMSEC study of communications being passed by military installations on the island of Guam in the Mariana Islands. NSA helped the Navy and Air Force in that part of the study dealing with compromising emanations (TEMPEST). In all, more than [redacted] COMSEC-trained people participated. The objective was to discover communications deficiencies that might be the cause of enemy foreknowledge of SAC B–52 strikes in Vietnam and then to make appropriate changes in communications practices. A more narrow objective was the determination of what intelligence, other than that from visual observation, might be available to the Soviet SIGINT trawlers on regular patrol just beyond the 3-mile limit off of Apra, the major harbor of Guam. The Soviet SIGINT vessel *Izmeritel*, or another trawler, had been on station continuously in these waters since late November 1964. During much of this period the USS *Proteus*, a nuclear submarine tender, was in the harbor and may have been of interest to the Russians.

Guam served as a key communications center for much of the Navy's operations in Southeast Asia and during the early years of the war was the only staging area for SAC B–52 bombing flights over Vietnam. The island's small size made it relatively easy to study the total communications environment. In contrast to several previous COMSEC surveys concentrating only on monitoring and analysis of plaintext communications, analysts during this study also inspected encrypted communications in order to evaluate the total communications with regard to space radiation, conduction of intelligence-bearing signals on power and signal lines, and the unintended coupling of signals through inadequate attention to Red/Black criteria.* The analysts did not test through cryptanalysis the security of encrypted traffic.

AFSS, NAVSECGRU, and NSA participants in the study coordinated their work. In keeping with the requirement to study all military-related communications on Guam, an AFSS mobile detachment examined Army elements there, especially those of the 515th Army Ordnance Company

*Red/Black criteria designate types of equipment, systems, and areas suitable for processing of classified information (Red) and not suitable (Black).

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



Soviet Trawler *Izmeritel* Off Apra, Guam, 1966

and the Strategic Communications ionospheric scatter facilities. In its review of Army communications, the AFSS detachment noted that 15 channels of the ionospheric scatter facility were passing traffic in encrypted form and one, carrying unclassified NASA traffic, was in clear text. These and other Army communications, the major part of which passed over Navy channels, appeared satisfactory. Primary focus of the study would be on Navy and Air Force communications.

Naval Communications

Coordinating with the AFSS mobile detachment on Guam, the Navy's COMSEC component on Guam, COMSEC 701, conducted a 6-week survey (1 November–10 December 1965) of internal and external Guam circuits. COMSEC 701 assigned thirty men to the survey, some of whom came from other Navy COMSEC units.

In monitoring Navy unclassified communications, COMSEC 701 employed three COMSEC single sideband positions and one VHF/UHF

position. In addition, COMSEC 701 installed four audio and four DC lines connecting COMSEC spaces with the Naval Communications Station Guam Circuit Control in order to monitor uncovered microwave and landline links. In all, the COMSEC unit sampled 42 uncovered circuits, 30 of which had off-island terminals. Of the latter, about a dozen were ships and aircraft.*

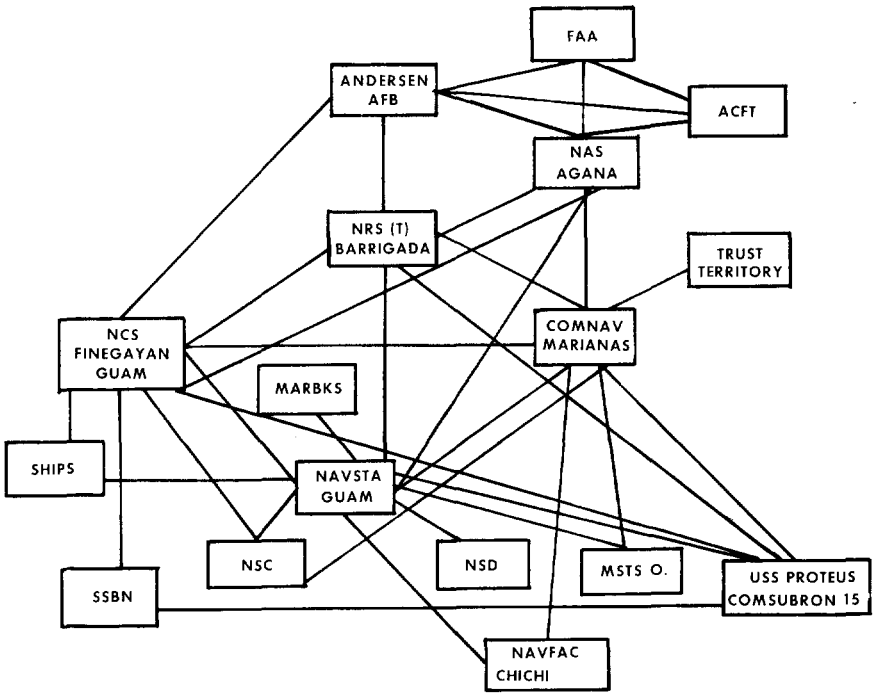
The monitoring team found that landline and microwave circuits yielded budget figures for specific projects, cargo and movement details for various ships, relationships between aircraft squadrons and carriers to which they were assigned, disposition and posture of tactical combat aircraft, and information on special airborne missions in Vietnam. References to ship-to-shore frequencies and antenna bearings, the COMSEC unit found, were passing in the clear over order wires.

Although the study called for broad monitoring coverage, radioteletype equipment was in too short supply to cover all links. To compensate, NAVSECGRU requested copies of teletype monitor logs. Accurate monitor rolls were often difficult to obtain, since they were often edited by communications personnel before they were given to the COMSEC unit. COMSEC monitoring gets its best results, of course, when communicators are unaware of the monitoring.

The COMSEC unit found only a few unauthorized communications practices that truly weakened transmission security. It discovered several unnecessary transmissions that could have aided enemy traffic analysis and identified the circuits carrying those transmissions. It also turned up many errors in the classification of messages.

To improve COMSEC, the NAVSECGRU COMSEC unit recommended that commands located close to the naval Communications Center make more use of couriers instead of depending on uncovered communications; that general use be made of air mail letters rather than electrical communications when practical; and that order wires be covered when appropriate cryptographic equipment became available. The COMSEC team observed that alternate covered routes for sensitive traffic were not then available. The only practical countermeasure against possible clandestine wire tapping and unauthorized microwave monitoring appeared to be the securing of all circuits.

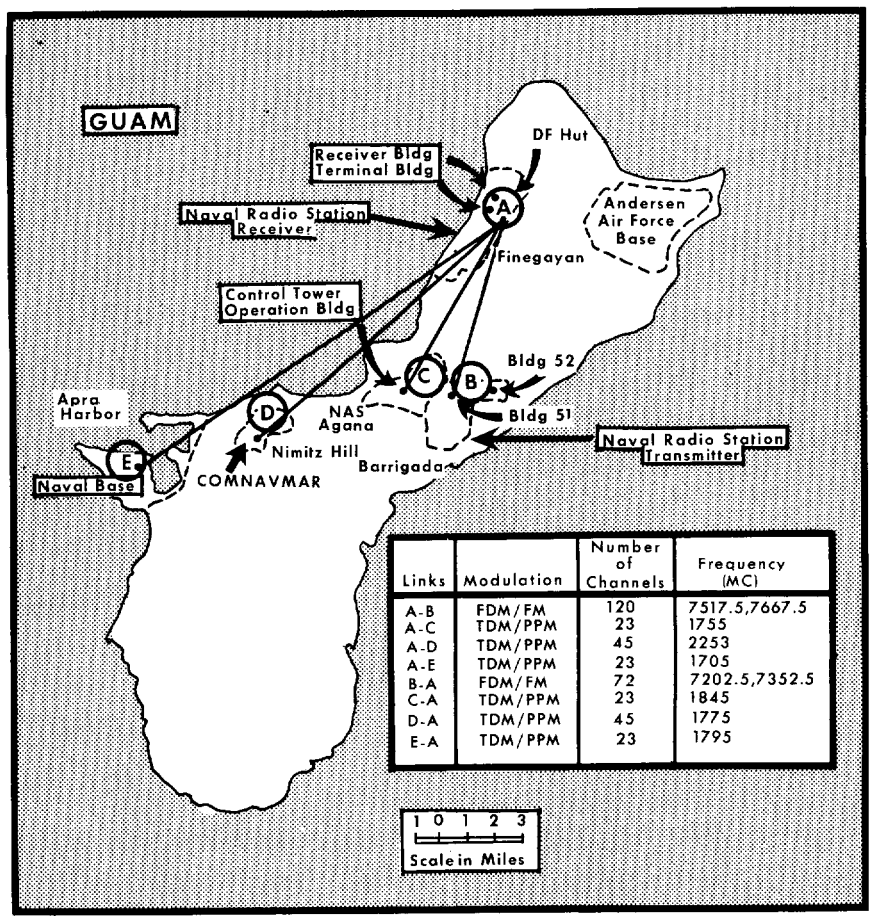
*See chart, page 99, for pertinent links in the Guam communications complex.



Communications Circuits Monitored in the Guam COMSEC Survey

COMSEC 701 also reported in its recommendations that physical security on Guam lacked proper emphasis. Sensitive naval communications activities needed fences, lights, acoustic conduit seals, positive secondary disconnect devices for telephones, and tighter control over public works maintenance personnel. All telephone lines on Guam passed through the Island Central Telephone Exchange, to which uncleared local and foreign repairmen and operators had access. A malpractice mentioned in connection with physical security was the occasional insecure disposal of unclassified and EFTO messages in a Dempster Dumpster along with unclassified trash.

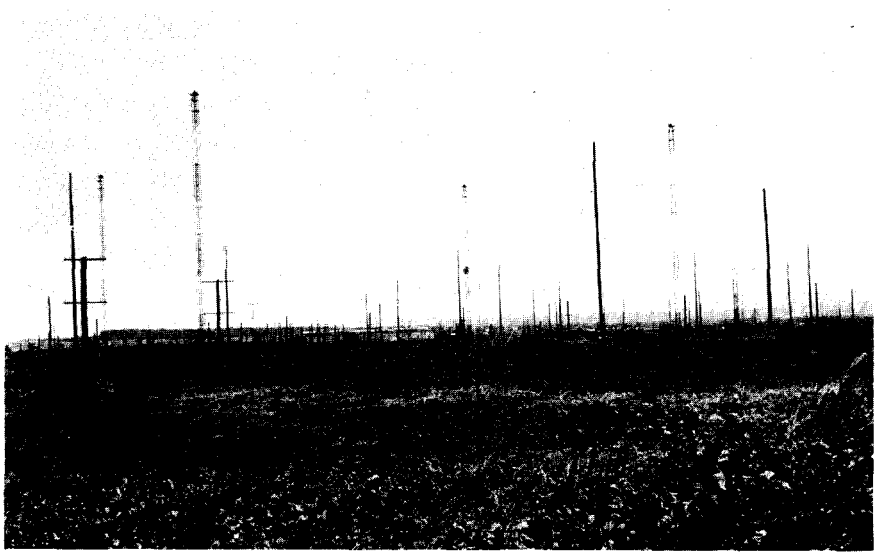
In summary, while many physical and communication security weaknesses identified in the Navy's survey had been previously known, COMSEC reindoctrination of personnel was desirable. As a result of the survey, COMSEC 701 was to make periodic sample surveys on a small scale to maintain vigilance over Navy circuits.



Links	Modulation	Number of Channels	Frequency (MC)
A-B	FDM/FM	120	7517.5,7667.5
A-C	TDM/PPM	23	1755
A-D	TDM/PPM	45	2253
A-E	TDM/PPM	23	1705
B-A	FDM/FM	72	7202.5,7352.5
C-A	TDM/PPM	23	1845
D-A	TDM/PPM	45	1775
E-A	TDM/PPM	23	1795

Air Force Communications

AFSS directed the Air Force Special Communications Center (AFSCC) to monitor and analyze the transmissions of SAC's 3d Air Division, Andersen Air Force Base, Guam, beginning on 30 October 1965. AFSCC's equipment capability permitted only two VHF, three UHF, and six telephone links to be monitored at any one time. During the monitoring, which lasted through 30 November, the specialists also covered two common user and fourteen dedicated telephone circuits. All together, the AFSCC unit examined VHF/UHF radio usage of fourteen Air Force elements.



Antenna Field at the Naval Radio Station, Barrigada

The monitors uncovered a large number of COMSEC malpractices and forwarded 25 transmission security message reports. A summary report stated that the operation had disclosed "considerable information on the tactics and procedures employed by the ARC LIGHT B–52 Bomber Force as well as the planning and operational support necessary for the conduct of the bombing raids on selected targets in RVN."

The monitors gained a clear picture of launch times for B–52 strikes from (1) traffic analysis of a prestrike encrypted MACV transmission of a TOP SECRET (FLASH) message to the Strategic Air Command (SAC), CINCPAC, JCS, 3d Air Division, and possibly the Joint Strategic Target Planning Staff; (2) voluminous cleartext transmissions by aircraft and munitions maintenance personnel on VHF radio nets approximately an hour before launch time, including identification of launch aircraft by tail numbers with statements such as "a goer must be ready by 0900"; (3) cleartext communications of a 4242d Strategic Wing plane to Andersen Air Force Base, Kadena Air Base, and Saigon during a weather scouting mission of the SAC air refueling area some 20 hours before

bombers were due over target; and (4) cleartext transmissions on radio circuits just before mission launch informing aircraft coming into Andersen AFB that the base would be closed for approximately 45 minutes for "high priority" traffic.

The monitors also turned up other sensitive information such as the Strategic Air Command's consideration of a proposal to permit ARC LIGHT B–52's to perform low-altitude optical bombing and the specific identification of equipment to be installed to make this possible, as well as SAC's plans to introduce a B–52D aircraft into the ARC LIGHT program so as to increase the internal bomb load capacity.

There were few instances where a sensitive item of information came only from one conversation. More frequently, disclosure of a particular item resulted from numerous attempts to talk around classified information over unsecured communications channels. This practice prevailed in long-haul communications such as those from Guam to Okinawa, Hawaii, and SAC headquarters in Nebraska as well as in on-base channels.

Even before the AFSCC survey was completed the Air Force, on 10 November 1965, began to use new procedures on the munitions maintenance net to eliminate from radio communications the use of aircraft tail numbers, the upload start and completion times, and personal names. Later tests showed the procedures were effective in eliminating this information, which had allowed continuity on the B–52 upload operations, as well as specifying the aircraft to participate in the missions. Similar changes in procedures were recommended for the aircraft maintenance network.

The Air Force had other COMSEC recommendations to consider as well: (1) making secure voice communications facilities available to all echelons to the maximum; (2) providing on-base approved circuits for coordinating classified activities when voice security equipment was not available; (3) using secure teletype (classified or unclassified EFTO) messages when possible in lieu of voice communications; and (4) establishing procedures for the use of operational codes to pass recurring reports (weather, aircraft departures, and so forth) for which secure communications were not available.

In summary, the Air Force had found a number of insecure communications practices that made vital intelligence available to the enemy. While the Air Force was unable to correct all the deficiencies that were brought to light, it did correct many of them. In one of those extremely rare occurrences, the enemy confirmed the effectiveness of at least one of the COMSEC corrective actions taken as a result of the survey. Immediately after being informed of the vulnerability of the weather report from the SAC weather scout aircraft, SAC directed that such transmissions cease and that the weather reports be filed in secure communications channels after the aircraft returned from its mission. Some time later, a defector from one of the Soviet SIGINT trawlers reported that one of the most reliable advance indicators of B–52 strikes had been the SAC weather scout reports; he added that these reports had disappeared in November 1965 and, after that, such extensive prior knowledge of the B–52 strikes had not been available to the Russians.

NSA TEMPEST Tests

At the request of the Chief of Naval Operations and the Chief of Staff of the U.S. Air Force, an NSA team conducted several phases of an on-site TEMPEST test between 30 January and 18 February 1966. (Navy and Air Force units participated in other phases of the survey.) The NSA team was to monitor selected microwave circuits and HF circuits and test their vulnerability, with particular emphasis on cipher-signal anomalies susceptible to exploitation. Defined as electrical irregularities during encryption of signals that result from modulation, coupling, or other cause, the anomalies might permit an alert enemy to recover plain language or other data useful to him.

The NSA team worked aboard the USS *Charles Berry* in an S–44-type shelter containing equipment for monitoring, recording, demodulating, demultiplexing, and analyzing signals in the MF–SHF range (500 KHz–10 GHz). While maintaining a watch over communications in the VHF/UHF range, the team also concentrated for four days on microwave links. The *Charles Berry* was stationed near the Soviet SIGINT trawler off Apra harbor for part of the test and then worked its way around the island for four days, staying three miles offshore.

During this time, the NSA team obtained over 77,000 feet of magnetic tape recordings.*

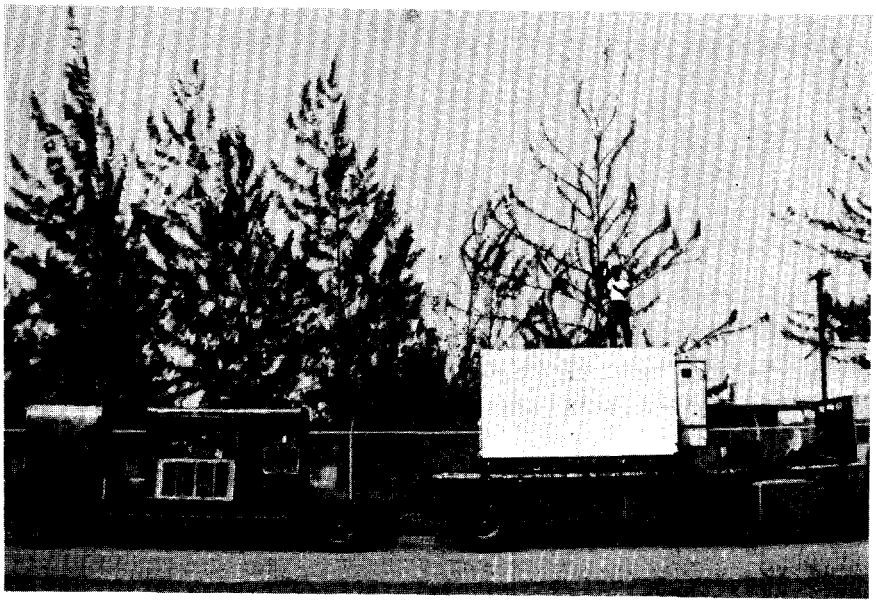
While in the vicinity of the trawler, the team heard no microwave signals. Off the north end of the island, however, it was able to hear three links when the ship's roll brought the team's antennas into direct line with the transmitters. Under laboratory conditions, NSA later evaluated HF communications intercepted by a NAVSECGRU team also on board the ship and found that no signals could be definitely identified as compromising cipher-signal anomalies. While making the shipboard survey, the NSA team noted that Air Force ground maintenance crews of Andersen Air Force Base could be heard from any point around the island. The communications were in plain language, and the NSA analysts could thus predict B–52 mission launchings "at least two hours prior to take-off."

In addition to the operations aboard the *Charles Berry*, the NSA team tested on land, monitoring the Finegayan-Barrigada microwave link from the naval radio station, recording each active link for later analysis. The team discovered that a high ambient noise level was modulating the microwave signal and masking normal anomalies, and therefore it could not definitely identify any compromising cipher-signal anomalies. The team also tested with negative results the communications of the Commander, Naval Forces, Marianas station on Nimitz Hill, the naval station at Apra harbor, and the naval air station at Agana.

Using a land position, the NSA team inspected the plain language voice circuits of the Air Force 1958th Communications Squadron transmitter site at Barrigada. The voice microphones for these circuits occupied the same spaces as teletypewriters, which were processing classified plaintext traffic, and it was suspected that audio-acoustic signals were present on the voice circuits. The NSA team failed to achieve conclusive results because of intercept limitations.

*National Security Agency [redacted] Analytic Studies, Special Report No. 4, sub: COMSEC Survey Guam, dated 23 June 1966, SECRET.

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



NSA's TEMPEST Shelter and Power Generator Used in the Guam Study

Navy TEMPEST Tests

The U.S. Naval Security Engineering Facility undertook the Navy's TEMPEST survey and prepared a number of technical reports in which it made recommendations for improvements.

At the NAVSECGRU headquarters at Finegayan the Navy team

[redacted] the use of KW-26 [redacted]

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

filters, better grounding, and filters on telephone lines leaving communications spaces.*

[redacted]

At the Communications Center and the Operations Control Center of the Naval Forces, Marianas, the team [redacted] The team noted that the doors to two copper-shielded rooms housing crypto-equipment were always open.

At the Naval Communications Station at Finegayan, [redacted] Marines guarded inside the buildings, but there was no physical security such as a fence outside the buildings. The team recommended that a security fence (preferably patrolled) be installed a minimum of fifteen feet from the buildings [redacted]

The Naval Air Communications Facility at Agana, nearly completed, was being constructed in accordance with DCAC C175-6A installation criteria. From a TEMPEST point of view, the facility was the most secure

*The sources for the Navy TEMPEST tests are U.S. Naval Security Engineering Reports: No. 1310-0025/RAS:va, Serial 310-0045, sub: TEMPEST Survey of Naval Security Guam, M.I. (U), 21 February 1966, SECRET; No. 1310-0025/DAS:va, Serial 310-0039, sub: TEMPEST Survey of Communications Spaces at U.S. Naval Station, Guam (U), 10 February 1966, SECRET; No. 1310-0025/RAS:va, Serial 310-0046, subj: TEMPEST Survey of Commander, Naval Forces, M.I., Communications Spaces (U), 21 February 1966, SECRET; No. 1310–0025/RAS:jp, Serial 310–0085, sub: TEMPEST Survey of Naval Communications Station, Finegayan, Guam, M.I., 27 April 1966, SECRET; No. 1310-0025/RAS:va, Serial 310-0047, sub: TEMPEST Survey of Naval Air Station Communication Spaces, Guam, M.I. (U), 21 February 1966, SECRET; and No. 1310-0025/DAS:eg, Serial 310-TR-007/67, sub: TEMPEST Survey of USS PROTEUS Secure Communications Systems (U), 16 February 1967, SECRET.

