7102000

ARMY SECURITY AGENCY

WASHINGTON, D. C.

SUMMARY ANNUAL REPORT

OF THE

ARMY SECURITY AGENCY

FISCAL YEAR 1947

Prepared under the Direction of

CHIEF, ARMY SECURITY AGENCY

February 1950

OSOAS-27

000 000

Plain cover [illegible]

HISTORICAL NOTE

Although this Summary Annual Report of the Army Security Agency is for the Fiscal Year 1947, it was not possible for it to be written earlier because the reports upon which it is based were not available.

It is a brief summary intended primarily only for the Chief of the Agency, viewing the year's work as a whole and making no attempt to differentiate between the responsibilities and successes of the various divisions, branches, and sections of which the Agency is comprised. This information may be found in the various Annual Reports on file in the Historical Section.

Historian, AS-SY
February 1950

TABLE OF CONTENTS

	PAGE
I. Introduction	1
II. Communications Security	7
III. The Production of Intelligence	20
A. Interception	22
B. Cryptanalysis	26
The Russian Systems	27
Other Nations	30
Soviet Satellites	30
European Neutrals	33
The Near East Group	36
The Latin-American Group	37
China	40
Commercial Traffic	41
C. Supporting Techniques	41
D. Production Figures	44

LIST OF EXHIBITS

	TAB
Nomenclature and Characteristics of Cryptologic Equipment	1
Cryptographic Traffic Volume Reports Received and Processed, 1 July 1946 to 30 June 1947.....	2
Flow Chart for Development of Cryptographic Devices.	3
Volume of Reports of Violations of Cryptographic Security, 1 July 1946 to 30 June 1947	4
Cryptographic Traffic Processed, 1 July 1946 to 30 June 1947	5

SUMMARY ANNUAL REPORT OF THE

ARMY SECURITY AGENCY

FISCAL YEAR 1947

I. Introduction

In the present Annual Report, intended to provide a brief summary of the achievements of the Army Security Agency during the Fiscal Year 1947, the work of the Agency is viewed as a whole, no attempt being made to differentiate between the responsibilities and successes of the various divisions, branches, sections, and detachments of which the Agency is comprised. Indeed, during the year under review, although some difficulties became apparent as a result of failure to make a clear-cut differentiation between "staff" and "operating" functions, there were no major regroupings within the Agency's internal structure. The organizational plan dated 7 November 1946 was maintained throughout the year except for minor changes below branch level. Nor was there any change in the twofold mission of the Agency as it operated under the Director of Intelligence, War Department General Staff:

1. The preservation of the security of U.S. Army communications.

2. The production of intelligence from intercepted communications of other nations, whether friendly or hostile.

Accomplishment of these two missions involved during the year

the employment of more than 5500 persons,[1] approximately 42 per cent of them military and 58 per cent civilians, and the expenditure of more than nine million dollars.

Despite the constantly unsettled international situation caused by the difficulty attendant upon efforts to negotiate the peace and to establish the United Nations, together with several highly explosive areas each capable of producing another war, the year was marked, so far as this Agency was concerned, by no developments of the magnitude of the war years which preceded. Reduction of strength brought about by the demobilization has been accomplished without wholesale dismissal but by this time voluntary resignation had largely ceased--this was the first full year of peace-time activity. Yet the day-by-day work of the Agency in fulfilling its mission resulted in solid achievement in many fields. The effort of the year was to maintain and improve the security of our own communications and to reduce to a state of readability the communications systems of foreign governments. Progress made in these directions will be described in greater detail later in this report.

A serious budgetary problem was experienced during the early months. In the following table are shown the sums (1)

1. This figure (2515 military, 2985 civilians) represents actual strength reports for the second business day April 1947 a period taken as typical.

originally requested by the Agency from the Director of the Budget; (2) those approved by the Director of the Budget and recommended to Congress by the President; (3) those actually appropriated by Congress (both originally for these purposes and in subsequent allotments of War Department funds); and (4) those actually obligated by the Agency throughout the year:

Purpose	Requested	Approved	Appropriated	Obligated
Maintenance of cryptographic equipment	$25,000	$17,500	$17,150	$154,043
Construction of intercept stations	7,700	7,700	7,546	268,365
Maintenance of intercept stations	8,600	8,600	8,428	5,827
Training	7,500	7,500	7,350	10,489
Machine rental and miscellaneous	627,988	418,197	409,633	396,910
Research and development, original	1,315,000	1,095,000	1,073,100	1,677,579
Increase June 1947			118,000	
Total			1,191,100	
Personnel, original	7,414,992	5,512,000	5,401,760	6,557,368
Increase Sept. 1946			2,047,000	
Total			7,448,760	
Totals	$9,404,780	$7,050,497	$9,090,167	$9,070,581

It will be noted that the Director of the Budget left untouched the requests in three of the smaller items and in the case of the others reduced the estimates to sums from 61 per cent to 85 per cent of what was asked. Congress, however, regularly reduced its appropriations to 98 per cent of what was recommended

by the Director of the Budget. Early in the year, however, it became clear that the original estimates, and consequently the appropriations, were far too low for the work to be done. For this reason steps were taken to secure an additional allotment for personnel which was received in the amount of $2,047,000 in September 1946 when the first quarter was still not ended. This eased the situation in this item and the total appropriation actually exceeded the amount obligated for the year, making possible the transfer of $959,410, with, of course, official approval, to the procurement program. Even this did not take care of the deficit in research and development and additional funds were obtained in June 1947 in the amount of $118,000. While in three cases the obligation exceeded the appropriations by very large ratios (890%, 350%, and 140%, respectively), these items were small and the relative increase in the total budget could be absorbed by the balance in the personnel fund.

It should be pointed out that in the case of this last-named fund, the sum originally requested would nearly have sufficed to care for this expenditure, had it not been for the 14 per cent blanket increase (with a statutory ceiling of $10,000) in civilian salaries created by act of Congress. At the beginning of the year it was feared that the Agency would be required to absorb the flat increase by economies producing a forced reduction in strength. Many other governmental

agencies appear to have been reduced to this extremity in order to keep their books balanced, but this Agency was fortunate in not being compelled to dismiss personnel as the result of the 14 per cent increase in salaries.

Furthermore, as this was the first year of peace-time operations, it was to be expected that greater experience in preparing budgetary estimates would presumably prevent the recurrence of under-estimates in the future.

One serious organizational problem, briefly indicated above, began to appear in this year. This was a result of the creation at the close of the war of the Army Security Agency as an autonomous organization under the Military Intelligence Division of the War Department General Staff. Various ties which had formerly existed between the Signal Security Agency and the Office of the Chief Signal Officer were cut. Hence, new mechanics for accomplishing the necessary administrative operations of the Army Security Agency, formerly conducted within the OCSigO for the SSA, had to be established. The obvious step was to form an ASA Staff for the purpose of relieving the operating divisions from much of the paper work involved in their relations with agencies outside Arlington Hall Station.[2]

2. See pp. 2-9 of Summary Annual Report of the ASA Staff for FY 46.

[illegible] the Staff organization[5] increased in size and scope of its activities and responsibilities. The many new and varied problems confronting a young organization were solved in a satisfactory manner. However, there were occasions when conflicts between members of Staff and members of operating divisions or independent branches occurred because of failure to establish a clear-cut distinction between Staff and command functions. The origin of this difficulty lay in the basic duality in the functions and responsibilities of the Deputy Chief, ASA, who had been given not only command functions but also Staff functions. From this duality stemmed a somewhat similar duality on the part of all the members of the Staff, since they were not only acting in Staff capacity but also as assistants to the Deputy Chief, ASA, who, as already noted, possessed both command and Staff functions. The effects of this duality in function and of the failure to change the organizational structure or to maintain the demarcation between Staff and command responsibilities were frequently reflected in the occurrence of [illegible], and inconsistencies in action. For example, recommendations from an operating unit, dealing with matters affecting outside agencies, might be changed or reversed by Staff without consultation with the personnel who originated the recommendation.

---

5. See Tab [illegible] of the Summary Annual Report of the ASA Staff for FY 46.

thus causing extensive duplicity action. However, as Staff members gained experience these objections became less frequent and better relations between Staff and operating personnel were established.

II. Communications Security

As had been said, one of the two primary responsibilities of the Army Security Agency was, in this year as in the past, the preservation of the security of U. S. Army communications against the possibility of enemy cryptanalytic attack. The magnitude of this task will be readily appreciated from a consideration of the volume of Army traffic passing during a typical month (January 1947):

Classification	Number of Messages		Number of Groups	
Secret	8,775	(25.2 %)	1,539,775	(32.8 %)
Confidential	20,580	(59.1 %)	1,907,317	(46.7 %)
Restricted	5,467	(15.7 %)	839,987	(20.5 %)
Total	34,820	(100 %)	4,086,077	(100 %)
Annual traffic estimated at this monthly rate	417,840		49,090,124	

From a volume of traffic such as this, a potential enemy, armed with modern means of cryptanalysis, might be presumed to be able to derive a considerable body of useful intelligence, unless the traffic itself is adequately protected.

