~~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.

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.

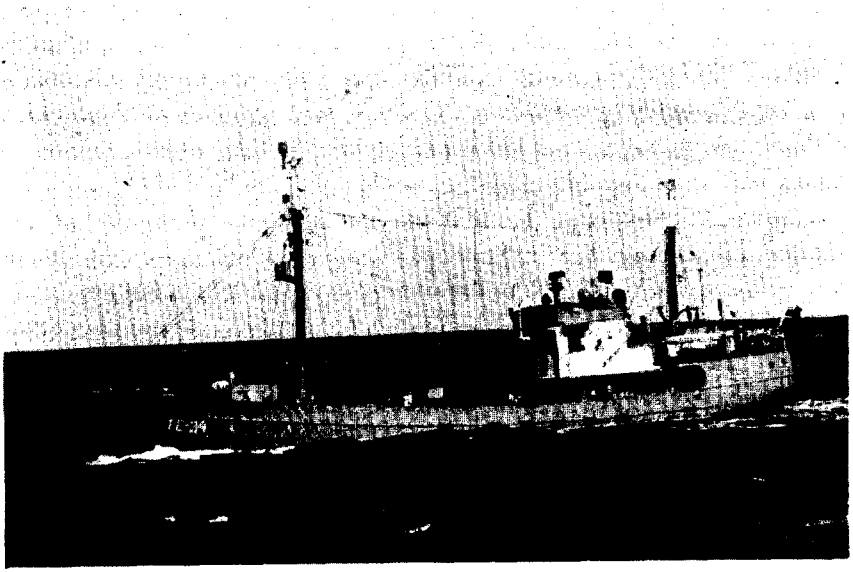
Guam

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).



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.*

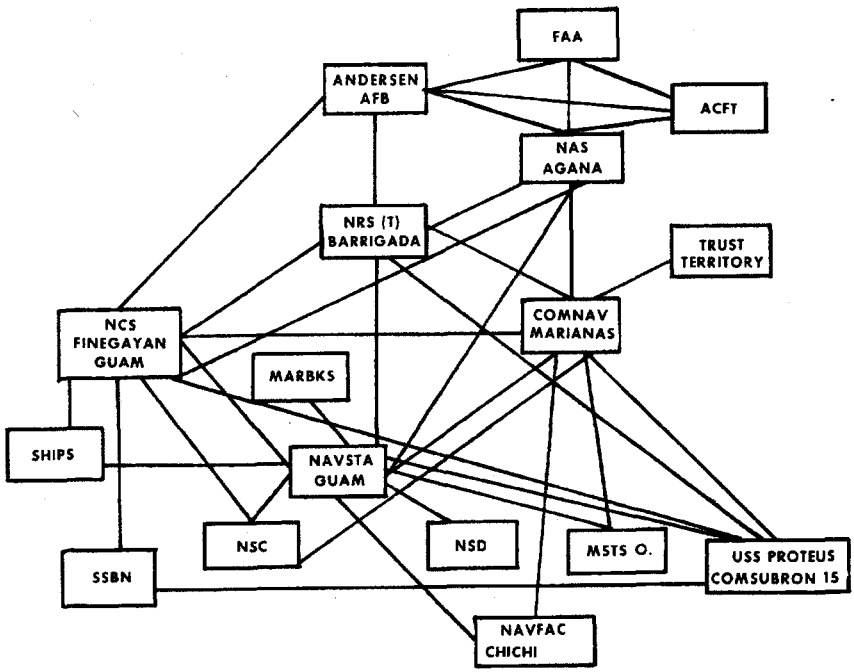
The monitoring team found that landline and microwave circuits yielded budget figures for specific projects, cargo and movement details for various ships, relationships between aircraft squadrons and carriers to which they were assigned, disposition and posture of tactical combat aircraft, and information 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.

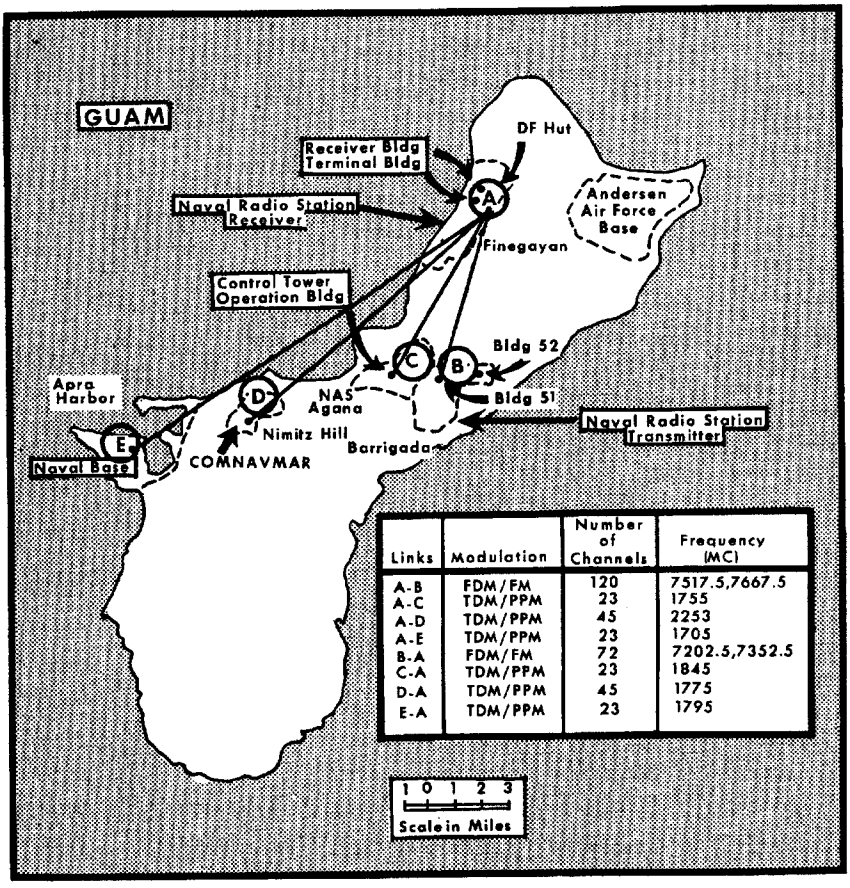
*See chart, page 99, for pertinent links in the Guam communications complex.