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

of the facilities surveyed on Guam. However, the team did recommend that filters be placed on the KW–26 equipment.

The team also surveyed the secure communications systems of the USS *Proteus* while it was tied up to a pier in Apra harbor. The ship's two active KW–26 and its AUTODIN (KG–13) circuits were connected to land lines,

While the various reports show that not all was secure from intelligence exploitation, the reasonable expectation of enemy exploitation was, in most cases, rather remote. From a COMSEC point of view, the Navy TEMPEST survey team's operations were quite successful.

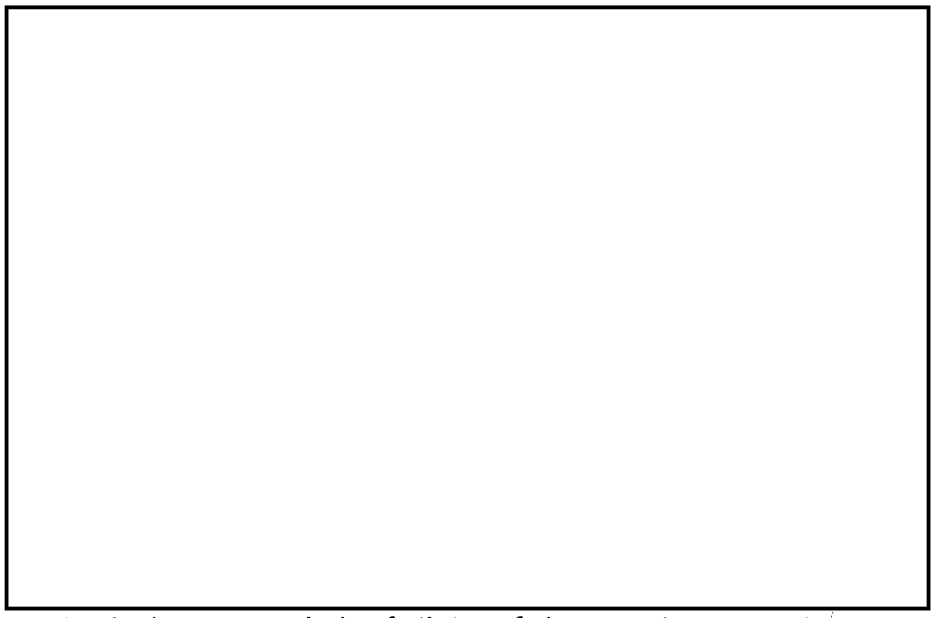
Air Force TEMPEST Tests

As their part in the TEMPEST survey the U.S. Air Force Security Service, during November 1965, tested Air Force communications facilities on Guam for compliance with "the intent of Federal Standard No. 222," the TEMPEST specifications for equipment usage. AFSS tested a frequency range from 15 kilohertz to 1 gigahertz, documenting its findings and making specific recommendations in three reports.* None of the facilities tested was completely free of TEMPEST problems. All Service communications centers tended, with few exceptions, to contain some hazards to security as a result of equipment design and the method of installation. The Air Force Guam surveys helped determine specifically the extent of these hazards.

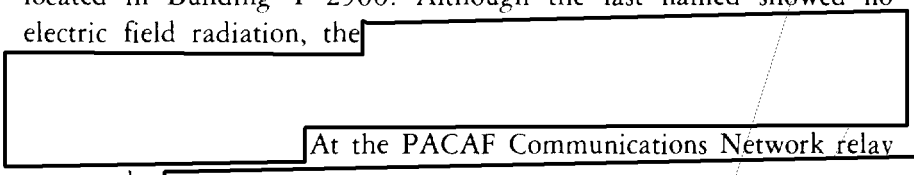
AFSS surveyed the facilities of the 3d Air Division (SAC), including the communications centers of the 27th Communications Squadron and the Special Security Office, as well as the electronic data processing equipment of the Data Services Division.

*USAFSS TEMPEST Test Reports: 1958th Communications Squadron (AFCS), Andersen AFB, Project 65-2; and 3d Air Division, Andersen AFB, Project 65-2; Air Force Systems Command, Operating Location 10. All three dated November 1965 and marked SECRET.

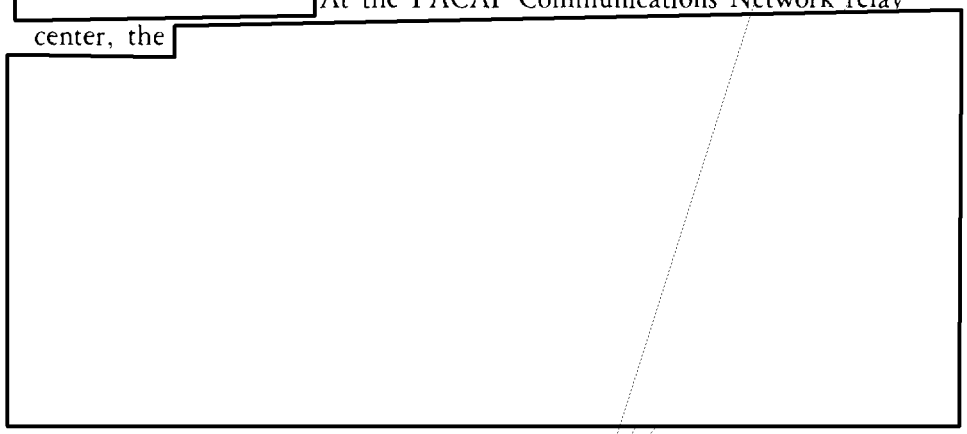
(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 403
(b)(3)-18 USC 798



AFSS also examined the facilities of the 1958th Communications Squadron at Andersen, including the PACAF Communications Network relay center, another relay communications center, and a terminal located in Building T-2500. Although the last named showed no electric field radiation, the



At the PACAF Communications Network relay center, the



*All figures given below for secure zones are for radii.

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

[redacted] While microwave transmissions in plain language could sometimes be heard at the three-mile limit, they were not intercepted in the location customarily occupied by the Soviet SIGINT trawler. Although by the end of 1967 TEMPEST corrective measures, consistent with funding and equipment limitations, were made for all Navy facilities on the island, the rehabilitation of the Naval Communications Station Guam [redacted] was not completed until early 1969. The Guam findings also gave added incentive to general corrective measures in Air Force facilities.

MARKET TIME

During the first three months of 1966, Navy COMSEC elements undertook a major study of communications of the U.S.-Vietnam Task Force 115 MARKET TIME operation.* With headquarters in Saigon and composed of both U.S. and RVN forces, the task force conducted surveillance, visit and search, naval gunfire, psychological warfare, and

*The primary sources for this MARKET TIME account were a report of the Commanding Officer, U.S. Naval Security Group Activity Kamiseya, Japan, and a report of the Officer in Charge, Communications Security Survey Team, Saigon. Both reports were enclosures to J-6 Memorandum for DIRNSA and others, sub: Communications Security Survey of MARKET TIME Communications, Serial J-6M-128-66, dated 27 May 1966, CONFIDENTIAL. A Navy publication, "Communications Security (COMSEC) Traffic Analysis Report for First Quarter CY 1966," is an excellent source for identifying the types of MARKET TIME intelligence information detected through monitoring.

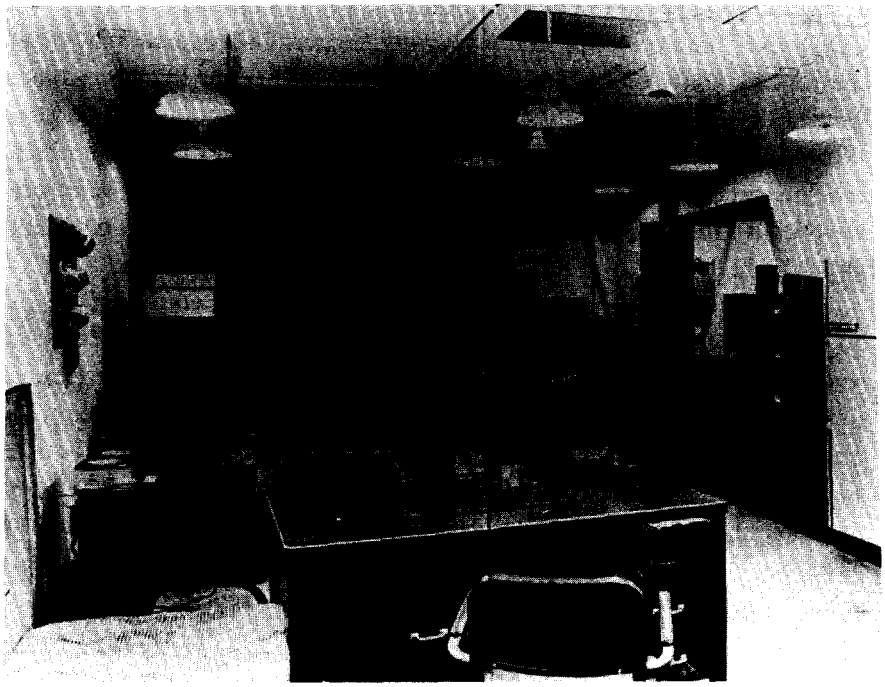
(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 403
(b)(3)-18 USC 798

other operations to secure the coastal regions and major rivers. Task Force 115 controlled its units through coastal surveillance centers at Da Nang, Qui Nhon, Nha Trang, Vung Tau, and An Thoi. Operations extended along the coast of South Vietnam from the 17th parallel to the Cambodian border in the Gulf of Thailand. Since almost all ship-to-shore and ship-to-ship communications were on uncovered voice circuits, they were highly vulnerable to enemy exploitation. The enemy might thus be obtaining intelligence that would allow him to avoid being intercepted by the MARKET TIME forces when he shipped supplies to communist forces in South Vietnam.

The enemy was well aware of the intelligence potential in maritime communications.

For the MARKET TIME COMSEC survey, the Navy had a team officer and one traffic analyst at Saigon; the analysis section of the Processing and Reporting Center, COMSEC 702, in Kamiseya, Japan; and [ ] monitoring positions and an analysis section at each of the Navy COMSEC units located in Guam, at Da Nang, at Vung Tau, on Okinawa, and aboard the USS *Jamestown*. The *Jamestown* monitored VHF/UHF frequencies and augmented shore station HF monitoring. COMSEC 703 in the Philippines allotted [ ] monitoring positions and an analysis section. In all, approximately [ ] COMSEC specialists were directly involved in the study.

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



COMSEC 705 Operations Area, Monkey Mountain

The COMSEC team officer in Saigon was to ensure the closest possible liaison with the MARKET TIME operational commander in compliance with CINCPAC orders: (1) to determine what traffic must flow during planning and actual operations; (2) to apply information regarding communications weaknesses and strengths gained by previous monitoring; (3) to determine what facilities were passing traffic and what additional facilities were available; (4) to recommend the preferred means of passing traffic and the best communications procedures and cryptographic aids to employ; (5) to conduct selective monitoring to evaluate recommended changes; and (6) to advise operational participants and make any additional recommendations.

The COMSEC components were to monitor and analyze MARKET TIME communications and to submit first echelon traffic analysis reports to the Chief, Naval Advisory Group, Saigon—so that he could

immediately apply important findings to operations—and to the COMSEC 702 Processing and Reporting Center. To the extent practical, the reports sent to Kamiseya went electrically since ordinary mail took from 20 to 30 days in transit and would therefore arrive too late to be of value in current operations. The COMSEC 702 PRC prepared second echelon reports based on an analysis of all traffic— both mail and electrically forwarded—that the participating COMSEC components monitored.

In this reporting scheme, the COMSEC units furnished the COMSEC 702 PRC with monitoring logs and a narrative of the intelligence recovered concerning the specific monitor logs. The center then issued COMSEC spot reports electrically to any units violating specific communication security procedures. On 17 February, the commander of Task Force 115 listed four areas in which disclosures could be serious: pending operations in MARKET TIME, intended movements on MARKET TIME patrols, geographical or grid positions or immediate area of operations while underway, and underway replenishment operations.

The PRC and other collection and reporting centers were to issue reports when any of the above disclosures was observed in MARKET TIME communications. While the PRC was unable to produce reports timely enough to affect current operations, the reports did provide useful information for general study of U.S. Navy communications procedures. The PRC recommended procedures, based upon the MARKET TIME experience, that would in the future allow more current second echelon reporting. These recommendations included the electrical transmission of all first echelon traffic analysis reports to the PRC from which second echelon reports would be prepared on a weekly basis.

The MARKET TIME COMSEC analysts found that a wealth of vital intelligence was being revealed over communications nets, HF voice circuits being the worst offenders. Just a few days after monitoring started, the analysts had almost completely recovered Task Force 115's order of battle. They were not only able to pinpoint the majority of the MARKET TIME vessels each day but also to recover patrol patterns and to predict positions hours in advance. All types of sensitive information were being passed on uncovered frequencies. Especially detrimental was the reporting of ship positions using the unsecured UTM grid

coordinates, which not only gave current locations but also identified forthcoming operations. Information on naval gunfire support missions went unprotected in several cases in such a manner as to pinpoint the intended target as much as ten hours in advance and to identify the location of the destroyer scheduled to fire the mission. The analysts also monitored sensitive information on underway replenishment, action reports, casualties, and the arrival and training of new units.

The compromise of intelligence was so prevalent that during the early phases of the survey a CTF 115 message went to all MARKET TIME and associated units stating: "CTF 115 receives daily analysis of MARKET TIME traffic monitored by COMSEC units. The scope and accuracy of these analyses, which are being made by outside observers using only such information as anyone can obtain by monitoring our circuits, is indeed sobering. For example, more detailed information regarding daily operations is often available from /this/ analysis than from official reports submitted by MARKET TIME units."* The message shows not only that the COMSEC monitoring teams had done their work well but also that the commander of TF 115 had taken heed.

The survey drew attention to a variety of COMSEC problems. Most arose at least in part as a result of MARKET TIME's inherent organizational complexity and varied communications structures. The task force incorporated elements of the U.S. Seventh Fleet, various aviation units, and U.S. Coast Guard and South Vietnamese vessels of various sizes. The U.S. vessels ranged in size from destroyers to Swift boats. Many of the participants had limited crypto-equipment, or none at all, and therefore had to use low-level manual systems. To acquire adequate communications netting, even the better equipped U.S. ships often had to use the communications modes and systems of the more poorly equipped participants. Thus it was difficult to communicate, let alone to communicate securely.

The COMSEC team officer at Saigon and the Navy's COMSEC 702 element in Japan noted these many problems and supported

*Commanding Officer, NAVSECGRU Activity Kamiseya report, title: Communications Survey of MARKET TIME, 18 April 1966.

recommendations and actions taken during the course of the survey. Specific problems and actions taken included:

a. Establishment of restrictions on the storage and handling of cryptomaterial was a problem for the South Vietnamese and/or smaller U.S. vessels.

b. Codes available for U.S. use (KAC–132 and KAC–138) were not suited, by vocabulary, for this type of operation. KAC–132 was restricted, moreover, to large U.S. vessels. KAC–138, a numeral code, was available to encrypt position coordinates (the code was authorized to be used in this manner, mixing the code groups and plain text); however, it was restricted to use for reporting while within sight of land or foreign vessels. CINC Pacific Fleet lifted the restriction on KAC–138. Also, starting on 10 March, with CINC Pacific Fleet approval, U.S. MARKET TIME participants began using KAC–140, an operations code designed for Vietnam.

c. Analysis of traffic encoded in KAC–140, upon its introduction, revealed that many units were habitually using stereotype expressions at the beginning and end of encrypted text. For example, many reports started with the words, "Contact Report Posit," and it was common practice to end with the encrypted group for "period." Such practices weakened the security of the code and consumed unnecessary manhours in the coding process. COMSEC 702 recommended that all task force units ensure that their communications personnel be "thoroughly indoctrinated in correct communications procedures and trained with the specific equipment that will be used." Such training service could be had by addressing the COMSEC elements at Da Nang and Vung Tau.

d. Because of the lack of cryptofacilities, especially on-line, it was operationally impracticable, and often impossible, for MARKET TIME units to establish secure rendezvous positions or submit late requirements to the replenishment ship. As a result, the major part of this information, including the times of rendezvous and units involved, was being passed in an exploitable manner. It was recommended that CINC Pacific Fleet authorize encrypted call signs for passing traffic encoded in KAC–132. The authority was granted and Commander, Seventh Fleet, established instructions for passing such communications on the area underway replenishment net.

e. KAC–140 provided the first effective code system to protect MARKET TIME operations. However, since its terminology was not extensive enough for detailed fast reporting, the survey team officer recommended that a new code be designed to fulfill MARKET TIME surface and air requirements. NSA produced a new code, KAC–183, which came into use later in 1966.

Largely as a result of the COMSEC actions taken, officials estimated that the volume of intelligence information subject to compromise on MARKET TIME circuits was reduced by at least 80 percent. Advocation of the minimize communications principle and other COMSEC techniques put forth in COMSEC lectures and training also helped. The practice of sending geographic positions with the UTM grid given in plain language almost completely disappeared.

Changes in the Navy's COMSEC organization and procedures also resulted. An additional eight persons would service MARKET TIME/GAME WARDEN monitoring and analysis requirements at the NAVSECGRU Activity facilities in Kamiseya. The Naval Advisory Group, Saigon, staff would make periodic visits to all coastal surveillance centers and in-port units to discuss COMSEC policies and problems.

Upon receipt of the Navy MARKET TIME COMSEC surveillance reports, the Communications-Electronics Directorate, J–6, of the U.S. Joint Staff, commented favorably on the operation, characterizing the reports as "an exemplary demonstration of what can be accomplished at relatively low-level tactical echelons with a well-planned and well-executed communications security operation." NSA also termed the study "an exemplary demonstration of the effective utilization of COMSEC surveillance resources."*

*J–6 Memorandum for Director of National Security Agency and others, sub: Communications Security Survey of MARKET TIME Communications, Serial J–6M–128–66, 27 May 1966, CONFIDENTIAL.
NSA Memorandum for the Director for Communications-Electronics, Joint Staff, sub: Communications Security Survey of MARKET TIME Communications, Serial N1042, 21 July 1966, SECRET.

The COMSEC survey improved only U.S. COMSEC. Since South Vietnamese ships participated in MARKET TIME operations, ideally, the survey should have examined COMSEC problems on Vietnamese circuits, but this was not done.*

Improvements in COMSEC as a result of the MARKET TIME survey were not permanent. A Navy COMSEC traffic analysis report for October–December 1966 showed that old problems neither die nor fade away:

> Plain language traffic passed on MARKET TIME circuits continues to reveal intelligence information such as: estimated times of arrivals and departures, positions, patrol reliefs and times of relief, operating areas, and current and intended operations.

GAME WARDEN

GAME WARDEN was the unclassified name for an extended series of naval operations designed to prevent Viet Cong infiltration and resupply across the Mekong River Delta and in the Rung Sat Special Zone—the major shipping channels to Saigon. In GAME WARDEN the U.S. Navy River Patrol Force, together with units of the RVN Navy, had a mission similar to that of the MARKET TIME forces, but with the added hazard of being constantly within range of weapons along the river banks. The patrols were to prevent men, equipment, and food from reaching Viet Cong strongholds in the Central Highlands of South Vietnam. Task Force 116 units engaged in GAME WARDEN used small craft such as river patrol boats (PBR's), which were served by HF CW/SSB and VHF/UHF voice radio circuits. COMSEC units monitored these circuits from the onset of GAME WARDEN.

Two COMSEC teams supported Task Force 116. The first was COMSEC Team Three, located in the Coastal Surveillance Center, Vung Tau, at the mouth of the main channel entrance to Saigon. CINC Pacific Fleet exercised operational control of the team, the Naval Advisory Group at Saigon providing working spaces, billeting, and message facilities and exercising administrative control. Additional administrative

*NSAPACREP Vietnam (C) Msg to DIRNSA, F46D–1365, sub: MARKET TIME COMSEC Survey Jan thru Mar 1966, 120629Z October 1969, CONFIDENTIAL.

and logistical support came from COMSEC 705 at Da Nang. From the time of its activation in February 1966 through the end of December 1967, COMSEC Team Three operated with six men and a chief petty officer.

The second COMSEC unit assigned to support Task Force 116 was Team Four, which began operations on 25 April 1967 from Vinh Long, South Vietnam. Team Four had seven men and a chief petty officer, all on 150 days' temporary assignment.

Both COMSEC teams providing support to GAME WARDEN performed two major functions. First, they gave practical and effective COMSEC assistance and guidance to communications operators on all Navy circuits in the area; second, they identified communications weaknesses and proposed corrective action for all U.S. forces using the frequencies that they monitored.

Both teams made daily first echelon traffic analysis reports on significant items of interest via electrical means to the Processing and Reporting Center at Kamiseya, to the commanders of Task Force 116 and 117, and to Commander, Naval Forces Vietnam, with information copies mailed to the Chief of Naval Operations and CINC Pacific Fleet. COMSEC TIMELY (rapid reporting of selected EEFI) and SPOT reports went electrically to appropriate addresses. Each month the chief petty officer in charge of each team submitted a letter report of operations to CINC Pacific Fleet, with information copies going to Commander, Naval Forces Vietnam, PRC Kamiseya, and other Navy commands. Also, a TRANSEC report summarizing COMSEC team activities went to COMSEC 705 at Da Nang for submission to the Commander, Naval Forces Vietnam, and subsequently to COMUSMACV.