Therefore, to protect the traffic, cryptographic equipment and systems of various types had to be supplied for message centers. The attached document, "Nomenclature and Characteristics of Cryptologic Equipment," (Tab 1) shows clearly the

systems in use or under development at the beginning of the year, together with their current status. It may be of interest to report the equipment and systems which were actually in use for the traffic of January 1947 already mentioned (Tab 2):

	Per Cent of Total Groups
SIGABA	40.0
SIGTOT	11.3
SIGCUM	25.0
One-time pad systems	2.4
Strip Systems	2.0
Combined Cipher Machine	5.0
M-209	0.5
SIGHUAD	15.0
SIGBRAT	0.8

New systems, however, had constantly to be under development in order to provide for replacement and for more adequate fulfillment of the basic military requirements not yet regarded as satisfactorily solved. Some idea of what work such development involves will be gained from the "Flow Chart for Development of Cryptographic Devices" (Tab 3) which clearly indicates the various steps to be traversed from the determination of the Basic Military Requirements and Preparation of the Military Characteristics to the point where the system is ready for distribution to the users.

Among the more significant developments during the year was the work done on the SIGROD cipher machine. As the strength of U. S. forces in advance areas was reduced, it was deemed unwise to expose to possible physical compromise the very secure SIGABA machine, based, as it was, on cryptographic principles

unknown to other nations. It was feared that the result of such compromise would affect U.S. Signal Intelligence potentials, though not the security of our communications. While the general nature of the SIGABA was believed known to the British from several occasions when British personnel had been permitted to see the machine in violation of the general policy not to divulge the SIGABA to them, they had never been given access to it so that it could be studied intensively. And TICOM reports had shown that the Germans were aware that the U. S. forces were using a high-grade machine but they had never learned anything technically useful concerning it. Hence, it was regarded as desirable to protect the machine, since its capture would certainly assist enemy cryptographic agencies in developing their own machines on the same principle.

What was needed, therefore, was a machine of relatively high security but using cryptographic principles known to other nations, so that in the event of its capture a potential enemy would gain no cryptographic technology which could be used against us, if war should come soon again. To solve this problem, a machine which, figuratively speaking, was the offspring of a "marriage" between the SIGABA and the SIGGUM and which was, therefore, dubbed the SIGBRAT was developed. Basically, the SIGBRAT used the SIGABA chassis, but provision was made to employ a set of only 5 rotors in cascade, the rotors being stepped practically odometrically. But as tests were

needs on the machine, of which two models had been constructed in February 1946 for an estimated cost of $4,500 each, and fifty more had ultimately been produced, though only nine had been issued, it soon turned out that the SIGSALY was not really secure enough for the needs which operational usage developed. The ASA had been informed that the machine would not be used for traffic higher than CONFIDENTIAL, whereas some of the users were sending TOP SECRET traffic in it. As a result, it was decided to make studies of a revision of the SIGSALY in which the same five rotors were retained, but by testing different combinations of the fast, medium, and slow rotors, it was hoped to find an arrangement in which the desired security would be added. This model, which was in reality identical with the Combined Cipher Machine and with the Navy CSP 1700, was deemed sufficiently secure to be regarded as successfully fulfilling the requirement, and in September 1945 a total of 600 of the machines were procured at a cost of $1,678.40 each. Distribution progressed to the point where 512 of the 600 machines made were in use, and all but one of the military attachés who held any machine at all were equipped with SIGROD.

Considerable work was still being done on the SIGJOBO and HALF-JOBO developments originated by the Navy. While the SIGABA was and is a highly secure machine, it has suffered from the disadvantage that, as originally developed, it was not possible to use it directly for teletype transmissions. That is, the

SIGABA requires an operator to encipher the plain text, the resultant cipher text being recorded on tape. This tape must then be handed to another operator who manually types the enciphered text on his teletype keyboard. In the case of incoming messages received by teletype, the received teletype copy must be used by the SIGABA operator as the text for his manipulation of the SIGABA keyboard to decipher the message. Consequently, much time is lost by the necessity for two keyboard operations and in message centers where volume of traffic is high this item is a serious problem, since there would naturally be a tendency to use less secure systems which could encipher and transmit with a single keyboard operation.

To obviate this difficulty, the SIGJODO was developed. Briefly, in the case of outgoing messages this machine takes the electrical signal output of a SIGABA (or SIGEBAT or SIGROD) and automatically converts it into its 5-unit teletype equivalent, the latter then being recorded in the form of a perforated tape or being transmitted directly if arrangements are made for on-line transmission.[4] Conversely, in the case of incoming messages the SIGJODO was intended to take the perforated teletype tape or, in the case of on-line transmission, the teletype

4. While simultaneous on-line transmission would appear to offer greatest possibilities for shortening time of encipherment and transmission, in actual practice most message centers find it more practical to use the SIGJODO to convert the SIGABA operation to a perforated tape which can then be fed into the transmitter when the circuit is free.

impulse received from the circuits, and convert the perforations or impulses to deciphering impulses on the SIGABA unit, the result being automatic decipherment and printing of the plain text message on the tape. The bare recital of these facts sounds simple, but to effect the conversion mentioned proved to be a technical problem which has never been wholly solved from the engineering point of view. In fact, it turned out to be more practical to modify the SIGJODO so that it could be used for the automatic decipherment of incoming messages, rather than for the automatic encipherment of outgoing messages. Moreover, message centers serving large headquarters where automatic operation is most useful, normally received a much greater volume of traffic than they send. Therefore, the HALF-JODO was developed; it would permit the use of SIGABA with teletype for automatically deciphering incoming messages -- for outgoing ones, the double operation of encipherment and transmission would still be needed, but this was a minor disadvantage compared with the impossibility of using SIGABA alone, either for incoming or outgoing teletype communications. While the successful completion of these two pieces of equipment would mark an important advance in cryptological research and development, both equipments are still in the stage of development and interim use.

Another important problem was caused by difficulties encountered in the use of one-time SIGTOT tapes. These tapes were originally all identical in appearance except for the

0-0 016

number stamped on the outside. Users were therefore frequently mistaking the sending tapes for the receiving, both of which were all-white in color, and the result was frequent compromise. In order to prevent further resurrence of such mishaps, tapes for receiving were henceforth to be colored red. At the outset, this change placed a considerable burden on production. The receiving tapes in storage were all dipped in a red dye so that they would be readily distinguishable from the sending, which were not dipped.

Much attention was also given to the development of a Cryptographic Van designed for combat operations in the future, and to the design and installation of cryptographic equipment in the Presidential plane. ASA personnel at various times actually supervised the installation of the equipment in the plane and accompanied it in flight.

A high-security speech equipment designed for operation in a trailer and also in a form that can be shipped by air, the AN/GSQ-2,3, was developed for the AGF and AAF. The AGF tested this equipment at Fort Bragg from March to June 1947, and the AAF was to test it soon. Research was also done on another AGF requirement, Speech Equipment AN/GSQ-5, a high-security device for use with telephone in medium echelons, and two major components of this device were developed here. Work was done also on the miniaturization of cifax and teletypewriter adapters. A laboratory model of AN/GSQ-4 was made, using as a basis a magnetic tape recorder which had been captured from the Germans at

the end of the war. With this model it was possible to test easily various transpositions and interlockings of enciphered speech in an effort to improve the insecure features inherent in the old SIGJIF (Speech Equipment AN/GSQ 1, 1A). In the field of ciphony, also, special vacuum tubes were adapted to a pulse-type system, replacing a mechanical component with an electrical component. In cifax development the emphasis was on improvements of the SFR-3D equipment, a medium-high-echelon enciphered facsimile equipment for the AAF.

In the electronic and electromechanical fields the ASA did work on the development of rotors and tubes for Converter MX-519()/TG, a highly secure teletype cipher machine for use by the AGF and the AAF. This machine which as yet, of course, is only in a research and developmental stage, is so designed as to increase very greatly the security of teletype transmissions using the Baudot code. At present, it is theoretically possible for a potential enemy cryptanalyst to solve messages transmitted in enciphered form by teletype whenever he has been fortunate enough to intercept no more than two messages which, through violations of cryptographic security principles, have been enciphered with precisely the same key. The MX-519()/TG when completed, will approximate the very high security of the SIGABA itself in that solution of messages will necessitate interception of at least 25 improperly enciphered messages all in precisely the same key. Since it is not likely that so many violations would occur in the traffic of any given day, all of them in depth, the

possibility of an enemy successfully solving messages enciphered in this machine is negligible. Therefore, it seems likely that the MX-519()/TG will ultimately replace the SIGABA because of its equally high security, and also replaced the SIGJODO and the HALF-JODO, because it will afford a means of automatic encipherment at least as rapid as that provided by these latter machines. Incidentally, the first completely electronic-governed motor for use with teletype was produced.

Further progress was made in development of extremely high-precision recorders and reproducers for ciphony, cifax, and frequency multiplexed signals. In all research and development the trend was to create high-speed crypto-equipment wherever possible.

Considerable work was done on the problem of storing cryptographic machinery, involving such tests as the proper way to seal the packages against moisture, proper lubrication, and so on. A particularly important phase of this activity involved what was to be done to the SIGSALY equipment. This was a very high security equipment originally developed entirely by the Bell Telephone Laboratories and purchased for the Army. Its purpose was the automatic encipherment of voice transmissions between high headquarters. Each terminal weighed approximately 30 tons and the cost per terminal was in the neighborhood of $450,000 installed. The SIGSALY had been withdrawn from use during the preceding year and the problem was the disposition of the 12 terminals. Originally the ASA had agreed with the Chief Signal Officer to destroy six of the terminals and to rehabilitate the

remaining six, keeping them in storage for war use. The ASA engineers were, however, of the opinion that this rehabilitation would be so costly as to make it more economical to manufacture entirely new equipment in the event of another war. Their opinion was corroborated by a Bell Telephone Laboratories engineer, and it was recommended that three of the terminals be retained for war use and that the other nine be dismantled, such parts as were originally leased to the Army by the manufacturers being returned to them and those parts which could be salvaged for use by the ASA would be retained, and the rest destroyed. These recommendations were awaiting approval at the end of the fiscal year.