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.

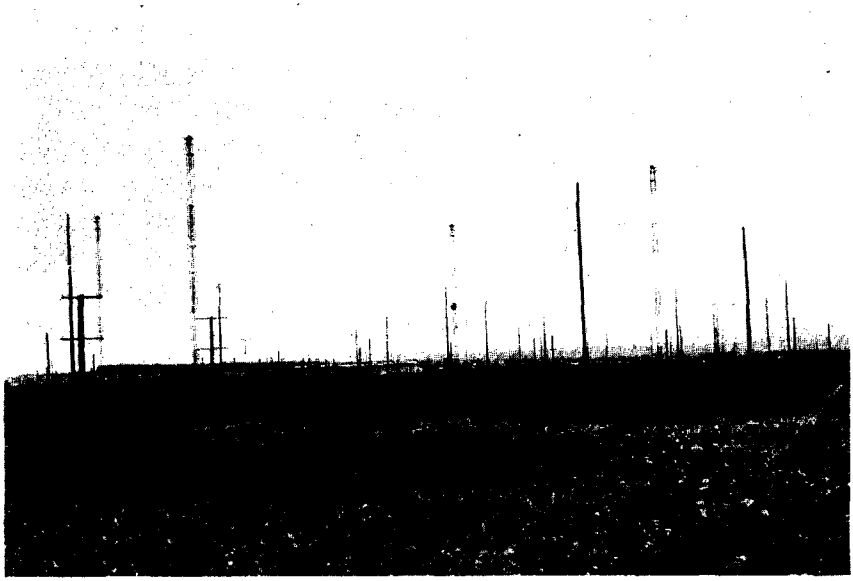
In summary, while many physical and communication security weaknesses identified in the Navy's survey had been previously known, COMSEC reindoctrination of personnel was desirable. As a result of the survey, COMSEC 701 was to make periodic sample surveys on a small scale to maintain vigilance over Navy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

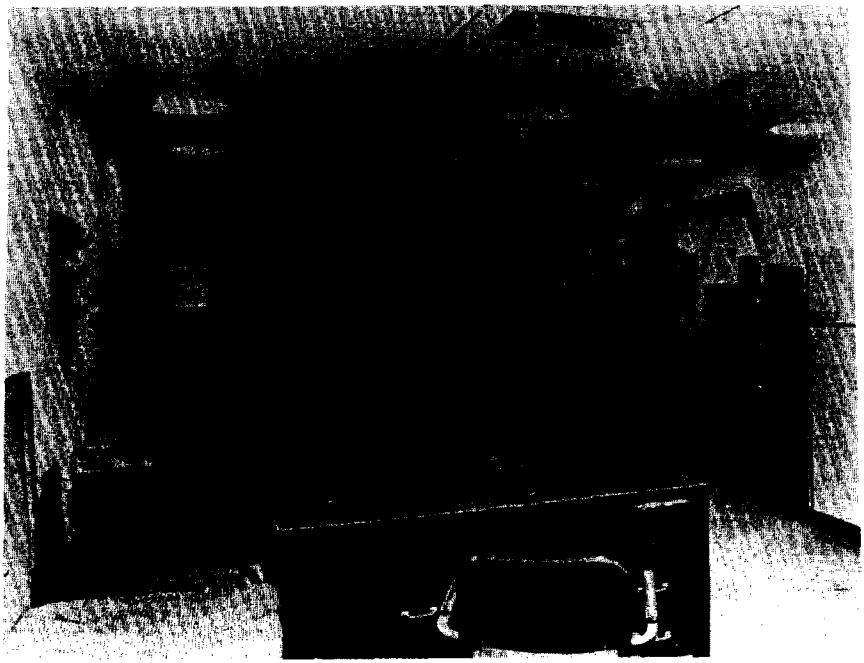
While in the vicinity of the trawler, the team heard no microwave signals. Off the north end of the island, however, it was able to hear three links when the ship's roll brought the team's antennas into direct line with the transmitters. Under laboratory conditions, NSA later evaluated HF communications 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



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

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.

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.

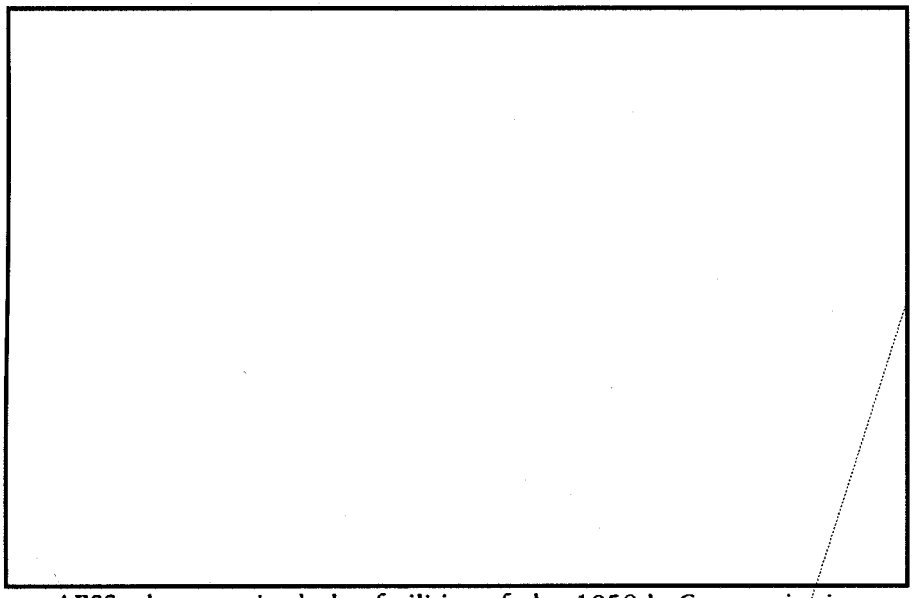
Air Force TEMPEST Tests

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.