Most of the naval vessels engaged in GAME WARDEN were small with limited communications capabilities. Cryptofacilities were nearly nonexistent, requiring the use of low-level code systems for transmitting classified information. One of the communications weaknesses identified, therefore, was attributable to the lack of an adequate cryptographic system for protecting information contained in operational reports. Although some units had the KAC–132, it was not suitable because of its large size and terminology, and the COMSEC teams therefore recommended KAC–140, the operations code designed for Vietnam use and approved by CINC Pacific Fleet for use by MARKET TIME and

GAME WARDEN. It was available from COMUSMACV. Not only did KAC–140 permit secure transmission of operational reports but it also provided a common cryptochannel among MARKET TIME, GAME WARDEN, USMACV, and USARV units operating in the area. COMSEC first echelon traffic analysis reports reflected a significant reduction in the availability of intelligence information to the monitors after KAC–140 came into use. KAC–140 accorded security to these communications until a new cryptographic system could be devised. KAC–140 was replaced on 1 August 1966 by KAC–183, which had cryptographic features and vocabulary more appropriate to these operations.

Monitoring continued to uncover many instances of specific information of direct value to the enemy. The Chief of Naval Operations' Quarterly Traffic Analysis Report for October–December 1966 gave representative examples of unsecured GAME WARDEN communications:

On 12 December PBR "PORPOISE 23" reported that she was aground and was attempting to free herself. At 2333Z the PBR advised "BOLD LAD" that she saw no hope of getting off until high tide and that she could use a case of C Rations. If this PBR had been visually sighted by the Viet Cong and they had received the previous transmission, they would know that the PBR was going to be vulnerable for several hours.

At 011245Z December "SHARK 8" (PBR) observed spotlights on the bank of a river and called "MOON RIVER," reporting the position as "KVQ HXZ." At 1314Z "MOON RIVER" requested permission from "BOLD LAD" (Army) to fire on coordinates XS 925 695, thereby linking the encoded coordinates (KVQ HXZ) to the unencoded positions coordinates, XS 925 695.

At 051604Z CTE 116.2.1.2 (located at Can Gio) transmitted his 041800H-051800H OPSUM to "MOON RIVER" (Nha Be); the OPSUM revealed that 20 PBRs were used for patrol, 12 from Cat Lo and eight from Can Gio.

The GAME WARDEN force included the following ships: TUTUILA (AGR 4), COMSTOCK, VERNON COUNTY, WESTCHESTER COUNTY, 3 PACVs, 23 MSBs, 9 MSLs, and at least 92 PBRs.

Other communications problems on which Teams Three and Four worked were the uncovered links between ships and their fire spotters

ashore. Until made secure cryptographically, these links were susceptible to enemy exploitation.

As a result of COMSEC operations in the Saigon area, naval commanders gained a better awareness of other communications weaknesses. COMSEC units were called upon to brief naval forces, using recent examples of problems and weaknesses to drive home their lessons. For example, COMSEC Team Three at Vung Tau participated in briefings and debriefings of units attached to Task Group 115.3.

Team members learned that personal visits with communicators were more rewarding than sending impersonal reports of discrepancies by mail. Once the offending operator realized that the COMSEC team was interested in helping him improve his procedures, his training moved along more rapidly. This lesson had been learned long before GAME WARDEN, but GAME WARDEN gave two COMSEC teams the opportunity to apply training and education concepts in an environment of actual need.

ARC LIGHT

First Year of COMSEC Operations

In June 1965 Strategic Air Command B–52's began missions over South Vietnam, a program having the unclassified nickname ARC LIGHT. The SAC bombers traveled approximately 2,500 nautical miles in-bound from their base on Guam and completed their round trips in approximately 12 hours flying time, including the time required for in-flight refueling. Each B–52 carried 51 bombs or 16 tons, and it was not unusual to have as many as 30 planes on a single raid. Acting on recommendations from in-country units and his immediate staff, COMUSMACV initiated the requests for ARC LIGHT strike missions, transmitting them to CINCPAC, who in turn requested final approval from the Joint Chiefs of Staff. When the JCS gave approval, a request for execution went to the 3d Air Division at Andersen Air Force Base on Guam.

It took an enormous volume of communications to initiate, approve, and execute a strike mission, and while some communications used to arrange the strikes were basically secure, others equally necessary,

including those to notify U.S. front line units of an impending strike, did not have proper protection. From the beginning of ARC LIGHT, U.S. officials were aware from ASA and AFSS monitoring reports that many of the communications were insecure. Some U.S. officials reasoned that any tip-off from the planes after they were airborne would not give the communists time to take positive action. Others were not convinced that the Vietnamese Communists had a SIGINT capability sufficient to exploit U.S. communications. Still others showed concern and were trying to resolve various aspects of the COMSEC problem. As time went on, considerable evidence accumulated showing that this enormous volume of communications with its full measure of COMSEC deficiencies was working against the objectives of the ARC LIGHT program. The Services, acting individually, attacked ARC LIGHT COMSEC problems and registered some success in eliminating deficiencies.

As the only U.S. COMSEC specialists in Vietnam at the beginning of 1965, the 101st ASA Security Detachment monitors, among other things, reported insecurities on air operations nets connecting the 2d Air Division with higher headquarters. Additional Army monitoring reports throughout 1965, along with Air Force reports, continued to show extensive use of plain language concerning the planning and coordination of air operations. In summer of 1966, the 101st Security Detachment reported on disclosures of planned ARC LIGHT strikes in the course of monitoring Capital Operations Center switchboard communications with air planning commands. From these and other in-country communications, ASA developed considerable information to document the COMSEC weaknesses associated with SAC air strikes. Employing all conventional telephone and radio monitoring positions at their disposal, ASA monitors determined that at times strike requests were passing up to corps level in the clear and that communications giving 48 hours advance notice to friendly troops operating in the strike areas also lacked protection. From its monitoring of in-country communications, ASA found that traffic reflected the enemy could have had from a minimum of one hour to at least 24 hours advance notification of a planned B–52 strike; that 21 transmissions monitored revealed strike objectives, participants, locations, times, and prestrike and follow-on operations; that implementing and coordinating procedures for strike planning and command and control were revealed in great detail; that traffic patterns

established were exploitable—reliable predictions of impending strikes could be based on conversations referring to FLASH messages confirming the target, giving or changing the time over target, or changing the target location—and that portions of a TOP SECRET contingency plan for the defense of South Vietnam were given when it was revealed that Guam-based B–52's were the major striking force, with a reaction time estimated at 12 hours.

During this period, the Air Force was accumulating similar evidence from AFSS monitoring of ARC LIGHT-related communications. Following the Guam study (late 1965–early 1966), AFSS monitored to the extent it could Air Force communications pertinent to ground administration, air-to-air coordination, air space requirements and flight plan arrangements, weather reconnaissance, tower directions, preflight testing of equipment, refueling operations, and in-flight reporting.

It was necessary operationally for in-flight B–52's to communicate, but the B–52's at the time had nothing authorized or on board for encryption except the manual general encryption code, KAC–72, and TRITON cryptomaterial for authentication. There was no ciphony equipment. When ARC LIGHT flights began, pilots transmitted in plain language while going to and returning from strikes, but after a few months the pilots were ordered to maintain radio silence at least while en route to their targets.

The Air Force tried in other ways to curtail insecurities in ARC LIGHT communications. It provided KY–3 and KY–9 ciphony equipment at Kadena Air Base, Okinawa, and at Andersen Air Base, Guam, to protect flight information and discontinued the practice of passing prestrike weather Combat Aircraft Report (COMBAR) information from KC–135 aircraft via HF single sideband transmitters. The Air Force also dealt with the major problem of altitude and air reservations. Before SAC missions could be launched toward Southeast Asia, the Air Force had to receive altitude reservations (ALTREV's) from the host countries over which the SAC aircraft had to fly. To arrange this, SAC requested altitude reservations from the Manila Area Control Center (ACC) through the Southeast Asia Military Air Route Facility (SEAMARF). The Manila ACC then transmitted Notices to Airmen (NOTAM's) over unsecured commercial channels to all interested ACC's, giving the specific air reservation information. The

NOTAM's went to the ACC's at Hong Kong, Saigon, Bangkok, Taipei, Singapore, and, sometimes, to the Australians. After a NOTAM was acknowledged by all ACC's, the Manila ACC granted the requested altitude reservation. SAC aircraft could be launched only after Manila's final approval was received. This procedure, allowing as it did the release of premission information at least six to nine hours before time-over-target of a mission, hardly met COMSEC requirements. The unsecured communications involved in these arrangements presented the enemy with a windfall of information.

On 21 April 1966, to tighten the security aspects of obtaining altitude reservations, SEAMARF, SAC, the Thirteenth Air Force, and the Pacific Air Force agreed on a number of procedures to reduce the ALTREV information in NOTAM's and to make more use of secured channels for coordination. It was hoped that the new ACC notification procedures, including ALTREV's, would be protected from unsecured transmission (except for local telephone systems at terminal points) until approximately two hours before SAC aircraft reached the proximity of each country's flight identification boundary. While the various parties involved in the arrangements for the most part met their obligations, prior warning time did not achieve the 2-hour goal the Air Force wanted.

CINCPAC's ARC LIGHT Survey

In mid-1966 SCA monitoring reports outlining ARC LIGHT communications insecurities took on added significance,

Citing DIA Intelligence Bulletin #200-66, which gave tangible evidence of the enemy's exploitation of U.S. communications on forthcoming B–52 bombing missions, Admiral Sharp, CINCPAC, on 28 July 1966 sent a brief, pointed message to the Joint Chiefs of Staff. Noting that he considered communications security a vital part of military operations, especially when trying to preserve an element of surprise in air strikes, Admiral Sharp stated that he needed a tri-Service, concentrated COMSEC survey, along the lines of the recent Navy survey in the MARKET TIME area. He wanted a survey of at least 30 days, to begin no later than 15 September.

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

The JCS approved the request, and Admiral Sharp promulgated orders to CINCUSARPAC, CINCPACFLT, CINCPACAF, COMUSMACV, and COMUSMACTHAI. The survey was to identify and correct any communications malpractices involving ARC LIGHT strikes that could result in tip-off and advance warning to Vietnamese Communists units.

Admiral Sharp set times for the submission of five periodic reports that would include recommendations for improvement and corrective actions taken. The reports would go to General Hunter Harris, Jr., CINC Pacific Air Force, whom Admiral Sharp designated as executive agent for the survey. General Harris, in turn, was to prepare a final report by the end of October for submission to Admiral Sharp.

The tri-Service monitoring and analysis elements to conduct the survey were:

Elements	*Positions*
1. Det 2, PAC Security Region (USAFSS in support of PACAF)	[redacted] (including those for the elements 2–6 listed on left)
2. 6922d Security Wing	
3. Det 5, 6922d Security Wing	
4. Det 7, 6922d Security Wing	
5. Det 1, 6988th Security Sq	
6. Det 1, 6927th Security Group	
7. 509th ASA Group (ASA in support of COMUSMACV)	[redacted] radio and [redacted] conventional telephone
8. Det 1, 101st Security Detachment (ASA in support of COMUSMACTHAI)	[redacted]
9. NAVCOMMSTA Guam (NAVSECGRU in support of CINCPACFLT)	
10. COMSEC 705 (NAVSECGRU in support of CINCPACFLT).	
11. Commander, Task Element 70.7.7.1 (NAVSECGRU in support of CINCPACFLT)	unknown
12. Commander, Task Element 70.7.7.2 (NAVSECGRU in support of CINCPACFLT)	unknown

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

Admiral Sharp's directive contained specific EEFI and areas of special interest. These were:

EEFI

a. How much time do enemy intelligence organizations have to react to ARC LIGHT tip-off? Indicate the first mention of ARC LIGHT strikes in monitored traffic. Indicate dates and times prior to strikes where amplifying information could have been obtained from traffic.

b. To what extent do communications prior to the ARC LIGHT strikes reveal strike objectives, participants, locations, times, equipment, or follow-on operations?

c. Is classified information transmitted in the clear over unprotected circuits?

d. What information is revealed concerning ARC LIGHT operations by the implementing and coordinating procedures required for strike planning?

e. What transmission security procedures have been most effective in security ARC LIGHT information? Give examples of use, changing frequencies, authenticators, call signs, or voice codes.

f. Has information been disclosed concerning command and control procedures, circuits, personnel, or locations?

g. Are there indications that tip-off may occur through other than communications weaknesses?

h. To what extent do communications traffic patterns give advanced warning of pending strikes?

i. What other information of special significance was disclosed either prior to, during, or after the ARC LIGHT strikes?

Areas of Special Interest

a. Assessment of previous strikes,

b. Target selection and subsequent coordination,

c. Logistics of launch, recover, and alternate air bases,

d. Coordination of SAR,

e. Route coordination (FAA, Navy, Army, etc.),

f. Clearance of friendly forces in strike areas (Army, Marines, Navy, allies),

g. Weather reporting.*

*CINCPAC Msg, sub: ARC LIGHT TRANSEC Survey (C), 151845Z August 1966, SECRET.

During the 30-day survey, SCA monitoring units covered a majority of those circuits known to carry ARC LIGHT information. The 509th ASA Group in Vietnam blanketed common-user lines of the major trunks, Field Force and subordinate unit switchboards, and VHF/UHF, AM, and FM radio nets in Vietnam as well as COMUSMACTHAI local switchboard circuits to Thailand air bases. NAVSECGRU elements monitored 66 tactical and air coordination voice circuits emphasizing voice communications in and out of Da Nang (Airborne Command Post PANAMA and so forth) and Guam, TTY, and other circuits. PACSCTYRGN covered 86 voice, TTY, and other circuits, concentrating on such long-haul voice communications as Guam to Philippine Islands, Vietnam, and Okinawa, and SAC Omaha to Okinawa.

Upon receiving reports from the survey participants, General Harris prepared for Admiral Sharp a final report outlining recommendations made and actions taken.* The report presented voluminous evidence of insecurity in ARC LIGHT communications. Perhaps the most telling argument for the need of COMSEC improvement was a list of over 50 monitored teletype transmissions that were related to actual time-over-target and demonstrated actual warning time available to the enemy. (For a partial list, see table, page 126.)

The COMSEC analysts, in fulfillment of EEFI, believed they had accumulated evidence of mission compromise in teletype communications for 26 of a suspected 30 ARC LIGHT strikes during the 30-day period.** The final report characterized the sensitive information derived from ARC LIGHT communications in this way:

> An average of approximately seven and one-half hours prior warning of each ARC LIGHT strike is available from teletype monitor. Of those warning times provided it was often the case that amplifying information could have been obtained from in-country telephone or radio-telephone monitors. This amplifying information included hints of such things as strike objectives, participants, locations, times and/or follow-on operations. In addition to this information there were other disclosures which provided analysts with a limited

*PACAF, Final TRANSEC Analysis Report, 15 September–14 October 1966 (SECRET, NOFORN), 28 October 1966.

**Actually B–52 strikes were averaging about 50 missions a month: 59 in September and 44 in October, 1966 (DIA SEA Military Fact Book for 1966).

Warning Time Revealed in Teletype Transmissions

Originator	*Time of Transmittal*	*Time-Over-Target*	*Warning* Time[a]
Kadena	151110Z Sep	152205Z	10+55
Saigon	151550Z Sep	152205Z	6+15
Saigon	170200Z Sep	170630Z	4+30
Kadena	172346Z Sep	180720Z	7+34
Saigon	180319Z Sep	180720Z	4+01
Clark	201635Z Sep	202215Z	5+30
Kadena	201750Z Sep	202215Z	4+25
Saigon	202100Z Sep	202215Z	1+15
Clark	210530Z Sep	211947Z	14+55
Kadena	210636Z Sep	211947Z	13+11

[a] Hours plus minutes.

insight into the coordinating procedures required for ARC LIGHT strike planning. The coordination of this data provided over an extended period of time could possibly lead to an eventual compilation of ARC LIGHT data: targets, priority assigned to different types of targets, equipment used, etc., which could eventually restrict the effectiveness of the overall ARC LIGHT program.*

Recommendations in the final report were not as impressive as were the insecurities found on all sides. The major part of the intelligence information obtained and recorded in the report had seemingly been passed in violation of the Pacific Command regulation concerning the use of EFTO procedures. This was noted, but the report made no recommendation as to how those violations could be corrected. The report did recommend that SAC, SEAMARF, the Thirteenth Air Force, and the Pacific Air Force develop a method of completely securing information on altitude reservations, and that, where applicable, every method at the disposal of user agencies be employed to ensure that code systems were used in accordance with authorized procedures. The report recommended a review of guidance documents governing the discussion of any information pertinent to ARC LIGHT missions to determine

*PACAF, Final TRANSEC Analysis Report, cited.

whether they did or did not specifically prohibit the transmission of intelligence similar to that noted. If not, the report recommended more specific guidance. The report also recommended stern penalties for violators.

CINCPAC subordinates took follow-on actions, apparently as a direct result of the joint monitoring operation. General Westmoreland, COMUSMACV, directed that those command elements cited in the final report for having divulged ARC LIGHT information conduct investigations into the areas of insecurity. General Westmoreland also spelled out for subordinate units policies and classification guidelines for ARC LIGHT in order to dispel apparent confusion on the subject. For example, the AFSS had reported in September that its Detachment 5, in monitoring unsecured communications, had reconstructed the entire geographic grid system being used for area target identification along with associated code names for discriminating grid blocks. The AFSS detachment at Tan Son Nhut informed MACV and SAC that they would have to discontinue using the seldom-changed code names to identify target areas if any COMSEC improvement were to be realized.*

The U.S. Army Vietnam (USARV) gave subordinates 30 days to improve their COMSEC and report actions taken. USARV emphasized use of low-level codes, available secure circuits, and couriers as steps to overcome the voice problem and directed commanders in particular to make use of available secure voice. Despite these and other measures, the basic COMSEC problems continued without a significant reduction.

In reviewing the ARC LIGHT survey, Admiral Sharp was unable to find much comfort in the results. The 30-day survey had been a successful tri-Service attack on a specific communications problem, and it had revealed an abundance of information as to what was causing the problem. In this, it had established a precedent for future tri-Service actions, but it had produced no effective solution to the complex problem.

Admiral Sharp was also displeased with the manner in which the survey had proceeded. In December 1965 he had promulgated the joint

*These codenames were not changed for months—until all targets in a particular geographical area had been hit. Such usage in unsecured communications as much as a month in advance of actual strike allowed enemy foreknowledge with ample time to minimize the damage or plan counteraction.

NSA-CINCPAC concept for COMSEC surveillance, but the COMSEC units had employed only conventional monitoring techniques during ARC LIGHT survey. The admiral believed that COMSEC surveillance techniques were not generally understood and felt that the stumbling block to their full use had been the failure of the various Services to issue necessary technical guidance. He asked the JCS to correct the situation. CINCPAC needed a procedure for bridging the gap between those who identified communications security deficiencies and recommended changes and those who had to make the changes.

In the PURPLE DRAGON survey, which followed on the heels of ARC LIGHT and had much the same objectives, CINCPAC was to apply the surveillance concept to achieve that end.

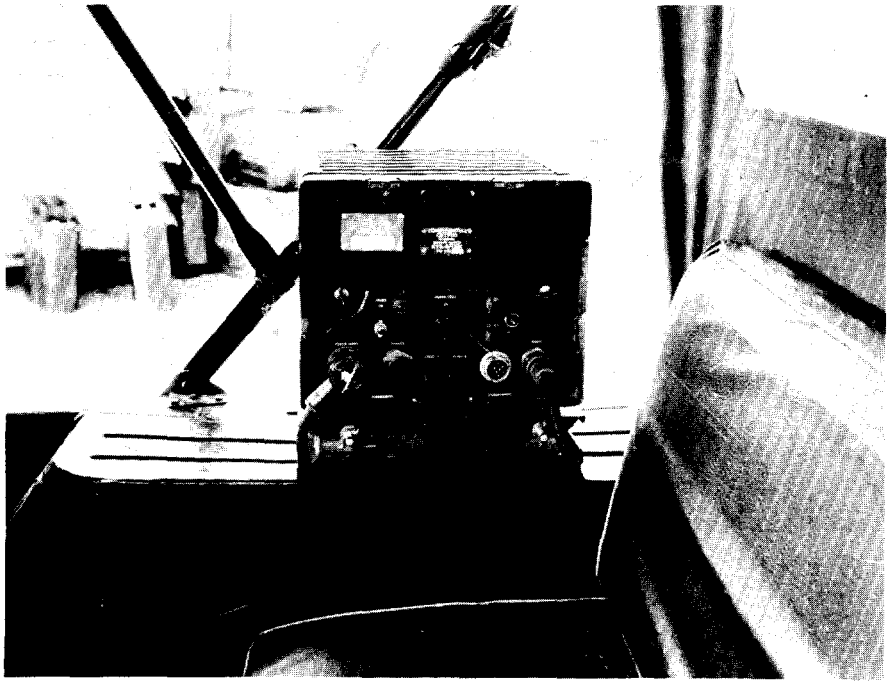
PURPLE DRAGON

At the same time that Admiral Sharp was developing his plans for the ARC LIGHT survey to determine from which sources forewarning of B–52 strikes could be acquired, [redacted]

In September 1966 JCS approved a plan that DIA had developed in collaboration with the Joint Staff, the Services, and NSA. The plan called upon CINCPAC to execute a 4-month field survey to ascertain the sources for enemy forewarnings. On 10 December 1966 the JCS approved CINCPAC's subsequent implementation plan, nicknamed PURPLE DRAGON. Admiral Sharp described the objective of PURPLE DRAGON as the improvement of operational effectiveness through operational security. To ensure the success of PURPLE DRAGON, Admiral Sharp assumed direct operational control and established a PURPLE DRAGON control group under Col. James Chance, USAF, on the J–3 CINCPAC staff.

