SRH-162

WALDMAN

HISTORY

of

SECURITY MONITORING

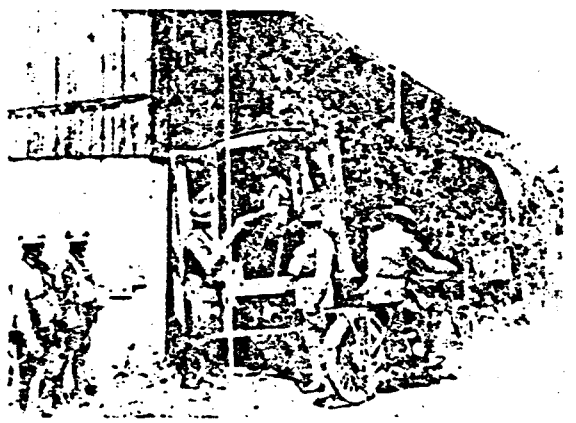
WWI to 1955

TABLE OF CONTENTS

THE HISTORY OF SECURITY MONITORING
PART ONE: WORLD WAR I

~~(Confidential)~~

The emergence of radio as a primary means of communication during World War I resulted naturally enough in the development of communication intelligence and communication security as we know them today. Easily intercepted radio messages produced valuable intelligence on enemy operations, and, conversely, gave the enemy information on our operations. Since there was no practical way of eliminating enemy intercept, the next best thing was to sample our own communications in order to discover what intelligence was being disclosed, and to take steps to minimize future disclosures. Thus, security monitoring came into existence.



A Typical World War I Radio Station

In July 1917, the Radio Intelligence Section, General Staff, GHQ, AEF, was formed in France, primarily for the purpose of attacking German military codes and ciphers. No communication security effort was in evidence during the first year, but an incident has been recorded which might have led indirectly to such an effort. American intercept operators, searching for an enemy station, picked up an unknown station transmitting an unfamiliar code. Sample messages were copied and turned over to the code section. Here they were puzzled over for some time, until finally it was discovered that they were training messages originated by an American station in Belgium. This was somewhat of a joke on the code experts, but it may have turned their thoughts to communication security. At any rate, a security sub-section was established shortly thereafter in February 1918.

The duties and functions of the security sub-section are best described in an actual report submitted by the sub-section to the General Staff on 5 May 1918. Portions of that report are quoted herewith:

"The Trench Code now in use by our Army is a production based scientifically on the actual solution of enemy Trench Codes, thus giving a practical code that can be used as the best means of wireless communication with absolute security; but it is not 'fool-proof.'

"Actual use of our code has shown that after all the care of producing a scientific, practical and secure code, it is used very carelessly and thoughtlessly in the field. This abuse of the Trench Code has in nearly all cases been due to the offenders' lack of knowledge of the use of code as a means of communication. It is, therefore, absolutely essential that before a man uses code, he must be thoroughly familiar with all fundamental principles of code and with the means of communication he is going to use.

"While General Orders and instructions given in the code book thoroughly cover the questions regarding the proper use of our Trench Code, it has been found that a strict surveillance of the actual use of the code is necessary to maintain discipline and keep our code reasonably safe from enemy solution.

"This surveillance of the actual messages sent by wireless is carried out in the following manner: a number of radio intercept* stations are installed along the entire front occupied

* 'Intercept,' as used above, is synonymous with 'Monitor,' as used today.