The cryptonets in existence at the beginning of the Fiscal Year 1947 are shown below, together with revisions made during the year in each case:

July 1946	June 1947
15 World-wide	Revised to consist of world-wide general and high command SIGABA systems, world-wide and stand-by strip systems.
17 Air and Airways Communications	Revised to consist of world-wide SIGABA, M-209, and general and stand-by strip systems.
22 European Area	Revised to consist of general and high command SIGROD systems, and a general and stand-by system.
33 G-2 Special Security	Revised to consist of one SIGABA system for the Pacific and one SIGABA system for the European area.
34 Army Security Agency SIGCUM Intercept	Discontinued and needs incorporated into Joint Army-Navy Cryptonet 40.

020

35	Army Security Agency Administrative and Operational	Distribution of systems discontinued and partially replaced by two SIGROD systems in Cryptonet 46.
40	Joint Army Navy	Revised to include additional systems. Consists of worldwide general, high command, very high command and intercept SIGABA systems, intercept SIGCUM system, and Worldwide strip system.
42	Military Attache	Consists of SIGTOT, one-time pad and strip systems. To be replaced on 1 August 1947 by three new area cryptonets, 47, 48, and 49.
44	White House	Consists of one SIGABA and one SIGTOT system.
45	Pacific-Asiatic Theater	Consists of high command and general SIGABA systems, M-209, strip, high command radio - teletype SIGCUM, and landline SIGCUM systems.
89	Domestic ASA, Navy Intelligence SIGNUAD	Revised to include additional holders and systems.
97	Training Cryptonet	Continued. Double transposition system discontinued and SIGROD system added.

NON-CRYPTONET SYSTEMS

265	Domestic SIGCUM	Continued. (Scheduled for replacement by SIGTOT).
274	First Army Area SIGCUM	Continued. (Scheduled for replacement by SIGTOT).
461	Military Attache and Allied Control Commission Strip	Discontinued 1 February 1947
462	Transportation Corps Strip	Continued.

463	U. S. Troops in India Strip	Continued.
464	U. S. Troops in India Stand-by Strip	Continued.
600	Central Intelligence Group CCM	Continued.
999	World-wide Strip for Restricted Traffic	Discontinued 1 January 1947.

SIGBRAT system 615 for use by MA's and ACC in Europe discontinued and replaced by CSF 1700 system 745 on 15 January 1947.

System 626 State-War-Navy Emergency strip issued 30 January 1947, effective upon receipt.

In July 1946 two cipher machine systems, the CCBF 0202 world-wide command, and the 620 limited combined intelligence data, were current for combined British and U.S. operations. By the end of the year three others had been added: The CCBF 0201 was reinstated for use in the Mediterranean and European areas and authorized for use by the Fifth Air Force in the Pacific; the CSF 2529 series Limited Combined Intelligence; and the CSF 5502 Limited Combined Intelligence Backup.

To keep all these systems in efficient operation involved a great amount of production of cryptographic material. Total production figures during the year were as follows:

documents printed	143,008
pages printed	10,397,037
tapes prepared	56,328
rotors wired	3,220

M-209 keys prepared	12,937
packages wrapped	18,435
pouches dispatched	5,663
registered accounts (monthly av.)	346

Though these figures represent an average increase of 69 per cent per month over production during the basic month of July 1946, the first of the year, personnel strength in these operations steadily shrank from 140 to 115 persons.

To make certain that the systems in use or planned for future use were really as secure as required, security studies were made on a large number of systems including the SIGROD and even the SIGABA. In the case of the latter, rotors were in some instances found to be capable of reconstruction under certain optimum conditions, usually present only when the system had been operated improperly, and even in these cases the compromise possible would effect only part of a day's traffic and not at all any traffic sent in other daily keys.

Transmissions of all Army traffic were, of course, monitored for such violations, a total of 230,031 violations being detected during the year, with action taken to call the violations to the attention of those responsible in order to prevent recurrence.

Active attention, as usual, continued in regard to reports of suspected compromise of cryptographic material and close check was kept on cryptographic security violations; 4,880 routine mail reports of violations of cryptographic security

were received during the year (Tab 4). Throughout the year requests were made of various headquarters for copies of encrypted traffic handled during a specified period. Such traffic was analyzed for security and procedural violations and a summary of those not previously noted was forwarded to the station concerned, though the violations were usually minor in nature. Traffic studied by this method consisted of 4,056 messages totalling 649,576 groups (Tab 5).

III. The Production of Intelligence

Despite the fact that Fiscal Year 1947 began about two months after the final cessation of hostilities in World War II and this was consequently, as has been said, the first full year of operations characterized as strictly "peacetime," fulfillment of the Agency's second mission--the production of intelligence from intercepted signal communications and allied sources--saw no abatement. Indeed, wartime activity in this respect differed neither in volume nor urgency but merely in the direction of the attack. Heretofore, the main emphasis had been upon the communications of the Axis powers. With these nations defeated, the changed political situation caused the main emphasis to shift to communications of the Soviet Union and its ever-increasing orbit of satellite nations. No change of importance occurred in the secondary emphasis, the attempt to produce intelligence from communications of neutral or friendly nations.

Had treaties of peace been concluded with reasonable promptness, this situation might have been different, but the fact is that the international tension was so great in the period under review that the term "cold war" has been aptly applied to it. International conference after conference took place without important settlements. Sessions of this kind, always accompanied by high volume of diplomatic communications passing between the various delegations and their principals, create correspondingly high tension in intercept and cryptanalytical activity. Speedy decryption and translation of such intercepted communications becomes imperative to keep American representatives fully informed during, as well as after, the negotiations. Among the more important international conferences of this year were the following:

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

Likewise the shooting down of U. S. transport planes in Yugoslavia in August 1946 and the Hungarian coup d'etat in May 1947, as well as the continuing guerilla warfare in Greece throughout the year, were special matters involving unusual attention.

To provide raw material necessary for cryptanalytic attack during such periods, existing intercept facilities had to be

expanded and special arrangements made. As nations gradually re-established diplomatic posts in various capitals, they provided in many instances for communication through national rather than commercial channels, a factor which had to be reckoned with.

Another perplexing problem developed from the languages met with in the traffic. Not only was there now a marked increase in the demand for Russian language experts, as will be readily understood, but also for several other languages which had either not been used in traffic hitherto studied or only in negligible volume. Since it was next to impossible to recruit sufficient experts of unquestioned loyalty to provide for this linguistic work, an intensive program of training had to be inaugurated within the Agency.

During the year procedures within the ASA and channels of liaison with other communications-intelligence agencies were gradually systematized and standardized by implementation of joint processing agreements with the British (LSIC), the Navy (CSAW), and the Canadians (CBO). The Joint Processing Allocations Group, the Joint Intercept Control Group, and the USCIBC subcommittees provided the machinery for determining high policy and initiating necessary actions.

A. Interception

In regard to this important first phase of production of intelligence the program of cooperation with LSIC was continued

in accordance with the general plan agreed upon in March 1946. One copy of all cryptographic traffic and some plain text was regularly exchanged with NCA, ISIC, and CBC. A major problem, ever present, was the duplication of prints received from the Shamrock operation in order to obtain the desired number of copies. This constituted a severe burden on teletype operators and several solutions were explored without success. A portion of the work load was lifted early in the year when the RCA commercial circuits converted to radio teletype and the resultant reperforated tape could be received here. Eventually, it was understood, all commercial companies would change to RTT operation and when this had come about, the problem would be solved. Some of the Shamrock material, however, was received in a form requiring photographic processing and shortages of photographic paper early in the year caused difficulties which were afterwards eliminated when the shortage of paper was alleviated.

Replacement of experienced teletype operators with inexperienced personnel in ASA intercept stations resulted in frequent breakdowns in efficient handling of traffic both at the source and at Arlington Hall Station. Definite improvement was noted, however, in the latter part of the year when the trend was to improve teletype preparation, transmission, and processing.

Postwar planning of permanent types of intercept stations was carried on. As the stations began to change from the

older type of manual monitoring to automatic-printer systems, there was also a change within stations to train personnel for the new methods and to arrange and procure and install suitable equipment for the new type of transmission. Planning for the future necessitated selection of new sites for intercept stations, and extensive radio propagation studies were made to determine the best sites. Postwar plans for stations 1, 2, 6, and 7, were completed, while those for stations 5 and 9 were currently being processed at the end of the year. In August 1946 alternate sites for the location of station 4 (Asmara) were under study because it was foreseen that the present site might have to be abandoned. Crete was recommended as the best possible site available.

