

5-2049, Friedman's
History, with Tabs.

5-3441. Entire document
includes Friedman's
history and all
attachments.

| | Total | Wash | Ed |
|------|-------|------|-----|
| O | 45 | 44 | 1 |
| W.O. | 0 | 0 | 0 |
| E.M. | 177 | 28 | 149 |
| Civ | 109 | 109 | 0 |

15 Aug 45

| | | | |
|-----|-------|------|------|
| O | 1777 | 661 | 116 |
| WU | 15 | 4 | 11 |
| EM | 3,877 | 1521 | 2356 |
| Civ | 5,661 | 5661 | 0 |

213

33
 +8

 41
 129

 170
 19
 26

 45
 42

 87
 48

 135

42
 48

 90
 37

 127
 Carter Machine
 4/15/41

SECRETCONFIDENTIALRESTRICTEDTODATE7 MayFROM

Commanding Officer (IS-1) ✓

Assistant Commandant (IS-1)

✓ Dir of Comm Research (IS-3)

Control O (IS-1A)

Fiscal O (IS-1B)

Administrative O (IS-2)

Post Adjutant (IS-2)

Intelligence O (IS-2)

Provost Marshal (IS-2)

2d Sig Serv Bn (IS-6)

Chief, Pers & Tng Div (IS-4)

Chief, Pers Br (IS-4A)

Chief, Tng Br (IS-4B)

O/C O Pers Sec (IS-4C)

Chief, Oper Serv Div (IS-5)

Chief, Comm Br (IE)

Chief, Lab Br (ID)

Chief, Machine Br (IN)

Chief, Supply Br (IS-5A)

O/C SSA Mail Unit (IE-2D)

Chief, Security Div (IS-8)

Chief, Prot Sec Br (AP)

Chief, Crypt Mat Br (IC)

Chief, Equipment Br (IF)

Chief, Comm Sec Br (IS-8A)

Chief, Intelligence Div (IS-9)

Chief, Lang Br (IB-1)

Chief, Mil Crypt Br (IB-2)

Chief, Gen Crypt Br (IB-3)

Chief, T/A and C Br (IB-4)

Chief, I & L Br (IR)

As discussed

As requested

Comments and return

Information and file

Information and forwarding

Information and return

Recommendation

See note on reverse

Signature if approved

Your action

~~SECRET~~~~CONFIDENTIAL~~~~RESTRICTED~~TO DATE 27 Apr FROM

Commanding Officer
 Assistant Commandant
 Dir of Comm Research
 Control O
 Fiscal O
 Administrative O
 Post Adjutant
 Intelligence O
 Provost Marshal
 2nd Sig Serv Bn
 Chief, Pers & Tng Div
 Chief, Pers Br
 Chief, Tng Br
 O/C Officer Pers Sec
 Chief, Oper Serv Div
 Chief, Communications Br
 Chief, Laboratory Br
 Chief, Machine Br
 Chief, Supply Br
 O/C, SSA Mail Unit
 Chief, Security Div
 Chief, Protective Sec Br
 Chief, Cryptographic Br
 Chief, Development Br
 Chief, Intelligence Div
 Chief, Language Br
 Chief, Mil Cryptanalytic Br
 Chief, Gen Cryptanalytic Br
 Chief, T/A and Control Br
 Chief, I & L Br

As discussed
 As requested
 Comments and return
 Information and file
 Information and forwarding
 Information and return
 Recommendation
 See note on reverse
 Signature if approved
 Your action

This is ~~prepaid~~ REF ID: A4148493
mentioned this morning
as being of possible
interest to Gen. Stoner.

This is only complete
copy we have & I
don't want to lose it.
If you decide to leave
it with Gen. Stoner,
pse insure its return.

J.

~~SECRET~~

REF ID: A4148493

ROUTING AND WORK SHEET

(PAR. 40.62 O.R.)

*Mrs. Highley;
File with paper
on this #1
J.*

SUBJECT

A History of SIS

| Number each action | To— | Memorandum | Name, Division or Branch, and Date |
|--------------------|----------------|--|---|
| 1 | Col. Corderman | <p>1. Some time ago, at the suggestion of Colonel Clarke, I undertook the preparation of a brief history of the Signal Intelligence Service. This has just been completed and the original copy is attached hereto. I presume that Colonel Clarke would still like to see this study.</p> <p>2. I have two additional copies, complete with exhibits, which are available for such purposes as you desire.</p> <p>3. Mr. Wahl, who is preparing a detailed historical study of crypt-analytic work in the Army, would like to take advantage of this brief survey which has been made. Are there any objections to my letting him have a copy?</p> <p>Attchd: Paper w/5 tabs</p> | <p>W. F. Friedman Dir. Com. Res. SPSIS-3 12 July 1943</p> <p><i>W.F.F.</i></p> <p><i>NSA-3411</i></p> <p><i>Mr. Friedman original was turned over to Col Clarke by me today. I would like a copy of the history for my use and file here.</i></p> <p><i>WPC</i> <i>13 July 43</i></p> <p>NSA LIBRARY S-2049 COPY NO. 1</p> <p><i>History 15</i></p> |

~~SECRET~~

HEADQUARTERS ARLINGTON HALL STATION
ARLINGTON, VIRGINIA

SPSIS-1

DATE _____

INFORMAL MEMO FOR: Mr. Friedman:

I wonder if Mrs. Highley couldn't finish this job? I have finished the re-typing, but it has not been proof-read, nor stamped SECRET.

Attached is a carbon of the first draft, which I took the liberty of marking up. This merely consists of changes in arrangement of sentences, and you may or may not find it of use. Colonel Corderman read the original and made no comments. Just drop this in the wastebasket if you don't want to bother.

Attached also are additional copies of the tabs which I had made. You will note they are clearer than the others, as I had them made from G-2 copies or originals.

M. Dyer

W. Preston Corderman
Colonel, Signal Corps
Commanding

RESTRICTEDCONFIDENTIALSECRET

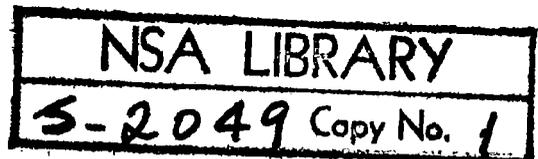
~~SECRET~~

A History of SIS

- 1 Col. Corderman
1. Some time ago at the suggestion of Colonel Clarke I undertook the preparation of a brief history of the Signal Intelligence Service. This has just been completed and the original copy is attached hereto. I presume that Colonel Clarke would still like to see this study.
 2. I have two additional copies complete with exhibits which are available for such purposes as you desire.
 3. Mr. Wahl who is preparing a detailed historical study of crypt-analytic work in the Army would like to take advantage of this brief survey which has been made. Are there any objections to my letting him have a copy?

Attchd:
Paper w/5
tabs

W. F. Friedman
Dir. Com. Res.
SPSIS-3
12 July 1943



~~SECRET~~

MASSIVE FILE

7/15/43
2/5/44

~~SECRET~~

Jul 1943

A BRIEF HISTORY OF THE SIGNAL INTELLIGENCE SERVICE

1. Prior to June 1917 no department of the Government conducted any cryptanalytic activities whatsoever. From June 1916 to about December 1920 a considerable amount of work along these lines was conducted purely as a patriotic enterprise and at his own expense by Mr. George Fabyan, whose Riverbank Laboratories at Geneva, Illinois, organized and provided elementary training for a small group of amateur cryptanalysts to work upon such codes and ciphers as were forwarded by the War, Navy, State, and Justice Departments. The group soon became somewhat proficient and grew in numbers, at one time reaching 30 persons. The undersigned directed the cryptanalytic operations and training at the Riverbank Laboratories from the time of the inception of this work until its close ~~thereat~~ in 1920, except for a period of a year (May 1918 - May 1919) when he was 1st Lieut., MID, serving at GHQ-AEF in the German code solving section.

2. *training(?)* a. In June 1917 the cryptanalytic activities of the War Department were initiated by Colonel Van Daman, G-2, with the commissioning of H. O. Yardley, a telegrapher at the State Department who had taken some interest in cryptography, who was given two civilian employees to assist him. The work grew rapidly and by the autumn of 1917 the increased staff was organized as a section designated as MI-8, which was subdivided into six subsections:

- Subsection 1. Code and cipher solution
- " 2. Code and cipher compilation
- " 3. Training
- " 4. Secret inks
- " 5. Shorthand and miscellaneous
- " 6. Communications (for MID only).

b. The functions and duties of these six subsections may be briefly outlined:

(1) The code and cipher solution subsection was what would now be called the cryptanalytic subsection. It was the largest of the subsections of MI-8 and performed the cryptanalytic work not only for the War Department but also for all other Government departments, including Navy, State, Justice, and the two censorships—Cable and Postal, which were then separate organizations.

(2) Despite the fact that under Army regulations the compilation and revision of codes was a function of the Chief Signal Officer, compilation activities under the Signal Corps were apparently in a moribund state. Information having been received that the Germans possessed copies of the War Department Telegraph Code, MI-8 deemed it advisable to establish a code compilation subsection, and that subsection produced several codes

NSA LIBRARY

5-2049 Copy No. 1

5-2049

~~SECRET~~

such as Military Intelligence Codes No. 5 and No. 9, small pocket codes for secret agents, and the like.

(3) In addition to training ^{its} own personnel, MI-8 trained ~~the majority of~~ ^{most} the personnel ~~sent overseas~~ ^{overseas} for cryptanalytic duties with ~~land~~ forces, both AEF and Siberia. It must be mentioned, however, that approximately 85 officers were trained at Riverbank Laboratories, where a six-week training course in cryptanalysis was given ^{them} these officers prior to their ~~shipment overseas~~ ^{departure for foreign duty}.

(4) A laboratory was established for the preparation of invisible inks for use by our own agents. It also examined letters for secret writing, and an average of over 2000 letters per week ^{was} examined for the military and postal censorship from July 1, 1918 to February 1, 1919.

(5) The shorthand subsection was organized to ~~handle~~ ^{decipher} captured documents and texts in various shorthand systems, especially German, which had to be deciphered. This was ~~in fact~~ the first subsection organized in MI-8, when the censorship began sending (October 1917) letters and documents supposed to be in cipher but which ~~turned out to be~~ ^{actually} in shorthand. In June 1918 the AEF requested 15 expert stenographers who could ~~take down~~ ^{record} verbatim examination of German prisoners. The required number was found and ~~shipped~~ ^{sent}. This subsection also provided trained linguists for MI-8 and the AEF.

(6) The communications subsection was established in MI-8 for handling messages to and from military attaches and intelligence officers serving abroad. In a period of nine months it sent and received about 25,000 such messages, practically all in code.