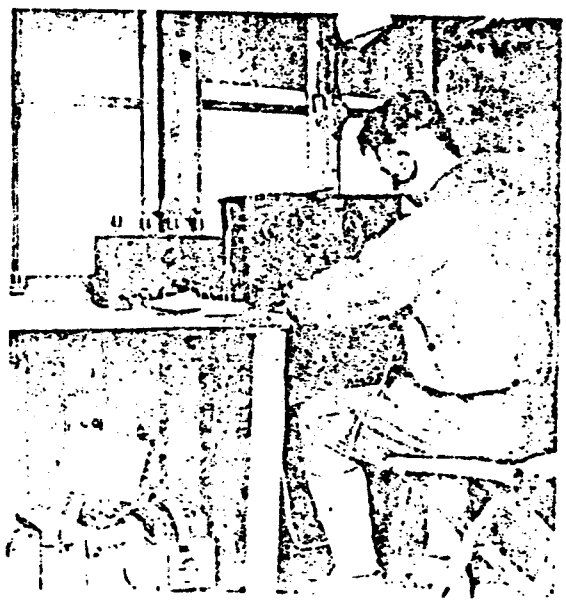
by our Armies. The duties of these stations is to intercept our Trench Code only. These are known as 'Control Stations,' and their sole purpose is to intercept all American messages which have been sent. The messages thus intercepted are sent into the 'Control Officer.' This officer must be thoroughly familiar with Trench Codes. He must be able to detect all infractions of instructions and General Orders covering the use of code and cipher. He must be able to suggest the best methods for using Trench Code and be so qualified that he can criticize intelligently and thoroughly the manner in which our Trench Code is being used in the field. His further duties are to see any weaknesses that make the present form of Trench Code vulnerable to enemy code men, and make recommendations in this way for improvements and corrections. In order to properly criticize and to detect any faults and weaknesses, the 'Control Officer' must place himself in the position of the enemy code man and study our messages from the enemy viewpoint.

"When messages are received by the 'Control Officer,' they are decoded, and if any violations of General Orders or instructions are found in a message which has been encoded, a letter is sent through military channels to the officer commanding the unit in which the message originated, over the signature of the Commanding General. The officer commanding the unit concerned is requested to make an investigation and report the action taken in each case to General Headquarters.

"Prompt and strict measures are taken when a message in the clear is intercepted. Documentary evidence proves that the enemy gained valuable information concerning our order of battle, etc., due to carelessness in the sending of clear English radio messages by operators and officers. Whether the message is of tactical value or merely irresponsible conversation does not matter. The enemy can make valuable deductions in all cases."

A few months after the submission of the above report, the functions of the Radio Intelligence Section were transferred to the Signal Corps. The security work then being done was expanded to include an examination into faulty call letter assignment and closer supervision over the assignment of organization code names.

Towards the end of the war, the dangers inherent in careless telephone conversations were realized. Wires were tapped near the front lines, and offenders were reported to their commanding officers in an effort to prevent repetitions.