Supply was a major problem for intercept facilities in Fiscal Year 1947. The Signal Corps budget had been drastically cut and as a result Signal Corps supply depots began to require specific authorization for issue of equipment to stations. This necessitated publication of specific tables of allowance including maintenance items and these tables were published in Sig 4-2. Justification of estimated budget requirements had to be more detailed, requiring long-range planning. Since the cessation of hostilities, the Signal Corps has been handicapped by insufficient personnel in supply depots to provide efficient service. Maintenance parts have been hard to obtain. On one occasion ASA personnel discovered that the Signal Corps was

actually declaring surplus items greatly needed by the ASA. But until the field units of ASA were furnished with T/A 32-1 in September 1946, they had no real authorization to draw supplies. Since then, the Signal Corps has been trying hard to provide equipment and maintenance parts for the intercept stations, despite the handicap of lack of personnel. Because supplies could not be drawn within the theater, an effort was made to supply everything needed from Arlington Hall Station. Consequently, a heavy load was thrown on Headquarters ASA which had to pack and ship an extra load of equipment. The supply problem, however, is expected to be less thorny in Fiscal Year 1948 because of the publication of a new procurement directive by the Signal Corps.

Lack of trained intercept personnel at the station was another major problem in Fiscal Year 1947 because of the too rapid discharge policy of the Army which brought about release of men before suitable replacements were available. No station has been at authorized strength during the year. Even so, improvements of the intercept facilities permitted an increase in volume of intercepts and greater penetration into the internal communications of several countries, particularly the Balkans. Results of research and development within the ASA were so successful that in many instances our new devices have been incorporated into Navy equipments. Engineers from CSAW, LSIC, and CBO have given their opinion that our intercept

equipment is superior to that available commercially.

B. Cryptanalysis

The cryptanalytic attack, including traffic analysis, carried on by the ASA during the year, was, of course, limited in scope by the exclusion of all strictly Naval traffic, which was the responsibility of the Navy. In addition, certain other types of traffic were transferred to the Navy during the year as the result of joint agreements. Before 1942 the Navy cryptanalytic organization had regularly carried all work on diplomatic systems. In that year, under the pressure of wartime urgency, the Navy had agreed to turn over to the Army all responsibility for diplomatic traffic and during the war did no such work. With the coming of peace, however, the Navy desired to resume work on diplomatic traffic of some countries and during the negotiations on this matter it was agreed by the Army with some reluctance to turn over to the Navy responsibility for traffic of certain governments. These were:

a. Siamese traffic, transferred in July 1946.

b. Portuguese traffic, except strictly military, in September 1946.

c. Spanish traffic, except strictly military, same month.

d. Belgian traffic, transferred a month later.

e. Chinese [redacted] traffic, transferred June 1947.

f. [redacted] traffic, transferred in June 1947.

g. Scandinavian traffic, transferred in July 1946.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

Transfer of these responsibilities usually involved transfer of some personnel as well. The chief point of attack was all phases of the Russian problem, the Chinese Communist study having ended when the Nanking-Yenan circuit was closed in March 1947.

The Russian Systems: The ASA shared with the Navy joint responsibility for cryptanalysis of the Russian communications, the Navy handling all naval, police, shipping, and weather communications, the remainder [redacted] being the responsibility of the ASA. Some indication of the importance of this effort will be seen in the fact that the number of people who worked on these problems increased from 283 at the beginning of the Fiscal Year 1947 to 443 at the end.[5]

Russian interception[6] was limited, at first, by informal agreement with the British and by the geographic location of ASA stations. Intercept during the greater portion of 1946, therefore, was directed to the Far Eastern Military District, the Tenth Air Army, the Maritime Military District, and some other traffic. An attempt was made as volume of intercept

---

5. The Pentagon Plain-Text Unit was inaugurated on 17 Apr 47 and began operations on 5 May 47. The unit (8 people) was organized for the purpose of exploiting Russian domestic traffic and translating significant items for the Bulletin.

6. The Research and Development program placed a very high priority on the TAPER problem of intercept.

improved to break out of the coastal areas into the East and West Siberian Military Districts, but with little success. Toward the end of the year, however, intercepts were being made increasingly of military traffic on the more important links in Europe.

By traffic analysis, the Far Eastern Military District Net was completely reconstructed. The Ninth and Third (?) Air Army nets were discovered and reconstructed during the year. The difficult European nets were studied for continuity, the majority of the work being done at ISIC. Baudot links were identified as to location and unit and were very successfully studied owing to the presence of abundant plain-text chatter which the Russians should in the interest of their security have prevented. As for intelligence produced by traffic analysis, the staff here was generally able to determine Order of Battle down to the level of division or brigade and to report any changes in unit location, subordination, etc. Traffic processed in June 1947 was as follows:

Type	Morse	non-Morse
	7,200	2,025
	4,500	25
	6,900	75
	3,300	8,875
	21,400	3,500
		5,500
Total Messages	43,300	20,000

Considerable cryptanalytic work was done on [redacted] systems and there was [redacted]

[redacted]

The Russians appear to have been tightening security techniques during the year. New techniques in [redacted] however, have been developed by the ASA. The intelligence value of [redacted] since it was in almost universal use by the Soviet army, navy, air, and police communications. The Russians apparently [redacted] a fact which shows either that they probably do not study their own traffic or, if they do, that they are not perhaps as proficient in cryptanalytic theory and technique as they might be.

About 80 per cent of all [redacted] Its intelligence value is high, giving details of strength and disposition of troops, supply and administration problems, construction and fortification in the Far East, [redacted] for this and other systems, political indoctrinations, and troop morale. There was no major cryptographic change during the year.

[redacted]

[redacted] of both military and air, but too little had been translated to assess the value of the intelligence. Increasing use [redacted] can be expected.

Work was also done on low-echelon systems, [redacted]

One system [redacted] was being operationally translated.

Other Nations: As for countries other than the Soviet Union, the ASA carried on traffic analysis, cryptanalysis, and translation of all traffic other than naval from the following [redacted]

Soviet Satellites: Traffic analysis was directed against Albanian, Yugoslavian, and Czech military and [redacted] and the Polish [redacted] Workers' Part nets with success in November 1946. In February 1947 complete files were being maintained and station identification made for the cryptanalytic units. Hungary sent all its [redacted] links, its military on an internal network. Several [redacted] military systems were under study. The chief intelligence contribution came from translations of [redacted] which gave

brief insight into the internal political situation in the spring of 1947.

Ninety per cent of all Albanian intercepts came from LSIC--in general the problem was solution of a large number of simple substitution ciphers, since the systems were very insecure.

The Bulgarian government sent all [redacted] on commercial lines and 3,427 messages were received, of which 2,036 were in known systems, 1,362 in plaintext, and 27 in unknown systems. Police traffic passed on an internal star-lateral net with control at Sofia--of the 5,117 messages received, 2,419 were in known systems, 2,657 in plaintext, and 41 in unknown systems. Air traffic passed on an internal net--total received 1,247, but these were of low intelligence value. At the beginning of the year all [redacted] plaintext messages were translated, 78 summarized. Two police systems were exploited, 239 cipher and 15 plaintext messages being translated. In the air systems 28 messages were translated but interception was discontinued in May 1947, due to low intelligence content. Bulgarian systems are generally [redacted]

Czech communications did not afford much possibility of

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

Polish traffic came mostly from LSIC and while considerable research was done on it at ASA, [redacted]

Considerable study of Yugoslavian traffic was carried on [redacted] Some plaintext was exploited.

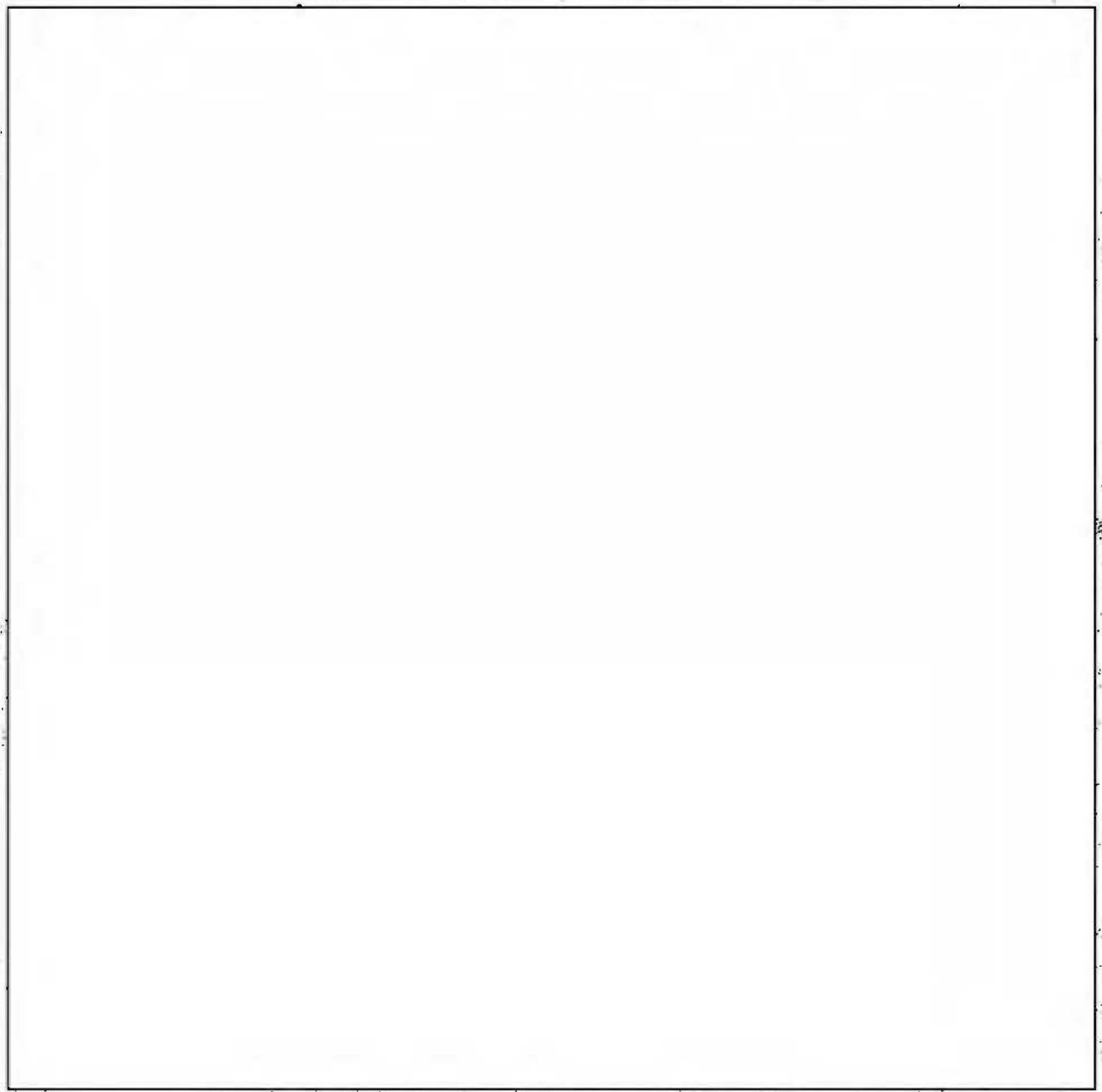
The Romanian [redacted] Traffic analysis was possible on the internal net through study of intercepts received from LSIC. Work on the internal traffic began in March 1947 [redacted]