The PURPLE DRAGON plan was first to identify all recurring or stereotyped indicators of forthcoming air operations, largely through

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



Jeep-mounted KY–8 Ciphony Device

exhaustive examination of U.S. communications passed prior to the air operations. Once the communications and other indicators had been established, CINCPAC would develop procedures to deny the information to the enemy. Along with the study of U.S. communications, PURPLE DRAGON specialists would consider the military operations themselves and counterintelligence.

The PURPLE DRAGON survey examined three categories of air actions: drones, air operations over North Vietnam, and air operations over South Vietnam. SAC employed drones in a program nicknamed BLUE SPRINGS (later BUMBLE BUG, BUMPY ACTION) to obtain reconnaissance photography in high risk areas of Communist China and North Vietnam. DC–130's usually launched the drones over Laos or the Gulf of Tonkin, and CH–3C helicopters recovered them in midair in the vicinity of Da Nang. All air strike operations over North Vietnam, whether by the Navy or the Air Force, had the nickname ROLLING

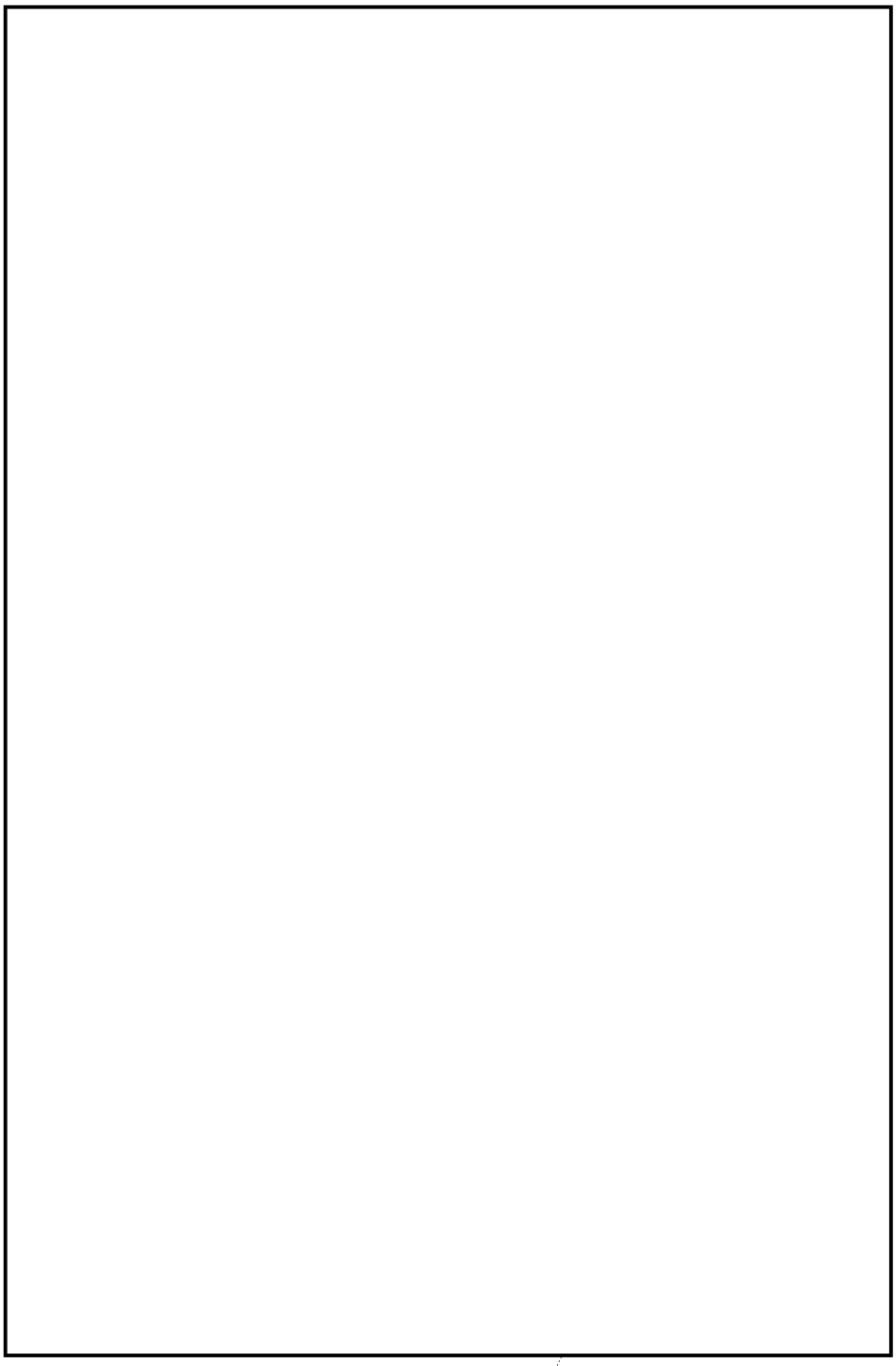
THUNDER. The third category, ARC LIGHT, was, of course, the B–52 strikes over South Vietnam.

PURPLE DRAGON operated with seven independent teams, each favorably located to carry out its assigned tasks. The Air Force had one team at Tan Son Nhut and another at Udorn to study ROLLING THUNDER operations. Each had an operations officer, a communications security officer, and members of the Air Force Office of Special Investigation. The Navy manned another team for ROLLING THUNDER coverage, using the Seventh Fleet as its base, with personnel in positions corresponding to those of the two Air Force teams. A third Air Force team, based at Kadena Air Base, Okinawa, covered both ROLLING THUNDER and ARC LIGHT operations. Another Air Force team covered ARC LIGHT from Guam. Still another Air Force team was at Bien Hoa to cover BLUE SPRINGS operations. These teams included SAC, AFSS, Office of Special Investigation, and PACAF officers. The remaining team was with MACV in Saigon. It covered flight route package #1,* forward air control (FAC) missions, and ARC LIGHT operations. In all, 39 men drawn from the Army, Marine Corps, and Air Force served on the Saigon team. Significant to the success of PURPLE DRAGON were the chiefs of the teams, each a senior air operations officer familiar with the air operations being investigated.

In addition to the seven teams, a CINCPAC J–3 staff unit of 5 men worked at CINCPAC headquarters on the three operational aspects of PURPLE DRAGON—operations survey, communications-electronics, and counterintelligence. Technical assistance for the J–3 unit came from the offices of NSA Pacific and the Defense Intelligence Agency.

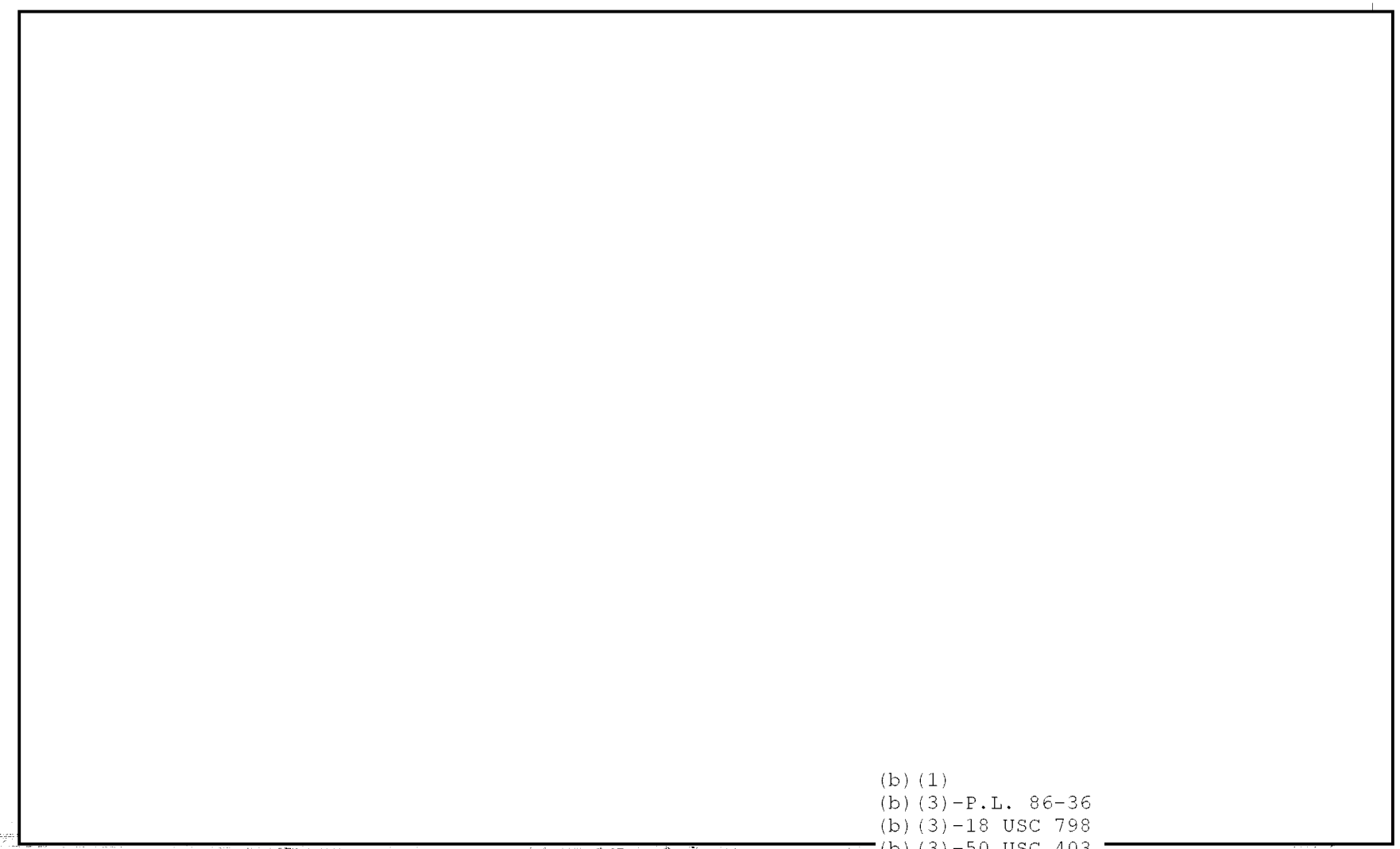
PURPLE DRAGON was to focus on what an enemy SIGINT organization might obtain and also on the damage that could be done through spy and other agent activity.

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



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

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



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

[redacted]

Corrective Actions

In the three types of air operations the PURPLE DRAGON teams examined, the element of surprise was too frequently lost and along with it the effectiveness of the operations. Of major concern was the increased threat to the lives of the ARC LIGHT and ROLLING THUNDER crews and the safe return of the planes and drones. In each of the three types, PURPLE DRAGON initiated some specific corrective action.

BLUE SPRINGS In studying drone operations, the Air Force team at Bien Hoa found that pre-operations planning messages were going via HF single sideband from Bien Hoa Air Base to Da Nang Air Base with BLUE SPRINGS information encoded in KAC–72, a SAC world-wide operations code. Disagreement existed among the specialists as to whether the Chinese Communists were actually decoding the messages or only relating them by traffic analytic considerations (lengths, timing, addresses, and so forth) to the drone reconnaissance missions. By observing only the message lengths and external characteristics of HF SSB transmissions encoded in KAC–72, PURPLE DRAGON personnel in December 1966 were able to accurately predict 18 of the 24 missions they tested. Of the 6 missions not predicted, 3 were canceled, one was planned 42 hours in advance, and the planning messages for 2 went by landline telephone instead of by HF SSB radio. [redacted]

[redacted]

There was also a general upgrading of COMSEC materials for BLUE SPRINGS communications. COMSEC improvement included the replacement, on 1 June, of KAC–72 with KAC–154. A new code, KAC–227, later came into use for communications formerly passed in KAC–72 but was not introduced specifically for communications

*See page 141.

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

associated with the drone program. For continued cover on the Bien Hoa–Da Nang link, the Air Force introduced a new code, KAC–238. In January 1968 the Air Force began using a KW–26 secured teletypewriter circuit, a still better method for these communications. Later in 1968, the Air Force installed a HY–2/KG–13 secure voice system for use between Bien Hoa and Da Nang for operational communications.

[redacted]

The PURPLE DRAGON survey was highly successful, therefore, in tightening BLUE SPRINGS security. The resulting increase in operational effectiveness was equally dramatic: the recovery rate of the drones increased from 35 percent to 70 percent by November 1967.*

ARC LIGHT [redacted]

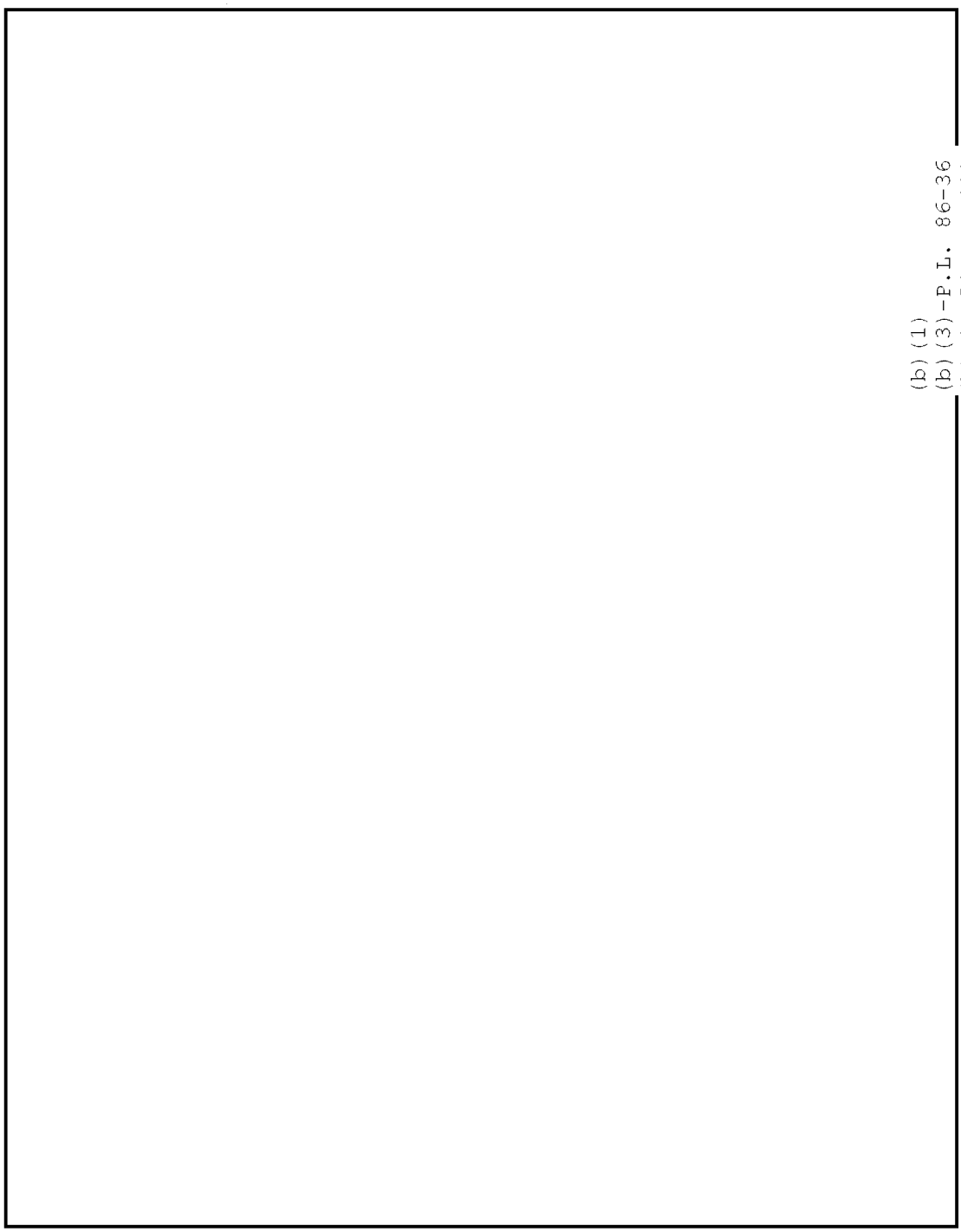
[redacted]

To achieve this success, the Air Force had to curtail the dissemination of information to civil aircraft traffic control authorities. Instead of passing altitude reservation requests in the clear several hours in advance to both Manila and Saigon, the Air Force began transmitting them only to Saigon and then only in classified form as an immediate action.

The PURPLE DRAGON teams dealt with the basic problems of general broadcast NOTAM's by eliminating the need for them. Air traffic control centers at Hong Kong, Manila, Taipei, and Bangkok had

*Some briefers attributed an even greater percentage increase in recovery of drones to the COMSEC measures taken. The percentages given were supplied by AFSS. Other factors such as the weapon firepower of the various enemy areas photographed would also affect the percentage of the recovery.

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



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

been including in their unclassified NOTAM's not only flight information for overflight of South Vietnam but also the estimated time of plane arrival (ETA) at Point Juliet, a common rendezvous for planes over water between Guam and South Vietnam. Using this information, PURPLE DRAGON analysts had been able to swing a time arc and predict with more than 80 percent accuracy the location and time-over-target of ARC LIGHT strikes. PURPLE DRAGON recommendations eventually led to the establishing of a corridor for entry into and exit from South Vietnam air space and to the declaring of a block of air altitude reservations on 24-hour reserve for SAC B–52's.

To offset the problem of releasing strike information to native villagers with the probability that the data would reach the enemy, certain areas known to be basically without friendly elements were declared "free areas for aircraft bombing." The result was that friendly forces stayed out of the free areas, except under special arrangement, and no notices of strikes were issued to local authorities. The Air Force also discontinued the practice of having B–52's call in launch reports (unencrypted over single sideband) to SAC headquarters each time a bomber departed Guam.

As a result of these steps, PURPLE DRAGON enjoyed success in restoring the element of surprise to SAC's B–52 missions, a goal not achieved as a result of the earlier Guam study or of CINCPAC's ARC LIGHT survey. The chart on the opposite page documents the PURPLE DRAGON success.

ROLLING THUNDER The PURPLE DRAGON teams working on ROLLING THUNDER could not bring about the dramatic improvements that those working on the drone and B–52 programs achieved. Although PURPLE DRAGON analysts identified several forewarning indicators that the enemy might have exploited in ROLLING THUNDER, [redacted] The PURPLE DRAGON teams nonetheless suggested a number of general actions to improve ROLLING THUNDER operational and communications security. These included reducing the number of recipients of flight information;

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

shifting, when possible, from unencrypted to encrypted communications; revising callsign usage; applying communications cover; revising code procedures; checking adherence to Red/Black criteria; and providing COMSEC education.

Admiral Sharp, CINCPAC, forged in PURPLE DRAGON a viable approach to attaining operational security (OPSEC) for air operations. By assigning COMSEC specialists to military operational staff elements, Admiral Sharp assured himself of COMSEC results. PURPLE DRAGON monitoring was in accordance with established guidelines for surveillance. Upon the completion of PURPLE DRAGON, Admiral Sharp asked the JCS to approve the establishment of a permanent operations security function on the CINCPAC staff [redacted]

[redacted]

JCS approved and Admiral Sharp created an 18-man OPSEC unit in the J-3 staff. While the PURPLE DRAGON field teams no longer existed, it became standard practice for about a third of the J-3 OPSEC staff to be on duty at field locations or in travel between them.

The effectiveness of the operations security approach, in which COMSEC surveillance played a major role and in which command emphasis on COMSEC was assured, led to a World-Wide Operations Security Conference held at Arlington Hall Station from 30 April through 2 May 1968. The purpose of the conference was to make information on CINCPAC's PURPLE DRAGON operations security program generally available and to promote use of the operations security concept in other commands and other geographic areas.

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

CHAPTER IV

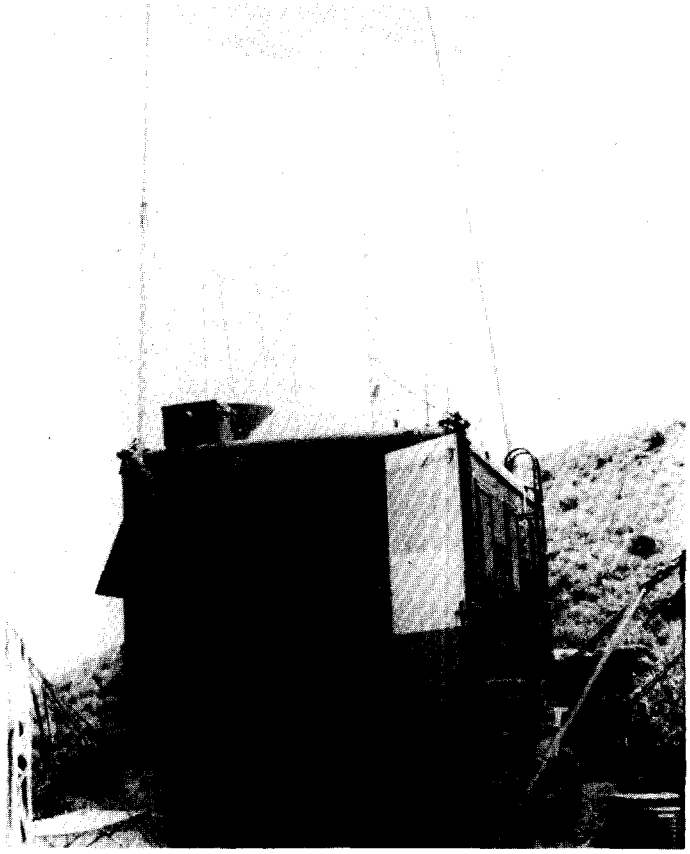
Communications Cover and Deception

Communications cover and communications deception consist of two separate but related techniques. Communications cover is the technique of concealing or altering the characteristics of communications patterns for the purpose of denying to the enemy information that would be of value to him. Communications deception is the deliberate use of communications to mislead the enemy and acquire a security, military, or political advantage.