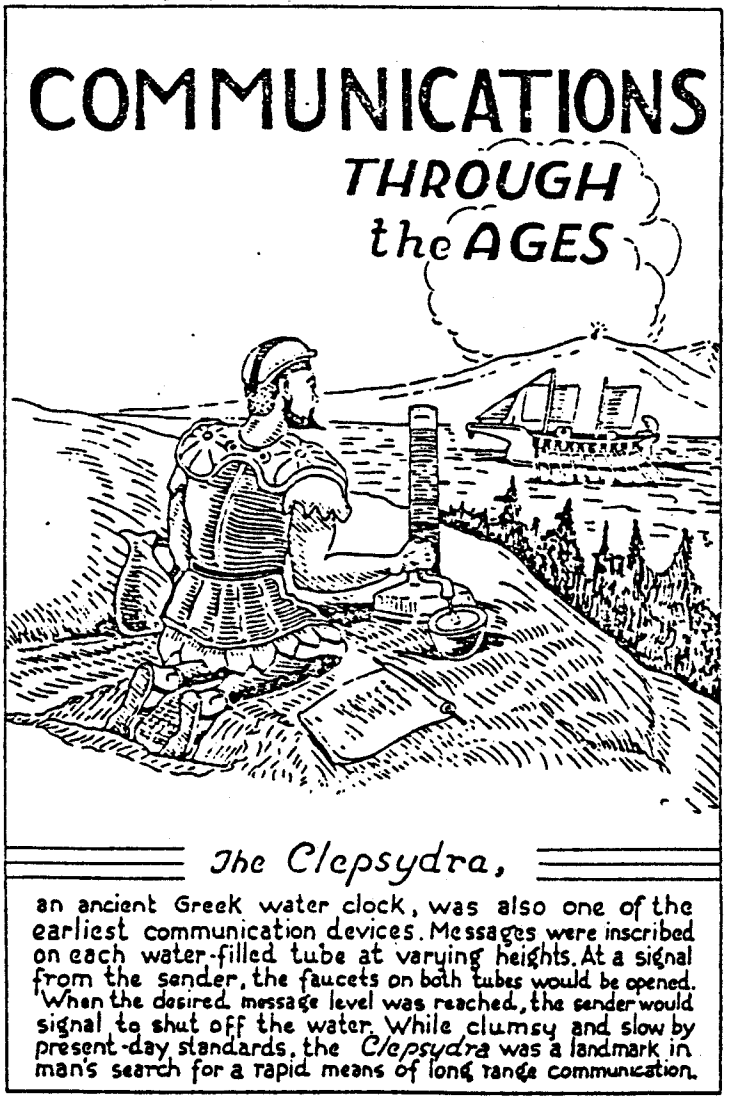


Security Monitor, Circa World War I

Just as the full value of communications as a source of intelligence had not been realized or exploited during the early World War I period, the need for communication security as a defensive measure had not been fully recognized or developed into a recognizable program. The art of deriving intelligence solely from the external features of messages, including traffic volume and flow, known today generally as traffic analysis, had not been invented as such. The violation of standing radio procedures as a source of intelligence had not been completely realized, hence 'procedure' analysis was non-existent during those early days.

THE HISTORY OF SECURITY MONITORING:

Despite the shortcomings of the signal security program during World War I, the formation of the tiny security sub-section in the AEF was actually a giant stride towards the vastly improved security program which exists today. Part Two of this series of articles will appear in the next issue of the Bulletin, and will trace the progress made in communication security monitoring subsequent to World War I.



The Clepsydra,

an ancient Greek water clock, was also one of the earliest communication devices. Messages were inscribed on each water-filled tube at varying heights. At a signal from the sender, the faucets on both tubes would be opened. When the desired message level was reached, the sender would signal to shut off the water. While clumsy and slow by present-day standards, the *Clepsydra* was a landmark in man's search for a rapid means of long range communication.

THE HISTORY OF SECURITY MONITORING

PART TWO: THE PEACE (1919-1941)

~~(Confidential)~~

The monitoring of electrical communications for security purposes was initiated in France during World War I with the formation of a security subsection of the Radio Intelligence Section, General Staff, AEF. The work of this sub-section was discussed in detail in Part One of this series, appearing in the preceding issue. Shortly before the Armistice, the functions of the Radio Intelligence Section were placed under Signal Corps control. This article covers the development of security monitoring during the period between the two World Wars.

THE CODE AND CIPHER SECTION

Immediately after World War I, the Signal Corps organized a Code and Cipher Section, primarily to compile codes and ciphers that would improve the security of our communications. A part of its work was devoted to the formulation of a program for the maintenance of security. The Army's experience in World War I had amply demonstrated that although technically sound cryptographic systems were provided, errors committed by code clerks might nullify the best efforts of the compilers. There were many examples in military history of defeats or disaster resulting from the interception by the enemy of plain-language messages, or of easily solved encrypted messages. The secure transmission of communications in time of war had been proved to be a vital necessity.

In themselves, codes and ciphers, however skillfully compiled, could not afford complete security. All systems had to be practical, and in actual combat where speed was essential, complicated methods could not be employed. The principle requirement for combat systems was to delay the enemy in his endeavors to ascertain tactical movements and the disposition of forces until such time as the information was out-of-date. It was evident, therefore, that systems should be secure enough to delay the solution of messages until such time as the information derived was of no value.

It was incumbent upon the Chief Signal Officer to train Signal Corps officers in the proper use of codes and ciphers, so that as few hints as possible might be given the enemy in the transmission of the message and the greatest delay possible imposed upon its solution. The Code and Cipher Section therefore prepared rules for the use of codes and ciphers embodying the best cryptographic practices. The rules were incorporated into the training literature to be studied by Signal Corps officers as part of a two-week course of instruction at Camp Vail, New Jersey (now Fort Monmouth).

There was no security monitoring during the Twenties, either planned or extant. The wheels of military progress moved rather slowly during these years, but matters were stepped up during the Thirties with the formation of the Signal Intelligence Service.

THE SIGNAL INTELLIGENCE SERVICE

The SIS was formed in 1930 in an effort to coordinate all cryptographic activities under the Signal Corps. Heretofore, the Military Intelligence Division had been responsible for the interception of enemy code and cipher messages. This responsibility was now assigned to the Signal Corps. The printing, storage, and handling of cryptographic materials was still the function of the Adjutant General, and remained so until 1934. The old Code and Cipher Section had become defunct the previous year, and its activities were assumed by the SIS.

