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.