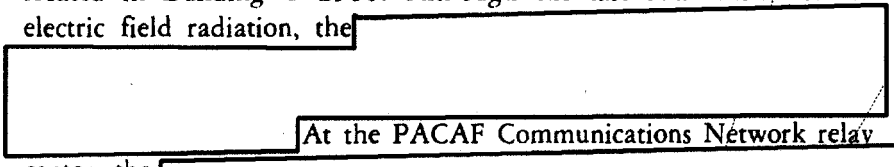
AFSS surveyed the facilities of the 3d Air Division (SAC), including the communications centers of the 27th Communications Squadron and the Special Security Office, as well as the electronic data processing equipment of the Data Services Division.

*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.

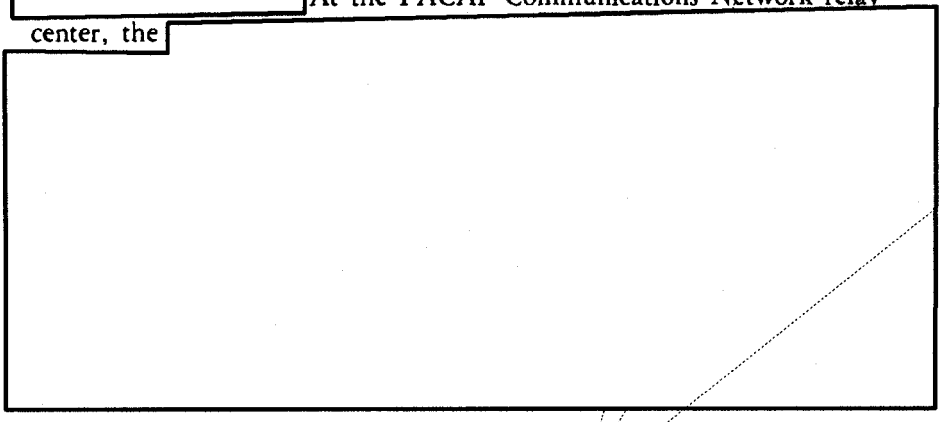
(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 403
(b)(3)-18 USC 798



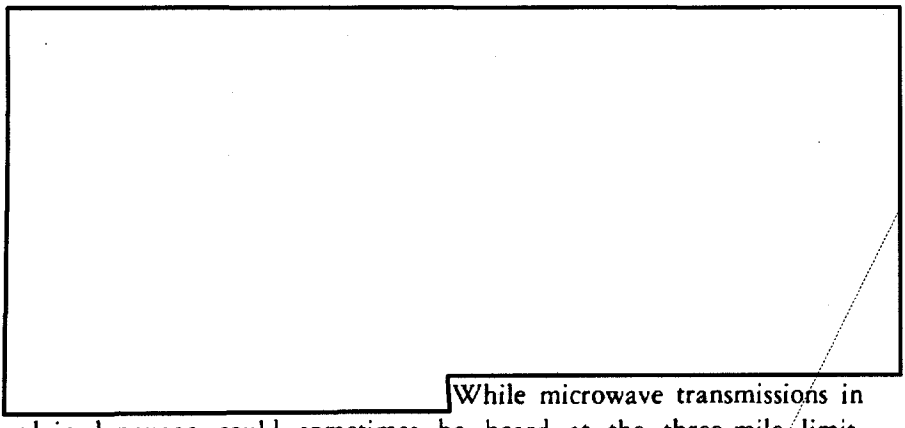
AFSS also examined the facilities of the 1958th Communications Squadron at Andersen, including the PACAF Communications Network relay center, another relay communications center, and a terminal located in Building T-2500. Although the last named showed no electric field radiation, the



At the PACAF Communications Network relay center, the



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



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 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.

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 [redacted] 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 [redacted] monitoring positions and an analysis section. In all, approximately [redacted] COMSEC specialists were directly involved in the study.

[redacted]

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

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

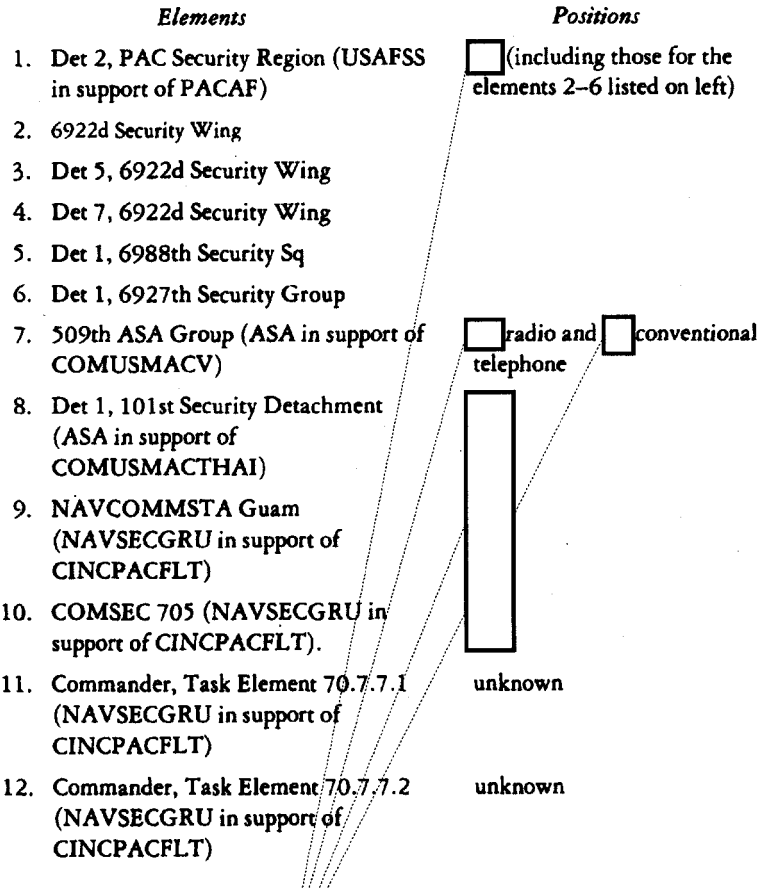
In mid-1966 SCA monitoring reports outlining ARC LIGHT communications insecurities took on added significance,

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.