Base units of the SIS were assigned to the War Department, the Corps areas and departments, GHQ, and the field armies. Communication security activities were restricted to the base units at GHQ and the field armies. The field units of the SIS were radio intelligence companies, which could be

assigned to any of the spheres of activity outside of the War Department. The RI companies were responsible for security monitoring and reporting, and cooperated with the base units where assigned.

In discussing SIS unit operation with respect to security monitoring and related activities, it must be realized this work represented only a small segment of the overall SIS mission. The primary SIS function was communication intelligence. The units concerned with security work operated as follows:

1. The SIS base unit at GHQ consisted of four sections, only one of which, in addition to other duties, was concerned with security. Violations of communication security and radio operating regulations that were reported by the RI companies and base units assigned to the field armies were studied, and reports were submitted to GHQ and elsewhere on request.

2. The SIS unit with a field army included a headquarters, with one or more RI companies operating under its direction and supervision. One section of the unit was engaged in monitoring friendly communications to discover violations of cryptosecurity rules and regulations, and in exercising surveillance over important wire lines. Reports were submitted to the SIS unit at GHQ, and to the signal officer of the unit concerned.

3. The RI company contained a headquarters platoon and three operational platoons. The intercept section of the headquarters platoon was made up of two teams operating four intercept stations each. These stations were not only to intercept enemy traffic, but to monitor friendly traffic when called upon to do so.

There was no table of organization for the RI company under this original concept, and none was to be instituted until the company had proved itself in active operation.

THE RI COMPANY IN ACTION

The first active radio intelligence unit was the 1st Provisional RI Detachment, organized at Fort Monmouth, New Jersey, in 1933. It operated until 1937, when it was expanded into the 1st Provisional RI Company. These units were primarily experimental, and were used for training and research in radio intelligence.

Three new RI companies were activated as National Guard units in 1939 in the wave of rearmament brought about by the declaration of war in Europe. These companies, along with the 1st Provisional RI Company, became known as Signal Radio Intelligence Companies, and were organized under T/O 11-77, with a few amendments to the original concept. The headquarters platoon now contained a "security monitoring section," the first organization of its kind so designated. The companies were assigned to field armies, and, in 1941, participated in the Carolina, Louisiana, and Arkansas and Texas maneuvers.

During the maneuver period, the security monitoring section monitored traffic, analyzed violations of operating regulations, and reported these to the signal officer of the unit concerned. In addition, such complete and accurate reports of order of battle, personnel, troop and supply movements, and map coordinates were compiled that, in one instance, when a report was shown to the maneuver commander, the unit was accused of stealing maneuver plans. The state of security in the communications of those pre-war days was pitifully bad, and, unfortunately, the reports were for the most part ignored, for the majority of officers were not yet convinced of the importance of communication security in the national defense effort.

After Pearl Harbor, the RI companies continued to operate both in the ZI and overseas, but security monitoring receded once more into the background. It was not until the European invasion that its importance was realized, and companies with specific monitoring duties were activated. With the employment of total encryption for overseas traffic, new techniques such

as traffic analysis and procedure analysis were to be developed, along with cryptanalysis, as a means of gauging the effectiveness of a security program. How this came about will be discussed in Part Three of this series, which will cover the World War II period.

THE HISTORY OF SECURITY MONITORING

PART THREE: WORLD WAR II

~~(Confidential)~~

SYNOPSIS

The monitoring of electrical communications for security purposes came into existence during World War I, when the need to minimize the amount of intelligence being made available to enemy interception was recognized. As recounted in Part One of this series, a security sub-section of the Radio Intelligence Section, GHQ, AEF, was formed in France for that purpose. After the conclusion of hostilities, no plans for security monitoring were made until the late Thirties, when the Signal Intelligence Service (SIS) organized the Signal Radio Intelligence (SRI) Company, under T/O 11-77. This company's principal mission was intelligence, but one of the intercept platoons was designated to perform security monitoring, and did so with great success in the maneuvers that preceded World War II. This phase was discussed in Part Two of the series. The present article continues the history through the conclusion of World War II. For purposes of brevity, activities in the European and Mediterranean Theaters of Operation will be discussed as typical of the overall situation.