Authorized communications cover and deception (CC&D) programs in Vietnam were administered and operated by a relatively small number of COMSEC specialists who normally were in close touch with monitoring and analysis programs and who used the product of the monitoring operations in planning CC&D operations. The specialists also used the findings of the monitors, [redacted] in altering operations underway and in evaluating them when completed. To assure security for their programs, CC&D specialists tended to compartment their functions or at least apply very rigidly the need-to-know principle. At the tactical level, operational commanders had responsibility for CC&D.

Within all three Services, CC&D expertise was scarce in the war zone. Until late 1966 no one in the Army on regular duty status in Vietnam was qualified to conduct a good communications deception effort. Those available after that time who did have the necessary experience worked primarily on other COMSEC tasks. Beach jumper units undertook CC&D functions for the Navy in the war zone. The Air Force did not have CC&D specialists permanently stationed in the war zone. Higher AFSS headquarters personnel—or those on TDY in the war area—supervised those CC&D operations conducted during this period. In comparison with known enemy employment of CC&D, U.S. forces made very little use of communications deception and ignored in large measure the possibility of using CC&D techniques to mislead enemy SIGINT operations, and hence enemy tactical reactions.

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



BJU COMSEC Van at Hill 327, Da Nang

NSA played a minor role in CC&D operations. It participated in the review of communications cover plans for operations in Vietnam and provided advice, through Headquarters, NSAPAC, on CC&D application by the Services.

Communications Cover

While the average COMSEC specialist applies his COMSEC skills primarily within a limited phase of electrical communications, the communications cover specialist employs a wide range of communications security techniques. In achieving cover, he considers the best application of (1) available cryptosystems for a specific communications requirement, (2) any nonelectrical communications, (3) techniques to minimize the intelligence vulnerability of communications, and (4) radio silence.

One often-recommended communications cover technique involves the flattening out of peaks and valleys in the volumes of communications passed by using dummy traffic or by minimizing the volume of messages normally passed as a result of crisis or just before an operation. This flattening of traffic volumes automatically appeared on many circuits in Vietnam as a result of near full-circuit utilization in the passing of valid traffic. However, flattening was at times used intentionally. The Air Force employed communications cover, to give one example, for SAC BLUE SPRINGS drone reconnaissance flights during 1967. To smooth out traffic patterns over an HF single sideband communications link between Bien Hoa and Da Nang, which was apparently being intercepted by the Chinese Communists, the control element sent a minimum of three transmissions daily. All of these were encoded in KAC–72 and consisted of a minimum of 45 groups. Communicators sent dummy messages ending with the phrase, "This is a sample message." Before the use of this cover, it was believed that the timing, length, and over-all characteristics of the occasional valid mission orders served as tip-offs to enemy analysts.*

Communications Deception

Communications deception is of two types. Imitative communications deception (ICD) involves intruding on an enemy's communications with signals or message traffic in imitation of his own communications for the purpose of deceiving him. This kind of deception requires great technical and linguistic skill and is difficult to achieve convincingly. There is no available record of any of the Services using ICD in Vietnam.

Manipulative communications deception (MCD), the second type of deception, is the use of one's own communications so as to cause an enemy to derive, and accept through his SIGINT, false information that would be disadvanteous to him. U.S. forces did employ this technique in Vietnam with mixed success. On some occasions U.S. forces combined communications cover with manipulative communications deception and referred to the results as manipulative communications cover and deception (MCCD).

*See also p. 134, above.

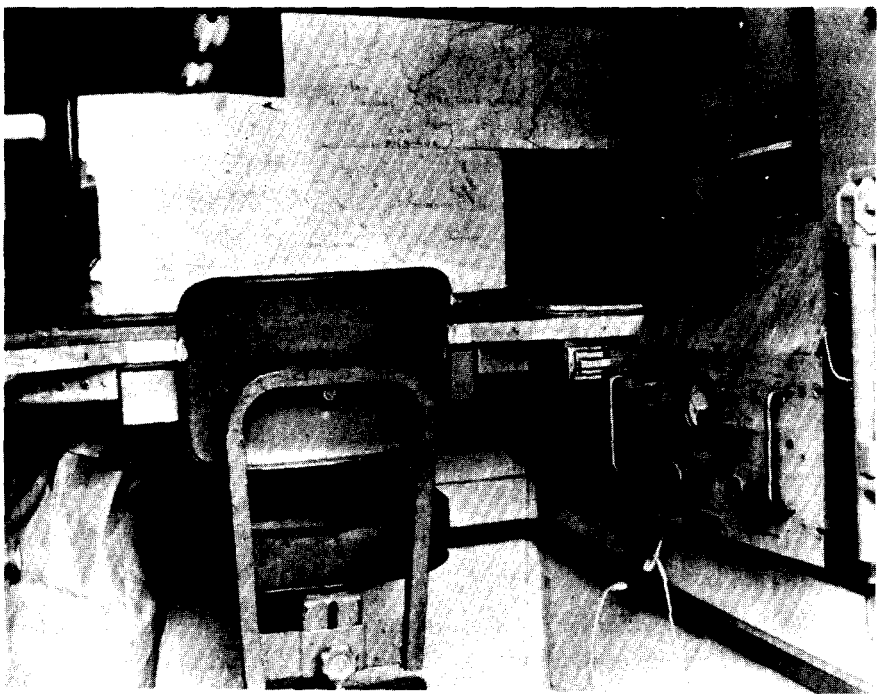
Army MCD

The Army seldom used MCD during the years to 1968; it was never used by a major Army command. More often than not, according to 509th ASA Group sources, the Army applications consisted primarily of homemade efforts attempted below division level and did not involve cryptologically trained personnel. Commanders simply composed and transmitted clear-text bogus messages over their own command radios and nets in an attempt to mislead the enemy concerning U.S. intentions. Army commanders rarely involved ASA specialists in these MCD attempts. There were, however, three Army MCD operations worthy of note.

The first was conducted between 29 March and 14 April 1966 by the 3d Brigade of the 1st Infantry Division during Operation ABILENE in Phuoc Tuy Province. [redacted] During the last days of the operation, the enemy had evaded all offers of battle, strongly suggesting that he might be engaging in close-in intercept of U.S. communications. The commanding officer of the 3d Brigade, assisted by the 337th ASA Company, drew up a communications deception plan to lure the enemy, if he was monitoring, back into the area of operations for an ambush. The plan was to make the enemy think the brigade had left the area. Thus, two U.S. companies stayed in concealed positions and maintained radio silence, while the remainder of the force obviously, and with normal communications, withdrew from the area, using several clear-text messages to reveal the withdrawal. The two companies were positioned for ready reaction in case the ruse succeeded. When the enemy did not reoccupy the area after three days, the stay-behind U.S. units also withdrew.

A second MCD attempt involved the 11th Armored Cavalry in 1967. One squadron of the regiment, apparently without assistance from its DSU, the 409th ASA Detachment, tried a similar ruse. The squadron sent out a bogus message in clear text to which the enemy, if listening, might have reacted. The message, from the regimental commander to the 2d Squadron, advised the squadron of indications that the enemy might be operating in the Quang Buan rubber plantation—near which, in fact, an enemy force was suspected—and directed the 2d Squadron to

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



Truck-mounted ASA Reporting and Analysis Center

send a troop to support infantry in that area for the next 36 hours. It was hoped that the troop would draw a major ambush in the area, for which a squadron reaction force was ready nearby. Again, however, there was no success. The 303d ASA Battalion first became aware of this MCD attempt when it monitored and investigated the clear-text message, which appeared to the ASA unit to have been a gross violation.

The third MCD operation did have a successful outcome. The 303d ASA Battalion in 1967 wanted to test the extent of VC interception by a planted, controlled breach of COMSEC. Lt. Col. Norman J. Campbell, the 303d commander at the time, reported:

> After losing some time attempting to approach the Corps (II FFV) staff on such an attempt (they opined they'd have to clear it with MACV, which would take quite a bit of staffing!), the CG, 199th Infantry Brigade (BG Forbes), said he could do this with us. Therefore, in an operation working with the DSU (856th RR Det), he ordered a battalion in the field to send a message by usual

communication, ordering several companies to remain out in separate field locations one night, rather than returning to the battalion base. At the same time, he ordered the companies, by discrete instructions, to disregard the message and surreptitiously return to the battalion base. This worked, apparently, proving that the VC were monitoring the nets, for the VC attacked the supposedly weakened battalion base that night, but since all three companies were in, the VC got clobbered and later relocated. At Corps, LTG Weyand thought this was a good start at /applying/ communications deception planning at Corps level which would be useful tactically to trap further VC reactions, and sent such a recommendation cable to MACV. However, not much appeared to have been done in this respect before I left SVN.

This is the only Army MCD operation in Vietnam in 1964–67 for which there is evidence of success.

Navy MCCD

In April 1965, with JCS authorization, Admiral Sharp encouraged the use of manipulative communications cover and deception in support of tactical operations against the Vietnamese Communists. General Westmoreland, over-all coordinator for the operations, and the three CINCPAC Service component commanders had authority to plan and conduct MCCD operations in accordance with the guidelines that CINCPAC set down. The CINCPAC directive specifically encouraged use of MCCD on the MACV–CTF 77 coordination circuits. CINC Pacific Fleet assigned to the commander of the Seventh Fleet the Navy responsibility for planning and conducting MCCD operations in the Southeast Asia area.

In June 1965 the commander of the Seventh Fleet held a conference with representatives from the Task Force 77 and 71 staffs, tactical deception units, and COMSEC units to discuss plans for using MCCD in Navy tactical operations. Although they did not adopt the plan, the representatives for a while considered a concept for the use of MCCD in MARKET TIME operations that would lure into a trap the enemy's large wooden junks and steel hull cargo vessels approaching from seaward. The concept called for the formation of a rigid outer barrier patrol by ships available to the commander of Task Force 71. After a given period of time, when it could be assumed that the North

Vietnamese had discovered the barrier pattern by analyzing uncovered communications, the ships would leave their patrol stations under total electronic silence and take up positions to close the weak points in the barrier. During this maneuver a tactical deception unit would maintain a communications picture indicating that the rigid barrier pattern was continuing. While this concept had merit and many supporters, it was never fully tested because there was no firm intelligence on the manner by which the North Vietnamese controlled the junks and cargo vessels.

The Navy conferees adopted no particular concept as a result of the MCCD meeting in June 1965, but one positive result was a recommendation that went first to CINC Pacific Fleet and then to CINC Pacific concerning communications and coordination control for MCCD. As a result, CINC Pacific modified its policy in August 1965, delegating responsibility for coordinating MCCD operations to Service component commanders and enabling Service components further to delegate approval authority for MCCD to lower echelon tactical commanders.

Although the initial MARKET TIME deception concept was never adopted as such, the commander of Task Force 71 employed a similar MCCD concept in MARKET TIME operations on several occasions during July 1965. The objective of the plan was to determine if changes in the location and pattern of the ships patrolling the outer barrier would result in corresponding changes in the infiltration patterns. Information derived from the operation would help in preparing follow-on deception plans.

On 20 July Task Force 71 had eight destroyer escorts on patrol in the northern portion of the seaward barrier, a thin defense for a large area. Through MCCD, the task force commander hoped to simulate the presence of eight additional Destroyer Squadron 19 ships in this northern area. The communications pattern was to give a picture of a strong lineal patrol in the northern area.

Two tactical deception teams, aboard two northern patrol ships, had the task of manipulating the communications of the Northern MARKET TIME Coordination and Reporting Net in order to present a picture of the strong lineal patrol. The net was an uncovered voice net on which operational and numerical codes rarely appeared and most traffic was in the clear. During the first deception period tactical units shifted to an alternate frequency so that the regular frequency carried only deceptive

traffic. During the second period the tactical units remained on the regular frequencies and deception traffic was superimposed on the circuit. The deception script called for the traffic to be predominantly plain text, with a small volume of encoded traffic to match actual traffic normally transmitted on the net.

To achieve realism, the tactical deception teams used the actual voice call signs of eight Destroyer Squadron 19 ships. The ships were actually just entering the WESTPAC area and would not be involved in any operations in MARKET TIME during the deception operation. For the period of deception, the commander of Destroyer Squadron 19 was to refrain from using these call signs on other than line-of-sight circuits.

The COMSEC unit at the Naval Communications Station Philippines was to monitor the Northern MARKET TIME Coordinating and Reporting Net and associated area circuits and report by message to the task force commander any discrepancies or variations in previously observed patterns or procedures that would inform the enemy that the operations were of a MCCD nature.

During the first few days of the deception operation, the COMSEC unit did detect and report deviations from previously observed patterns and departures from realism—misuse of operational and numerical codes, employment of dummy codes and authentication systems rather than actual systems, improper preparation of deception messages, referencing of HFDF positions not coinciding with reported positions, citing of unrealistic underway replenishment schedules and times, and other irregularities suggestive of communications deceptions. The COMSEC monitoring reports also showed, as a by product, that the entire barrier operation, including positions, movements, patrol areas, and future plans, was susceptible to reconstruction through intercept and analysis of communications going over the Northern MARKET TIME net.

Perhaps the major reason for possible failure of the operation was a lack of continuous liaison between the commanders of Destroyer Squadron 19 and Task Force 71 during the MCCD period. Unknown to the commander of TF 71, two of the ships of the destroyer squadron went to Subic Bay and were transmitting on the Subic Harbor Common Net—a medium frequency net—when the deception operation started. Therefore, the same voice call signs were appearing at the same time on

the Subic Harbor Common Net and the MARKET TIME circuits, a point the enemy could hardly fail to notice.

By 24 July, the end of the first deception period, Task Force 71 had corrected most of the deficiencies, and the stage was set for another MCCD attempt. CINC Pacific Fleet issued new, completely fictitious voice call signs for use by the deception teams in the second phase of the deception operation. The commander of Task Force 71 objected to this on the ground that it would be immediately apparent to an enemy analyst that these were deceptive calls, but CINC Pacific Fleet overruled the objections. Therefore, on 27 July 1965, eight new voice call signs appeared on the communications net as hypothetical ships. Upon the appearance of these eight new voice call signs, the COMSEC unit immediately tagged them as deceptive, based on observation of the previous deception effort.

Other than the obviously fictitious voice call signs being used, the second attempt at deception proceeded very well. The lessons learned from the first attempt were put to good use. The general opinion was that the second attempt could have been quite successful had not the enemy already been alerted to look for deception because of the errors made during the first operation. Through use of more sophisticated COMSEC techniques such as HFDF, frequency measurement, and observation and comparison of background noise associated with the voice, the COMSEC unit was able to determine that transmissions purportedly originating from five different units were all emanating from a single platform.

The result of the July deception operation was inconclusive. No variation in the infiltration patterns of the North Vietnamese junks came to light. However, the MCCD operation probably achieved, as a minimum, CINCPAC's secondary objective of reducing the credibility of these communications and consequently making analysis by the enemy more difficult.

On 30 July 1965 the commander of Task Force 115, a joint commander under COMUSMACV, assumed responsibility for the MARKET TIME operations and discontinued deception activity.

Although many recommendations for the use of deception were made and considered, the Navy undertook no other significant MCCD operation in the years up to 1968, primarily because of a lack of security in communications, lack of security from visual observation, and rules of

engagement requiring detailed coordination with the South Vietnamese before each actual operation. However, the Navy did institute a broad CC&D educational program designed to reach all command levels responsible for CC&D operations.

There is no documentary evidence at hand to indicate that the Marine Corps conducted any major MCCD operations during this period. In October 1966 the commander of the III Marine Amphibious Force drafted an order setting forth basic policy and procedures for the employment of deception in support of ground tactical operations, along with specific examples and operational areas in which deception could be employed. The order was submitted through General Westmoreland to Admiral Sharp but was never approved for execution.

The Navy learned several valuable lessons for evaluating its MCCD operations in 1965. Although the Navy did have the ability to undertake tactical MCCD (and ICD, for that matter) with its trained tactical deception units, a general knowledge of how to use these assets was completely lacking among commanders, their planning and operational staffs, and personnel at all levels. The primary lesson learned was that the same men who conduct real operations must plan and conduct MCCD operations, and the commanders must assume MCCD responsibility rather than assigning it to the technical tactical deception units. Deception operations must also be completely realistic and must be genuinely integrated with actual operations.

Air Force MCCD

In World War II and the Korean War, enemy aircraft aggressively contested Allied control of the skies; however, in the Vietnam War the air over North Vietnam was relatively free from challenge by enemy aircraft. Most American planes shot down fell to antiaircraft fire and surface-to-air (SAM) missiles. Until 2 January 1967, the entire 23 months of the air war had produced only 27 air-to-air "kills" against the North Vietnamese, and only 10 U.S. aircraft had fallen prey to enemy MIG's. Shying away from dogfights, North Vietnamese pilots preferred to harass U.S. fighter-bombers on their runs over North Vietnam,

attempting to make the U.S. planes jettison their bomb loads short of the targets or to burn extra fuel in evasive maneuvers.

In December 1966 the Seventh Air Force planned an aerial ambush, Operation BOLO, to force a confrontation with the enemy's best aircraft—the MIG–21 Fishbed fighters.* BOLO involved both electronic (radar) and manipulative communications deception. The essential feature of the plan, implemented on 2 January 1967, was a deception that would cause the enemy to assume that a flight of the U.S. 1,600-mile-per-hour F–4C Phantom fighters was actually a flight of the slower moving U.S. F–105 bombers against which the MIG–21 had a better than equal chance in air-to-air combat.

The plan of operation was to fly the superior U.S. F–4C's from bases in Thailand and South Vietnam, using flight paths, speeds, and communications duplicating those of the well-established flight characteristics of the slower F–105's. It was hoped that the deception would be effective until the F–4C's were in visual contact with the MIG–21's rising to meet them. When the engagement took place, other F–4C's, including some that had flown up along the Gulf of Tonkin, were to guard known North Vietnamese airfields for 53 minutes to prevent the enemy aircraft from returning to them.

In all, 52 F–4C's and 24 F–105's flew to North Vietnam in Operation BOLO using the Laos and Gulf routes. The first three flights through Laos proceeded to the northern tip of the mountains located north of Phuc Yen to engage the Phuc Yen MIG cover air patrol. Two flights from Da Nang hovered northwest of Haiphong in case MIG's tried to run in that direction. Also, SAM suppression flights (IRON HAND) trolled for SAM's northwest of Phuc Yen and north and southeast of Kep.

Arranging deception for the operation was not easy. Extreme caution was necessary to keep from compromising plans through loose talk or other action such as necessary relocation of aircraft. To the extent practical, the F–4C's were physically disguised to simulate the larger

*Two primary sources were used for this description. The one, a special historical study written by the historian at the PACSCTYRGN soon after Operation BOLO, was forwarded by a USAF letter to NSA, sub: Material for NSA/SCA Cryptologic History, 3 July 1969, TOP SECRET Codeword. The other was a USAFSS draft input to the History project, Vol V, Part III, Chapter 3, TOP SECRET Codeword, undated.

F–105's on the enemy radar screens. While in flight, the F–4C's flew at speeds and altitude normal to those of the F–105's. The F–4C's achieved communications deception by using F–105 call signs and standard communications frequencies. At the time, the F–4C's and the F–105's both operated in flight without ciphony; for the most part, all communications were in plain language.

For certain essential information the regular practice was to use red and yellow color codes, which allowed for low-grade encryption of information such as the status of enemy aircraft. For the BOLO operation, planners introduced several changes. One was the use of new "one-operation" code communications systems. North Vietnamese airfields used by MIG aircraft were each given a code name. Also, four special code words, each with a specific meaning, were assigned to the operation: *LAS VEGAS* meant situation as expected, MIG's reacting; *EL PASO* meant situation not as expected, MIG's quiet; *LOS ANGELES* meant MIG's disengaging; and *NEW YORK* meant Chinese aircraft coming over border.