3. At the height of its development, which was reached in November 1918, MI-8 was, for those days, a rather large unit, consisting of 18 officers, 24 civilian cryptographers and cryptanalysts, and 109 typists and stenographers. The time had come for the establishment of a definite policy for the future. Now, the guiding heads of Military Intelligence at that time fully recognized the high importance and value of the services rendered by the MI-8 cryptanalytic bureau, because they had been in positions ^{to not directly} ~~and~~ the products of the daily activities of the bureau ~~came directly~~ ^{and} to their notice and they could not fail to note their influence and bearing, ~~which the work had~~, not only upon the military and naval, but also upon the diplomatic, political, and economic phases of the conduct of the war. They therefore had practical experience in the matter and could bring the weight of their positions of influence and their actual experience to bear upon those ^{who held} ~~in charge of~~ the purse strings, with the result that they were able to obtain funds sufficient to keep a fairly large organization intact for a year or two. An annual appropriation of \$100,000 was recommended in a memorandum for the Chief of Staff from the A. C. of S., G-2, dated May 16, 1919, (Tab A attached) to be used as follows:

~~SECRET~~

~~SECRET~~

| | | |
|----------------------------|-----------|---------------|
| Rent, light, and heat | \$ | 3,900 |
| Reference books | | 100 |
| Personnel: Chief (Yardley) | | 6,000 |
| 10 code and cipher experts | @ \$3,000 | 30,000 |
| 15 code and cipher experts | @ \$2,000 | 30,000 |
| 25 clerks | @ \$1,200 | <u>30,000</u> |

\$ 100,000

to move

The item for "rent, light, and heat" is explainable ^{ed by the fact that it was decided} when it is noted that the bureau ~~was to be moved~~ from Washington with a view to hiding its existence. Of the \$100,000 recommended, the State Department was to provide \$40,000 and \$60,000 was to be provided for expenditure by the A. C. of S., G-2 on "confidential memoranda" against funds pertaining to "Contingency Military Intelligence Division" -- that is, by vouchers not subject to review by the Comptroller General. The paper containing the recommendations made by the A. C. of S., G-2 to the Chief of Staff was "OK-ed" and initialled by Acting Secretary of State Polk on May 17, 1919, and within three days of the initiation of the paper (May 19) it was approved by the Secretary of War over the signature of General March, Chief of Staff (see top sheet of Tab A). Next came the question of actually obtaining the funds. In this connection Tab B shows a copy of a letter dated May 24, 1922 from the then Secretary of State to Senator Radsworth, who was Chairman of the Senate Appropriations Committee. With the letter went a special memorandum and a copy of it is included in Tab B. Evidently the funds were obtained. The plan was put into effect, the bureau was installed in a private house at 22 East 38th Street, New York City, and all personnel together with ~~and~~ existing records were moved thereto.

provided for

4. The foregoing funds took care of the bureau for the FY 1920, but when in June 1920 it came time to set up the budget for FY 1921, the purse strings were already beginning to be pulled tighter. Many of the "old-timers" in G-2 had gone to other assignments; those remaining and the newcomers in G-2 apparently did not have the background of the story, nor the foresight and the influence to press the matter so far as the War Department was concerned. The appropriation was at once cut in half, that is, to \$50,000, of which the State Department share still continued to be \$40,000. It is possible that the G-2 thesis was that since the work done by the bureau was primarily, if not solely, for and of interest to the State Department at that period in our affairs, all or nearly all of the funds should be provided by that department. The War Department overlooked some very important points in the situation -- points which will be brought up and emphasized later in this summary. Near the close of FY 1921, when it appeared that a further contraction in funds could be anticipated, an attempt was made to obtain State Department support before Congressional appropriations committees, and

~~SECRET~~

SECRET

the A. C. of S., G-2 succeeded in getting the Secretary of State to write a letter to the Chairman of the Senate Appropriations Committee. A copy of this letter is attached as Tab B. The A. C. of S., G-2 also presented his views before the committee in closed session, during which open reference ^{was made} to ~~the exhibits~~ ^{and exhibits of previous} of cryptanalytic work ^{as evi-} denced by a memorandum attached to Tab B. ^{Apparently the Committee had} The showing ^{made} must have been impressive, for there was not, in FY 1922, another sharp ^{decrease} in funds allotted for cryptanalytic work. However, in order not to break the continuity of the history, at this point, will merely be stated that year by year the funds provided for the maintenance and operation of the bureau became more and more constricted, ~~until~~ ^{By} the autumn of 1929 the following tabulation, based upon a letter dated July 17, 1929 from Major O. S. Albright, G-2, to the Chief Signal Officer (General Gibbs), ^{shows how the} bureau had been permitted to deteriorate to the degree indicated by

| | |
|--|-----------------|
| Rent | \$ 3,000 |
| Books, postage, travel and transportation, misc. | 2,370 |
| Personnel: | |
| 1 Chief (Yardley) | 7,500 |
| 1 code & cipher expert | 3,660 |
| 1 translator (Jap) | 3,750 |
| 1 secretary | 1,800 |
| 1 clerk-typist | 1,600 |
| 1 clerk-typist | 1,320 |
| | <u>\$25,000</u> |

5. Of the total appropriation of \$25,000, the State Department furnished \$15,000, the War Department \$10,000. At this time the activities of the bureau had become so reduced that it was sending in only occasional translations of a few Japanese and a few Mexican diplomatic messages. No research whatsoever was conducted in cryptanalysis; there were no training activities, no intercept, no direction-finding studies, no secret ink work. The personnel consisted of six persons all told, and 37% of the total payroll went to one man, who had little interest other than to continue as long as possible to maintain himself in the sinecure into which he had been permitted to establish himself. He not only had his well-paying Government position but was engaged commercially in other activities.

6. In the summer of 1929 Major O. S. Albright, Signal Corps, was assigned to ~~be~~ ^{serve} on the staff of the A. C. of S., G-2 to supervise and coordinate such of the cryptographic and cryptanalytic activities of the War Department as remained. After a careful ~~study~~ ^{survey} of the situation and an appraisal of ~~how the existing cryptanalytic bureau, was and was not serving the functions for which it had been or should be intended,~~ ^{the operations of} Major Albright came to the conclusion that the entire picture was wrong. He felt that while the ~~the product of "bulletin"~~ ^{Producing} which the bureau was ~~typing and~~ ^{producing} intermittently was indeed of primary interest for ~~its own sake~~ ^{to the State Department,} and while the War Department had only a secondary interest in the ~~"bulletin"~~ ^{"bulletin"} for the information it ~~gave,~~ ^{gave,} the primary interest of the War Department in

Certainly, he felt that

SECRET

The bureau was concerned in deciphering operations and ob-fectoria

cryptanalytic studies in peace time was that ~~it was intended~~ to engage in research and to ~~provide means for training~~ specialized personnel for immediate war-time effectiveness. Major Albright found that not only was there very little if any training being conducted but also that all persons in the bureau, except for one clerk receiving the least pay, were "getting along in years" ^{and of practically no} ~~their~~ potential usefulness for possible wartime service, ~~practically all~~. Moreover, the bureau was now hidden away in a public office building in New York (under cover of the "Code Compilation Company" for alleged purposes of security) and far away from direct supervision of ~~anybody connected with the War Department or of G-2, so that nobody knew what was going on, how the office was administered, etc.~~ ^{It was later learned that} Yardley devoted most of his time to two or three private enterprises, (commercial code compilation, real estate brokerage, consultant in code matters to commercial firms) and he was having a "field day" at Government expense. There were, in addition, several other weighty factors which motivated Major Albright in preparing a G-2 study (Tab C) recommending that the bureau be ~~taken out of G-2~~ and its functions ^{from G-2} transferred to the Signal Corps. Chief among these was the desirability, if not necessity, of placing all cryptographic and cryptanalytic work of the War Department under one agency, rather than distributing it among three (The Adjutant General, for printing, storage, issue, and accounting of codes; the Chief Signal Officer, for compiling codes and ciphers; Military Intelligence, for solution of codes and ciphers). A memorandum on the same subject was prepared by Lieut. Col. W. K. Wilson of the War Plans and Training Section of G-2, and is also attached hereto (Tab D). The reasons given in the G-2 study and in Colonel Wilson's memorandum were apparently deemed valid by the Chief of Staff, for Major Albright's recommendations were approved in April 1929 and steps were soon initiated by G-2 and the Chief Signal Officer to put them into effect. The recommendations carried with them merely ~~the wording of changes to be made of~~ ^{in the wording} AR 105-5, specifying the duties of the Chief Signal Officer, ~~these duties being enlarged to include~~ ^{these duties} the printing, storage, distribution, and accounting of codes and "in time of war the interception of enemy radio and wire traffic, the goniometric location of enemy radio stations, the solution of intercepted enemy code and cipher messages, and laboratory arrangements for the employment and detection of secret inks."

7. However, before anything could be done ~~actually~~ ^{effect the} to transfer the activity, a new and very disturbing factor entered into the picture. In March 1929 a new administration took office, in which Mr. Stimson became Secretary of State. For a few weeks no "bulletins" from the cryptanalytic bureau in New York were given him, the intention being to "go slow" until he had become sufficiently well oriented in the duties of his office to warrant bringing to his attention the highly secret (and in the then current view, highly "unethical") activities engaged in by War and State Departments by means of funds provided in large part by the latter Department. Early in May 1929, however, the time was deemed ripe for this

measure, and (according to Yardley) it was with some trepidation that a few translations of Japanese code messages were placed on Mr. Stimson's desk. There seems to be some reason to believe that his reaction was violent and his ~~action~~ ^{is} drastic. Upon learning how the material was obtained, he characterized the activity as being highly unethical and declared that it would cease immediately, so far as the State Department was concerned. To put teeth into his decision he gave instructions that the necessary funds of the State Department ~~would~~ ^{be} withdrawn at once ⁽¹⁾.

It was only after considerable pressure by the A. C. of S., G-2 that he was dissuaded from this course, which might have had serious consequences by suddenly throwing out of employment the six people concerned, at a time of ~~the~~ ^{there} economic depression. ~~For~~ ^{These} workers had only special training in a field wholly useless to commercial, industrial, shipping or banking firms, or to other government departments, or to educational institutions, ^{and}

An arrangement was therefore ~~made~~ ^{made}, to close the office immediately so far as active work was concerned, but to keep the personnel on the payroll for the time necessary to wind up affairs and get the files in shape ready to turn over to the Signal Corps. This took a couple of months, and at the end of June 1929 the employees were given three months' pay in advance in a lump sum, to tide them over the period in which they might be jobless. Since they had been paid out of "confidential funds" they had no civil service status and no retirement benefits; moreover, they were ineligible for transfer to other Government positions. ~~Of course, the danger was that~~ ^{and} their dissatisfaction with ~~what~~ ^{what} must have appeared to them as high-handed, arbitrary action on the part of a new official, ~~and that their helplessness~~ ⁱⁿ (the serious personal situation created for them in the midst of a serious economic depression) by this drastic action, might lead them to indiscretions which might prove most embarrassing to the Government and ~~have~~ ^{have} ~~serious~~ ^{serious} consequences upon national defense. ~~It turned out that, whatever their private feelings,~~ ^{It turned out that,} all the discharged personnel, except the chief beneficiary of the old regime, remained loyal and did the best they could to find jobs.

8. In October 1929 I was sent by the Chief Signal Officer to New York to take over the ~~boxed up~~ ^{boxed up} records and files of the defunct Bureau and to oversee their transportation to Washington. ~~The~~ ^{The} Cryptanalytic activities, research, and training now being under the Chief Signal Officer, immediate steps were taken completely to reorganize the bureau and its work. ^{The} funds available ~~were, of course, very slim -- only what remained of the~~ ^{were, of course, very slim -- only what remained of the} War Department's ~~contribution of \$10,000 for the FY 1930, was available,~~ ^{contribution of \$10,000 for the FY 1930, was available,} because the remainder of the State Department's share of \$15,000 had already been withdrawn, by the State Department, as indicated above. An offer of employment was made to Mrs. Wilson, the Japanese expert with Yardley, but she was unable to accept, since it involved moving to Washington and she

(1) A number of years later (1941) Yardley told me that he had been misinformed as to Mr. Stimson's attitude and that it was really the President (Mr. Hoover) who "killed" the bureau, not Mr. Stimson. There may be some grounds for believing this, and it would be interesting to know the truth.