The constantly crucial situation in Central Europe and the Balkans kept the priority assignments for interception of satellite traffic ever increasing, but the cryptographic systems used by these countries were extremely secure [redacted] In the case of other countries, the low-grade and medium-grade systems were brought to a greater degree of readability, and encouraging progress was made on the high-grade, [redacted]

European Neutrals: Except for the [redacted] most of the Greek intercepts [redacted] The Greeks use codes and code reconstruction has been progressing with some success. First translations of messages in a new code were published five months after introduction of the system. Some use was made of IBM machines for decoding. Much of the information obtained had high intelligence value, [redacted] having included 82 such messages.

The Italians have been sending fewer messages than formerly [redacted] doubtless largely for economy reasons; yet, [redacted] were opened during the year. [redacted] which was introduced despite continuance of old compromised codes, was the chief problem. [redacted] was introduced and discontinued. The double-transposition cipher had been introduced by the Italians on the

basis of instructions given them in 1944 by an ASA officer assigned to this duty. While it was realized that an improvement in the quality of Italian systems might cause the ASA difficulty in reading the resultant traffic, it was feared that unless this were done, other nations would be able to read the Italian systems in use to the harm of the United States.



[redacted]

The ASA had no commitment for work on Spanish systems bther than military [redacted] after October 1946. All military intercept [redacted] which discontinued coverage late in the current period. [redacted] traffic was exceedingly scant. In addition, there was a small amount of traffic the nature of which was not understood.

Portuguese [redacted] problems were turned over to CSAW.

The Swiss used commercial channels for traffic but in reduced volume since other means of communication had become possible. [redacted]

intelligence from the six Arabic countries is considerable. Iraq supplied the most intelligence out of Cairo concerning the Arab League. [redacted] Lebanon was best on Moscow's attitude towards the Arab world. [redacted]

[redacted]

[redacted] has long been a better source of data on Syrian internal events than the Syrian government itself. [redacted] Syria, and Lebanon, were all good sources [redacted] A total of 423 messages were published in [redacted]

The governments of Iran and Afghanistan used similarly weak systems which were easily solved. As to intelligence value, 160 Iranian messages [redacted]

Egyptian and Ethiopian systems were also not very secure; Egypt introduced, surprisingly enough, [redacted] and this was insecurely operated and solved.

In summary, a large percentage of the intercepted traffic was decrypted, producing a high intelligence value. The following statistics are illuminating:

Country	Intercepts	Decrypts	Trans/Summ	Dipl/Summ
[redacted]	5126	5050	2383	276
	5698	5048	1731	123
	8078	4040	1248	162
	1668	1191	465	55
Totals	20570	15329	5827	616

The Latin-American Group: Work on Brazilian intercepts included cryptanalysis [redacted]

traffic. Work on code reconstruction was pushed ahead.

Since the ASA had the benefit of a compromised copy of a [redacted] Argentinian code, the chief problem in this traffic was solution of encipherment in some circuits, plus research on other Argentinian systems which was partially successful. Nine systems were in use as the year ended. Traffic analysis was confined to material intercepted by station 78B which consisted of air traffic. During the year Argentina appeared more conscious of a need for security and more sophisticated cryptographically. Intercepts numbered [redacted] of which [redacted] were decoded, [redacted] translated, and [redacted] summarized. Of the [redacted] plaintext messages received, [redacted] were translated and [redacted] summarized.

The Bolivians used only three systems [redacted] intercepts of which [redacted] messages were decrypted, [redacted] translated, and [redacted] summarized.

Chilean systems underwent no serious change during the year. Of [redacted] intercepts, [redacted] were decrypted, [redacted] translated, and [redacted] summarized. The intercepts not decrypted were [redacted] of very low intelligence value.

Some encipherments of Colombian code messages were solved but only [redacted] intercepts were received. However, [redacted] messages were decrypted during the year, [redacted] translated, and [redacted] summarized.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

The year's cryptanalytic work on Ecuadorian traffic involved code recovery and solution of two enciphering keys. The code is [redacted] key recovery is constantly in progress. Of [redacted] intercepts received, [redacted] translated, and [redacted] summarized.

The Peruvians used a few systems [redacted]

Paraguay used a single system but though it has been studied from time to time, no success has been achieved. However, only [redacted] encoded messages were intercepted during the year. Of the [redacted] plaintext messages received, only [redacted] were deemed worthy of Bulletin publication and [redacted] were summarized.

The Uruguayans use three code systems with very light encipherments. Of [redacted] intercepts, [redacted] were decrypted, [redacted] translated, and [redacted] summarized. Of [redacted] plaintext messages examined, five were translated and eight summarized.

Venezuela has [redacted]

Only [redacted] messages were intercepted during the year

Traffic of Guatemala, Honduras, Mexico, Nicaragua, Costa Rica, Salvador, and the Dominican Republic, was received and processed. In regard to Mexico, our commitment covers only [redacted]

The Dominican Republic sent only traffic. The bulk of the traffic of these countries was very slight and offered no major problems. The Honduran system cannot be read for lack of traffic

PL 86-36/50 USC 3605
EO 3.3(h)(2)

China: Interception of Chinese traffic is difficult and often poor, while the systems are relatively secure. The policy was to maintain a vigorous cryptanalytic attack

Every effort was exerted to provide solution of the Communist traffic, but this, like the military, failed to yield. The language experts made a creditable record in reconstruction and translation. The work was more concerned with

The intelligence value of this traffic was high, containing

discussions of the Chinese Nationalist army organizations; actual battle reports; unit strength reports; order of battle; antagonism of Chinese Communists towards the United States forces in China; Kuomingtang-Communist negotiations; Chinese reparations claims against Japan; spy activities of Chinese Communists; the Franco-Viet Nam conflict, etc.

Commercial Traffic: The ASA also received 20,813 coded commercial messages as well as 126,819 plaintext intercepts. Commercial traffic passed in greater volume than hitherto as wartime restrictions were relaxed. A large amount of traffic from [redacted] Lack of personnel, however, prevented any attempt at solution. An arrangement was made whereby messages encoded in [redacted] could be decoded by IBM procedures, thus saving time of personnel. The intelligence derived from these commercial messages included financial, scientific, and technical matters, personalities, shipping, and communications data.

C. Supporting Techniques

The work of the traffic analysis and cryptanalysts who attacked these messages was supported by a large staff of other people who provided assistance by supplying services of four types: (1) photographic; (2) IBM machinery; (3) Electronic and

electromechanical research and development; and (4) information.

The Photographic laboratory was at first hampered by serious shortages of photographic paper but finally this situation improved and it was possible to bring the photographing of the TICOM materials to a current basis. A very elaborate project, consisting of a microfilming of the entire files of the Security and Operations Divisions, was completed, and a beginning was made on the files of the Research and Development Division. Films of these files were deposited for safe-keeping in the storage depot at New Cumberland. The photographic laboratory also did a considerable volume of work on the project known as the Shamrock Operation which has already been mentioned. One of its most interesting special projects was a test of the physical security of the one-time pad in current use. Two tests were made: in the first the pad was opened, its contents photographed, and the pad restored to its original state, in six hours. In the second test, this was done in four hours. In neither instance was it possible to distinguish between the compromised and uncompromised copies. In addition twelve pieces of mail were examined for secret writing and two officers were trained in the laboratory, one in photography, the other in secret inks.