The geographic reference plotting system (GEOREF)* was to be used to give MIG locations and consisted of two letters for GEOREF block designation and two numbers (rounded off at the 10's digit). Headings of enemy MIG's were to be given only to the nearest 10 degrees and given in two digits. When a MIG heading was unknown, a two-digit number higher than 36 would be used. MIG altitudes were to be given in thousand-foot increments and passed as two digits. When the altitude was unknown, an exceedingly high number would be passed, for example, 99. Insertion within the GEOREF of odd (1 or 3) and even

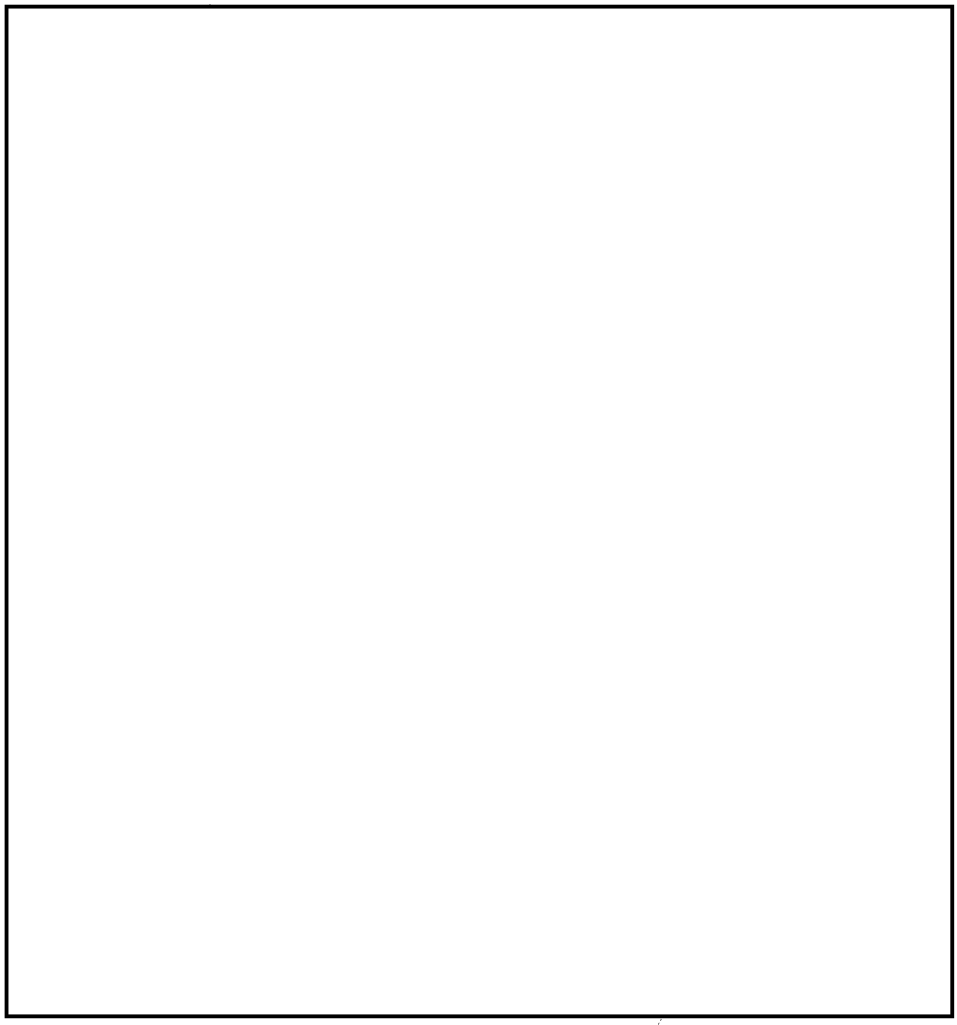
*In the geographic reference plotting system, the world is divided into 288 15-degree quadrangles. Each of these 15-degree quadrangles is identified by a two-character designator (row and column coordinates). Each of these 15-degree quadrangles is broken down into 1-degree quadrangles, which are again identified by two-character designators. Characters used for these identification purposes are the letters A through Q, omitting the letters I and O. When reporting a GEOREF position, the 1-degree quadrangle is followed by the longitude minute coordinates of the position within the 1-degree quadrangle. Two 15-degree GEOREF quadrangles (UH and VH) cover the majority of the Southeast Asian area of interest.

numbers (2 or 4) indicated, respectively, launch and recovery of MIG's. Some specific examples of possible use were:

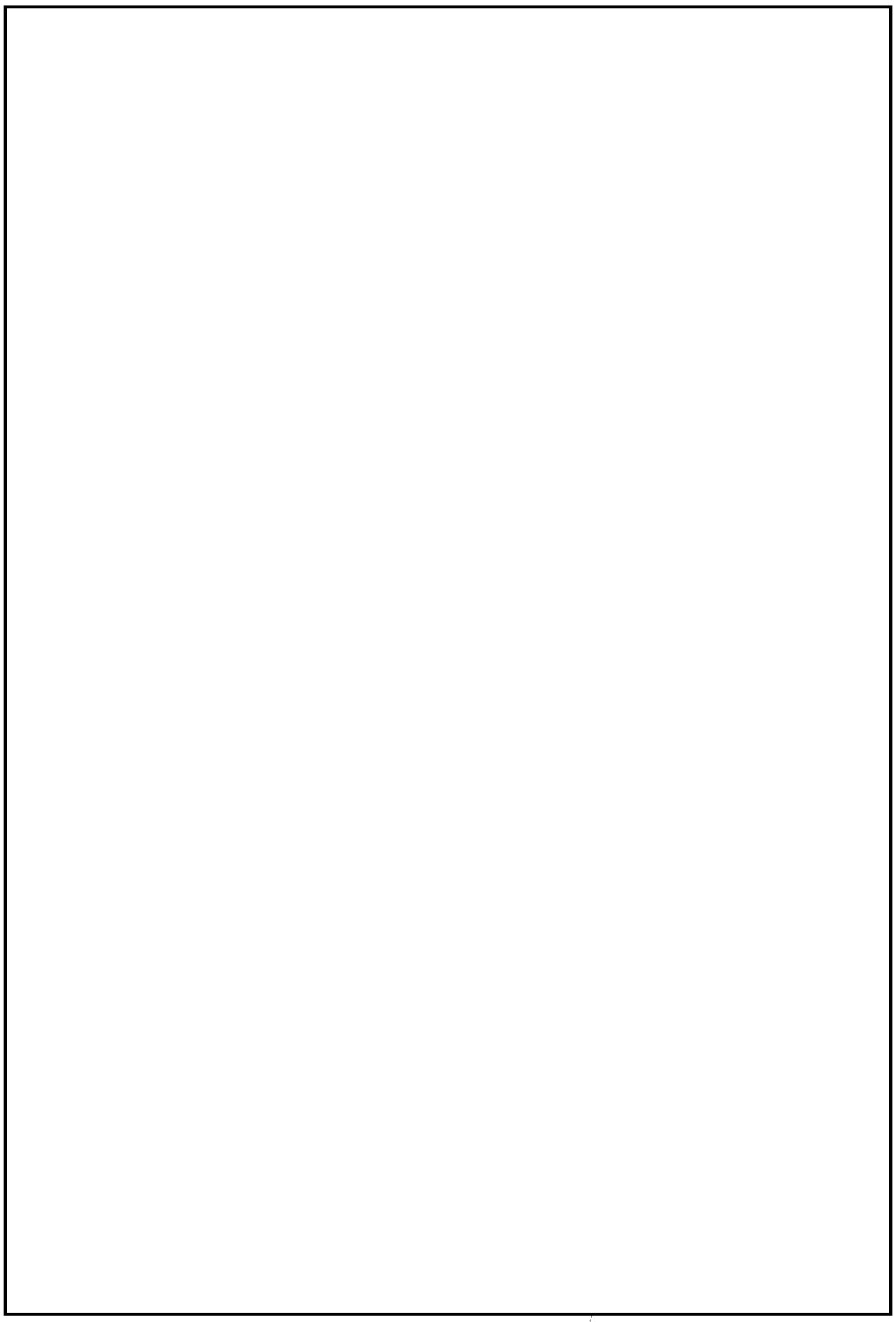
ETHAN BRAVO (daily MIG call word) AG 27 15 would mean "MIG's over mountain heading 270 degrees at 15,000 feet."

ETHAN BRAVO *Chicago* YG 44 99 88 would mean "MIG's landing Kep."

ETHAN BRAVO *Frisco* AG 33 85 99 would mean "MIG's scrambling from Phuc Yen."



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



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

Operation BOLO, as is frequently the case when MCCD is employed, required that communications facilities be used in an unusual manner and that there be no pre-operation practice. The revised alert warning and special code usage also added complexity for communicators during the relatively short time of operation when tension of battle was at its peak. Postoperation analysis indicated that the special techniques for achieving security of communications did not cause any significant difficulty. PACSCTYRGN commended its Southeast Asia units for the initiative they displayed in response to Operation BOLO, saying that the actions demonstrated the unique capability of AFSS to support tactical air operations.

Equal praise is due those who planned and initiated the deception without which the MIG kill would have been impossible. Accounting for 7 MIG–21's in 12 minutes—in effect destroying one-third of the enemy's MIG–21 inventory—was a remarkable feat.

A number of other BOLO-type missions were flown over the ensuing months, the first on 23 January 1967, but either there was a pattern that alerted the North Vietnamese or other factors went wrong. Whatever the reason, none of the later missions achieved the success of BOLO.

Although all the Services engaged in communications cover and deception operations in the 1965–67 period, the sum total could not be called a success. However, through their failure and occasional successes, the Services did develop some basic theories upon which they could predicate later CC&D operations. CC&D operations should not be attempted by communications specialists acting alone; they need the full knowledge and cooperation of appropriate operations personnel, a clearly defined purpose, and a reasonable chance of achieving desired results. Even though CC&D operations might not require much time, expense, or effort on the part of communicators, often, especially for CC&D of a

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

more strategic nature, they mean putting hard-to-hide military resources (troops, ships, or planes) into a deceptive posture to correspond with false communications fed to the enemy, deployments that could be expensive and time consuming and could require resources, often in short supply, that conventional operational requirements make unobtainable. In addition, good CC&D operations need an effective means [redacted] of evaluating the enemy's response during and following the deception. Caution must also be used to prevent the enemy from overreacting.

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

CHAPTER V

Lessons Learned

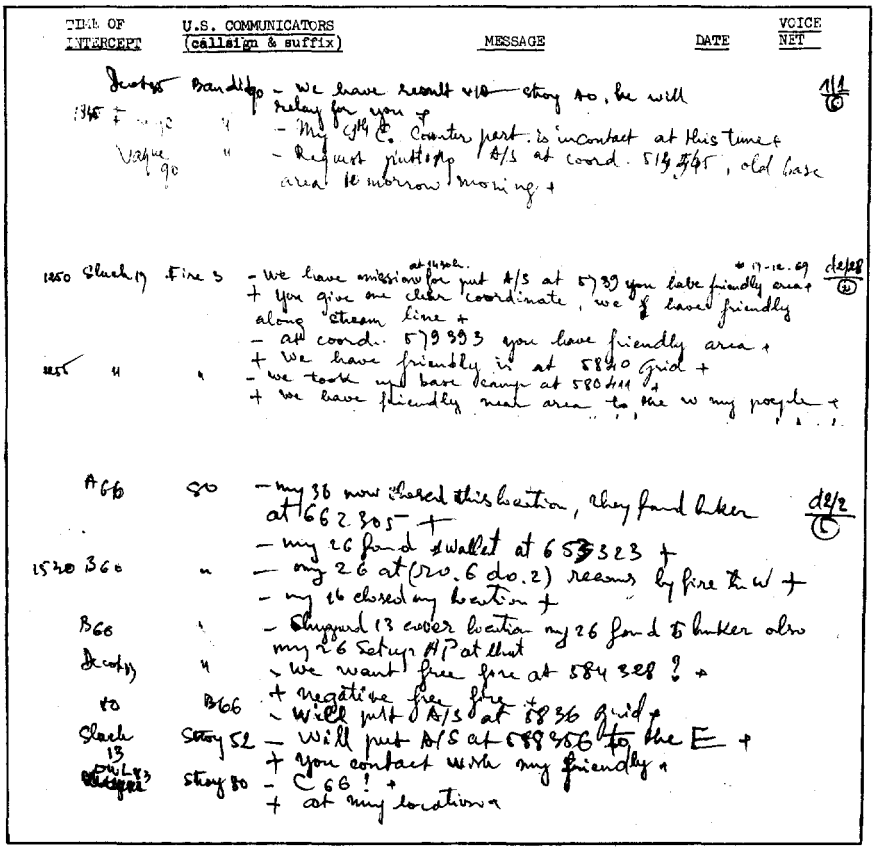
COMSEC Education

One major lesson learned from COMSEC monitoring in Vietnam is that a commander's attitude toward COMSEC determines in large measure the degree of COMSEC awareness within his organization. Ironically, for one reason or another it was often difficult to convince a commander that the enemy had an effective SIGINT operation targeted against him. [redacted] More often than not, it was only when the full implications of COMSEC deficiencies became apparent—sometimes painfully apparent—to him through COMSEC monitoring reports that the commander in Vietnam took steps to improve his COMSEC practices.

[redacted]

The U.S. COMSEC community should of course take all steps possible to indoctrinate the U.S. tactical commander in COMSEC before his arrival in the war zone and should not relegate this task to comparatively low-ranking COMSEC personnel working in the field. The U.S. COMSEC organizations have numerous examples from monitoring and analysis with which to demonstrate the consequences of poor COMSEC practices to the commander's complete satisfaction. They need to con-

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



TIME OF INTERCEPT	U.S. COMMUNICATORS (callsign & suffix)	MESSAGE	DATE	VOICE NET
[illegible]	Bandido 90	- We have result VID — story 80, he will relay for you +		11/C
1345 [illegible]	"	- My Gia Đ. Counter part is in contact at this time +		
Vague	"	- Request pinpoint A/S at coord. 514745, old base area 1K tomorrow morning +		
1250 Shark 13	Fire 5	- We have mission at 4 p.m. for put A/S at 5739 you have friendly area + * 17-12. 69		dc/28 D
		+ You give me other coordinate, we'll leave friendly along stream line +		
		- add coord. 579393 you have friendly area +		
1255	"	+ We have friendly in at 5840 Grid +		
	"	- we took up base camp at 580411 +		
		+ We have friendly near area to the W my people +		
	A66 80	- my 36 now closed this location, they found holes at 662305 +		dc/2 C
		- my 26 found 1 wallet at 653323 +		
1530	B66 "	- my 26 at (220.6 do.2) reasons by fire to W +		
		- my 16 closed my location +		
	B66 "	- Shipyard 13 cover location my 26 found 5 bunker also my 26 Setup AP at that		
	Bandido "	- We want free fire at 584328 ? +		
	to B66	+ negative free fire +		
		- Will put A/S at 5836 Grid +		
Shark 13	Story 52	- Will put A/S at 589306 to the E +		
[illegible]	Story 80	+ you contact with my friendly +		
		- C66 ! +		
		+ at my locations +		

Vietnamese Communist Intercept of U.S. Clear-text Communications. The communications give information on future U.S. air strikes (A/S). (Source: ASA TAREX unit.)

TIME OF INTERCEPT	U.S. COMMUNICATORS (callsign & suffix)		MESSAGE	DATE	VOICE NET
					1/1 6
	Decot 35	Bandit 90	We have result V/R Stroy AO, he will relay for you+		
1835	Fire 90	"	My 9th Co counterpart is in contact at this time+		
	Vague 90	"	Request position A/S at coord 514545, old base area tomorrow morning+		
				17-12-69	D2/28 2
1250	Sluch 17	Fire 3	We have mission at 1430 for put A/S at 5739 you have friendly area+		
			+You give one slear coordinate, we have friendly at coord 579393 you have friendly area+		
1255	"	"	+We have friendly is at 5840 grid+ We took up base camp at 5804;i+		
					D2/2 5
	A66	80	My 36 now closed this location, they found bunker at 662305+		
			My 26 found 1 wallet at 653323+		
1530	B60	"	My 26 at (R0.6 D0.2) reachs by fire to W+		
	B66	"	My 16 closed my location+		
			Sluggard 13 cover location my 26 found 5 bunker also my 26 set up AP at that+		
	Decot 33	"	We want free fire at 584328?+		
			+Negative free fire+		
	80	B66	Will put A/S at 5836 grid+		
	Sluch 13	Stroy 52	Will put A/S at 588356 to the E+		
			+You contact with my friendly+		
	OWL 83	Stroy 80	C66?+		
			+At my location+		

Typescript of Intercept

vince the commanders that the enemy has an active, sophisticated SIGINT program in the war zone, [redacted] They need to assure that the commander going to Vietnam understands that COMSEC is, in fact, the only weapon he has against the enemy SIGINT organization.

The COMSEC community has taken a few steps to achieve this indoctrination for service personnel. It has arranged for improved briefing materials for use in COMSEC education of higher level Service officers. The Army and NSA have exchanged prepared briefing aids for use in briefings of this kind, and the National Cryptologic School at NSA, starting about 1967, has been offering courses to Service personnel that highlight the enemy SIGINT threat and stress the importance of communications security. The NSA school courses have been of significant value to those who have attended, but unfortunately attendance has generally been limited to those already serving in cryptologic positions; few prospective commanders of combat units have attended. NSA and SCA headquarters have also prepared educational briefings for use by CINCPAC and CONUS-based commands. There remains, however, no uniform, comprehensive COMSEC educational program for tactical commanders.

Despite the various constructive efforts the COMSEC community has made, it has still failed to convince some tactical commanders that they need COMSEC at all. As late as May 1969, NSA received word that a U.S. Army brigade commander in South Vietnam had requested "that all COMSEC support to his unit be discontinued."*

The COMSEC community must also give attention to Service communicators. When commanders are COMSEC-conscious, their communicators generally adhere to prescribed routines. When the commander is not so predisposed, Service communicators who are aware of the implications of COMSEC can still help protect communications. Here again awareness of the enemy's SIGINT operations can provide the necessary conditioning for acceptance of COMSEC advice. [redacted]

*From a "FACT SHEET," sub: COMSEC Support to 1st Bde, 5th Inf Div, prepared by Maj. W. F. Gress, 20 May 1969, CONFIDENTIAL.

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

[redacted] As in the case of the commanders, the ideal would be to indoctrinate communicators before they arrive in the war zone.

The CC&D Paradox

Events have shown that the U.S. Services were not well prepared to employ communications cover and deception. When CC&D operations were tried, the deception techniques, difficult to apply successfully even under optimum conditions, worked best when they involved SCA personnel and when operations staffs and commanders planning the CC&D had direct responsibility for conducting it.

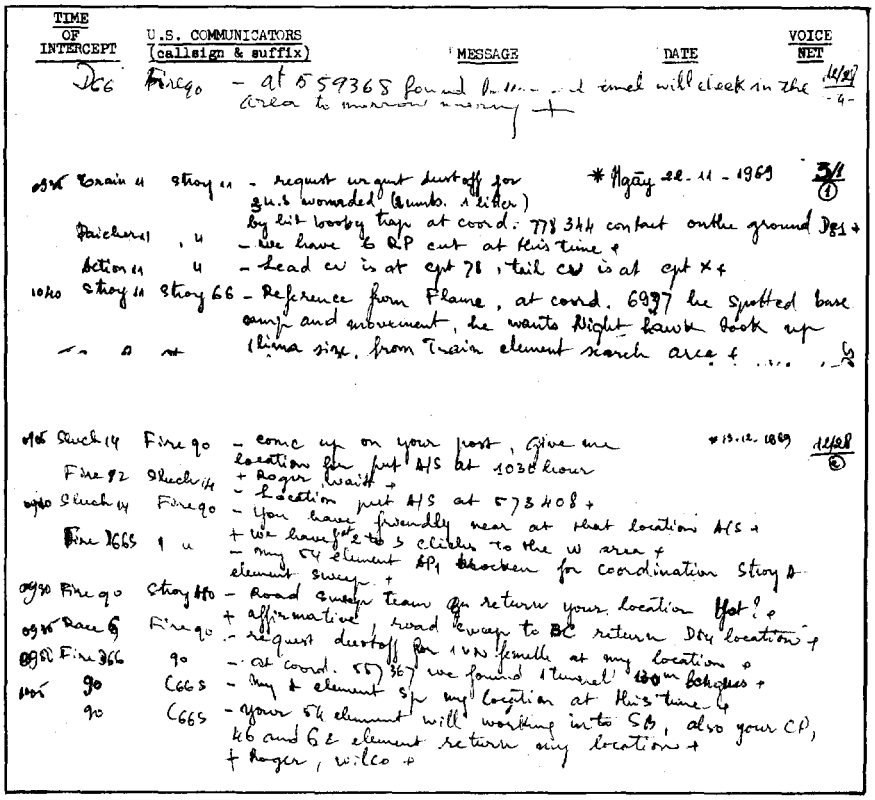
It is of interest to note that, except for some "home-grown" deception operations planned and conducted without consultation with SCA personnel, the Services often seemed reluctant even to use either imitative communications deception or manipulative communications deception. Paradoxically, the enemy practiced ICD with frequent success. The U.S. appears to have lost a good opportunity to put the enemy at a military disadvantage through communications deception at the tactical level. Success in deception such as that achieved by the Air Force in Operation BOLO, which accounted for the loss of one-third of the NVN MIG–21's, certainly should have stimulated other major U.S. deception operations.

The Armed Forces in Vietnam also had only limited success in applying communications cover. General overloading of communications circuits, a common situation during at least the early war years, inhibited the application of communications cover on most traffic lanes. For successful communications cover operations COMSEC specialists obviously must first have a communications structure with enough flexibility to permit the alterations required.

New Concepts for Old Problems

At the beginning of U.S. combat involvement in Vietnam, the concept in monitoring called for the U.S. specialist to duplicate what an enemy SIGINT analyst might attempt. If the U.S. analyst failed to make

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



TIME OF INTERCEPT	U.S. COMMUNICATORS (callsign & suffix)		MESSAGE	DATE	VOICE NET
1156	Fire 90		- at 559368 found [illegible] will check in the area to maintain [illegible] +		11/27 -4-
0956	Train 11	Story 11	- request urgent dustoff for 3 U.S. wounded (1 numb, 1 litter) by hit booby trap at coord: 778344 contact on the ground DS1 +	* Ngày 22-11-1969	3/1 ①
	Patches 11	11	- we have 6 RP out at this time +		
	Action 11	11	- head cu is at cpt 78, tail cu is at cpt X +		
1040	Story 11	Story 66	- Reference from Flame, at coord. 6997 he spotted base camp and movement, he wants flight hawk back up (lima size, from Train element search area + [illegible]		
0956	Stuck 14	Fire 90	- come up on your frost, give me location for put H/S at 1038 hour	* 13.12.1969	12/28 ⑤
	Fire 92	Stuck 14	+ Roger, wait +		
0956	Stuck 14	Fire 90	- Location put H/S at 573408 +		
	Fire 1665	1 11	+ We have 2 to 3 clicks to the W area +		
			- my 54 element APs checken for coordination Story 1 element sweep +		
0930	Fire 90	Story 110	- Road sweep team on return your location Hot? +		
0956	Race 6	Fire 90	+ affirmative / road sweep to BC return DS4 location +		
0956	Fire 366	90	- request dustoff for 1 VN female at my location +		
1005	90	C665	- at coord. 55)367 we found 1 funeral 130 on bokgues +		
	90	C665	- my 6 element sp my location at this time +		
			- your 54 element will working into 56, also your CP, 46 and 62 element return my location +		
			+ Roger, wilco +		

Vietnamese Communist Intercept of U.S. Clear-text Communications. The communications reveal specific information on future U.S. operations—locations of air strikes (A/S), medical evacuation (DUSTOFF), and troop movements—often with several hours advance notice. (Source: ASA TAREX unit.)