~~SECRET~~

had a husband and child in New York. Another employee, Mr. Victor Weisskopf, had a business in New York and refused to move to Washington. The female clerical employees were deemed unsuitable for our purposes and, moreover, having no civil service status, they could not be taken on by transfer. An offer of temporary employment was made to Yardley but ~~he and~~ ^{and} refused ~~the tender~~. Instead, he proceeded secretly to prepare a book which first appeared in the form of articles in the Saturday Evening Post, and ~~was~~ ^{was} later ~~appeared~~ ^{published} in much expanded form under the title, "The American Black Chamber." The book and articles were highly sensational and made damaging disclosures concerning the most secret activities ever conducted by the Government. Before the appearance of the articles and book, however, he had taken certain steps to protect himself from possible prosecution for his disclosures, among which was to resign his commission as Major in the Military Intelligence Reserve. Of course, had the authorities understood the real purpose of his resignation they might have prevented it so as to retain some hold on him. But being in doubt or in ignorance of his real motives and deeming it just an act of pique, the resignation was accepted. The unfortunate consequences attendant upon the publication of the book need no elaboration herein. Suffice it to say that our amicable relations with the British, who resented the disclosure of certain information obtained from them by Yardley as a commissioned officer, were disturbed; much more serious, our precarious relations with Japan were brought to a boiling point when about 30,000 copies of the Japanese translation of The American Black Chamber were sold in Tokyo in a period of less than a month (perhaps the book was subsidized by the Japanese Government itself). The bad odor into which all cryptanalysts and cryptanalytic activities fell, as a result of the difficulties which the publicity given the matter by Yardley's disclosures occasioned high government officials, had a bad effect upon the attempted reorganization of the cryptanalytic bureau by the Chief Signal Officer. Funds were hard to get, and State Department support was lacking, ~~if not in the other direction altogether~~. The most serious consequences of Yardley's disclosures, however, came ten years later, and their effects can hardly be estimated. I refer here to the jolt which his book gave the Japanese cryptographers, leading them out of their blissful ignorance and causing them to develop really complex methods which are now giving us so many difficulties. The same is true probably as regards the German and Italian cryptographers — their education has been entirely at Uncle Sam's expense and the final consequences of Yardley's work can not yet be foreseen. They may well turn out to be disastrous.

9. Without delay, as indicated in the beginning of the last paragraph, the Chief Signal Officer proceeded, as energetically as possible under the circumstances, to carry out the mission assigned to him. The reorganized code and cipher solving section was placed under the War Plans and Training Division, since the code compilation section was already there. A rather detailed directive, which was prepared by G-2 and approved by the Secretary of War (Tab E), became the guiding plan of the reorganized service, which was now named the Signal Intelligence Service. Its personnel, consisting of myself and one or two clerks, soon was augmented by a half dozen more

~~SECRET~~

employees. Training literature and courses in cryptanalysis and cryptography were prepared and put into good usage at once. A great deal was done in expanding our cryptographic work also, by preparing reserve editions of existing codes, compiling and devising new codes and ciphers, developing cipher apparatus, and so on. Cryptanalytic work was put on a firm basis of research and training, with emphasis on the latter, for there existed no intercept service and the raw material could not be obtained. (Yardley had been able to get a small amount of material from the cable companies but this source had practically "dried up" by 1929 due to fear on the part of the companies.) Hence an intercept service now was organized and grew very slowly. All phases of signal intelligence were unified under one service and taken under study and action. Moreover, important cooperation with the Navy in the same type of work was ~~was~~ initiated. How the activity has expanded since then requires no comment at this time. However, a few words about relations with the Navy are pertinent.

10. Cryptanalytic activities in our Navy Department were practically non-existent until after the close of the last war, during which, as was noted above, whatever problems they had in cryptanalysis were referred to MI-8. But in 1921 the Navy, recognizing the important role which cryptanalysis was bound to play in future, began building up a large unit in the Navy Department, with echelons afloat. Whereas the Army placed emphasis upon civilian training, the Navy placed emphasis upon officer training; and for each dollar the Army was able to obtain for cryptanalytic and cryptographic work the Navy was able to obtain three to five dollars, until by 1939, as far as concerned numbers of officers and civilian personnel engaged in these activities, amount of equipment on hand, and funds available for research, the Navy had considerably outstripped the Army. However, it may be said, with some justifiable pride ~~perhaps~~, that while they were ahead of us in quantity, we were ahead in quality, for all the important developments in both the cryptographic and the cryptanalytic fields must be credited to Army personnel. At first, cooperation between the two services was intermittent and at times very indifferent—the usual mutual suspicions and jealousies pervaded our relationships. But, happily, for the past four or five years cooperation has been much more wholehearted, with the result that it may now be said without reserve that, as regards their cryptographic and cryptanalytic activities, technical cooperation between the Army and Navy in these fields is so close as to be the same as though they were under one head. This, of course, is as it should be and must be in order to gain the desired result from such activities.

11. It would be of utmost value to the winning of this war if the Government were now in a position to read the codes and ciphers of all the foreign powers whose actions and probable intentions are of interest and importance in our prosecution of the war. It could have been in this fortunate position had it given to cryptanalytic studies the attention

~~CONFIDENTIAL~~

ARLINGTON HALL STATION

Date _____

TOFROM

_____ Commanding Officer _____
 _____ Executive Officer _____
 _____ Asst. Executive Officer _____
 _____ Adjutant _____
 _____ Asst. Adjutant _____
 _____ Chief, Headquarters Branch _____
 _____ Chief, A Branch _____
 _____ Chief, B Branch _____
 _____ Chief, C Branch _____
 _____ Chief, D Branch _____
 _____ Chief, E Branch _____
 _____ Chief, F Branch _____
 _____ Dir. of Com. Research _____
 _____ Dir. of Training _____
 _____ C. O. of Troops _____
 _____ Property Officer _____
 _____ Personnel Officer _____
 _____ Provost Marshal _____
 _____ Classified Mail Room _____
 _____ Secretary to C. O. _____
 _____ File Room _____

_____ Comments & Return _____
 _____ Recommendations _____
 _____ Information _____
 _____ Information & Return _____
 _____ Inf. & Forwarding _____
 _____ Your Inf. & File _____
 _____ Signature, if approved _____
 _____ See Note on Back _____
 _____ AS Requested _____
 _____ AS Discussed _____
 _____ Your Action By _____

Note: It seems to me No. 1 should be the necessity for factual knowledge of intentions of potential enemies; No. 2 the protection of our own systems (now included in No. 4); then 1, 2 and 3.

which they deserve during peacetime and had provided funds for their continuity on a scale sufficient for the purpose for which they are intended. The matter can be summarized very succinctly in this statement: Actual or physical warfare is intermittent, but signal security warfare, especially cryptanalytic warfare, is continuous. It is vital that this be understood by those who exercise the control over such studies.

12. There are four basic reasons why this continuity in cryptanalytic studies is so important. They will be discussed briefly:

(1) It must be realized that cryptanalytic activities have no counterpart in civil life. Therefore, on the outbreak of war there is no important source from which trained, experienced personnel can be drawn for immediate usefulness. Since skill in cryptanalysis can hardly be developed in a short time and cryptanalytic units capable of producing quick results can not be improvised in a hurry, unless there is a good-sized nucleus of such trained and experienced personnel no good cryptanalytic operations can be conducted in the early phases of a war; that is, just at the time when results can usually be obtained most easily and when such results are extremely important. Moreover, it is in the upper strata of cryptanalytic brains that continuity in studies is most important. It is possible, under pressure, to obtain large numbers of recruits of high intelligence from colleges and universities, but until they have had at least five years actual experience and training they are wholly unprepared to attack the more difficult problems encountered in modern, up-to-date secret communications. Consider the present "Purple" system, for example. It required almost two years of concentrated effort to break down this system and it was indeed fortunate that this had been accomplished by September 1939. If we had only been able to start this study in December 1941 it would not have been possible to read those messages short of two years' study, if at all, because the problem is so difficult to begin with, and moreover, the volume of traffic available for analysis would be so small compared to what it was shortly before December 7, 1941. Moreover, if we did not have the two years' experience with the ordinary "Purple" the task of reading the special "Purples" now occasionally employed would be extremely more difficult, if it could be done at all before too late to be useful. Again, our present difficulties with Japanese military systems are in large part occasioned by our failure to devote sufficient study to these systems over the past few years; but it must be realized that limitations on funds and personnel made such studies impossible, because with the small staff of SIS personnel from 1930 to 1940 it was all that this personnel could do to keep abreast of the Japanese diplomatic systems, for which G-2 was clamoring.

(2) Continuity in cryptanalytic studies also requires continuity in intercept work, for without the basic raw material no studies at all can be conducted on actual traffic and purely theoretical studies may be

~~SECRET~~

far off the real target altogether, no matter how successful. Continuity in intercept work means, of course, that the equipment and personnel of the intercept service have to be maintained and thus, these are available on the outbreak of war, for immediate, useful work. Unless cryptanalytic studies are pursued the need for the maintenance of adequate intercept stations soon disappears, for it presently begins to look as though the work done by the intercept personnel is useless and funds for this activity are withdrawn.

(3) Continuity in cryptanalytic studies is necessary because cryptanalysis is not a static science or art -- it must progress as cryptographic science progresses. In the past few years great strides have been made in the latter, especially as regards the development of complex electrical and mechanical cryptographic devices and machinery. Moreover, the cryptanalytic work done during the last war has been publicized. As alluded to above, "The American Black Chamber" in particular has exercised a wide influence in putting certain nations which had been quite backward in their cryptography on their guard, causing them to engage in studies and developments for the improvement of their codes and ciphers. The result is that the cryptographic systems of these nations have become more and more difficult to analyze. It is important to note that improvement in cryptography usually comes in successive small steps, and if the opposing cryptanalyst can keep in step with these progressive increases in complexity he can, as a rule, be in a position to read the new systems almost as fast as they are put into usage. If there is much of a lag in the cryptanalysis the cryptographer gets too far ahead for the cryptanalyst to catch up quickly; in some cases catching up becomes impracticable or impossible.

(4) Finally, it may be noted that continuity in cryptanalytic studies brings improvements in our own cryptographic systems and methods, without which we may be lulled into a false sense of security and remain blissfully ignorant of what some foreign cryptanalytic bureau may be doing with our supposedly secret communications. It can be said that the greatest blow that can be dealt to signal security work is loss of continuity in cryptanalytic studies, for it means that a disastrous blow has been delivered to technical efficiency of both the cryptographic and cryptanalytic services for war-time functioning.

13. It may be pertinent to add that the British Government began its cryptanalytic activities in 1914 and never desisted from them for even a month since then, though of course on a smaller scale than was reached at the height of these activities in 1918-19. However, it was on a scale sufficient to enable them to keep up with the diplomatic traffic of most of the governments of any consequence in the world in which they had an interest. The British built up a corps of about 35 to 40 able cryptanalysts, including Army and Navy officers permanently assigned to cryptanalytic

~~SECRET~~

duties. They maintained cryptanalytic units in London, India, Africa, China, and so on — the officers being transferred from one unit to another but constantly staying in cryptanalytic work. The result is that today, while our SIS has solved and can perhaps again solve more difficult individual problems, in overall coverage of the field the British organization is considerably ahead of ours. It is clear that no country is too small for them to have an interest in that country's secret communications, and they are today able to read the traffic of most countries on which they have had continuity since the last war.