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:



(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,

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

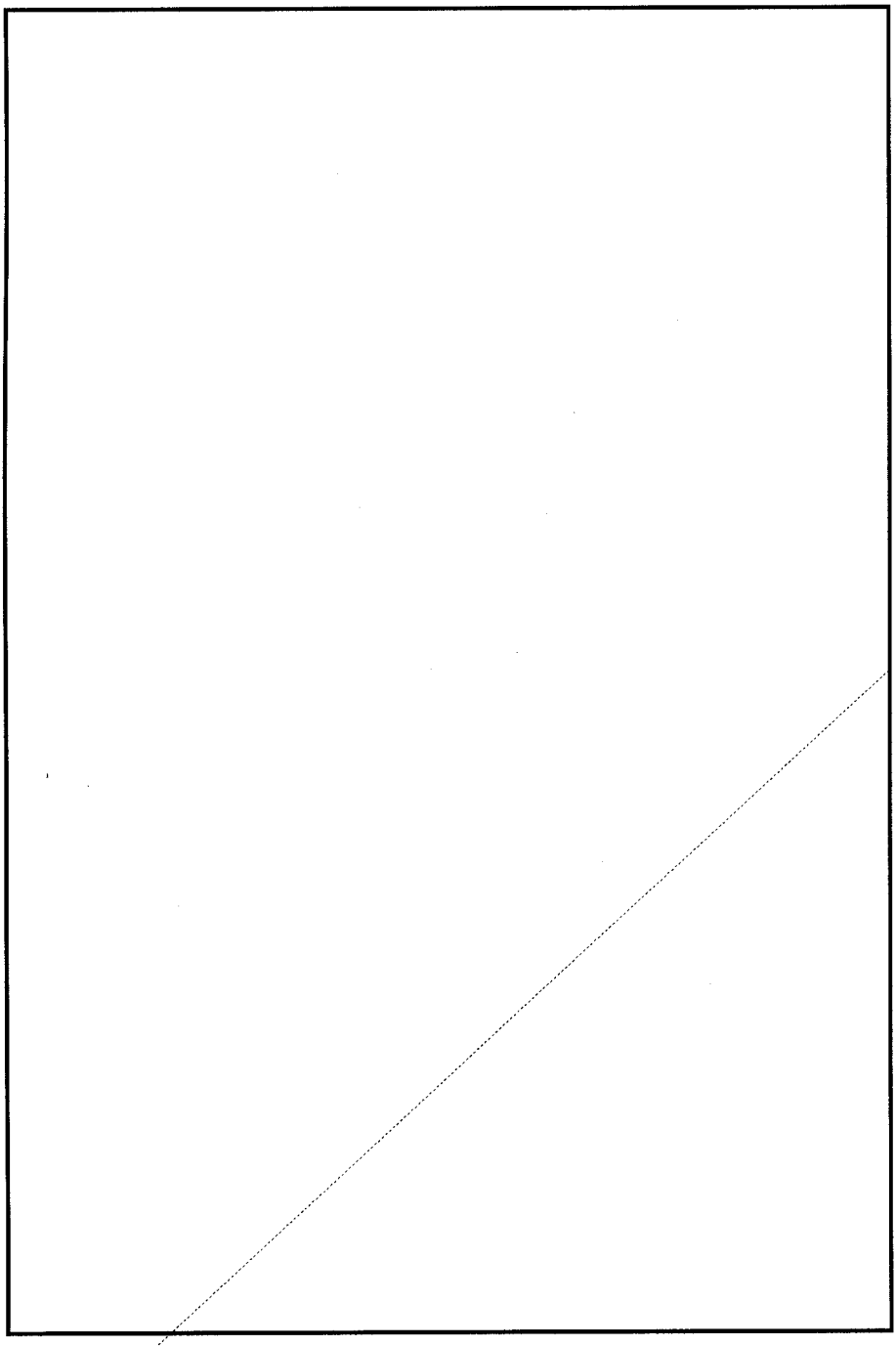
THUNDER. The third category, ARC LIGHT, was, of course, the B–52 strikes over South Vietnam.

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]

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.

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.*

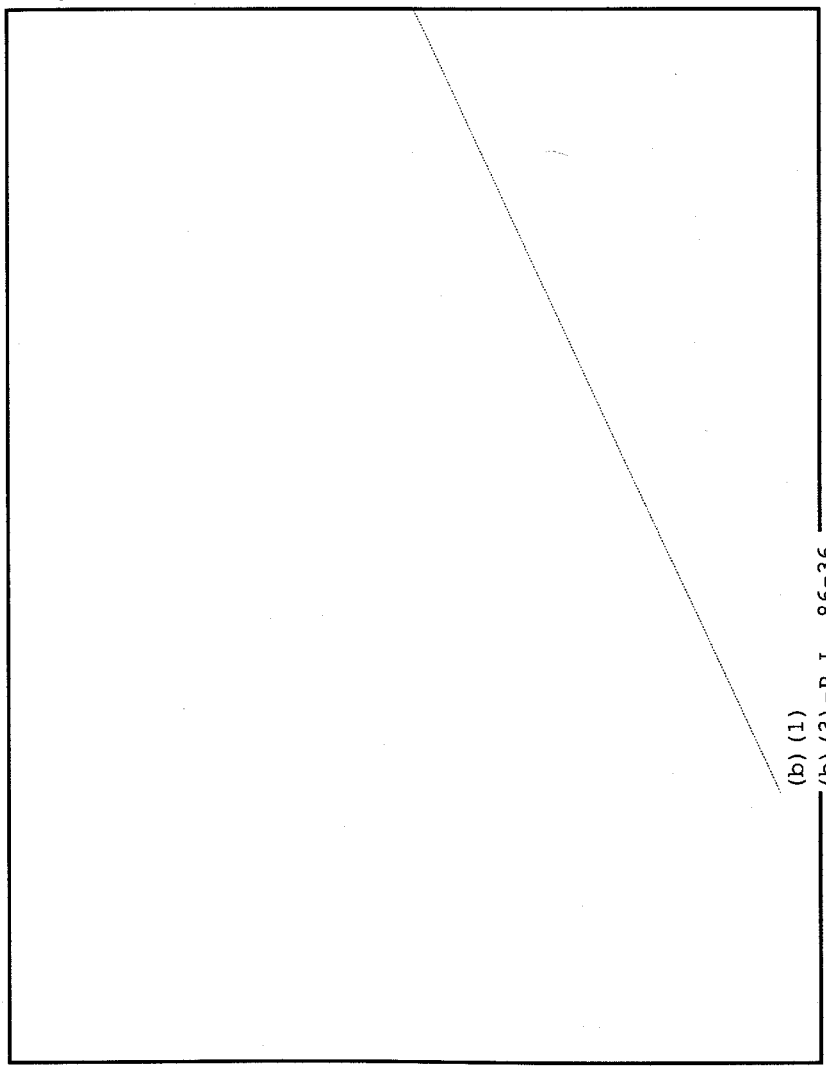
ARC LIGHT [redacted]