NEW TECHNIQUES

The greatest advance made during World War II, security-wise, was in the development of techniques for the examination of monitored traffic. Up to this time, violations were handled in a relatively unscientific manner. Consequently, no basis on which to plan an effective counter-intelligence program existed. Now, in World War II, security traffic analysis and procedure analysis were developed to the point where each bit of information, no matter how isolated, could be scientifically evaluated, and an estimate made of the standard of communication security that could be attained.

THE SIS

The Signal Intelligence Service, formed in 1930, was the backbone of all World War II security monitoring activities. As in pre-war days, base units of the SIS were assigned to the War Department, corps areas and departments, theaters and field armies. At first, the SRI Company was the only SIS unit for field support. Later in the war, the Signal Information and Monitoring* (SIAM) Company was organized under T/O & E 11-87S, and SIS field units were reorganized under T/O & E 11-500 as Signal Service Companies. In all instances, the base units coordinated the work of the field units, and were responsible for notifying offending units of the violations committed. This was the SIS operation on paper. In reality there were many variations and deviations dictated by the circumstances of war.

THE SRI COMPANY

It became evident early in the war that the Signal Radio Intelligence Companies were not to play a major role in communication security activities. When the first companies arrived in England for training, all efforts were made to develop their intelligence potential, and the security mission was performed (if at all) indifferently. Monitoring operators were usually those who had failed to make the grade as intercept operators, and the general attitude among the personnel concerned was that their function was relatively unimportant. Although this attitude and these circumstances prevailed throughout most of the war, there were isolated instances in North Africa and after the Normandy invasion when SRI Companies performed important security missions, which will be noted in subsequent paragraphs.

THE STATE OF SECURITY IN 1943

The concept of monitoring in the Spring of 1943 was based on the assumption that signal personnel were aware

* At first, Staff Information and Monitoring

of the importance of radio security as a counter-intelligence means. Headquarters were expected to monitor their own nets to a large extent. Final reports were to be forwarded to the Chief Signal Officer, Washington. Policy and procedure in the theater would be based on these reports and on trips to units by SIS personnel.

The actual situation was quite different. Signal officers were either too busy to give adequate attention to their own nets, or lacked the facilities to do so. Wherever monitoring was attempted, it was received with suspicion and resentment by commanders, who failed to recognize the potentialities of enemy intercept. Radio procedure was in a chaotic state, due largely to the lack of any centrally issued instructions. Attempts to rectify this situation by the issuance of local instructions were unsuccessful, due to inevitable conflicts.

THE AFHQ MONITORING SERVICE (NATOUSA)

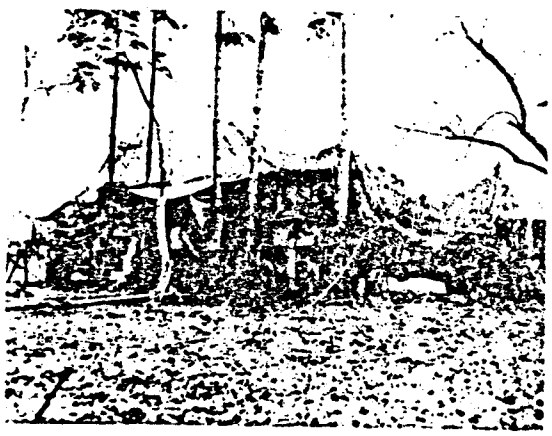
To achieve some sort of integration in the monitoring mission, and to restore some sort of order in communication channels, the SIS Radio Security Section in North Africa merged with the 123rd SRI Company in September 1943, to form the AFHQ Monitoring Service. They operated with moderate success for one month, until the 123rd was ordered to Italy. The principal accomplishment of the service was in spreading the doctrine of counter-intercept to several of the larger headquarters. The limited size of the section made it impossible to maintain adequate coverage of high level and low level nets.

AFHQ maintained, in addition, a telephone monitoring service, established at the Headquarters switchboard.

Security Monitoring in North Africa during World War II

Lines to be monitored were assigned by G-2. All conversations on these lines were checked, and when anything suspicious was heard, a recorder was turned on, and the rest of the conversation taken down. A report was then typed, including the recorded conversation and whatever collateral information the operator had picked up before turning on the recorder. These reports were turned over to G-2 for action. The fact that violators were not, except in a very few instances, signal personnel, made it impossible to handle these violations through signal channels, and the nature of the information disclosed precluded the use of normal command channels. G-2 action, though rather slow, on the whole proved reasonably effective in reducing subsequent violations for short periods, but new leaks tended to develop as old ones were closed, and it cannot be said that the rule against using telephones for classified information was observed to anything like a desirable degree.