14. Finally, if we are not to repeat once more the mistakes made at the close of the last war in respect to signal security work, every effort should be made to place the present organization on the most firm, permanent foundation it is possible to erect. The service should not be considered as merely an appendage to the functions performed by the Signal Corps only in time of war but as a permanent service that operates on a large scale in peace-time as well as in war-time.

William F. Friedman,
Director of Communications Research.

Originally written
and dated June 29, 1942.
Minor changes made on
April 2, 1943.

Att.: 5 TABS, A to E, incl.

EXECUTIVE DIVISION
MILITARY INTELLIGENCE BRANCH

In replying refer to

10304-20
.. I. 8

WAR DEPARTMENT
OFFICE OF THE CHIEF OF STAFF
WASHINGTON

~~Secret~~
T

May 16, 1914

~~SECRET~~

TAB
A

MEMORANDUM FOR THE CHIEF OF STAFF.

Subject: Permanent Organization for Code and Cipher Investigation and Attack.

1. Herewith is transmitted a memorandum embodying a plan for a permanent organization for code and cipher work to be maintained by joint annual appropriation of \$60,000.00 by the Military Intelligence Division and of \$40,000.00 by the Department of State and to be controlled by the Director of M. I. D.

2. The Acting Secretary of State has been consulted and concurs in the proposed plan.

3. Authority is requested for the establishment and maintenance of the organization proposed and for the annual expenditure for this purpose by the Director of M. I. D. on confidential memorandum of \$60,000.00 of funds pertaining to "Contingency Military Intelligence Division, General Staff."

M. Churchill
M. Churchill,
Brigadier General, General Staff,
Director of Military Intelligence.

*Initials of
F. L. Pack
Acting Secretary of State*

vnj

Karch

E

EXECUTIVE DIVISION
MILITARY INTELLIGENCE BRANCH

replying refer to

10994-20
M. I. 8WAR DEPARTMENT
OFFICE OF THE CHIEF OF STAFF
WASHINGTON.~~Secret~~

May 16, 1919.

~~SECRET~~

MEMORANDUM FOR THE CHIEF OF STAFF.

Subject: Plans for M. I. 8.

1. HISTORY.

1. Previous to June, 1917, neither the War Department nor any other department of Government had any organization for code and cipher attack, and the only work of this character that had ever been done was the sporadic reading of a few simple ciphers by individuals and the more numerous decipherments volunteered by Mr. George Fabyan of Geneva, Illinois, who at his own expense brought together and supported a staff to whom elementary instruction in cipher attack was given at the Army Service Schools, at Fort Leavenworth. On June 10, 1917, the code and cipher work of Military Intelligence was begun by the appointment of one officer, who, with two civilian employees, was expected to encode and decode the official messages of Military Intelligence, supply enciphering tables, and attack enemy codes and ciphers. The work, however, grew rapidly and in the autumn of 1917 the increased staff was organized into a central code and cipher section to do the work of all departments of the Government.

2. At the height of its development, in November, 1918, the Section consisted of eighteen officers, twenty-four civilian cryptographers, and one hundred and nine typists and stenographers. In consequence of demobilization, it now consists of fifteen officers, seven civilian cryptographers and fifty-five typists and stenographers.

3. During the eighteen months since it seriously began to function, the section has deciphered ten thousand seven hundred and thirty-five messages in five hundred and seventy-nine code and cipher systems. Of the systems of foreign governments the Section now controls the following as completely as if they were our own systems:

| | |
|--|-----|
| Argentinian Diplomatic Code | 1 |
| Brazilian Diplomatic Code | 1 |
| Brazilian Diplomatic Cipher | 1 |
| Chilean Diplomatic Codes | 2 |
| Costa Rican Diplomatic Codes | 3 |
| Cuban Diplomatic Code | 1 |
| German Diplomatic and Intelligence Codes | 7 |
| German Diplomatic and Intelligence Ciphers | 5 |
| Mexican Diplomatic and Consular Ciphers | 541 |
| Spanish Diplomatic Codes | 16 |
| Spanish Consular Code | 1 |

579

~~SECRET~~

- 2 -

4. Work upon other codes is in such a state of advancement that with adequate personnel the following will certainly be solved by the end of June:

| | |
|--------------------------|-------|
| German Diplomatic Codes | 3 |
| Panama Diplomatic Code | 1 |
| Spanish Diplomatic Codes | 3 |
| | <hr/> |
| | 7 |

5. In the account just given no note is taken of the enormous number of personal codes and ciphers submitted by the Postal Censorship or of the letters examined in our laboratory for secret writing -- 2000 a week for several months. Also unnoted is the large amount of work involved in our own communications, in compiling cipher tables and code books, and in training military attaches, code clerks, and cryptographers.

II. VALUE OF THE WORK. The Chief value of all this work has resided in the large and constant stream of information it has provided in regard to the attitudes, purposes, and plans of our neighbors. But a few selected examples will emphasize the results of the past and the possibilities of the future:

1. Insight into German Secret Service.

a) The Waberski Cipher is an official letter of introduction given by Minister von Eckardt to Pablo Waberski, a secret agent of the German government, addressed to all German consular agents in Mexico, ordering them to furnish him aid and support, provide funds, and forward his messages in code as official. This was captured on a German spy and was a principal factor in his conviction. For this cipher and its decipherment see Exhibit A.

b) The von Magnus Cipher -- known officially as "Document PQR" -- is a very long and elaborate quadruple transposition cipher, addressed by the German Charge d' Affaires in Mexico City to all German consular officials in Mexico, giving directions concerning the careful and complete destruction of correspondence, accounts, receipts, lists, registers, and all other papers having to do with "the Secret Service and the representatives of the General Staff and the Admiralty Staff" and the preservation of "the strictest silence concerning the existence and activities of these representatives now and for all future time, even after the conclusion of peace." For this cipher and its decipherment see Exhibit B.

c) Of the numerous German code messages deciphered by M. I. 8, two belong specifically under this head. The first was sent

~~SECRET~~

- 3 -

out by wireless from Nauen and intercepted by our stations sixty-four times between January 13 and February 2, 1918. It includes an order from the German Foreign Office to the recipient to avoid negotiations with the Japanese, because "communication through you is too difficult" and the Japanese have "representatives in Europe"; and presents a plan for providing Mexico with arms, and machinery and technical staff for the manufacture of arms and air-craft. The second message -- also a wireless from Nauen, intercepted in February 1918 -- informs the German Minister in Mexico of the deposit of ten million pesetas in the German Oversea Bank, Madrid, which he is authorized to offer to the Mexican Government as a "preliminary amount" "on supposition that Mexico will remain neutral during war." See Exhibit BB.

2. Special War Measures. The most important message of this character deciphered by M. I. 8 is the code cablegram sent by Ambassador von Bernstorff on January 21, 1917 to the German Consul at Manila ordering him to take up at once the question of making useless the machinery of interned German vessels or, in case that proved impossible, of sinking them. (For message and decipherment see Exhibit C.) It will be noted that this message was sent ten days before the declaration of unrestricted submarine warfare. If the U. S. Government had possessed at that time an organization capable of deciphering this and the other messages relating to this subject -- as was later done by M. I. 8 -- precautions against the crippling of these vessels could have been taken, with a saving to this government conservatively estimated at twenty-five millions of dollars.

Although M. I. 8 as an organization did not take part in any of the work on the front, it was in constant communication with G-2, A-6, and furnished and trained most of its personnel. The distinction between M. I. 8 and G-2, A-6, is therefore purely one of names and the work of G-2, A-6 should be taken into consideration in estimating the value of an organization for code and cipher attack. The following incidents illustrate not only the value of this work in actual military operations but also the absolute necessity of preparing in advance the trained personnel required by this work.

a) In March 1918 the Germans put into service along their entire western front a new code, different from anything they had had. By the second day after it was issued the complete system had been worked out by the experts of ourselves and our allies and we were reading it currently before the Germans themselves had become familiar with it. Colonel Moorman, chief of G-2, A-6, the authority for this incident, justly remarks: "While it is too much to say that it changed the result of the war, it certainly cost the lives of many German soldiers and saved many of the Allies."

~~SECRET~~

- 4 -

b) In 1916, when the Germans made their great withdrawal in Flanders, the code experts of the British gave G.H.Q. advance information not merely of the fact of the intended withdrawal but also of the time and manner of it. But at that time the officers in charge of operations were skeptical of code attack and put no faith in the information until they woke one morning and found the Germans gone. Similar skepticism, says Colonel Moorman, awaited the first message deciphered by G-2, A-6, giving definite information of an intended attack, but in this instance also the attack itself authenticated the work of the code-men.

3. Value in Peace Time. As has been set forth above, M.I.8 is now able to decipher as promptly as if they were in our own codes the messages of a considerable number of foreign powers and by the end of this month will have made notable additions to its list. If it is worth while to know exactly what instructions foreign powers give to their representatives at Washington, it is important to maintain M. I. 8 with a sufficient personnel in time of peace. If the impressions and opinions of diplomatic representatives at other capitals and the instructions they receive as to attitudes and actions are of importance for the maintenance of peace, the cheapest, indeed the only, way to keep constantly and promptly informed on these matters is to preserve M. I. 8 with a suitable personnel. Intimate knowledge of the true sentiments and intentions of other nations may often be an important factor in determining whether we are to have peace or war.

Two recent incidents may be cited out of many in the experience of M. I. 8.

a) On April 26, 1919, M. I. 8 furnished decipherments of five code messages which passed between Berlin and Madrid on that very day. This was of course possible only through the magnificent service of the intercepting station at Houlton, Maine. See Exhibit CC.

b) Yesterday's newspapers published the announcement of the Mexican government that certain unnamed friendly nations of Latin America had urged upon it a coalition in opposition to the Monroe Doctrine. Information on this point was sent by M. I. 8 to the State Department on April 23 in a message sent by cable to the Mexican Department of Foreign Relations on April 17 and submitted to M. I. 8 on April 22. A copy of the message is attached as Exhibit D.

4. When this world war was precipitated neither we nor any of the Allies had had sufficient experience in code and cipher attack or possessed anything like an adequate personnel. This is established not only by the statements of well-informed officers but also by such

~~SECRET~~

- 5 -

facts as that so late as the autumn^{of} 1916 the heads of the British Army were still skeptical of the results obtained by the code-men; see above.

Code attack is indeed still in its infancy. It is capable of rapid and incalculable development. If we do not take part in this development, we shall be helpless when the next war comes, and it is by no means certain that we shall then have allies upon whom we may rely for knowledge which we should have developed for ourselves. The rapid advance in methods of attack is indicated by such facts as the following:

When the war began, British officers declared that the Playfair cipher - the official cipher of the British Army - was indecipherable. Messages in this system can now easily be solved in thirty minutes, and the system has been abandoned as insecure. When the United States entered the war the official cipher was the Army disk with running key. This method was believed by experts of the Army to be indecipherable. By November 1917 M. I. 8 had shown that it was not only decipherable but yielded easily to scientific attack. The number of official ciphers and codes which have been successfully attacked by M. I. 8 bears witness to the same truth. Scores of systems submitted for Army use as invulnerable have been examined by M. I. 8 and rejected as insecure.