TIME OF INTERCEPT	U.S. COMMUNICATORS (callsign & suffix)		MESSAGE	DATE	VOICE NET
	D66	Fire 90	At 559368 found bunker and tunnel will check in the area tomorrow morning+	D2/28 2	
				22-11-1969	3/1 1
0935	Train 11	Stroy 11	Request urgent dustoff for 3 U.S. wounded (2 amb. 1 litter) by bit booby trap at coord. 778344 contact on the ground D81 +		
	Paicher 11	"	We have 6 RP cut at this time +		
	Action 11	"	Lead cv is at cpt 78, tail cv is at cpt x +		
1040	Stroy 11	Stroy 66	Reference from Flame at coord. 6937 he spotted base camp and movement, he wants Night Hawk took up 1 lima size from Train element search area +		
				13-12-1969	D2/28 2
0905	Sluch 14	Fire 90	Come up on your post, give me location for put A/S at 1030 hour+		
	Fire 82	Sluch 14	+Roger wait+ Location put A/S at 573408+		
0910	Sluch 14	Fire 90	You have friendly near at that location A/S+		
	Fire D66S	"	+We have F at 2 to 5 clicks to the W area+ My 54 element AP 1 brocken for coordination Stroy A element sweep+		
0930	Fire 90	Stroy A80	Road sweep team sp return your location yet?+		
			+Affirmative, road sweep to BC return D54 location+		
0935	Race 6	Fire 90	Request dustoff for 1 VN female at my location+		
0950	Fire D66	90	At coord 557367 we found 1 tunnel 130M bunkers+		
1005	90	C66S	My A element sp my location at this time+		
	90	C66S	Your 54 element will working into SB, also your CP, 46 and 62 element return my location+		
			+Roger, Wilco+		

Typescript of Intercept

headway in an attack on U.S. communications, then all was presumed well. However, such was seldom the case since the COMSEC analyst nearly always recovered sensitive information from the U.S. communications. In a sense, the COMSEC analyst therefore became a policeman writing out tickets for violations. One lesson learned in the early period was that this traditional COMSEC concept had limitations and that better use could be made of the specialized COMSEC skills. For better use of these skills, a closer working relationship between the COMSEC specialist and command, staff, and communications personnel became necessary.

Without changing its objective of securing U.S. communications, the COMSEC community has gradually been moving toward a new *modus operandi*—COMSEC surveillance. Under the new concept, analysts are not limited to reviewing monitored communications, but have access to all operational information—operational plans, communications modes, cryptographic systems, and other data—to help them in planning with the Service communicators for secure communication. COMSEC officials, after much consideration, designated a substantial number of COMSEC personnel as surveillance specialists. Monitoring therefore became as much a review of how well field-level COMSEC specialists had planned as it was a check on how well communicators themselves adhered to COMSEC procedures. COMSEC surveillance bridged the gap between communicator and COMSEC specialist and helped erase the image of the policeman. The new approach proved highly successful in the PURPLE DRAGON survey and other joint undertakings to achieve operational security for U.S. forces in Southeast Asia. While not all SCA and NSA personnel were in agreement, by 1968 there was general recognition that COMSEC objectives could best be achieved through the new approach.

Monitoring, however, will always be needed in one form or another. COMSEC specialists can arrange for secure equipment, educate commanders in the importance of communications security, instruct communicators in the use of codes, ciphers, and machines, enter into planning for communications support of the military operations, and participate in command actions to improve over-all operational security. But unless communications are monitored in order to measure the effectiveness of steps taken in the name of COMSEC, the Services will

have no means of evaluating the extent to which their communications may be feeding information to a SIGINT-hungry enemy. Despite sophistication in the design and manufacture of cryptomaterials, the United States will remain vulnerable to enemy SIGINT activity until the U.S. Services develop a commensurate sophistication and command emphasis in the use of those cryptomaterials.

Full Treatment for the Patient

This review of monitoring and analysis operations to 1968 has shown that the greatest COMSEC improvement has resulted when there was a combined Service attack on a single problem of general concern—

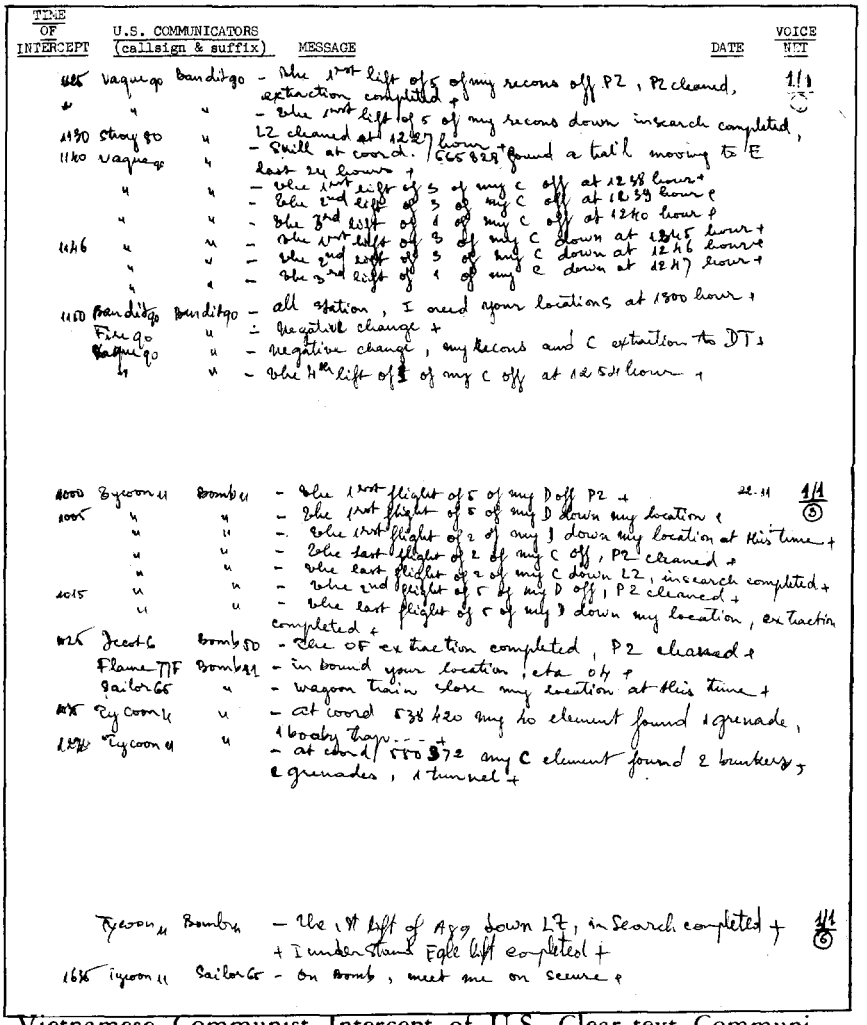
The PURPLE DRAGON, Guam, and MARKET TIME operations produced results far more meaningful than would have been the case had each Service performed its monitoring functions alone. The assigning of an operations name or nickname to the operation and the designation of an executive agent from among the Services, as in ARC LIGHT, or a joint command as in PURPLE DRAGON, seem to act as catalysts upon the participants.

Assumption of control at a joint command level brought the most advantages. It made possible more specific tasking for COMSEC analysts, improved exchange of COMSEC technology among the Services, and brought forth more comprehensive reporting by field elements for cryptologic and Service officials at higher levels of command. It also brought a more complete component command emphasis to correct deficient communications practices of all kinds, thus overcoming the usual practice of treating one symptom of a disease but allowing the patient to die of another. Finally it caused a wider appreciation of the quality and quantity of intelligence that the enemy could gain through lax COMSEC practices—this, a direct result of more comprehensive review of communications by all Services working on common objectives.

Better Systems, Better COMSEC

The 1965–67 Vietnam experience was no different from other recent war experiences in one major respect. So long as a communications system

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



TIME OF INTERCEPT	U.S. COMMUNICATORS (callsign & suffix)		MESSAGE	DATE	VOICE NET
1115	Vaquero	Banditgo	- Blue 1st lift of 5 of my recons off P2, P2 cleared, extraction completed +		1/1
"	"	"	- Blue 1st lift of 5 of my recons down in search completed,		
1130	Stray 80	"	L2 cleared at 1247 hours +		
1140	Vaquero	"	- Skull at coord. 655828 found a trail moving to E last 24 hours +		
	"	"	- Blue 1st lift of 3 of my C off at 1238 hours +		
	"	"	- Blue 2nd lift of 3 of my C off at 1239 hours +		
	"	"	- Blue 3rd lift of 1 of my C off at 1240 hours +		
1146	"	"	- Blue 1st lift of 3 of my C down at 1245 hours +		
	"	"	- Blue 2nd lift of 3 of my C down at 1246 hours +		
	"	"	- Blue 3rd lift of 1 of my C down at 1247 hours +		
1150	Banditgo	Banditgo	- all station, I need your locations at 1800 hour +		
	Fuego	"	- negative change +		
	Vaquero	"	- negative change, my recons and C extraction to DT's		
	"	"	- Blue 4th lift of 1 of my C off at 1250 hours +		
0000	Tycoon 11	Bomb 11	- Blue 1st flight of 5 of my D off P2 +	22.11	1/1
1005	"	"	- Blue 1st flight of 5 of my D down my location +		(5)
	"	"	- Blue 1st flight of 2 of my J down my location at this time +		
	"	"	- Blue last flight of 2 of my C off, P2 cleared +		
	"	"	- Blue last flight of 2 of my C down L2, in search completed +		
1015	"	"	- Blue 2nd flight of 5 of my D off, P2 cleared +		
	"	"	- Blue last flight of 5 of my D down my location, extraction completed +		
1125	Jeep 6	Bomb 80	- Blue OF extraction completed, P2 cleared +		
	Flame TF	Bomb 81	- inbound your location, eta 04 +		
	Sailor 65	"	- wagon train close my location at this time +		
1135	Tycoon 4	"	- at coord 538420 my 60 element found 1 grenade, 1 booby trap +		
1135	Tycoon 11	"	- at coord 550372 my C element found 2 bunkers, 2 grenades, 1 tunnel +		
	Tycoon 11	Bomb 4	- Blue 1st lift of Agg down L7, in Search completed + + I understand Eagle lift completed +		1/1 (6)
1655	Tycoon 11	Sailor 65	- On Bomb, meet me on secure +		

Vietnamese Communist Intercept of U.S. Clear-text Communications. The communications reveal tactical operations. "Meet me on secure" (last line) refers to the use of KY–8 ciphony equipment. (Source: ASA TAREX unit.)

TIME OF INTERCEPT	U.S. COMMUNICATORS (callsign & suffix)		MESSAGE	DATE	VOICE NET
				1/1 3	
1125	Vague 90	Bandit 90	The 1st lift of 5 of my recons off P2, P2 cleared, extraction completed+		
	"	"	The 1st lift of my recons down in search completed, LZ cleared at 1227 hour+		
1130	Stroy 80	"	Skill at coord 665328 found a trail moving to E last 24 hours+		
	"	"	The 1st lift of 3 of my C off at 1238 hour+		
	"	"	The 2nd lift of 3 of my C off at 1239 hour+		
	"	"	The 3rd lift of 1 of my C off at 1240 hour+		
1146	"	"	The 1st lift of 3 of my C down at 1245 hour+		
	"	"	The 2nd lift of 3 of my C down at 1246 hour+		
	"	"	The 3rd lift of 1 of my C down at 1247 hour+		
1150	Bandit 90	Bandit 90	All station, I need your locations at 1300 hour+		
	Fire 90	"	Negative change+		
	Vague 90	"	Negative change, my recons and C extraction to DT+		
				22-11	1/1 3
1000	Tycoon 11	Bomb 11	The 1rst flight of 5 of my D off P2 +		
1005	"	"	The 1rst flight of 5 of my D down my location +		
	"	"	The 1rst flight of 2 of my D down my location at this time +		
	"	"	The last flight of 2 of my C off, P2 cleaned +		
	"	"	The last flight of 2 of my C down L2, in search completed +		
1015	"	"	The 2nd flight of 5 of my D off, P2 cleaned +		
	"	"	The last flight of 5 of my D down my location extraction completed +		
1025	Decot 6	Bomb 50	The CF extraction completed, P2 cleared +		
	Flame 77F	Bomb 11	In bound your location, eta 04 +		
	Sailor 65	"	Wagoon train close my location at this time +		
1035	Tycoon 11	"	At coord 538420 my 40 element found 1 grenade 1 booby trap +		
				1/1 6	
	Tycoon 11	Bomb 11	The 1st lift of AS9 down LZ, in search completed+		
1635	Tycoon 11	Sailor	+I understand egle lift completed On bomb, meet me on secure+		

Typescript of Intercept

places main reliance on individual restraint by Americans, it will fail in the long run to have sufficient COMSEC to deny advantages of one kind or another to an enemy. As Americans, we do not appear to learn from past mistakes. Three primary COMSEC problems existed in World War II: unnecessary transmissions and operator chatter, excessive use of clear text when suitable codes and ciphers were available, improper use of authorized codes and transmission procedures. That our enemies took advantage of our laxity in World War II is well documented. German SIGINT operations accounted for much of the cunning of General Rommel, the "Desert Fox" of North Africa during World War II. German SIGINT operations help to explain the German successes in their air defense against Allied bombing from England, in the heavy American losses at Salerno in 1943, and in Field Marshal von Rundstedt's 1944–45 winter campaign known as the Battle of the Bulge.

While U.S. SIGINT played an important role in the Battles of Midway and the Coral Sea in the Pacific, Japanese SIGINT—intercept from plain language messages—was forecasting the attacks that Australian and American forces were planning for the Pacific islands. Despite the documentation from World War II, similar documentation from the Korean War, and abundant evidence from Vietnam, too many American military commanders still fail to believe in the enemy's known SIGINT capabilities, and therefore still fail to appreciate the value of good COMSEC practices.

The greatest COMSEC weakness of all results from the American penchant for transmitting a great deal of information rapidly, often without adequate consideration of intelligence value, at times without consideration even for the need of the communication. In this circumstance, there were only two realistic approaches to achieve COMSEC improvements. The first was to employ more, easier-to-use, cryptosystems to reduce sharply the amount of information being sent in the clear. The second was to introduce "a whole series of new transmission systems" to make U.S. traffic difficult to intercept.

Introduction of several newly designed manual systems along with the KW–7 and KY–8 family of voice equipment helped to reduce the volume of clear-text transmissions, and this brought a measure of relief. Nothing was done, however, to introduce communications or crypto-

equipment of low interceptability. Neither the KY-8 nor the KW-7 equipment has traffic flow security safeguards, although both do allow encryption of message heading information of value to enemy analysts.

The use of on-line teletype and voice ciphony (KY-8) reduced the chance of human error and made possible the desired fast but protected communications required by commanders in tactical operations. The latter was not available, however, for all authorized levels of command requiring communications. As in the case of the 25th Division,* introduction of such easy-to-use, on-line equipment brought decisive improvement in COMSEC. The Vietnam experience revalidated the formula "better systems, better COMSEC."

Command Emphasis

The most important of lessons learned, implicit in much of what appears in these pages, is that command emphasis on COMSEC is mandatory. The historical record shows the obvious: commanders who emphasize COMSEC have secure communications; those who do not, have insecure communications. Command emphasis takes on many forms—a commander personally reviewing COMSEC violation reports, a commander reprimanding offenders, a senior command releasing the names of violators, and so forth—but whatever the form, command emphasis must balance initiatives put forth by the COMSEC community if the United States is to offset the losses resulting from enemy SIGINT operations.

A commander who gambles with COMSEC gambles with the lives of the men he commands.

*See pp. 43–45 above.

List of Abbreviations

ACC	area control center
AF	Air Force
AFSCC	Air Force Special Communications Center
ALTREV	altitude reservation
AM	airmobile; amplitude modulation
AR	Army Regulation
ARVN	Army of the Republic of Vietnam
ASA	Army Security Agency
BJU	beach jumper unit (Navy)
CAAT	COMSEC Assistance Advisory Team
CC&D	communications cover and deception
CINCPACFLT	Commander in Chief, Pacific Fleet
CINCUSARPAC	Commander in Chief, U.S. Army, Pacific
COMBAR	Combat Aircraft Report
COMSEC	communications security
CTF	Commander, Task Force (Navy)
CTZ	corps tactical zone
DATSUM	Daily Activity Summary
DIA	Defense Intelligence Agency
DRV	Democratic Republic of Vietnam
DSU	direct support unit
DTOC	Divisional Tactical Operations Center
EEFI	essential elements of friendly information
EEI	essential elements of information
EFTO	encrypted for transmission only
ELSEC	electronic security
ETA	estimated time of arrival
EW	electronic warfare
FAA	Federal Aviation Administration
FAC	forward air controller

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

FFV	Field Force Vietnam
FMFPAC	Fleet Marine Force, Pacific
FS	Federal Standard
HFDF	high frequency direction finding
HOC	hours of coverage
ICD	imitative communications deception
JCS	Joint Chiefs of Staff
JUSMAAG	Joint U.S. Military Assistance Advisory Group (Thailand)
MAAG	Military Assistance Advisory Group (Vietnam)
MACTHAI	Military Assistance Command, Thailand
MACV	Military Assistance Command, Vietnam
MAF	Marine Amphibious Force
MARBKS	Marine barracks
MCCD	manipulative communications and cover deception
MCD	manipulative communications deception
MEB	Marine Expeditionary Brigade
MEDIVAC	medical evacuation
MSTS O	Military Sea Transport Service, Office
NAS	Naval Air Station
NAVFAC	Naval Facility
NAVSECGRU	Naval Security Group
NAVSTA	Naval Station
NCS	Naval Communications Station
NOTAM	Notices to Airmen
NRS	Naval Radio Station
NSAPAC	National Security Agency, Pacific
NSC	Naval Supply Center
NSD	Naval Supply Depot
NVA	North Vietnamese Army
NVN	North Vietnam
OB	order of battle
OPSEC	operations security
PACAF	Pacific Air Force
PACSCTYRGN	Pacific Security Region (Air Force)

PBR	patrol boat, river
PDS	practices dangerous to security
PDSR	Practices Dangerous to Security Report
PRC	processing and reporting center
PWI	prisoner of war interrogation
ROK	Republic of Korea
RRC	radio research company
RRU	radio research unit
R/T	radiotelephone
RTP	radioteleprinter
RVN	Republic of Vietnam
RVNAF	Republic of Vietnam Armed Forces
SAC	Strategic Air Command
SAM	surface-to-air missile
SCA	Service Cryptologic Agency
SD	security detachment
SEAMARF	Southeast Asia Military Air Route Facility
SEAWBS	Southeast Asia Wideband System
SIGO	signal officer
SIGSEC	signal security
SOI	signal operation instructions
SOU	special operations unit
SS	security squadron (Air Force)
SSB	single sideband
SSBN	nuclear power ballistic missile submarine
SSG	Special Support Group
SSI	standing signal instructions
SVN	South Vietnam
SW	security wing (Air Force)
TAD	temporary additional duty
TAREX	target exploitation
TF	task force
TIOI	TRANSEC Item of Interest
TRANSEC	transmission security
TSAR	Transmission Security Analysis Report
TSIS	TRANSEC Interim Report
TSMR	Transmission Security Message Report

TSMS	Transmission Security Monthly Report
TSSR	Transmission Security Summary Report
TSV	transmission security violation
TSVR	Transmission Security Violation Report
TTY	teletypewriter
USARV	U.S. Army Vietnam
VC	Viet Cong; Vietnamese Communist
WESTPAC	Western Pacific
WG	wing (Air Force)
WW II	World War II

Index

ABILENE, Operation: 142
Abrams, Lt. Gen. Creighton W.: 19

[redacted]

Air Force Security Service
  COMSEC monitoring equipment: 72, 73, 74, 75
  COMSEC operations: 77–84, 89, 96–97, 100–03, 107–09, 120, 121, 123, 125, 127, 130, 134, 139, 149–53
  COMSEC organization: 20, 72–76
  COMSEC strength: 73, 74, 75–76
  Special Communications Center: 100–03
Air Force Security Service units
  PACSCTYRGN Detachment 2: 72, 73, 76, 77, 78, 123
  6922d Security Wing: 72, 123
  6922d Security Wing Detachment 4: 76
  6922d Security Wing Detachment 5: 72, 73, 74, 77, 79–80, 82, 123, 127
  6922d Security Wing Detachment 7: 72, 74–76, 77, 80, 83, 123
  6927th Security Group Detachment 1: 123
  6988th Security Squadron: 77
  6988th Security Squadron Detachment 1: 123
Air Force units. *See also* Air Force Security Service units.
  Pacific Air Force: 73, 122
  Seventh Air Force: 73, 75, 77, 81, 84
  Thirteenth Air Force: 74, 75, 122
  2d Air Division: 73, 79, 120
  3d Air Division: 100, 107–09, 119
  8th Tactical Fighter Wing: 151, 152–53
  388th Tactical Fighter Wing: 83
  4242d Strategic Wing: 101–02
  1958th Communications Squadron: 104
Air operations. *See* ARC LIGHT; B–52's; BLUE SPRINGS; ROLLING THUNDER.
Altitude reservations (ALTREV's): 121–22, 135
Analysis. *See* Monitoring and analysis.
ARC LIGHT, Operation. *See* B–52's, operations by.
ARC LIGHT COMSEC studies
  September–October 1966: 122–28, 163
  December 1966–March 1967: 128, 129, 130, 131, 135, 137
Area control centers (ACC's): 121–22
Army Security Agency
  COMSEC education by: 48–54
  COMSEC operations: 19, 20, 22, 23, 25, 27–45, 48, 49, 51, 91–95, 120, 123, 125, 130, 139, 142, 143, 158
  COMSEC organization: 20, 21–27
  COMSEC strength: 20, 21, 22, 23, 24, 25, 26–27
  monitoring equipment: 22, 30
  TAREX: 44, 49, 51, 158
Army Security Agency units
  509th Group: 8, 24–25, 27, 49, 123, 125, 142
  303d Battalion: 24–27, 35, 37, 52, 143–44

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

313th Battalion: 24–27, 37
USASA Company, Saigon: 25, 37
325th Company: 52
337th Company: 142
371st Company: 52, 91–92
101st Security Detachment: 22–25, 28–29, 37, 38, 45, 93, 120, 123
104th Security Detachment: 22, 23
409th Detachment: 142
856th Detachment: 143–44
82d Special Operations Unit: 21, 22, 24
400th Special Operations Unit (Prov.): 21
Capital Monitoring Team: 25
COMSEC Assistance and Advisory Teams (CAAT's): 49
DSU's, general: 23–27, 37, 52
Army units. *See also* Army Security Agency units; Field Forces Vietnam.
U.S. Army Vietnam: 127
1st Cavalry Division: 44–45, 50, 52, 90–95
1st Infantry Division: 35, 44–45, 142
9th Infantry Division: 52
25th Infantry Division: 9–11, 43–45, 48
173d Airborne Brigade (Separate): 39, 52–53
199th Infantry Brigade (Separate): 143–44
11th Armored Cavalry: 35, 142–43
Advisory Team 75: 38
"Australian ICD Incident": 9–11

B–52's
operations by: 90, 96, 101, 119–20, 121–22, 128, 129

[redacted]

B–52D's: 102
BACK PORCH: 84
Barlow, Howard C.: 2
Blauvett, Lt. Col. Richard B.: 35–36
BLUEBIRD Advisory Group: 38
BLUE SPRINGS: 129, 130, 134–35, 141
BOLO: 149–53, 159
Brookshire, Lt. Col. Grail L.: 35
Brown, Maj. Jerry L.: 19
BUMBLE BUG. *See* BLUE SPRINGS.
BUMPY ACTION. *See* BLUE SPRINGS.