[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

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;

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

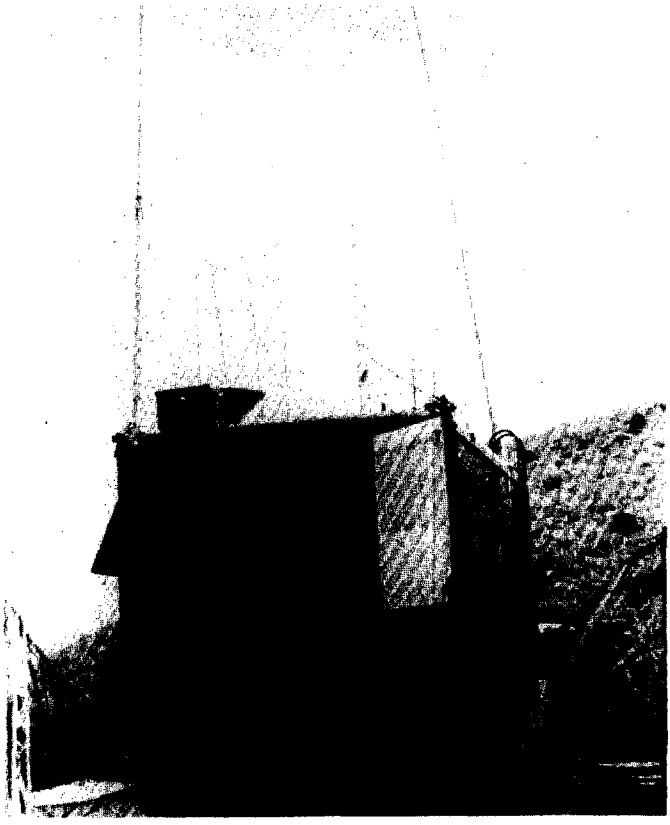
CHAPTER IV

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.



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).

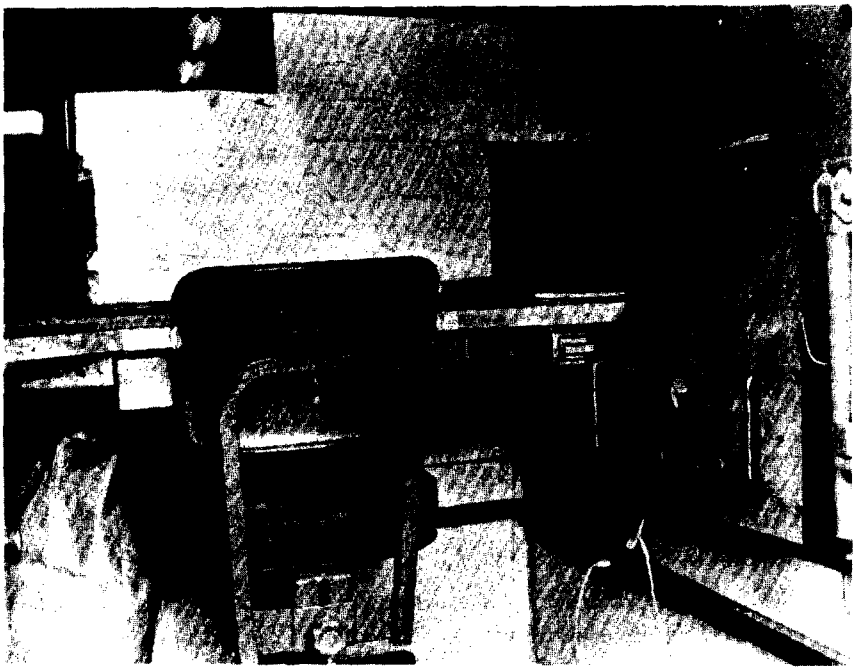
*See also p. 134, above.