It is definitely known to us that two at least of our most important allies have arranged to maintain in the future large and powerful organizations for code and cipher attack, for the development of new methods, and for the training of an adequate personnel. It is probable that other nations, of whose plans we know nothing, will pursue the same policy. For among the lessons taught by this war two are of special importance to the cipher expert:

a) That speed in the solution of messages is of the very essence of the matter. To decipher a message announcing an attack a week - or even a minute - after the attack has occurred may be interesting but is of no operative value.

b) That speed is attained by experience and that experience cannot be improvised. To solve the first Chilean code required several months; the second was solved on the basis of twenty messages in less than a month.

III. CONCLUSION. In view of the facts recited and suggested in the preceding paragraphs, it seems imperative that this Government should maintain in time of peace as well as in time of war an organiza-

~~SECRET~~

- 6 -

tion of skilled cryptographers sufficient in number to carry out the program of deciphering promptly all foreign code and cipher messages submitted to it, of solving new codes, of developing new methods and of training an adequate personnel.

IV. RECOMMENDATIONS.

1. Experience has shown that such an organization as is proposed will be best equipped to secure results if it has access not only to the sources of information and of material controlled by the Army, but also to the special sources controlled by the State Department. The achievements of M. I. 8 have been due in no small measure to the fact that during the war it has been serving both these departments of the Government. Therefore after consultation with the Director of M. I. D. and with responsible officials of the State Department it seems desirable to recommend continued cooperation between the two departments, with acceptance of the financial assistance heretofore approved by the State Department, and with administrative control vested as heretofore in the Director of M. I. D.

That the organization should consist of civilians as indicated by the following facts:

a) After the demonstration afforded by the incident of the German withdrawal from Flanders recorded above, the British adopted the policy of searching the British Empire for the best code and cipher brains of the Empire, and results justified this policy.

b) The success of M. I. 8 has been due to an attempt from the first to carry out a similar policy.

c) The type of thinker with necessary language qualifications required for code and cipher attack is a special type - difficult to find in the Army, where an entirely different type is more useful, and not easily inducted into the Army if discovered in civil life.

d) The salaries suggested have been determined after very careful study of the situation. Men and women of the high qualifications necessary can hardly be attracted to the work and - what is equally important - retained in it for smaller salaries. During the war M. I. 8 was for patriotic reasons able to command the services of both civilian officers and civilian cryptographers for emoluments far below those actually received by these officers and cryptographers in civil life. Such sacrifices can of course not be expected in time

~~SECRET~~

of peace.

2. It is estimated that the annual expenses of an adequate organization would be approximately as follows:

| | | |
|------------------------------------|----|-------------------|
| Rent, Light, and Heat | \$ | 3,900.00 |
| Reference Books | | 100.00 |
| Personnel: Chief | | 6,000.00 |
| 10 Code & Cipher Experts @ \$3000. | - | 30,000.00 |
| 15 Code & Cipher Experts @ 2000. | - | 30,000.00 |
| 25 Clerks @ 1200. | - | 30,000.00 |
| | \$ | <u>100,000.00</u> |

3. The placing of \$40,000.00 annually at the disposal of the Director of M. I. D. by the State Department and the authorization of the Secretary of War for the annual expenditure by the Director of M. I. D. on confidential memorandum of \$60,000.00 of funds pertaining to "Contingency Military Intelligence Division, General Staff" would make possible the execution of the plans outlined above.

M. Churchill

M. Churchill,
Brigadier-General, General Staff,
Director of Military Intelligence.

vhj

WAR DEPARTMENT

THE ADJUTANT GENERAL'S OFFICE

WASHINGTON

IN REPLY
REFER TOAG 311.5 (4-14-30)
Pub.SSL-AWO
April 22, 1930.

SUBJECT: Codes, Ciphers, Secret Inks, Radio
Interception and Goniometry.

To: THE CHIEF SIGNAL OFFICER.

1. With reference to the responsibilities devolving upon the Chief Signal Officer in accordance with Army Regulations 105-5, and Changes No. 1 thereto, dated May 10, 1929, the following statement of War Department policies is transmitted.

2. a. Army Regulations 105-5 as amended by Changes No. 1, places the responsibility for the following activities upon the Chief Signal Officer:

- (1) Code and Cipher Compilation.
- (2) Code and Cipher Solution.
- (3) Interception of enemy radio and wire traffic.
- (4) Location of enemy radio transmitting stations by goniometric means.
- (5) Laboratory arrangements for the employment and detection of secret inks.

b. The fundamental reason for placing the responsibility for these duties upon the Chief Signal Officer is that all correlated duties in connection with secret communication may be assigned to one operating agency for efficiency of operation. To serve this purpose these duties will be organized by the Chief Signal Officer into a single coordinated service.

✓ c. Within the discretion of the Chief Signal Officer it is suggested that "Signal Intelligence Service" be the designation for this coordinated service.

3. The general mission of this service is, as for all other military services, the proper organization and development in peacetime to the end that the service may be prepared to operate at maximum efficiency in war.

4. The specific missions of this service may be stated as follows:

a. The preparation and revision of all codes, ciphers and other means of secret communication to be employed by the Army in time of peace and war.

✓ Note: In this connection it should be noted that in accordance with current Army Regulations this office is responsible for the printing of codes

0050
311.5
AG 311.5 (4-14-30)

TAB
E

and ciphers, for their distribution in accordance with distribution tables prepared by the Chief Signal Officer, and for their accounting.

b. In time of war the interception of enemy communications by electrical means, the location of enemy radio transmitting stations by goniometric means; and in peace time the necessary organization and training of personnel and the necessary development of equipment to render this service capable of immediate operation in war.

c. In time of war the solution of all secret or disguised enemy messages or other documents that may be intercepted by the Army, or forwarded by other agencies to the Army for solution; and in peace time the necessary research work, and the organization and training of personnel to render this service capable of immediate operation in time of war.

d. Laboratory arrangements for the detection of intercepted enemy documents written in secret ink, and for the selection and preparation of secret inks to be employed by authorized agents of our own forces in time of war; and in peace time the necessary research work to render this service capable of immediate operation in war.

5. Upon mobilization the various activities of this service will operate at the following headquarters:

a. Under the War Department:

(1) The preparation of all means of secret communication employed by the Army in peace and war including secret inks, except that, upon its organization, GHQ will begin the preparation of field codes and ciphers required for current replacement for subordinate units.

(2) The interception of enemy communications by electrical means, including the necessary goniometric work incident thereto.

(3) The detection and solution of secret or disguised enemy communications including those written in code, cipher, secret ink or those employing other means for disguise.

b. At General Headquarters:

(1) The preparation of field codes and ciphers for employment by subordinate units to replace those previously prepared under the War Department during peace time.

(2) The interception of enemy communications by electrical means.

(3) The location of enemy radio transmitting stations by goniometric means.

(4) The detection and solution of secret or disguised enemy

communications including those written in code, cipher, secret ink or those employing other means for disguise.

c. At Headquarters of Field Armies:

(1) The interception of enemy communications by electrical means.

(2) The location of enemy radio transmitting stations by goniometric means.

(3) The solution of intercepted enemy code or cipher messages by the assistance of cipher keys and solved codes as furnished by the service at General Headquarters.

6. Based upon the policies expressed above the Chief Signal Officer will submit at a conveniently early date a recommended draft for an Army Regulation to cover the functions and duties of this service. He will also take the necessary steps to draw up such additional regulations to cover the activities of this service as he deems appropriate for publication.

7. Peace Time Objectives:

In addition to the provisions expressed above, efforts to attain ultimate peace time objectives with reference to certain activities of this service will be made by the Chief Signal Officer as outlined in the following paragraphs.

a. Code Compilation.

(1) The ultimate aim of this activity is the preparation of authorized codes, satisfactory in character and sufficient in the number of copies and editions, for employment by the Army during both peace and war. Upon the outbreak of war it will become necessary for purposes of secrecy to change certain characteristics of the codes employed during peace, and the required number of copies of each code will be greatly increased. Since the preparation and publication of codes requires considerable time, it would be improvident to wait till the outbreak of war to begin this work.

(2) Therefore, as a peace time objective, the Chief Signal Officer will make the necessary arrangements to the end that as funds become available there will be at all times in the possession of this office for immediate distribution one edition of each authorized secret code, with cipher tables if necessary, and in the possession of the Chief Signal Officer two reserve editions of such codes and cipher tables.

b. Code and Cipher Solution.

(1) The ultimate peace time objective of this activity is the training of sufficient personnel to the end that they will be expert in solving enemy code and cipher messages in war. It is evident that much time will be required for this training. Also, since large commands

require the operation of this activity in the conduct of their peacetime training, it is necessary that it operate for them during their training exercises, such as during the joint Army and Navy Maneuvers held periodically in the Hawaiian and Panama Canal Departments and on the Atlantic seaboard, or during combined maneuvers in the Eighth or other Corps Areas. It is evident therefore that the peacetime organization and training of this activity should contemplate, first, training personnel, and second, furnishing specialists to large commands for peacetime maneuvers after personnel has been sufficiently trained. To accomplish this end it would seem that, at the present inception of this new service, its peacetime training should be centralized under the office of the Chief Signal Officer, and that the comparatively small number of trained personnel required should be sent to corps areas and departments for assignment only for the period of maneuvers, and upon completion of maneuvers should be returned to the office of the Chief Signal Officer. This procedure insures the necessary continuity of their initial training under the Chief Signal Officer, whose office is the only military agency at the present time qualified to carry it on. However, each corps area or department which requires this service should be in a position ultimately to function independently with reference to it. It would seem therefore that the Chief Signal Officer should be prepared to furnish trained specialists of this service for permanent assignment to such corps areas and departments as the War Department may later decide, when the training has progressed to such extent that sufficient personnel are able to function as independent units.

(2) The peacetime organization and training of this service will be based on the procedure as indicated above.

c. Radio Intercept.

(1) This activity is very closely related in its operation to code and cipher solution, in that the interception of enemy messages answers no purpose unless the messages are solved, and on the other hand, the solution service depends primarily upon the activities of the intercept service for work material. It is evident therefore that the operation of both services should be carried on in close liaison. Hence the ultimate training of both services involves mutually coordinated operation.

(2) The chief peacetime problems confronting the radio intercept service are first, the development of equipment, and second, the development of the technique of the operating personnel. The second is incident to the first and may be considered as one with it. It is evident that there is the same need for this service as for the code and cipher solution service in the peacetime maneuvers of large commands. It is also a possibility that during peacetime or during periods of strained relations the War Department or Commanders of Departments and of certain corps areas may desire the operation of this service, provided the services of a code and cipher solution agency can be made available. It is also

evident that the practical operation of this service is regional and cannot be concentrated in any locality as can the code and cipher solution service. In other words intercept stations must be located at certain critical points where their operation may be effective, such as within departments or certain corps areas, while the code and cipher solution service may be located in Washington or any other place, provided proper communication facilities may be made available between the two services.

(3) It would seem therefore that the peace time activity of the radio intercept service should be directed toward objectives stated in chronological sequence as follows:

(a) The development of equipment directly under the Chief Signal Officer.

(b) The location of an intercept station to be prepared to operate directly under the Chief Signal Officer.