The Agency also maintained a large branch devoted to the application of IBM techniques in support of cryptanalytic and

traffic analysis attack. Approximately 152 machines of all designs were in use during the year, the high peak being 154 machines in May and June 1947, the low in October 1946 when there were 151. Since the Agency did not own the machines but rented them from the IBM corporation, it was forced to pay a total rental for the year of $266,856.26. A good idea of the volume of this work may be gained from the fact that total consumption of all the types of standard IBM cards was 57,272,000. Other supplies, including standard IBM papers not readily reducible to a common denominator, were of course in addition to this figure.

Considerable time and effort was spent during the year by the Agency's Research and Development Laboratories on the design and construction of high-speed cryptanalytic equipment continuing one of the most significant trends in cryptanalysis brought about by wartime experience.

Finally, there was another large group of people assigned to the information service. Their task was to gather, record, and make readily available a huge amount of information on every conceivable subject which might be needed by the operating sections. A good idea of the vast extent of this work may be gained from the fact that never fewer than 152 persons were engaged on this work, and for fully a third of the year there

were more than two hundred.[9]

D. Production Figures

In terms of production of intelligence the following figures, furnished by the General Cryptanalytic Branch, will be illuminating:

	Total	Monthly Avge.
Intercepts	1,534,866	127,905
Original Messages	1,294,089	107,841
Plain Text	473,918	39,493
Encrypted	820,171	68,347
Encrypted Messages:		
In exploitable systems	336,296	28,025
In research	421,411	35,118
Not worked on	62,464	5,205
Messages decrypted	174,271	14,523
Messages Published:		
Plain text	9,725	810
Encrypted	51,540	4,295

It will be seen that 41 per cent of the total number of encrypted messages were in exploitable systems, 21 per cent were decrypted, and 51 per cent were in various stages of research, while less than 8 per cent were not worked on.

Statistics furnished by the Information and Documents Branch of messages published in its Daily Bulletin are as follows:

---

9. Included in this total personnel figure of course are those of the Information, Bulletin, Library, Documents, Special Projects, and Liaison Activities Sections. There was a sharp gain in personnel in January 1947 with the addition of the Special Projects Section. Beginning in February newly employed personnel were assigned from the Training School.

Messages counted by serial number	48,022
Number of parts published	76,635
Average monthly output	10,388
Average daily output	341

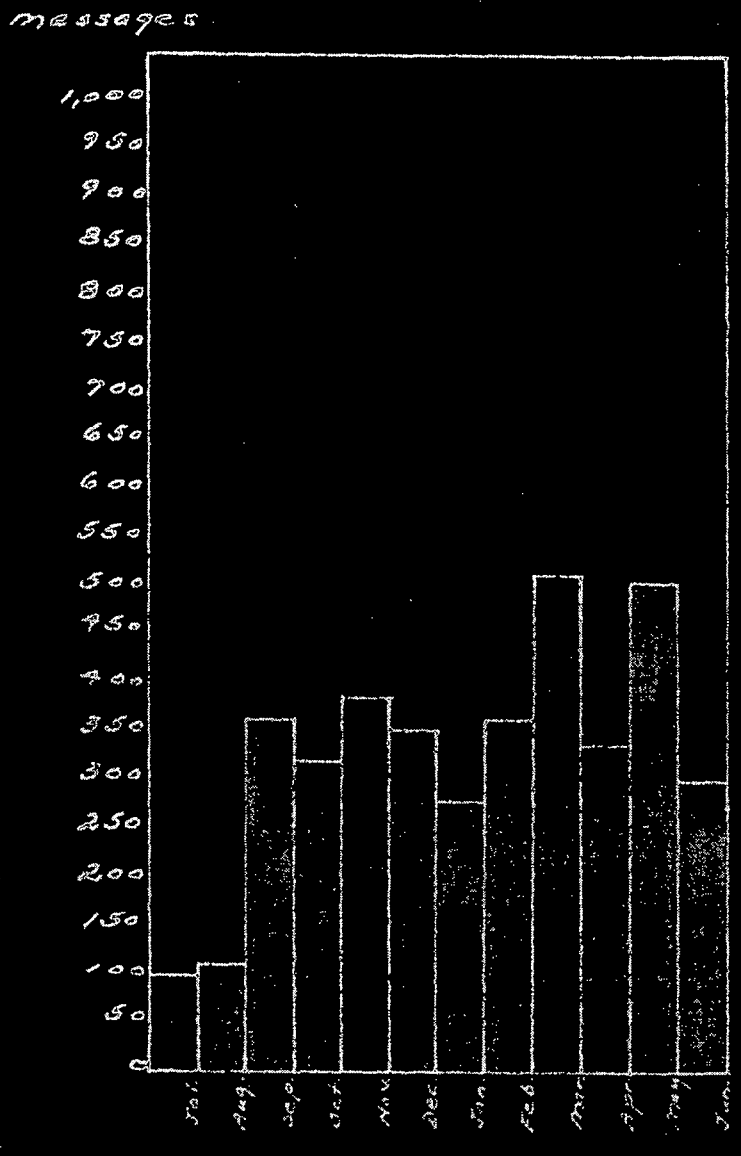
There is a discrepancy between these two sets of production figures which may be explained by remembering that they are not intended to record precisely the same fact. The first set records the number of messages counted as they left the cryptanalytic sections for the Bulletin, while the second records the number counted as they left the Bulletin in published form. Furthermore, the large number of different cryptanalytic sections were apt to count messages by different systems. A given message received in several parts might be counted as a unit by one group, as several messages by another. The number of parts of messages published offers perhaps the most reliable gauge of production since it reflects the amount of work needed to prepare for use a given series of messages.