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



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

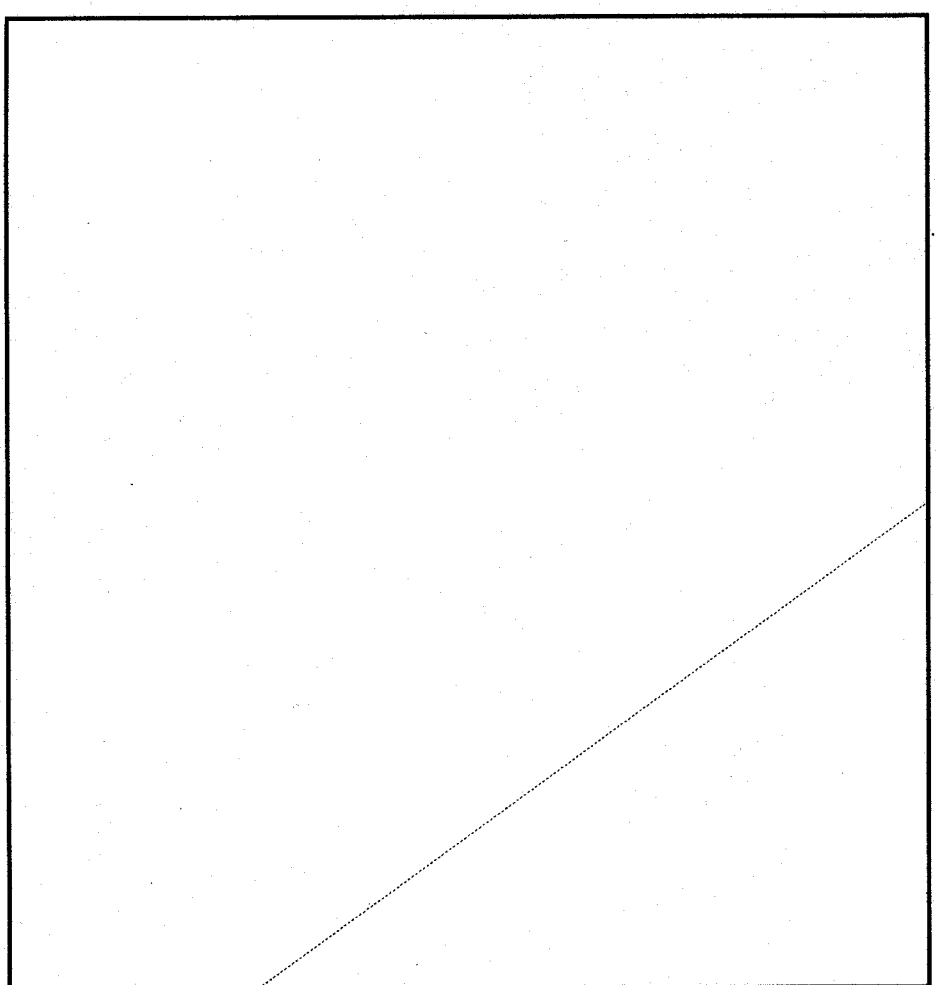
*In the geographic reference plotting system, the world is divided into 288 15-degree quadrangles. Each of these 15-degree quadrangles is identified by a two-character designator (row and column coordinates). Each of these 15-degree quadrangles is broken down into 1-degree quadrangles, which are again 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.

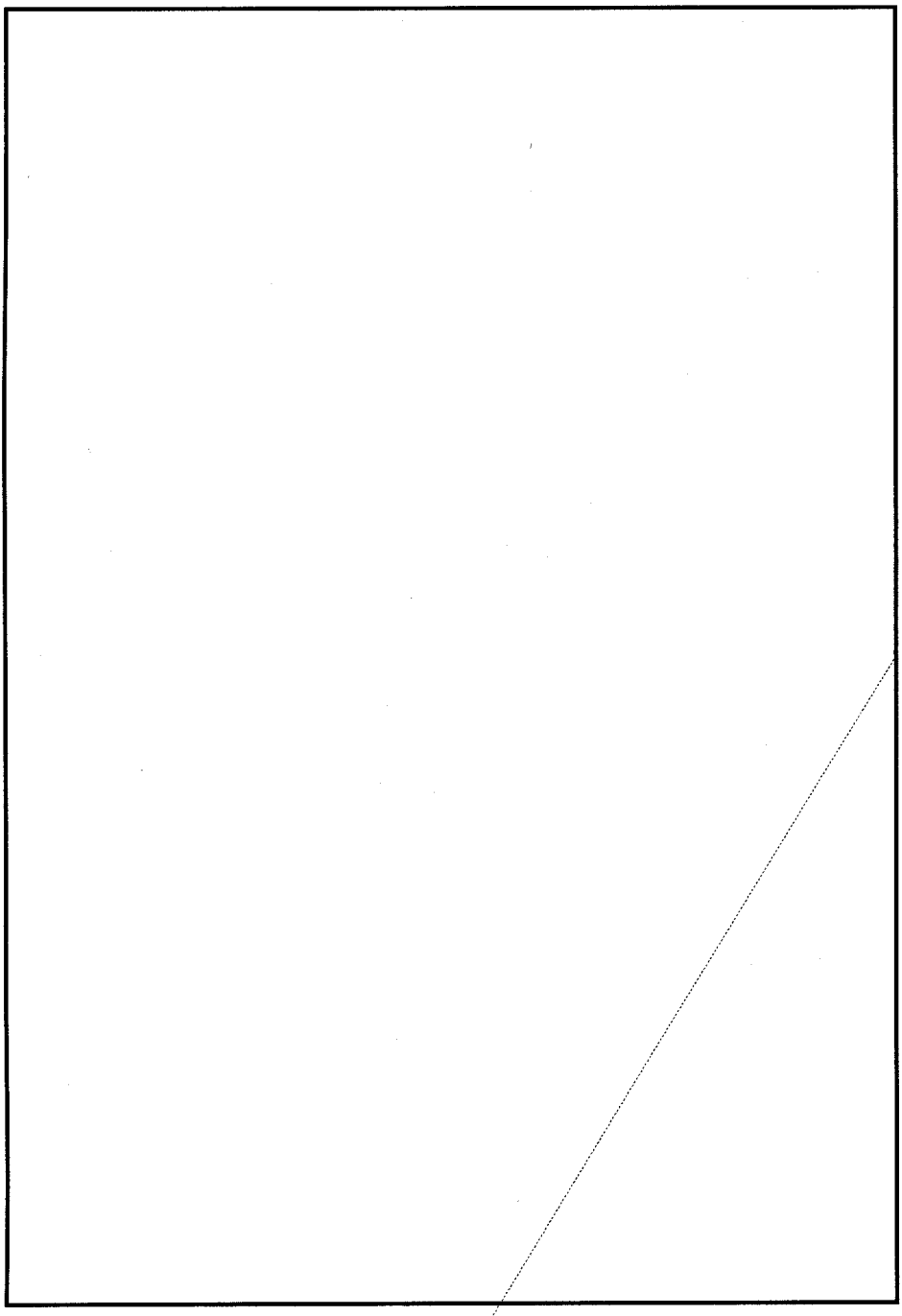
numbers (2 or 4) indicated, respectively, launch and recovery of MIG's. Some specific examples of possible use were:

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."





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.