While these activities were at their peak, a new concept of monitoring was being formulated with the activation of the Fifth Army's SIAM Company. With SIAM in operation, AFHQ was able to devote all of its efforts to fixed theater channels and generally higher level communications.



Monitor Trucks using Camouflage Nets, in France, 1944

SIAM

In the concept of SIAM operation, security monitoring became, for the first time, separated from intercept. Its new bedfellow was information monitoring, the purpose of which was to keep Army Headquarters informed of the tactical situation and troop disposition in anticipation of requests for reinforcements, supplies, and tactical deployment. SIAM developed in the following way:

In September 1942, during the Battle of El Alamein, a British staff officer tuned in a civilian radio which he found in a house near the scene of a tank battle, and overheard some of the radiotelephone transmissions emanating from the tanks. All of the messages were sent either in the clear, or in easily understood "double-talk." The officer realized that these transmissions enabled him to follow the course of the battle. He reported the incident to his headquarters, and the idea of a monitoring detachment for both security and information purposes was born. As a result, the British organized the "J" Service, and later supplemented it with the "Phantom" Service, both of which were highly successful in providing higher commanders with tactical information.

When the U. S. forces came into action in North Africa, the commanders became familiar with the value of the "J" and "Phantom" Services, and decided that a similar system would be desirable for themselves. This led to the organization of the Fifth Army's Provisional SIAM Company. For the information mission, SIAM detachments obtained tactical data from the division G-3, and encoded and transmitted messages of tactical importance to higher levels. For the security mission, SIAM detachments monitored, analyzed, and reported security violations to commanders as a function separate from information reporting. The SIAM Service was developed from personnel in the signal units under the control of Fifth Army at that time. Personnel and equipment of the SRI platoons of four divisions were placed under direct control of the Army Signal Officer through the Army SIS

Officer. These platoons formed the SIAM platoons at division level. In order to form the two corps platoons and one army platoon needed for the SIAM company, personnel were borrowed from two signal companies.

During the first week of the invasion of Italy (9 September 1943), the Fifth Army SIAM Service began to monitor for security and information. The value of the company as a provider of tactical information began to be recognized in the drive from the Garigliano River to link up with the Anzio beachhead, and in the drive to Rome and to the north. In the latter instance, it became evident that a breakthrough had been achieved, and the situation became so fluid that it was impossible to install and maintain wire communications fast enough to keep pace with the progress, so that the bulk of the traffic naturally shifted to radio. SIAM, therefore, provided the divisions most of their early information about the location of flanking elements and progress on other sectors of the front. SIAM situation reports at this time were so accurate, and were received so much more quickly than the information transmitted through regular channels, that they began to be accepted as official.

In May, 1944, the Fifth Army's suggested table of organization was approved by the War Department as T/O & E 87S. The SIAM company was to consist of one headquarters platoon, one army platoon, four corps platoons, eight division platoons, and four armored division platoons. One of the problems encountered in activating such an organization was that of personnel. There simply were not enough trained personnel available to staff the platoons. The four SIAM companies that were formed in the Third, Fifth, and Seventh Armies (two in the Fifth) bore little resemblance to the organization on paper. For the most part, they had to train their own personnel, and since the tactical information required continuous 24-hour monitoring, the required coverage for security analysis was often lacking.

SIAM, although not entirely successful, represented an important milestone in the development of security monitoring. Through the combining of the security mission with the information mission, skeptical commanders were made to realize that monitoring was a weapon to serve their needs rather than the obtrusive nuisance they had imagined it to be.

THE SIGNAL SERVICE COMPANY

Shortly after the SIAM companies were activated in 1944, the Signal Service Companies, with SIS functions, were reorganized under T/O & E 11-500. The company operated in two echelons: a company headquarters and two platoon headquarters. The platoons were organized around the radio intelligence intercept team.

From a security monitoring standpoint, the Signal Service Company did not make much of a mark during World War II. The intelligence mission occupied most of the company's time (as in the SRI company) and by the time they were able to concentrate on security monitoring, the war was over.

Shortly after V-J Day, when ASA was formed, the SRI and Signal Service companies were transferred to ASA control, and were generally the initial bases for the present day security monitoring program. How this came about will be discussed in the final article of this series, which will bring the history up-to-date.