NOMENCLATURE AND CHARACTERISTICS OF CRYPTOLOGIC EQUIPMENT

NAME	TYPE NUMBER	SHORT TITLE	STATUS	TO MEET BMR	M/C'S FROM	TYPE OF ENCRYPTMENT	OPERATION	METHOD	OUTPUT	TRAFFIC CAPACITY	APPROX SIZE (CU FT)	APPROX WEIGHT (LBS)	POWER SUPPLY	ASSOCIATED EQUIPMENT	REMARKS
RYP DEVICE	CSP 845		IN USE INTERIM			LITERAL	MANUAL	OFF-LINE	INDICATES ONLY		108	5	NONE	NONE	
BLE TRANSPOSITION			IN USE ADEQUATE			LITERAL	MANUAL	OFF-LINE	INDICATES ONLY				NONE	NONE	
ERAL ONE TIME PADS			IN USE ADEQUATE	XXX		LITERAL	MANUAL	OFF-LINE	INDICATES ONLY		335		NONE	NONE	
TIME PAD MACHINE			IN USE ADEQUATE			LITERAL	TAPE	OFF-LINE	TO MEET REQ		25.37	240	60 CYCLE 115 V AC	NONE	CAPABLE OF USING ONE TIME PADS
DES	M-209-A		UNDER DEV INTERIM	XXX	AAF	LITERAL	MANUAL	OFF-LINE	INDICATES ONLY		18	5	NONE	NONE	IN FLIGHT WEATHER ONLY
DGC	M-209-B		STANDBY		WE	LITERAL	MANUAL	OFF-LINE	INDICATES ONLY		FITS IN GI SHIRT POCKET		NONE	NONE	MORE COMPACT, EASIER TO OPERATE THAN DIFF SH SLIDEY
VERTER	M-228		IN USE, INTERIM	X		LITERAL	MANUAL	OFF-LINE	PRINTED TAPE		24	1 1/2	NONE	NONE	USING ASSOCIATED EQUIPMENT ISSUED ON TYR
VERTER	M-228	SIGCUM	IN USE INTERIM	XXX	WE	TELETYPE SIGNAL	KEYBOARD OR TAPE	ON LINE OR OFF LINE	TELETYPE SIGNALS		5.7	18	60 CYCLE 110 V AC OR 40 CYCLE 220 V AC	3 SUBSET, TELETYPEWRITER AND ASSOCIATED EQUIPMENT	
VERTER	M-228-A	SIGCUM	IN USE INTERIM	XXX		TELETYPE SIGNAL	KEYBOARD OR TAPE	ON LINE OR OFF LINE	TELETYPE SIGNALS		5.7	18	60 CYCLE 115 V AC OR 40 CYCLE 220 V AC	3082 SUBSET, TELETYPEWRITER AND ASSOCIATED EQUIPMENT	
VERTER	M-284	SIGAIN	IN USE INTERIM	XXX		TELETYPE SIGNAL	KEYBOARD OR TAPE	ON LINE OR OFF LINE	TELETYPE SIGNALS		2.7	250	60 CYCLE 115 V AC OR 40 CYCLE 220 V AC	ONE UNIT OF TRIAD 2 RECEIVERS AND 1 PRINTER SET TO 84	
E-TIME TAPE TELETYPE		SIGTOT	IN USE, ADEQUATE	XXX		TELETYPE SIGNAL	TAPE	ON LINE OR OFF LINE	TELETYPE SIGNALS		11	90 OF TEN 2.5	110 AC/DC	131 SUBSET TELETYPEWRITER AND ASSOCIATED EQUIPMENT	
VERTER	M-134-C	SIGARA	IN USE, INTERIM			LITERAL	KEYBOARD	OFF-LINE	PRINTED TAPE		3.5	37	105-125 AC/DC 24 V DC	NONE	
VERTER ATTACHMENT	AN/GSA-8	SIGJOOG	UNDER DEV INTERIM		WE	LITERAL	TAPE	OFF-LINE	TELETYPE SIGNALS		5.0		110 AC	SIGARA, SIGROG, SIGRAT	AN AUXILIARY ASSEMBLY FOR OPERATING M-134-C FROM TTY TAPE THE PREPARATION OF TTY TAPE FROM THE M-134-C
VERTER ATTACHMENT		SIGJOOG	UNDER DEV INTERIM			LITERAL	TAPE	OFF-LINE	PRINTED TAPE		35	75	110 AC/DC	SIGARA, SIGROG, SIGRAT	AN AUXILIARY ASSEMBLY FOR OPERATING M-134-C FROM TTY TAPE
VERTER	CSP MARK II	SIGCUM	IN USE INTERIM		MAY	LITERAL	KEYBOARD	OFF-LINE	PRINTED TAPE		3.5	35	110 AC/DC 24 V DC	NONE	
VERTER	M-228-(V)	SIGRAT	IN USE INTERIM		WE	LITERAL	KEYBOARD		PRINTED TAPE		3.5	37	110 AC/DC 24 V DC	NONE	
VERTER	M-228-(V)	SIGRED	IN USE INTERIM		WE	LITERAL	KEYBOARD	OFF-LINE	PRINTED TAPE		3.5	35	110 AC/DC 24 V DC	NONE	
VERTER	M-228-(V)		UNDER DEV ULTIMATE	XX					PRINTED PAGE OR TAPE			15		TELETYPEWRITER	
VERTER	M-209-(V)		UNDER DEV ULTIMATE	XX	AAF				PRINTED PAGE			21		TELETYPEWRITER	
VERTER	M-228-(V)		UNDER DEV	XX OF INTERIM XX ULTIMATE	AAF	TELETYPE SIGNAL	TELETYPE KEYBOARD	ON LINE	TELETYPE SIGNALS					TELETYPEWRITER	
VERTER	M-228-(V)		UNDER DEV ULTIMATE	XXXX	AAF	LITERAL	MANUAL	OFF-LINE	INDICATES ONLY	5 SECONDS PER CHARACTER	APPROX SIZE OF WRIST WATCH		NONE	NONE	
VERTER	M-209-(V)		UNDER DEV ULTIMATE	XXXX	AAF	TELETYPE SIGNAL	KEYBOARD	ON LINE	PRINTED TAPE OR PAGE					TELETYPEWRITER	WEATHER
ECH EQUIPMENT	AN/GSQ-220 (V)	SIGSALY	IN USE INTERIM	XXX	NONE	VOICE SIGNAL	VOICE	ON LINE	ELECTRICAL SIGNALS	AUTOMATIC	47 BAYS	ONE TERMINAL SECTIONS	115/230 V AC 50/60 CYCLE	TRANSMITTING AND RECEIVING EQUIPMENT	ROOM IN WHICH EQUIPMENT IS USED MUST BE AIR CONDITIONED
ECH EQUIPMENT	AN/GSQ-(V)	SIGGP	IN USE INTERIM	X	AAF	VOICE SIGNAL	VOICE	ON LINE	ELECTRICAL SIGNALS	AUTOMATIC	3.9	80	24 V DC	TRANSMITTING AND RECEIVING EQUIPMENT	
ECH EQUIPMENT	AN/GSQ-(V)	SIGTOG	UNDER DEV	XXX	AAF	VOICE SIGNAL	VOICE	ON LINE	ELECTRICAL SIGNALS	AUTOMATIC			115/230 V AC 50/60 CYCLE	TRANSMITTING AND RECEIVING EQUIPMENT	WHEN MOUNTED IN VAN BECOMES S-GRAT
ECH EQUIPMENT	AN/GSQ-(V)	SIGRIT	UNDER DEV	XXX ULTIMATE X INTERIM	AAF	VOICE SIGNAL	VOICE	ON LINE	ELECTRICAL SIGNALS	AUTOMATIC	14.36	9000	115/230 V AC 60 CYCLE	TRANSMITTING AND RECEIVING EQUIPMENT	
ECH EQUIPMENT	AN/GSQ-(V)		UNDER DEV ULTIMATE	X	AAF	VOICE SIGNAL	VOICE	ON LINE	ELECTRICAL SIGNALS	AUTOMATIC	14.36	9000		TRANSMITTING AND RECEIVING EQUIPMENT	
ECH EQUIPMENT	AN/GSQ-(V)		UNDER DEV ULTIMATE	XX	AAF	VOICE SIGNAL	VOICE	ON LINE	ELECTRICAL SIGNALS	AUTOMATIC				TRANSMITTING AND RECEIVING EQUIPMENT	
ECH EQUIPMENT	AN/TRA-15, 18		UNDER DEV INTERIM	XX	SIGNAL CORPS ITEM	VOICE SIGNAL	VOICE	ON-LINE	ELECTRICAL SIGNALS	MULTI-CHANNEL SPEECH	36	350	115 V AC 50/60 CYCLE	AN/TRC-5,6	PULSE CODE MODULATION
CSIMILE EQUIPMENT	AN/GXA-2	SIGFAX	IN USE INTERIM	XX	NONE	FACSIMILE SIGNAL	PAGE SCANNING	ON LINE	ELECTRICAL SIGNALS		149	1000		TRANSMITTING AND RECEIVING EQUIPMENT	
CSIMILE EQUIPMENT	SPRS		UNDER DEV ULTIMATE	XX	AAF	FACSIMILE SIGNAL	PAGE SCANNING	ON LINE	ELECTRICAL SIGNALS					TRANSMITTING AND RECEIVING EQUIPMENT	

CRYPTOGRAPHIC TRAFFIC VOLUME REPORTS RECEIVED AND PROCESSED

1 July 1946 – 30 June 1947



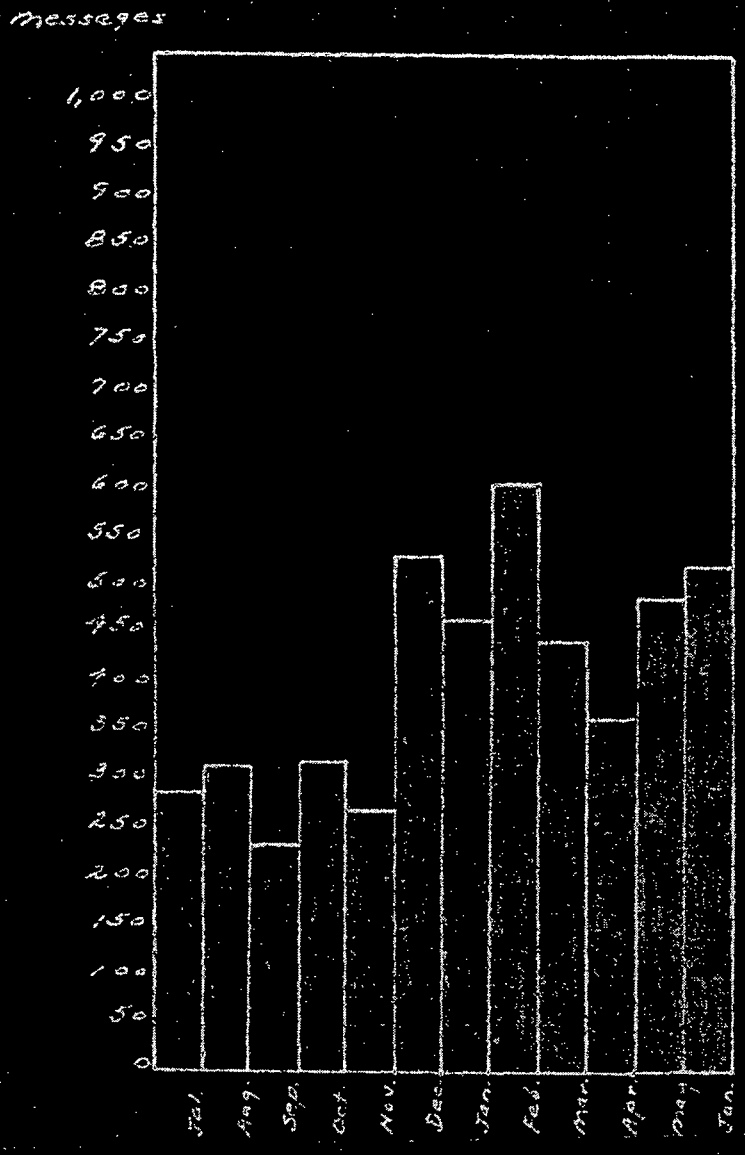
Jul.	100	Jan.	285
Aug.	114	Feb.	363
Sep.	363	Mar.	522
Oct.	339	Apr.	396
Nov.	393	May	516
Dec.	352	Jun.	301