[redacted]

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

[redacted]

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

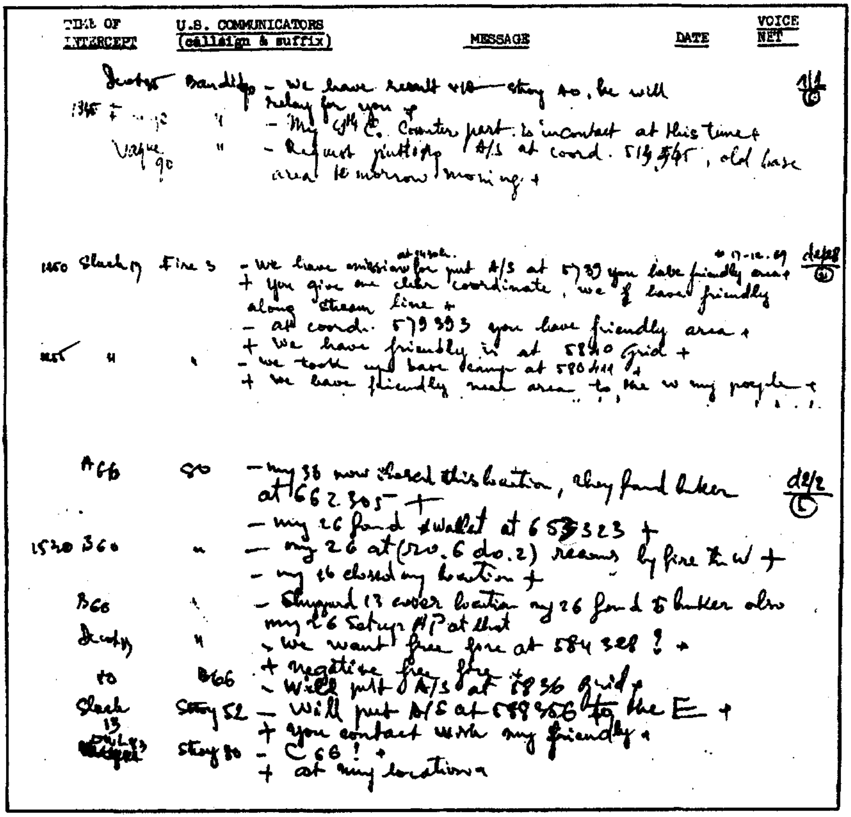
Lessons Learned

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-


TIME OF INTERCEPT | U.S. COMMUNICATORS (callsign & suffix) | MESSAGE | DATE | VOICE NET

relay for you +

– Request putting A/S at coord. 514 545, old base area tomorrow morning +

– We have mission for put A/S at 5739 you have friendly area +

+ You give me clear coordinate, we have friendly along stream line +

– at coord. 579 393 you have friendly area +

+ We have friendly in at 5840 grid +

– my 26 found wallet at 653 323 +

– my 26 at (520.6 do.2) reasons by fire to W +

– we want free fire at 584 328 ? +

+ negative free fire

– Will put A/S at 588 356 to the E +

+ you contact with my friendly +

– C 66 ! +

+ at my location +

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+		
			+We have friendly is at 5840 grid+		
1255	"	"	We took up base camp at 5804[illegible]+		
					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 (BO.6 DO.2) reochs by fire to W+		
			My 16 closed my location+		
	B66	"	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.

[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

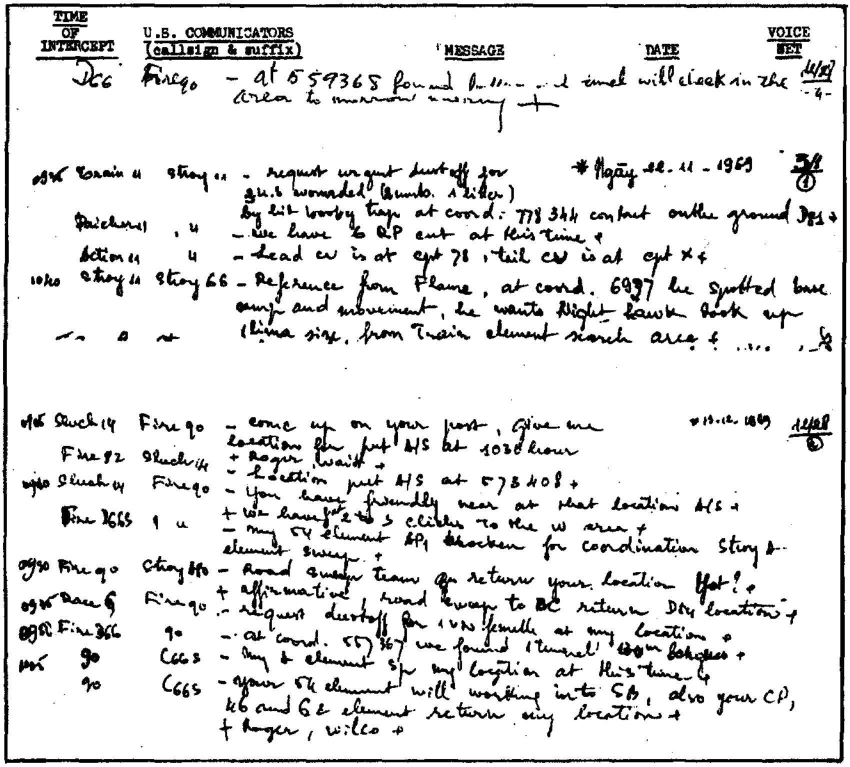
Events have shown that the U.S. Services were not well prepared to employ communications cover and deception. When CC&D operations were tried, the deception techniques, difficult to apply successfully even under optimum conditions, worked best when they involved SCA personnel and when operations staffs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