C–130's: 77–79
Campbell, Lt. Col. Norman J.: 35, 143–44
Captial Operations Center (Saigon): 120
Carter, Lt. Gen. Marshall S.: 128
Central Office for South Vietnam (COSVN): 3
Chance, Col. James: 128
Charles Berry, USS: 103, 104
Chausteur, Maj. John: 152
China. *See* Communist China.
Coast Guard, U.S.: 113
Codes. *See* Cryptosystems.
COIN: 82
Combat Aircraft Report (COMBAR): 121
Command emphasis. *See* Communications security, commanders' attitudes toward.
Communications, monitoring of. *See* Monitoring and analysis; Violations, causes of.
Communications cover and deception (CC&D) operations
Air Force: 139, 148–53

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

Army: 139, 142–44
compared with enemy CC&D: 139–40
definition of: 139
electronic deception: 149
evaluation of: 153–54, 159
ICD, enemy: 8–11
ICD, U.S.: 141
Marine Corps: 148
MCCD: 11–12, 141, 144–53
MCD: 141, 142–44
Navy: 11–12, 139, 144–48
responsibility for: 144

Communications Improvement Memoranda: 63

Communications security (COMSEC), general
commanders' attitudes toward: 2, 15–16, 19, 30, 34, 39, 42, 43, 45, 48–49, 50–54, 55, 67, 68–71, 83, 84, 88, 91, 92, 93, 94, 113, 119, 120, 122, 127, 128, 155, 158, 166, 167
conventional monitoring: 1–84, 91–128
division of responsibility: 2
during various wars, compared: 2, 53, 163, 166
evaluation of: 155, 158–59, 162–63, 166–67
functions of: 1
shortages of equipment: 98
shortages of personnel: 11, 76, 88
status of, 1960: 20
status of, March 1966: 95
status of, 1968,: 49, 68
strength: 11, 20, 21, 22, 23, 24, 25, 26–27, 54, 55, 58, 62, 63, 64, 73, 74, 75–76, 88
surveillance: 49, 87–90, 128–38, 162–63

[redacted]

Compromises, security. *See* Violations.
COMSEC Traffic Analysis Report: 69
Consolidated Cryptologic Program (CCP): 2
CRITICOMM, security of: 21

Cryptosystems
AN series: 7, 12
for BOLO: 150–51
compared with those of World War II: 53
HY-2/KG-13: 135
KAC-F: 95
KAC-J: 83, 94, 95
KAC-P/Q: 43, 44
KAC-Q: 95
KAC-Q/P: 52
KAC-21: 95
KAC-24: 95
KAC-72: 121, 134
KAC-132: 114, 117
KAC-138: 114
KAC-140: 114, 115, 117–18
KAC-154: 134
KAC-183: 115, 118
KAC-227: 134
KAC-238: 135
KAG-21: 94
KAG-24: 91
KG-13: 107
KL-7: 3, 91, 92, 94
KW-7: 30, 91, 92, 94, 166–67
KW-26: 30, 105–06, 107, 108, 135
KY-3: 121
KY-8: 30, 44, 49, 94, 95, 166–67
KY-9: 121
KY-38: 53
M-209: 12

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

manpack: 53
manual: 13
one-time pads: 20
PALMER JOHN: 73
POLLUX: 22
PYTHON: 3
SHACKLE: 43
shortages of: 83–84, 113, 114, 117, 121
SLIDEX: 3, 12
TRITON: 121
unauthorized: 7, 14, 44, 45, 48, 52, 53, 55, 92, 93, 94

Daily Activity Summary (DASUM): 80
Deane, Maj. Gen. John R., Jr.: 52–53
Defense Intelligence Agency (DIA), and PURPLE DRAGON: 128, 130
Denholm, Maj. Gen. Charles J.: 33–34, 44
DePuy, Maj. Gen. William E.: 50–51

Education, COMSEC
methods: 34, 43–44, 49, 51–52, 65–67, 68, 158
problems: 50–54, 155, 158–59
programs: 48–49, 99, 114, 115,

Equipment, crypto-. *See* Cryptosystems.
Equipment, monitoring
Air Force: 72, 73, 74, 75
Army: 22, 30
Navy and Marine Corps: 63, 64, 65

F–4C's: 149, 150, 151, 152
F–105's: 149, 150, 152
Field Forces Vietnam
I: 25, 37
II: 25, 35–36, 37, 39, 42
Fingerhut, Walter C.: 88
Fisher, Robert A.: 87
Forbes, Brig. Gen. Robert C.: 143

GAME WARDEN
COMSEC study of: 116–19
operations: 64, 115, 116
Geographic reference plotting system, defined: 150n
Guam COMSEC study: 89, 96–109

Hancock, USS: 3
Harris, General Hunter, Jr.: 123, 125
Heiss, Lt. Col. John L., III: 53
Henchman, Lt. Col. John M.: 10–11
Hyland, Vice Adm. John T.: 60

Imitative communications deception (ICD). *See* Communications cover and deception, ICD, enemy, *and* ICD, U.S.
IRON HAND: 149
Izmeritel: 96

Jamestown, USS: 58, 110
Jarrett, Maj. George V.: 48
Johnson, Lyndon B.: 82
Johnson, Admiral Roy L.: 55, 57, 59, 60

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

Joint Chiefs of Staff
and ARC LIGHT COMSEC study: 122, 123
and PURPLE DRAGON: 128
Joint U.S. Military Assistance Advisory Group (JUSMAAG), Thailand: 22, 23, 25

Karch, Brig. Gen. Frederic: 55
[redacted]
Kinnard, Lt. Gen. Harry W. O.: 50
Knowles, Maj. Gen. Richard T.: 50
Korean War, COMSEC in: 2, 166
Krulak, Lt. Gen. Victor H.: 55, 56, 68

Lessons learned: 155, 158–59, 162–63, 166–67
[redacted]

Malpractices, COMSEC. *See* Violations.
Manipulative communications deception (MCD). *See* Communications cover and deception, MCCD *and* MCD.
Marine Corps
COMSEC operations: 55–57, 63, 65, 66–68
MCCD operations: 148
Marine Corps units
Fleet Marine Force, Pacific: 55
Ninth Marine Expeditionary Brigade: 55
III Marine Amphibious Force: 9, 66, 68, 148
1st Marine Division: 68
3d Marine Division: 68
1st Marine Air Wing: 68
First Radio Battalion: 55–56
Sub Unit One, First Radio Battalion: 56–57, 63, 65, 66–68
MARKET TIME
COMSEC survey: 58, 59, 69, 89, 109–16
MCCD operations: 11–12, 144–47
tactical operations: 58, 59, 64, 109–10
McConnell, General John P.: 73, 82, 83, 84
McNamara, Robert S.: 74
Mearns, Maj. Gen. F. K.: 43
Melanson, Capt. Leo M.: 52
MIG–21's: 149, 150, 151, 152, 159
Military Assistance Advisory Group (MAAG), Vietnam, COMSEC inspection of: 20
Military Assistance Command, Thailand (MACTHAI), COMSEC operations for: 23, 25
Military Assistance Command, Vietnam (MACV)
COMSEC for: 20, 22, 23, 25, 28–29, 34
and increased COMSEC strength: 74, 75
J–2, and COMSEC: 48
Monitoring and analysis
[redacted]
of Air Force ground administration: 121
AFSS: 72, 73, 76, 77, 83, 89, 96, 100–03, 107–09, 120, 121, 125, 134
of air-to-air coordination: 121
of air space requirements: 121
ASA: 22, 23, 25, 29, 30, 33, 34, 35, 42, 43–45, 48, 91–95, 120–21, 125, 143
communications not monitored: 30, 77

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

concept of conventional: 159, 162
concept of surveillance: 87–90, 128, 162
of control tower directions: 121
of encrypted material: 22, 30, 89, 96
equipment for: 22, 30, 63–65, 72–75
of FM: 30, 34
of HF: 72, 73, 74, 83, 103, 110, 112, 116, 134
of in-flight reporting: 121
of manual Morse: 22, 30, 93, 116
Marine Corps: 65
and MCCD operations: 146
of MF–SHF range: 103–04
of microwave range: 34, 98, 103, 104
mobile: 22, 23, 29, 30
multichannel: 30, 73
Naval Security Engineering Facility: 105–07
NAVSECGRU: 54–55, 58, 64–65, 67–68, 89, 96–99, 104, 109–19, 125, 130
NSA: 89, 96, 103–04, 109
percentage of coverage: 19, 34, 64
premanent detachments: 23
of preflight testing of equipment: 121
quantity of: 22, 34, 42, 65, 93
of plain English: 77, 91, 96, 112, 125
of radio, general: 33, 35, 43–45, 48, 65, 77, 100, 120, 125
of radiotelephone: 19, 22, 25, 30, 33, 44, 73, 75, 91, 93
of radioteletype: 22, 30, 33, 34, 93, 125
of refueling operations: 121
and refusal to change plans: 19, 35
of single sideband: 30, 34, 72, 97, 116, 134
successful, causes change of plans: 19, 35, 68
of telephone: 22, 25, 30, 33, 35, 44, 73, 98, 100, 120, 125
of troposcatter: 34, 74
of UHF: 72, 73, 74, 75, 76, 77, 83, 97, 98, 103, 110, 116, 125
of VHF: 72, 73, 74, 75, 76, 77, 97, 99, 101, 103, 110, 116, 125
of weather reconnaissance: 121
Moore, Maj. Gen. Joseph H.: 73

National Cryptologic School: 158
National Security Agency
and CC&D operations: 140
COMSEC responsibility of: 2
and COMSEC surveillance: 87, 88, 89, 128
and Guam COMSEC study: 89, 96, 103–04, 109
and PURPLE DRAGON: 128, 130
Naval Security Group
COMSEC education by: 63, 65–67, 68
COMSEC operations: 54–55, 58, 63–71, 89, 96–99, 104, 105–07, 109–19, 123, 125, 139, 144, 146
COMSEC organization: 20, 54–62
COMSEC strength: 54, 55, 58, 62, 63, 64
monitoring equipment: 63, 64, 65
Naval Security Group units
afloat: 54, 58, 60–61, 63, 104, 110
COMSEC 701: 54, 97–99
COMSEC 702: 54, 69, 110, 112–15

COMSEC 703: 54, 146
COMSEC 704: 54
COMSEC 705: 57–58, 59–60, 117
COMSEC 706: 62
COMSEC Team, Naval Support Group Da Nang: 57–58
COMSEC Team One (Alpha): 54, 63, 65
COMSEC Team Two (Bravo): 60–61, 63, 65
COMSEC Team Three (Delta): 58–60, 116–19, 123
COMSEC Team Four: 62, 117–19
COMSEC Team Five: 61–62
COMSEC Team Saigon: 58
COMSEC Team Vietnam (C): 55–56, 64, 66
Detachment Delta, Naval Communications Station Philippines: 58
NAVSECGRU Activity Hanza: 54
NAVSECGRU Activity Kamiseya: 54, 55, 59–60, 62, 115
NAVSECGRU Headquarters, Finegayan: 105–06
shore-based: 54, 55–60, 62, 64, 65, 97–99, 104, 105–07, 109–19
Naval units. *See also* Naval Security Group units.
Beach Jumper Unit One: 61–62
Destroyer Squadron 19: 146
Naval Advisory Group, Saigon: 59, 111–12, 115, 116
Naval Air Communications Facility Agana: 106–07
Naval Communications Station Cam Ranh Bay: 62
Naval Communications Station Finegayan: 106
Naval Communications Station Guam: 54, 106, 123
Naval Communications Station Philippines: 54, 55, 62
Naval Forces, Marianas: 106
Naval Security Engineering Facility: 105–07
Seventh Fleet: 54, 55, 113
Task Force 71: 144, 145–47
Task Force 76: 61
Task Force 77: 144
Task Force 115: 58, 59, 109–10, 112–13, 147
Task Force 116: 59, 62, 116, 117
Task Force 117: 62, 117
Task Group 76.4: 61
Task Group 76.5: 61
Task Element 70.7.7.1: 123
Task Element 70.7.7.2: 123
Nicholson, Col. Tom M.: 15–16
NIGHTSTICK: 89
North Vietnam. *See* Vietnamese Communist threat.
North Vietnamese Central Research Directorate: 6
Notices to airmen (NOTAM's): 121–22, 135, 137

O'Connor, Maj. Gen. George G.: 52
Office of Special Investigation (AF): 130
Olds, Col. Robin: 151, 152
Operational security (OPSEC): 138

Philco Tropo system: 84
Positive identification radar advisory zone (PIRAZ): 64
Practice Dangerous to Security Report (PDSR): 37

Prestrike Report: 80
Proteus, USS: 96, 107
PURPLE DRAGON COMSEC study: 88, 90, 128–38, 163

Ranger, USS: 5
Red/Black criteria: 96
Reichard, Maj. George D.: 48
Reporting, of malpractices. *See also reports by name.*
AFSS: 72, 77, 79–81, 82, 83
ASA: 36–43
Marine Corps: 68
NAVSECGRU: 54–55, 63, 67, 68, 69–71, 112, 117, 118
Republic of Korea, cryptosystems for: 12
Republic of Vietnam
COMSEC of: 2–3, 6, 7, 12, 20, 22, 23, 25, 28–29, 38, 82
and GAME WARDEN: 116
and MARKET TIME: 109–10, 113, 116
ROLLING THUNDER: 128–29, 131, 134, 137–38
Ryan, General John D.: 83

Search and rescue (SAR) operations: 64
Service Cryptologic Agencies. *See* Air Force Security Service; Army Security Agency; Naval Security Group.
Sharp, Admiral U. S. G.: 87–88, 90, 122, 123, 124, 125, 127–28, 138, 144, 145, 148
SILVER BAYONET
COMSEC study: 48, 50, 89, 91–95
operations: 90, 94
[redacted]
Southeast Asia Military Air Route Facility (SEAMARF): 121–22, 127
Strategic Air Command. *See* ARC LIGHT; B–52's.
Surveillance, COMSEC
and COMSEC studies: 128–38
concept of: 87–90, 128, 162
evaluation of: 49, 162–63

TAREX (target exploitation): 44, 49, 51, 158
TEMPEST: 1, 96, 103–09
Tet offensive (1968), and naval COMSEC operations: 62
Thailand
COMSEC operations in: 22
counterinsurgency operations (COIN): 82
Timmes, Maj. Gen. Charles J.: 20
TRANSEC Analysis Notes (TAN's): 81
TRANSEC Interim Summary (TSIS): 81
TRANSEC Item of Interest (TIOI): 80–81
TRANSEC Review Board (Seventh AF): 84
Transmission Security Analysis Report (TSAR): 37
Transmission Security Message Report (TSMR): 80, 83
Transmission Security Monthly Summary (TSMS): 80, 101
Transmission Security Summary Report (TSSR): 37
Transmission Security Violation Report (TSVR): 37, 38, 41
[redacted]
Viet Cong. *See* Vietnamese Communist threat.

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

Vietnamese Communist threat
[redacted]
jamming: 9
SIGINT operations: 1, 2–11, 19, 35–36, 43–44, 49, 122, 139, 155, 158, 159
and VC COMSEC practices: 110

Violations. *See also* Reporting, of malpractices.

Violations, causes
cipher-signal anomalies: 103, 104
communications structures: 113, 117
correction of: 20, 38, 43–44, 48–49, 65–71, 82, 84, 94–95, 102–03, 104–05, 106, 107, 108, 109, 113–14, 115, 116, 117–18, 121, 122, 126–27, 131, 134–35, 137–38, 162, 163, 166–67
daily F–105 reports: 83
data processing equipment: 107–08
EFTO procedures: 126
equipment design and installation: 105, 106, 107
excessive communications: 44, 53, 166
failure to authenticate: 8, 44, 54, 55, 93
improper use of codes: 55, 58, 83, 114, 116
lack of command emphasis: 2, 15–16, 35–36, 43, 45, 48, 50–54, 55, 67, 69–71, 91, 93, 94, 120, 155, 158, 167
long-term use of code names: 55, 82, 127
organizational complexity: 113
refusal to use cryptosystems: 20, 91–92, 166
shortages of cryptosystems: 83–84, 113, 114, 117, 121
short-tour dilemma: 11
unauthorized codes: 7, 14, 44, 45, 48, 52, 53, 55, 92, 93, 94
unencrypted communications: 3, 5, 6–7, 19, 20, 44, 91, 93, 98, 101–02, 104, 116, 120–21, 166
vague guidelines: 13, 81

Violations, information revealed
in action reports: 113
on aircraft operational areas: 83
on air operations, general: 3, 5, 6–7, 38, 68, 73, 77, 78–79, 82, 83, 96, 98, 101–02, 104, 120, 125, 126, 128, 134, 135, 137
on air reconnaissance: 38, 72
on air refueling: 78
on air tactics: 78
on air-to-air coordination: 78
on antenna bearings: 98
on bomb damage assessments: 77
on budget figures: 98
on call signs: 38, 44–45, 52, 53, 73, 93, 94
on carrier-air squadron relationships: 98
on casualties: 113
on classified equipment capabilities: 93
on command and control systems: 72
on frequencies: 38, 52, 93, 94, 98
on grid coordinates: 38, 73, 82, 93, 94, 112–13, 118, 127
on locations of units: 38, 39, 44, 93, 94
on logistics: 93
on medical evacuation: 15
on MIG alerts: 77
on naval order of battle: 112, 118
on orbits: 83

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

reporting on: 34, 36–43, 54–55, 63, 67, 68, 69–71, 72, 77, 79–81, 82, 83, 112, 117, 118, 123, 125
on SAM alerts: 77
on search and rescue: 79
on ships' movements and cargo: 98
on special navigation techniques: 78
on TACAN azimuths: 83
on tactical plans, general: 35, 38–39, 44, 52, 93, 94, 102, 116, 120–21, 134
on tactical operations, general: 93, 94, 116, 118–19
on time-over-target: 73, 83
on troop movements: 113
on troop training: 113
on types of aircraft: 72
on underway replenishment: 113
on VIP trips: 19, 38, 73, 82
Violations, rates of: 42–43, 44
Violations, sources of
Air Force: 8, 14, 72, 73, 77–78, 82, 83, 101–03, 104, 107–09, 120–21, 125, 126, 127, 134, 135, 137
Army: 15, 19, 20, 35, 38–39, 40–41, 43–45, 48, 52, 53, 54, 91–95, 125, 127
MACV: 127
Marine Corps: 68
Navy: 3, 5, 55, 58, 68, 98, 105, 106, 107, 112–13, 114, 116, 118
RVN: 2–3, 6, 12, 35, 38, 53, 82, 110
TEMPEST: 103–09

Walker, Col. Robert T.: 20
Walt, Lt. Gen. Lewis W.: 68
Westmoreland, General William C.: 49, 127, 144, 148
Weyand, Lt. Gen. Frederick C.: 144
Wiretapping
enemy: 44
guarding against: 98
World War II, COMSEC in: 2, 53, 166
World-Wide Operations Security Conference, 1968: 138