THE HISTORY OF SECURITY MONITORING

PART FOUR: 1945 TO DATE

(Confidential)

SYNOPSIS

The first attempt at monitoring friendly electrical communications was made during World War I, when a security sub-section of the Radio Intelligence Section, GHQ, AEF, was formed in France. After the Armistice, no further plans were made until the late Thirties, when the Signal Intelligence Service (SIS) organized the Signal Radio Intelligence (SRI) Company under T/O&E 11-77, with a primary mission of communication intelligence (COMINT) and a secondary mission of communication security (COMSEC). Security monitoring was successfully performed by this organization during the pre-war maneuvers in 1940 and 1941, but when the United States entered World War II COMSEC was almost completely subordinated to COMINT. The two functions were separated in 1944 when Security monitoring was combined with information monitoring and the Signal Information and Monitoring (SIAM) Company was activated, first as a provisional company, and later under T/O&E 87S. Patterned after the British "J" and "Phantom" Services, SIAM made its mark primarily as a provider of tactical information, though it did serve to promote COMSEC consciousness in supported commands, a service that was likewise performed by the SIS Radio Security Stations at various oversea headquarters. In the latter part of the war, Signal Service units were organized under T/O&E 11-500 to perform COMSEC missions. This marked the first time that organizations were formed for the sole purpose of performing communication security monitoring and analysis. In this, the final part of the history, we will see how security monitoring became unified under the Army Security Agency in 1945, and how it developed from that time forward.

THE FORMATION OF ASA

At the close of the war in Europe, there were fourteen Signal Service Companies and ten SRI Companies in operation in the ETO. The four SIAM Companies were disbanded when a large percentage of their personnel were returned to the U.S. The SIS Sections remained attached to theater headquarters. In the Far East, four SRI Companies continued to operate in the war against Japan. By August, the machinery had been set into motion to combine all Army COMINT and COMSEC (cryptologic) organizations into a single agency. Our experiences in World War II had demonstrated that the cryptologic problems of all commands throughout the Army were so closely interrelated that the full potentialities of COMINT and COMSEC activities could be realized only by placing them under the control of a single commander who could coordinate them on a world-wide basis. Accordingly, all cryptologic functions, facilities, and personnel of the Army, except those which were integral to the signal communication system (eg, cryptocenters) were combined on 15 September 1945 to form the Army Security Agency. From that date forward, COMINT and COMSEC organizations have been attached rather than assigned to the commands they support. ASA organizations performing security monitoring and analysis execute missions requested by supported commands, while operational control and technical direction of the monitoring and analysis operations are responsibilities of the Agency.

POSTWAR DEVELOPMENT

Security monitoring, like many of the Army's functions, suffered from immediate postwar demobilization. A decisive victory had been won over the Rome-Berlin-Tokyo axis. Yesterday's enemies were powerless to exploit our communications. This, together with the return to peacetime operating conditions, resulted in a rather sharp curtailment of the Army's communication security operations. During the final months of 1945, monitoring was continued, but on a reduced scale. Full-scale security monitoring and analysis were resumed in 1946, subsequent to the

formation of ASA, Europe and ASA, Pacific (now ASAFE) as branches of the parent organization in Washington.*

In 1948, when the Army and Air Force were separated, the task of monitoring Air Force communications was assumed by the U.S. Air Force Security Service, to which ASA COMSEC organizations supporting the Air Force were transferred.

ASA IN SUPPORT OF A FIELD ARMY

By January 1950, plans for a new ASA field army support organization reached the drawing board stage. A new concept entitled, "ASA in Support of a Field Army," outlined the Communication Reconnaissance Organization, which was put into effect the following year. The plan as finally approved reorganized the ASA support structure for the field army. The COMSEC mission of the Agency in support of a field army was to furnish the necessary facilities and supervision to insure compliance with COMSEC regulations, to distribute and account for cryptomaterial within the command, and to keep the commander advised on the security of his signal communications and of ways in which their security could be improved.

The plan was worked out with the recognition that the ever increasing use of electrical communications facilities by U. S. forces had compounded the need for communication security support to commanders at all echelons. It was realized that such support was mandatory if we were to deny the enemy access to the intelligence that would be passing over these facilities.