(c) When equipment has been developed and obtained in sufficient quantity, the location of stations at critical points as follows, in the Hawaiian, Panama Canal and Philippine Departments, and in the Eighth and Ninth Corps Areas; these stations to operate under the department and corps area commanders concerned; the Chief Signal Officer to recommend when such stations should be established, at which time the matter will be taken up by the War Department with department and corps area commanders concerned.

(4) It is contemplated that

(a) should certain interceptions be desired by the War Department, which condition does not exist at the present time, the Chief Signal Officer will be called upon to recommend what station or stations can best perform the service, and the War Department will issue necessary instructions.

(b) Should interceptions be desired by department or corps area commanders concerned, they will obtain them by means of the facilities under their control.

(c) Messages in code or cipher intercepted by stations under the control of the Chief Signal Officer will be transmitted for solution to the code and cipher solution service operating under him.

(d) Messages in code or cipher intercepted by stations under control of department or corps area commanders will be transmitted by mail to the War Department for solution by the code and cipher solution section operating under the Chief Signal Officer until such time as a code and cipher solution service shall have been established under the control of the department or corps area commanders concerned.

(5) The peace time organization and training activities of the radio intercept service will be based upon the provisions contained in this paragraph. (c)

d. Goniometry.

Goniometric work in its results may be considered as divided into two phases, one which is supplemental to radio interception, and one which gives the location of enemy radio transmitting stations and thus indicates the enemy's tactical disposition. The work of these two phases, while serving two different purposes, is performed by the same or similar equipment and personnel. The chief peace time problem of the goniometric service is the same as that of the radio intercept service, namely, the development of suitable equipment and methods. These close relations between the goniometric service and the radio intercept service indicate that a basis of peace time activities similar to that stated for the radio intercept service should be adopted for the goniometric service, and that the development of equipment, the organization and training of personnel, and the location of stations of the goniometric service should be carried out in a manner similar to that of the radio intercept service as outlined in paragraph c above.

e. Secret Inks.

The peace time objective of activities in connection with secret inks is the establishment of a small laboratory for the conduct of research work which will result in the war time objective of the establishment of an agency for the detection of secret inks employed by the enemy, and for the recommendation of suitable secret inks to be employed by authorized agents of our own forces.

By order of the Secretary of War:



Adjutant General.

C O P Y

May 24, 1922.

The Honorable

James W. Wadsworth, Jr.,

United States Senate.

Sir:

I am taking the liberty of addressing you on the subject of the Military Intelligence appropriations now pending before your committee in order that you may have cognizance of the very direct manner in which the interests of the Department of State are involved. My attention was first drawn to this matter through notification from the War Department of the withdrawal of a number of military attaches from our embassies and legations abroad because of a lack of funds to provide for their maintenance. Several communications have since been received from our diplomatic representatives protesting to the Department against the withdrawal of the military attaches, on the ground of their practical value in relation to the essential work of the missions.

I have thought that perhaps a word from me in this connection would serve a useful purpose in indicating the manner in which these officials, while dealing primarily with military intelligence, are really the complement of the diplomatic establishment, in which capacity they render most valuable assistance to this Department.

As you are well aware, the military factor in international questions is one of the greatest importance, especially in Europe, at

this time. No precise general view can be had of a foreign political, or economic situation without due regard to considerations of military policy and the influence which militaristic tendencies exert in national matters. It is in this domain that the military attache becomes a useful adjunct to the diplomatic mission. His contact with important personages who direct the course of military affairs, combined with the technical advice which he is able to supply are often indispensable to an intelligent understanding of the course of events in a particular country.

In the same manner the Military Intelligence Division in Washington, which has developed its facilities to a very high degree, is of the utmost value to the Department of State through the information which it is able to supply. There is a daily contact between this Department and the Military Intelligence Division of the War Department. In fact that agency is the medium of liaison, or in other words, it is the interlocking link through which the work of the two Departments is coordinated. I do not desire to have the appearance of intruding in a matter relating to the appropriations of another Department but as the Military Intelligence Division, and especially the military attaches, really serve both Departments I feel that an expression of my views may serve a useful purpose in establishing the facts for your consideration.

I have the honor to be, Sir,

Your obedient servant,

(signed) Charles E. Hughes.

(Note: In a closed session the Director of Military Intelligence presented the attached memo. and exhibits mentioned therein. W.F.F.)

(Then Secretary of State. W.F.F.)

it was made available can hardly be estimated. Information of equal importance was missed in 1917 because of our lack of an efficient code and cipher section.

Codes and ciphers are constantly developing. Even a temporary stop in the work means losing touch with current changes. It is like the loss of a link in a chain or a cog in a wheel.

TO DISCONTINUE OUR CODE AND CIPHER SECTION NOW WILL, ALMOST CERTAINLY, MEAN THAT WE WILL ENTER THE NEXT WAR AS POORLY PREPARED FOR THE HANDLING OF THE ENEMY'S SECRET MESSAGES AS WE WERE IN 1917.

~~SECRET~~ NEED FOR A CODE AND CIPHER SECTION.

SECRECY IN REGARD TO A CODE AND CIPHER SECTION IS
ESSENTIAL TO ITS SUCCESS. THE FACT OF ITS EXISTENCE SHOULD NEVER
BE MENTIONED PUBLICLY AND UNNECESSARILY.

In 1917 and 1918 the solution of many important messages was so delayed due to our lack of preparation and previous study that much of their value was lost. Studies are now continuously under way which if continued will, it is believed, prevent a similar delay in the future.

Had we, for example, been able to read the one message (Exhibit No. 1) ordering the disabling of German ships in American ports as promptly as we could now read similar messages the saving alone would have been sufficient to maintain the code and cipher section on a peace basis for many years.

In 1918 our code and cipher section had so improved that messages of vital and immediate importance were read in time to be of the greatest value. Examples of these are orders for attack or retreat knowledge of which enabled our troops to take full advantage of movements on the part of the enemy. On November 2nd, 1918 a German Radio message gave plans for a general withdrawal from Roumania on account of lack of ammunition and other supplies. This message was intercepted by an American Radio Station, deciphered and translated and placed in the hands of the Supreme War Council within 48 hours. The importance of such information at the time

G-2/65-9-D-2

G-2
OSA

APR 29 1929
65-9D-2
4 1929
WAR DEPARTMENT

Handwritten notes and stamps on the right margin, including a large 'C' and the number '11-5'.

MEMORANDUM FOR THE CHIEF OF STAFF:

TAB
C

Subject: Responsibility for the Solution of Intercepted Enemy Secret Communications in War.

I. The problem presented.

Should the Signal Corps be charged with the solution of enemy code or cipher messages and the detection of enemy secret ink documents intercepted in time of war?

II. Facts bearing upon the problem.

1. Under present policies G-2 is charged with the solution of code and cipher messages and the detection of secret ink documents of the enemy intercepted in war or other emergency which requires such action.

2. Under present policies, the Signal Corps is charged with the compilation of codes and ciphers for use by the Army, and with the interception of enemy radio traffic which includes enemy code and cipher messages.

3. It is apparent that the operation of a code and cipher solution service and a service for the detection of secret inks is not a normal General Staff function as contemplated by the National Defense Act, but is an operating function which should be performed by an existing service branch if practicable. The present policy which charges these duties to G-2 is a continuance of World War policy which was adopted in haste and in accordance with the exigencies of the situation existing at the time.

4. All of the afore mentioned duties, viz., code and cipher solution, code and cipher compilation, code and cipher interception, and the detection of secret inks, are very closely correlated. From the viewpoint of efficiency in operation these duties should be assigned to one operating agency so that they may be organized into a properly coordinated whole. The present assignment of these closely allied duties makes for a division of responsibility between G-2 and the Signal Corps which presents

difficulties, particularly in connection with organizing and training in time of peace for war. It seems logical, therefore, that the Signal Corps should be charged with all phases of this work to the end that it may be properly coordinated as an organized entity, and still remain as at present under the General Staff control and supervision of G-2.

III. Action recommended.

The Secretary of War directs:

1. That the Signal Corps be charged with the duties pertaining to the solution of enemy codes and ciphers and the detection of secret inks in war, in addition to those duties with which they are now charged pertaining to the compilation of codes and ciphers required by the Army and to the interception of enemy radio and wire traffic in war.

2. That the Handbook for the War Department General Staff of October, 1923, Chapter III, paragraph under "Communications Section" on pages 21 and 22 be changed to read as follows:

"This section is charged with the formulation of War Department policies relative to codes and ciphers and with the supervision of all means of secret and confidential communication in the Army. It supervises the preparation of codes and ciphers for use in peace and war and attempts the solution of enemy codes and ciphers and secret ink documents in war--it arranges with the Signal Corps for the interception of enemy radio traffic, and in time of war supervises the interception of enemy radio and wire traffic, the solution of enemy codes and ciphers, and the detection and employment of secret inks."

3. That Army Regulations 105-5, paragraph 2e, specifying in part the duties of the Chief Signal Officer, be changed to read as follows:

"e. The preparation and revision of the War Department ~~Telegraph Code and other codes and ciphers required by the Army.~~ all codes and ciphers required by the Army, and in time of war the interception of enemy radio and wire traffic, the goniometric location of enemy radio stations, the solution of intercepted enemy code and cipher messages, and laboratory arrangements for the employment and detection of secret inks."

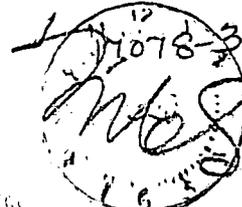
IV. Concurrences.

- A. C. of S., G-1
- A. C. of S., G-3
- A. C. of S., G-4

War Plans Division

The Chief Signal Officer (IM)

-) concurs.



APR 4 1929

By Order of the Secretary of War
(Sgd) C. P. STUBBS
General
Chief of Staff

A. G. O. APR 5 1929

STANLEY H. FORD,
Colonel, General Staff,
A. C. of S., G-2.

OFFICE OF CHIEF OF STAFF



OUT

APR 5 1929

APR 5 1929

ghm

G-2/65-9-D-2

C O P Y

/April 4, 1929

MEMORANDUM FOR THE CHIEF OF STAFF:

Subject: Responsibility for the Solution
of Intercepted Enemy Secret Com-
munications in War.

I. The problem presented.

Should the Signal Corps be charged with the solution of enemy code or cipher messages and the detection of enemy secret ink documents intercepted in time of war?

II. Facts bearing upon the problem.

1. Under present policies G-2 is charged with the solution of code and cipher messages and the detection of secret ink documents of the enemy intercepted in war or other emergency which requires such action.

2. Under present policies, the Signal Corps is charged with the compilation of codes and ciphers for use by the Army, and with the interception of enemy radio traffic which includes enemy code and cipher messages.

3. It is apparent that the operation of a code and cipher solution service and a service for the detection of secret inks is not a normal General Staff function as contemplated by the National Defense Act, but is an operating function which should be performed by an existing service branch if practicable. The present policy which charges these duties to G-2 is a continuance of World War policy which was adopted in haste and in accordance with the exigencies of the situation existing at the time.

4. All of the afore mentioned duties, viz., code and cipher solution, code and cipher compilation, code and cipher interception, and the detection of secret inks, are very closely correlated. From the viewpoint of efficiency in operation these duties should be assigned to one operating agency so that they may be organized into a properly coordinated whole. The present assignment of these closely allied duties makes for a division of responsibility between G-2 and the Signal Corps which presents

C P P Y

difficulties, particularly in connection with organizing and training in time of peace for war. It seems logical, therefore, that the Signal Corps should be charged with all phases of this work to the end that it may be properly coordinated as an organized entity, and still remain as at present under the General Staff control and supervision of G-2.