TIME OF INTERCEPT	U.S. COMMUNICATORS (callsign & suffix)		MESSAGE	DATE	VOICE NET
[illegible]	Fire 90		– at 559368 found [illegible] will check in the area to [illegible]		11/[illegible] -4-
[illegible]	Train [illegible]	Story [illegible]	– request urgent dustoff for [illegible] wounded (1 [illegible] 1 litter) by [illegible] booby trap at coord. 778344 contact on the ground [illegible]	* Ngày [illegible]-11-1969	[illegible] (1)
	[illegible]	"	– we have 6 RP out at this time +		
	Action [illegible]	"	– lead [illegible] is at cpt 78, tail [illegible] is at cpt X +		
10[illegible]	Story [illegible]	Story 66	– Reference from Flame, at coord. 6997 he spotted base camp and movement, he wants Night hawk [illegible] up [illegible] size, from Train element search area +		
[illegible]	Stuck 14	Fire 90	– come up on your post, give me location for put A/S at 1030 hour	* [illegible]-12-1969	11/[illegible] (6)
	Fire 92	Stuck 14	+ Roger, wait +		
[illegible]	Stuck 14	Fire 90	– Location put A/S at 578408 +		
			– You have friendly near at that location A/S +		
	Fire 66S	"	+ we have [illegible] 2 to 3 [illegible] to the W area +		
			– my [illegible] element [illegible] for coordination Story [illegible] element sweep +		
09[illegible]	Fire 90	Story [illegible]	– Road sweep team [illegible] return your location [illegible]? +		
			+ affirmative, road sweep to BC return [illegible] location +		
09[illegible]	Race 6	Fire 90	– request dustoff for 1 VN female at my location +		
09[illegible]	Fire 366	90	– at coord. 557367 we found 1 tunnel [illegible] +		
[illegible]	90	C66S	– my [illegible] element [illegible] my location at this time +		
	90	C66S	– your [illegible] element will working into [illegible], also your CP, [illegible] and [illegible] 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 wnb. 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+		
			+Roger wait+		
	Fire 82	Sluch 14	Location put A/S at 573408+		
0910	Sluch 14	Fire 90	You have friendly near at that location A/S+		
			+We have F at 2 to 5 clicks to the W area+		
	Fire D66S	"	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

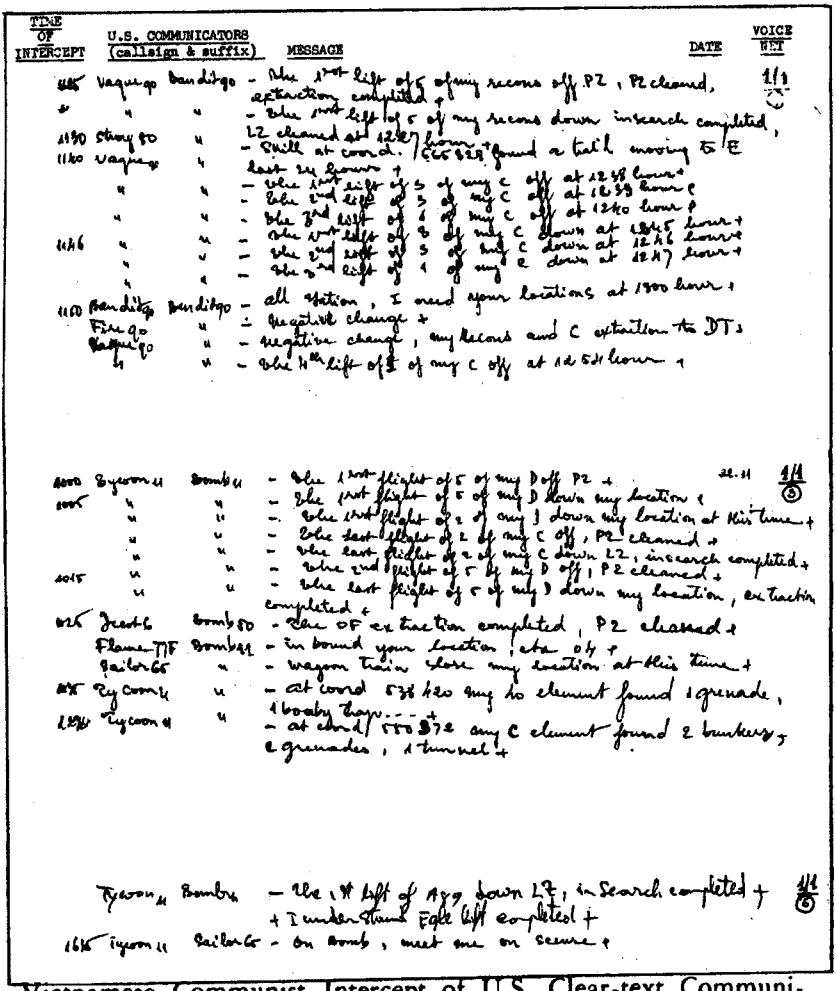
This review of monitoring and analysis operations to 1968 has shown that the greatest COMSEC improvement has resulted when there was a combined Service attack on a single problem of general concern—

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



TIME OF INTERCEPT | U.S. COMMUNICATORS (callsign & suffix) | MESSAGE | DATE | VOICE NET

1115 Vaquero Bandido – Blue 1st flight of 5 of my recons off P2, P2 cleared, extraction completed + 11/1

" " " – Blue 2nd flight of 5 of my recons down in search completed,

1130 Stingray " L2 cleared at 1242 hours

1150 Vaquero " – Still at coord. CC 828 + found a trail moving S to E last 24 hours +

" " – Blue 1st flight of 5 of my C off at 1238 hours +

" " – Blue 2nd flight of 5 of my C off at 1239 hours +

" " – Blue 3rd flight of 1 of my C off at 1240 hours +

1146 " " – Blue 1st flight of 5 of my C down at 1245 hours +

" " – Blue 2nd flight of 5 of my C down at 1246 hours +

" " – Blue 3rd flight of 1 of my C down at 1247 hours +

1150 Bandido Bandido – all station, I need your locations at 1500 hours +

Fireglo " – Negative change +

Vaquero " – negative change, my recons and C extraction to DT +

" " – Blue 4th flight of 5 of my C off at 1258 hours +

1000 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 D 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 +

025 Jeep 6 Bomb 50 – Blue OF extraction completed, P2 cleared +

Flame TIF Bomb 22 – in bound your location, etc 0/4 +

Sailor 65 " – wagon train close my location at this time +

035 Ty Coon 4 " – at coord 538 420 my lo element found 1 grenade, 1 booby trap... +

1135 Tycoon 11 " – at coord 550 572 my C element found 2 bunkers, 2 grenades, 1 tunnel +

Tycoon 11 Bomb 4 – Blue 1st lift of 499 down L7, in search completed + 1/1 (5)
+ I understand Eagle lift completed +

1165 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 C7 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 A89 down LZ, in search completed+		
1635	Tycoon 11	Sailor	+I understand eglo 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
[redacted]	
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

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

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