The Communication Reconnaissance Group (T/O&E 32-500) was created to support field armies. ASA units organized under T/O&E 11-500 were reorganized under T/O&E 32-500 during 1951. The new group organization included communication security personnel and facilities to provide direct support at army, corps, and division levels.

The group headquarters and headquarters company performed cryptomaterial supply and maintenance functions for the field army at large, supervised and coordinated the security support activities of subordinate ASA units, and provided direct monitoring and analysis services to the field army headquarters and army troops.

Each corps of the field army was served by a Communication Reconnaissance Battalion which included one security company, the sole function of which was to provide direct security monitoring and analysis support to the corps and its subordinate divisions. Detachments from the security company supported individual divisions. Teams from the detachments operated in regimental and battalion areas when necessary to insure adequate monitoring coverage of division communications.

Facilities were provided to monitor radiotelegraph, radiotelephone, teletypewriter, and telephone communications. The various nets and circuits were monitored on a rotating basis. Particular attention was devoted to nets and circuits which were most vulnerable to interception and which experience showed would be most likely to carry information of the greatest intelligence value to the enemy.

Spot reports of serious violations found in monitored transmissions were made to the supported commands to assist them in taking immediate corrective action. Periodic communication procedure analysis reports were made to assist commanders in improving the operating and transmission security discipline of their signal communication systems. Security traffic analysis reports were submitted periodically to keep commanders informed of the amount and kinds of military information which could be presumed to have been exposed to interception by the enemy, to assist them in making realistic appraisals of the transmission security of their commands, and to aid them in taking direct, effective action to eliminate correctable weaknesses.

** Other ASA oversea headquarters were organized within the next three years.*

Encrypted traffic was obtained from the supported commands, decrypted, and examined for deviations from crypto-operating instructions. Violations discovered were reported to assist the supported commands in maintaining high standards of cryptosecurity.

Action in Korea proved that the communication reconnaissance organization possessed great flexibility and was capable of providing support to field armies which do not follow the "book" type of organization.

Military operational specialist and equipment requirements, internal and external organizational relationships, missions, functions, work procedures, and reporting systems were closely studied in various oversea commands in a wide variety of situations. A number of adjustments in organization, equipment, and doctrine were made as a result of these studies. T/O&E 32-500 was revised, and a series of fixed T/O&E's (32-51, 32-55, 32-56, and 32-57) were prepared to reflect these changes. The Communication Reconnaissance Groups were reorganized under the new fixed T/O&E's during the current year.

The principal modifications that have been made in the communication security components of the group have undergone no substantial change; however, the cryptomateriel supply and maintenance functions of the group headquarters are scheduled to be transferred to the Signal Corps as a result of a recent redefinition of ASA functions in AR 10-122, 23 June 1955. This regulation also added to the security support responsibilities of the Agency, but the effect which these additions will have on the organization and functions of the Communication Reconnaissance Group cannot be described until current studies are completed.

The transmission and cryptographic security analysis functions formerly performed by the headquarters of the security company for the corps at large are now performed by the headquarters of the Communication Reconnaissance Battalion (T/O&E 32-56). The battalion headquarters has also been made responsible for monitoring the communications of corps headquarters and corps troops.

The battalion contains two operations companies (T/O&E 32-57), each of which has two division support platoons. These platoons are organized and equipped to provide both COMSEC and COMINT services. The COMSEC section of the platoon consists of a number of monitoring teams which can be deployed in the division area in a variety of combinations to obtain adequate coverage of division communications.

MONITORING ABOVE FIELD ARMY LEVEL

Communication Reconnaissance Detachments (T/O&E 32-500A) provide monitoring and analysis services to communication and theater zone organizations. These detachments are organized under a cellular rather than a fixed T/O&E because the composition of the forces they support varies considerably from one oversea command to another. Oversea ASA's supervise and coordinate all security monitoring and analysis activities of the communication reconnaissance organizations in their areas, and, in addition, furnish direct monitoring and analysis support to the senior army headquarters in the oversea commands. Direct monitoring and analysis support is furnished to ZI organizations by Army Security Agency, Washington, and by ASA general reserve units.

The COMSEC activities of ASA at all echelons of command are integrated into a single world-wide program administered by ASA, Washington, because the communications of all commands are so closely interrelated that the security of each is dependent to a large degree on the security of the others.

This article concludes the series on the history of security monitoring.