III. Action recommended.

The Secretary of War directs:

1. That the Signal Corps be charged with the duties pertaining to the solution of enemy codes and ciphers and the detection of secret inks in war, in addition to those duties with which they are now charged pertaining to the compilation of codes and ciphers required by the Army and to the interception of enemy radio and wire traffic in war.

2. That the Handbook for the War Department General Staff of October, 1923, Chapter III, paragraph under "Communications Section" on pages 21 and 22 be changed to read as follows:

"This section is charged with the formulation of War Department policies relative to codes and ciphers and with the supervision of all means of secret and confidential communication in the Army. It supervises the preparation of codes and ciphers for use in peace and war and attempts the solution of enemy codes and ciphers and secret ink documents in war. It arranges with the Signal Corps for the interception of enemy radio traffic, and in time of war supervises the interception of enemy radio and wire traffic, the solution of enemy codes and ciphers, and the detection and employment of secret inks."

3. That Army Regulations 105-5, paragraph 2e, specifying in part the duties of the Chief Signal Officer, be changed to read as follows:

"e. The preparation and revision of the War Department Telegraph Code and other codes and ciphers required by the Army, all codes and ciphers required by the Army, and in time of war the interception of enemy radio and wire traffic, the goniometric location of enemy radio stations, the solution of intercepted enemy code and cipher messages, and laboratory arrangements for the employment and detection of secret inks."

IV. Concurrences.

| | | |
|--------------------------|---|---------|
| A. C. of S., G-1 | } | concur. |
| A. C. of S., G-3 | | concur. |
| A. C. of S., G-4 | | concur. |
| War Plans Division | | concur. |
| The Chief Signal Officer | | concur. |

This was approved by General Sumnerall, C of S, on April 5, 1929.

STANLEY H. FORD,
Colonel, General Staff,
A. C. of S., G-2

approved copy files 'w. S. J. in G-2

MILITARY INTELLIGENCE DIVISION

Replying refer to

WAR DEPARTMENT
OFFICE OF THE CHIEF OF STAFF
WASHINGTON

G-2
OSA

65-9D-2-150

March 18, 1929.

MEMORANDUM FOR COLONEL FORD;

Subject: Memorandum for the Chief of Staff
submitted herewith.

TAE
D

1. In connection with the memorandum for the Chief of Staff submitted herewith for your approval recommending that the Signal Corps be charged with the solution of codes and ciphers and the detection of secret ink documents of the enemy intercepted in war, the following amplifying comments are submitted.

2. a. When analysed it is evident that code and cipher compilation, code and cipher solution, code and cipher interception, and the detection of secret inks are very closely allied duties, both from the viewpoint of technique and also of practical operation.

b. In technique the solution of enemy codes and ciphers is very closely related to the compilation of codes and ciphers for use by our own forces, since similar principles are applied in both and operatives in either line of work must be expert in both.

c. In its operation, the solution of enemy codes and ciphers is very closely related to the work of compiling codes and ciphers for our own use, since for secrecy's sake our own codes and ciphers should not be similar in construction and form to enemy codes and ciphers; and closely related to the work of intercepting enemy code and cipher messages, since the particular enemy stations which are sending the type of code or cipher messages desired for solution must be selected for interception; and closely related to the work of detecting enemy documents written in secret ink, since both classes of work, though differing in technique, are in the same category with reference to their operations, that is, both are solutions of secret enemy communications.

3. a. In connection with the difficulties of organizing and training in these duties, which difficulties are increased

-2

by the present division of responsibility with reference to them, the following comments seem pertinent.

b. The work of cryptanalysis (code and cipher solution and its correlary; compilation) is highly technical and requires a high degree of training for operatives. This training requires much time and must be carried out by the Army, since there is no source in civilian pursuits from which this class of technician can be drawn. At the present time there is only one individual in the Army who is technically expert in this work, Major W. K. Friedman, Signal Reserve, who is employed in his civilian capacity by the Signal Corps and has charge of the Signal Corps Code and Cipher Compilation Section in the Office of the Chief Signal Officer.

c. In time of war a corps of expert operatives will be required in the War Department for both compilation and solution of codes and ciphers, and also for the solution of codes and ciphers at General Headquarters in the Theatre of Operations and at the Headquarters of Field Armies. Peacetime preparation requires the training of such personnel and their tentative organization into units. Under present arrangements, G-2 of the War Department has no expert to conduct this training, and in the past has had to borrow the Signal Corps expert for such limited amount of training which it has been possible to give. Moreover, the only G-2 personnel available for this training are reserve officers, who obviously cannot be made experts in this work by the comparatively small amount of training which they receive as reserve officers.

d. As an example of the consequences of these unsatisfactory conditions the status of code and cipher solution in joint Army and Navy exercises may be cited. During the last such exercise held in the New England area, the Signal Corps expert, Mr. Friedman, was borrowed by the War Department and given charge of code and cipher solution work for the exercise. He obtained the services of two officers of the MI-Reserve and one Signal Corps officer and creditably carried out such work as he could with such an extemporaneous and untrained organization. During the last joint exercises held in the Panama Canal Department and those held in the Hawaiian Department, enemy messages were intercepted but no attempt was made to solve those in code or cipher due to the absence of personnel qualified for the work.

-3

4. If the Signal Corps could be given the entire responsibility for the operation of all of these duties, it would go a long way toward smoothing out many of the present troubles. Training could be coordinated, personnel could be assigned for training, and in time arrangements could be made for qualified personnel at headquarters carrying on joint or other maneuvers requiring this work. G-2 would of course, continue to get out policies for and to supervise this work as at present. Of course, results from this change would not be apparent probably for some time, but it is thought that these recommendations are the first step in the proper direction.



W. K. WILSON,

Lieutenant Colonel, General Staff,
War Plans and Training Section.1 Incl.
Memo. for
Chief of Staff.

~~SECRET~~

O. C. S. O.

IN REPLY
REFER TOWAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON2-18-36
Date 8H.P.R.
Initials

February 18, 1936

MEMORANDUM FOR: The Chief Signal Officer.

SUBJECT: Increase in personnel for the Signal Intelligence Service.

I. Papers accompanying:

1. Letter to the Chief Signal Officer from The Adjutant General, dated April 22, 1930, Subject: Codes, Ciphers, Secret Inks, Radio Interception and Goniometry.
2. General Background.
3. Personnel available and required for the Signal Intelligence Service.
4. Organization of Communication Security Group (formerly Code and Signal Section) and Registered Publication Section, Navy Department.
5. Signal Corps Board Case No. 200, January 19, 1935.
6. Letter dated March 20, 1935, to The Adjutant General, Subject: Increases in Civilian Personnel, FY 1937, and 1st Ind. thereto, dated March 27, 1935.
7. Estimates for FY 1938.

II. The Problem presented:

What action by the Chief Signal Officer is necessary in order to enable him to discharge the duties prescribed by Par. 2e, AR 105-5 as amended by Changes No. 1, August 21, 1934.

III. Facts bearing on the Problem:

1. For many years the Chief Signal Officer has been charged with responsibility for compiling codes and ciphers, for locating enemy radio stations by goniometry, and for intercepting enemy electrical communications in time of war.

2. In May, 1929, responsibilities in connection with solving enemy codes and ciphers, and maintaining a secret ink laboratory were transferred from G-2 to him.

Special 320.2
+ 230
+ 200.3

(18 Feb. 36)

~~SECRET~~

3. In a letter dated April 22, 1930, the War Department set forth certain general principles for the guidance of the Chief Signal Officer in carrying out his responsibilities in these matters. A copy of this directive is attached hereto. Reference is made specifically to Pars. 2 b, 3 and 7 b thereof, and to Incl. 2, General Background.

4. In August, 1934, responsibilities in connection with the printing, storage, accounting, and distribution of codes and ciphers were transferred from The Adjutant General to him. (Changes No. 1, AR 105-5, August 21, 1934.)

5. From 1920 to 1930 the Chief Signal Officer had funds sufficient to employ but one cryptanalyst @ \$5600 per annum, and one typist at \$1440. With the additional responsibilities given him in 1929, funds were made available to employ the following total personnel:

| | |
|---|---------|
| 1 Principal Cryptanalyst, P-6 | \$5600 |
| 3 Junior Cryptanalysts, P-1, @ \$2000 | 6000 |
| 1 Cryptanalyst Aide, SP-5 | 1800 |
| 2 Asst. Cryptographic Clerks, CAF-3, @ \$1620 | 3240 |
| | <hr/> |
| Total | \$16640 |

No additional funds were furnished to provide personnel for the additional responsibilities noted in Par. 4.

6. The present duties in connection with:

a. Compilation, proofreading, storage, distribution, and accounting of codes and ciphers.

b. The activities connected with the devising and testing of cryptographic machinery,

c. The activities connected with the preparation of instructional material in cryptography and cryptanalysis and the conduct of training in the Signal Intelligence School and Army Extension Courses in these subjects,

are so numerous that the present very limited civilian personnel available to the Chief Signal Officer is not able even to keep up with these duties, let alone do any real work in cryptanalytic research and solution of current material. If these duties alone are to be properly performed, an increase in personnel is absolutely essential. An analysis of the personnel required is included in Incl. #3, Personnel Available and Required for the Signal Intelligence Service.

7. The assignment of Regular Army officers to cryptanalytic work and research on current material is impracticable because they cannot be kept on such assignments continuously and in order to develop the skill

~~SECRET~~

required for success in this specialty continuous application and long, practical experience are absolutely requisite. Reserve officers (except for those who are also civilian employees now engaged in this work in this office) will never be more than suitable, selected personnel to be trained as assistants after the emergency breaks. Hence, the civilian employee is the sole practicable answer to the problem.

8. In 1934 the matter of the peace-time development of the Signal Intelligence Service was made the subject of special study by the Signal Corps Board in Case No. 200, copy of which forms Incl. #5. The Board recommended that one (1) civilian cryptanalyst be assigned to each of the six (6) Signal Intelligence Detachments (overseas Departments, 8th and 9th Corps Areas and Fort Monmouth). The enlisted personnel for these detachments was included in the increase in the strength of the Signal Corps under the 1936 appropriation bill, but it is impossible to furnish the six civilian cryptanalysts required for these detachments until this personnel is obtained and trained by the Chief Signal Officer.

9. Under date of March 20, 1935, the Chief Signal Officer requested authority to present in connection with the 1937 estimates a requirement for two (2) Assistant Cryptographic Clerks at \$1620 per annum and two (2) Junior Cryptanalysts at \$2,000 per annum. The War Department approved the inclusion of this additional personnel in the Signal Corps preliminary estimates. The limiting figure, designated by the War Department under date of August 5, 1935, for Project No. 1 "Personnel" of the Signal Corps estimates to be submitted to the Bureau of the Budget was reduced to such a point as to necessitate the deletion of these four positions from the FY 1937 estimates. One of the contributory factors in the necessity for this deletion was, no doubt, the lack of support by representatives from the A. C. of S., G-2, whose assurance of cooperation in defense of this item had been obtained in advance, but who failed to appear at the hearing when held.