FLOW CHART FOR DEVELOPMENT OF CRYPTOGRAPHIC DEVICES

PHASE	DUTIES OF ASA			CONTRACTORS DUTIES
	RESEARCH AND DEVELOPMENT DIV	SECURITY DIV	OTHER	
DETERMINATION OF BASIC MILITARY REQUIREMENT AND PREPARATION OF MILITARY CHARACTERISTICS I	1. REVIEWS SIMILARITY OF MILITARY REQUIREMENTS AND EFFECTS TECHNICAL COORDINATION WITH OTHER WAR AND NAVY DEPT R & D AGENCIES.	REVIEWS AND INITIATES REQUIREMENTS AND REVIEWS AND PREPARES MILITARY CHARACTERISTICS OF PROPOSED NEW DEVELOPMENT.	WDGAS 24 DETERMINES NECESSITY OF PROPOSED NEW DEVELOPMENT ASAIC REVIEWS REQUIREMENTS AND CHARACTERISTICS, ASSIGNS ASA PRIORITY FOR DEVELOPMENT, AND SUBMITS RECOMMENDATIONS TO WDGSTG	
DETERMINATION OF BASIC SYSTEM II	1. SELECT BASIC SYSTEM BEST SUITED TO REQUIREMENTS. 2. PREPARATION OF SPECIFICATIONS. 3. ESTIMATE COST OF PRODUCTION OF ENGINEERING AND SERVICE TEST MODELS. 4. SECURE PATENT APPROVAL	1. APPROVE BASIC SYSTEM TO BE DEVELOPED. 2. REQUEST R & D TO UNDERTAKE DEVELOPMENT	ASAIC: REVIEWS SPECIFICATIONS AND FORWARDS TO WL FOR APPROVAL WDGAS 24 REVIEWS SPECIFICATIONS WDGAS 24 REVIEWS PLAN TO INSURE CONFORMANCE WITH APPROVED BUDGET ESTIMATE.	
DEVELOPMENT AND PRODUCTION OF ENGINEERING MODELS III	1. NEGOTIATE DEVELOPMENT CONTRACT. 2. MAINTAIN LIAISON WITH CONTRACTOR 3. DETERMINE AND SECURE PATENT RIGHTS 4. PREPARE DEVELOPMENT PROGRAM		ASAIC EFFECTS NECESSARY COORDINATION OF DEVELOPMENT BETWEEN INTERESTED ARMS AND SERVICES	PRODUCE ENGINEERING MODEL
TEST OF ENGINEERING MODELS IV	1. MAKE OVERALL TESTS TO CONFIRM CONTRACTORS FINDINGS. 2. PREPARE REVISED SPECIFICATIONS AS DICTATED BY TESTS 3. MAINTAIN LIAISON WITH CONTRACTOR	MAKE SECURITY AND PRACTICABILITY EVALUATION OF DEVICE		MAKE COMPONENT PART'S TESTS AND INITIAL OVERALL TESTS
SECURITY STUDIES V	1. REVIEWS SECURITY TESTS AND PREPARE REVISED SPECIFICATIONS AS REQUIRED	1. ASCERTAIN AND PREPARE SECURITY TESTING ARRANGEMENTS (COST) 2. DEVELOP AND CONDUCT SECURITY TESTS 3. MAKE FINAL SECURITY EVALUATION OF DESIGN AND SYSTEMS	WDGAS 23 ASSISTS IN CONDUCTION OF SECURITY TESTS	
PRODUCTION OF PROTOTYPE VI	1. [illegible] AND FINAL SPECIFICATIONS FOR PRODUCTION OF TYPE 2. DETERMINE DESIGN FEATURES TO MEET REQUIREMENTS 3. REVIEW COST OF PRODUCTION	1. ADVISE ON [illegible] ASPECTS OF DESIGN 2. FACILITATE PRODUCTION [illegible]	[illegible] ESTIMATES	1. DESIGN AND CONSTRUCT PROTOTYPE. 2. PREPARE OPERATING DATA FOR MAINTENANCE, REPAIR AND OPERATION 3. REVISE [illegible] OF PRODUCTION MODELS
ENGINEERING TESTS OF PROTOTYPE VII	1. MAKE LABORATORY TESTS FOR STRENGTH, TYPE, STABILITY, MAINTENANCE REQUIREMENTS, PERFORMANCE, ETC 2. TESTS UNDER ACTUAL FIELD CONDITIONS	REVIEW TEST RESULTS AND COMMENT THEREON 2. MAKE RECOMMENDATIONS ON TYPE CLASSIFICATION	ASAIC: REVIEWS RECOMMENDED TYPE CLASSIFICATION AND FORWARDS RECOMMENDATION TO WDGS FOR APPROVAL	
PRODUCTION OF SERVICE TEST MODELS VIII	1. PREPARE SPECIFICATIONS 2. PROVIDE TECHNICAL DATA FOR MAINTENANCE, REPAIR, AND OPERATION	1. REVIEW SPECIFICATIONS 2. STANDARDIZE AFTER DETERMINING BASIS OF ISSUE		1. PRODUCE SERVICE TEST MODELS
SERVICE TESTS IX	1. PROVIDE TECHNICAL TRAINING FOR INTRODUCTORY TEAMS	1. PREPARE INSTRUCTION MANUAL AND REPORTS 2. ARRANGE FOR SERVICE TEST OF EQUIPMENT 3. TRAIN INTRODUCTORY TEAMS 4. DISTRIBUTE MANUALS AND EQUIPMENT TO TESTING UNITS 5. RECOMMENDS TYPE RECLASSIFICATION.	ASAIC: REVIEWS MAINTENANCE REPAIR, AND OPERATIONAL MANUALS WDGAS 19 ALLOCATES SERVICE TEST AND INTRODUCTORY TEAMS WHEN NECESSARY ASAIC: REVIEWS AND FORWARDS RECOMMENDED TYPE RECLASSIFICATION.	
PRODUCTION AND DISTRIBUTION OF ADOPTED TYPE TO USING AGENCIES X	1. PREPARE FINAL SPECIFICATIONS BASED ON RESULTS OF SERVICE TESTS 2. ADVISE SECURITY DIVISION REGARDING MAINTENANCE REQUIREMENTS	1. TAKE OVER LIAISON WITH CONTRACTOR 2. INITIATE PROCUREMENT DISTRIBUTE, TRAIN MAINTENANCE PERSONNEL, PREPARE SYSTEMS, ETC 3. PREPARE T/E OR RECOMMENDED DISTRIBUTION	WDGAS 24 REVIEWS AND APPROVES OR PREPARES T/E OR SIGE PERTINENT TO NEW DEVICE	1. MANUFACTURE EQUIPMENT 2. PREPARE MANUFACTURING DRAWINGS.

Volume of Reports of Violations of Cryptographic Security

1 July 1946 - 30 June 1947

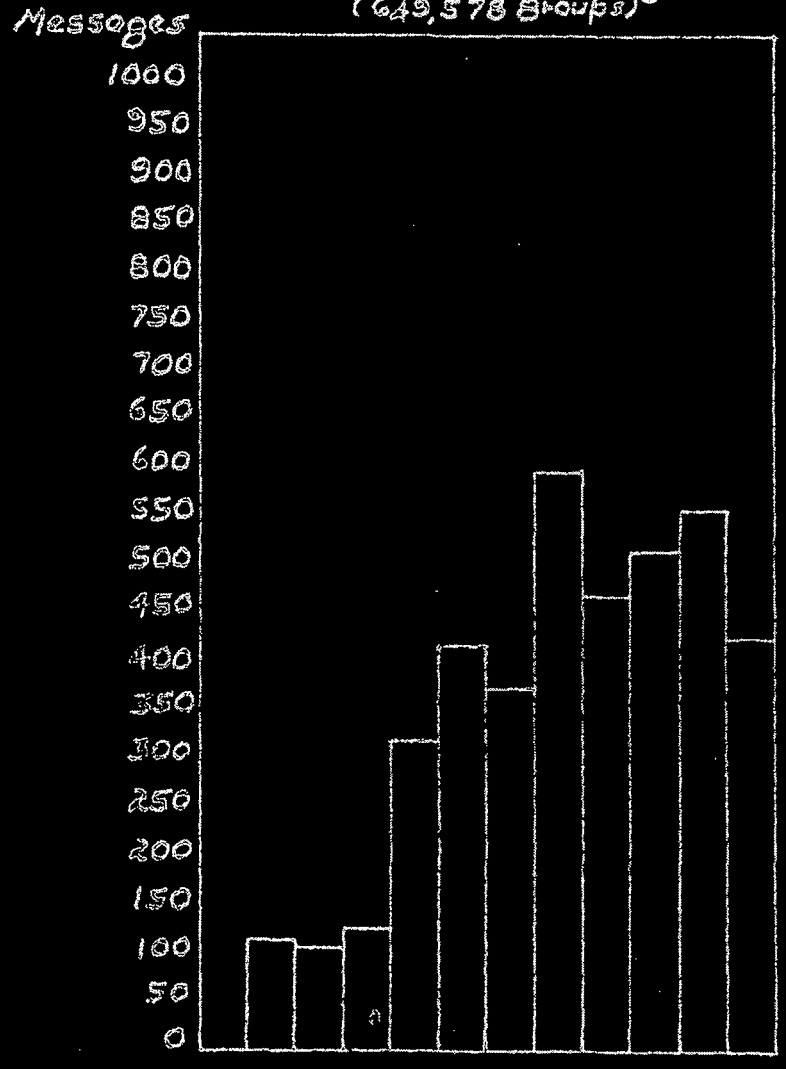


Jul.	281	Jan.	467
Aug.	315	Feb.	602
Sep.	240	Mar.	449
Oct.	317	Apr.	366
Nov.	274	May	470
Dec.	542	Jun.	537

CRYPTOGRAPHIC TRAFFIC PROCESSED

1 July 1946 - 30 June 1947

Total - 4,056 messages
(649,578 Groups)



Jul		Jan	381
Aug	115	Feb	601
Sep	107	Mar	461
Oct	133	Apr	518
Nov	328	May	557
Dec	424	Jun	431