IV. Opinion of the Officer-in-Charge, War Plans & Training Division:

1. Such a serious shortage of trained personnel exists in the Signal Intelligence Service that that service cannot fully perform its peace-time mission.
2. Should this shortage of personnel be allowed to continue, no Signal Intelligence Service worthy of the name will be available during the early phases of an emergency when the most valuable results should be expected from this agency.

V. Action recommended:

1. That if funds in the amount of \$7240 accrue by savings under Project 1, FY 1937, that these savings be used for the employment of two (2) Assistant Cryptographic Clerks @ \$1620 and two (2) Junior Cryptanalysts @ \$2000, to be obtained and trained in this office as soon as possible.

~~SECRET~~

2. That if no such savings can be foreseen, funds be diverted from other projects and allocated to Project 1, FY 1937, for the foregoing purpose.

3. That estimates for FY 1938 include the funds set forth in Incl. 7, for personnel for the Signal Intelligence Service.

VI. Concurrences:

Fiscal Division (*per*) concurs, *except that application of savings on diversion of funds (per VI+2) will be dependent upon a consideration of other Sig. personnel needs*

Executive Officer () concurs. *arrived.*

W. S. Rumbough
W. S. Rumbough,
Major, Signal Corps.

Inclosures:
6 documents.

- 4 - ~~SECRET~~

~~CONFIDENTIAL~~IN REPLY
REFER TOWAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

8

320-3-8.D.B.

August 19, 1935

MEMORANDUM TO: Major Rumbough.

1. It is believed that the time has come when the Signal Intelligence activities of the Chief Signal Officer should be organized on a more extensive basis than is now the case, in order that personnel for efficient operation may be available when the situation will require their services. It is hardly necessary to point out that on account of the long period of time it takes before a real expansion can be accomplished we must begin several years in advance of the time when the funds will become available for actual expenditure. It is also essential in view of the long period of special training required for cryptanalytic personnel before they can actually do useful work.

2. There is therefore submitted herewith for your consideration an outline and a chart covering the expanded and reorganized Signal Intelligence Section. Attention has been given to the necessity for providing opportunity for advancement of Signal Intelligence personnel commensurate with the increasingly difficult and responsible duties to be performed by them as they progress in the work. This is also essential if we are going to make it worthwhile for young men with ability to devote their lives to such a restricted field as cryptography and cryptanalysis, which presents no competitive opportunities for advancement in the commercial world.

3. In my opinion, if the Signal Intelligence activities and personnel are expanded as shown on the attached organization chart, the establishment of a separate division in this office would be warranted.

4. There is attached, for comparison, a chart covering the present organization of the Signal Intelligence Section, showing the funds now expended for personnel. It should be added that we have inserted in the preliminary estimates for FY 1937 provision for two Assistant Cryptographic Clerks, CAF-3, and two Junior Cryptanalysts, P-1. These are intended for service with Radio Intelligence Detachments in the field. In any case, allowing for two years' minimum period of training, they will not be ready for actual work until about July 1939, and then they can not be expected to be experts.

5. There is also attached, for comparison, a chart covering the present organization of the Code and Signal Section, Navy Department. It should be added that the Chief of that section has recently stated that they are going to expand still further and have started to make provision for several more positions in the upper brackets of the professional grades, P-3, 4, 5 and 6.

~~CONFIDENTIAL~~

Spec 320-2 (S.S. H. [unclear]) (19 Aug 1935)

~~CONFIDENTIAL~~

6. Realizing that it will take some time before real progress can be made in the way of expansion, and that in any event a nucleus for that expansion must be retained, I urgently recommend that steps be taken at once to bring about an administrative reclassification of the present personnel of the Signal Intelligence Section. This is not at all difficult to accomplish. It should be done in order that the present personnel may have some hope of advancement within a short time if they remain in the work, and under the Chief Signal Officer. If it is not done, soon we shall find that the Signal Intelligence Section has become merely a training ground for other departments. Incidentally, in this connection, I have it on the best authority that the cryptanalytic section of the Coast Guard is now making administrative reclassifications of their present personnel, [who were only on July 1, 1935, reclassified from subprofessional (SP-5) grade to P-1] to P-2 and P-3. Their personnel have not had either the training or experience of our own; in my opinion, with a full knowledge of their work, they are less able cryptanalysts than are our own.

7. It is also realized that the Chief Signal Officer has done all that he could with the funds available for promotions. We are about to lose one excellent man whose services we will find it very difficult to replace. It is only my sincere desire that our present organization be not completely disrupted within a year or two by other separations which leads me to urge the advisability of taking this matter up as far as possible in the War Department before becoming resigned to the impossibility of accomplishing the ends sought for herein.

William F. Friedman
William F. Friedman

Attached:

- Outline of proposed organization.
- Chart of proposed organization
- Chart of present organization
- Chart of Code & Signal Section Organization.

~~CONFIDENTIAL~~

Organization and Duties
Signal Intelligence Division.

1. ADMINISTRATIVE SECTION

A. Personnel -

- 1 - Major
- 1 - Captain
- 1 - Principal Cryptanalyst P-6
- 1 - Cryptographic Clerk CAF-4
- 1 - Asst. Cryptographic Clerk CAF-3
- 1 - Multilith-mimeograph-tabulating machine operator CAF-4
- 1 - Clerk, typist CAF-2

B. Duties -

- 1 - Administration and coordination of sections of Signal Intelligence Division.
- 2 - Technical supervision and coordination of Signal Intelligence Service, including designation of specific missions of Radio Intelligence Detachments in the field.
- 3 - Liaison with signal intelligence agencies of other government departments.
- 4 - General liaison with other divisions of OCSigO.
- 5 - Liaison with MID on Signal Intelligence matters.
- 6 - Correspondence and files of division.
- 7 - Reproduction and distribution of copies of documents for all sections of the Division.
- 8 - Maintains reference library and information center for Signal Intelligence Division, including information, maps, charts, and documents

Amk. 11

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

pertaining to communication systems of the world and the International Telecommunications Union.

- 9 - Preparation of special reports as required.
- 10 - Preparation of material and participation in work of Army-Navy Committees on signal intelligence matters.
- 11 - Preparation of unit plans for signal intelligence activities under war plans and general mobilization plans.

2. CRYPTOGRAPHIC SECTION

A. Personnel:

- 1 - Cryptanalyst P-4
- 1 - Junior Cryptanalyst P-1
- 1 - Asst. Cryptographic Clerk CAF-3

B. Duties:

- 1 - Compilation, production and revision of all codes, cipher tables, cipher keys, and cipher alphabet strips.
- 2 - Direction and coordination of new codes and ciphers, and changes of editions of codes, ciphers, cipher tables, cipher keys employed in the military establishment.
- 3 - Proofreading of cryptographic and cryptanalytic publications.
- 4 - Design of cryptographic systems, apparatus, and mechanisms; preparation of patents covering new apparatus, and liaison with Signal Corps Patents Section.
- 5 - Liaison with Government Printing Office on printed cryptographic publications.
- 6 - Technical liaison with cryptanalytic section, with communications security section, and with other arms and services and with Signal Corps personnel in connection with design and service testing of

new codes, ciphers, cipher machines, and improvements in our own systems of secret communication.

- 7 - Studies in connection with improvements and new developments in use of tabulating machinery for cryptographic and cryptanalytic work.

3. CRYPTANALYTIC SECTION

A. Personnel:

- 1 - Lieut. (language officer)
- 1 - Senior Cryptanalyst P-5
- 1 - Cryptanalyst P-4
- 1 - Associate Cryptanalyst P-3
- 1 - Asst. Cryptanalyst P-2
- 1 - Junior Cryptanalyst P-1
- 1 - Cryptanalyst Aide SP-5
- 1 - Senior Cryptographic Clerk CAF-5
- 1 - Cryptographic Clerk - CAF-4

B. Duties:

- 1 - Solution of intercepted traffic.
- 2 - Translation of solved messages when required, and research in foreign languages in connection with cryptanalysis.
- 3 - Research in cryptanalysis and preparation of technical papers based thereon.
- 4 - Intercept traffic analysis, including research in radiogoniometry, means and methods of locating fixed or mobile stations. Technical liaison with field radiocompass stations.

~~CONFIDENTIAL~~

- 5 - Liaison with cryptographic section and with communications security and training section in connection with improvements in communication security measures and in training problems arising out of cryptanalytic studies.

4. COMMUNICATIONS SECURITY AND TRAINING SECTION

A. Personnel:

- (1) Captain
- 1 Cryptanalyst P-4
 - 1 Asst. Cryptographic Clerk CAF-3
 - 1 Clerk, typist CAF-2

B. Duties:

- 1 - Conducts Signal Intelligence School for training of regular army, reserve officers, enlisted, and new civilian personnel of Signal Intelligence Service in all phases of signal intelligence and communications security.
- 2 - Conducts Army Extension subcourses in signal intelligence work.
- 3 - Prepares instructional manuals on signal intelligence and communications security subjects.
- 4 - Prepares and delivers lectures at service schools on signal intelligence and communications security.
- 5 - Supervises communications security in the military establishment, including War Department Message Center.
- 6 - Technical liaison with Fort Monmouth in training of radio intelligence personnel at the Signal Corps School.
- 7 - Analysis of our own traffic for purposes of communication security.
- 8 - Technical liaison with cryptanalytic section and cryptographic section in connection with improvements in our own codes and ciphers arising

out of communication security studies.

5. REGISTERED PUBLICATIONS SECTION

A. Personnel:

- (1) Captain
Assistant
1/Cryptographic Clerk CAF-3
- (1) Clerk, typist CAF-2

B. Duties:

- 1 - Storage of registered cryptographic publications, including supervision of measures for safeguarding vaults.
- 2 - Issue of registered cryptographic publications, including preparation of distribution tables based upon current needs and war plans.
- 3 - Accounting of cryptographic publications.

6. SECRET INKS AND SECRET SIGNALLING SECTION

A. Personnel:

- 1 - Chemist-Physicist P-2
- (1)- Clerk, typist CAF-2

B. Duties:

- 1. Operation of secret ink laboratory.
- 2. Research in preparation and detection of secret inks.
- 3. Collection, evaluation and preparation of information on systems of secret signaling, including radio, optical, acoustical and thermal methods.
- 4. Technical liaison with Signal Corps Laboratories in regard to research in subjects mentioned under 3.

~~CONFIDENTIAL~~

Administrative Section

1 Major
 1 Captain
 1 Principal Cryptanalyst P-6
 1 Cryptographic Clerk CAF-4
 1 Asst. Cryptographic Clerk CAF-3
 1 Multilith-mimeograph-tabulating
 Machine Operator CAF-4
 1 Clerk, typist CAF-2

Cryptographic Section

1 Cryptanalyst P-4
 1 Jr. Cryptanalyst P-1
 1 Asst. Cryptographic Clerk CAF-3

Cryptanalytic Section

1 Lieutenant (language officer)
 1 Senior Cryptanalyst P-5
 1 Cryptanalyst P-4
 1 Associate Cryptanalyst P-3
 1 Asst. Cryptanalyst P-2
 1 Jr. Cryptanalyst P-1
 1 Cryptanalyst Aide SP-5
 1 Senior Cryptographic Clerk CAF-5
 1 Cryptographic Clerk CAF-4

Communications Security and
Training Section

(1) Captain
 1 Cryptanalyst P-4
 1 Asst. Cryptographic Clerk CAF-3
 1 Clerk, typist CAF-2

Registered Publications Section

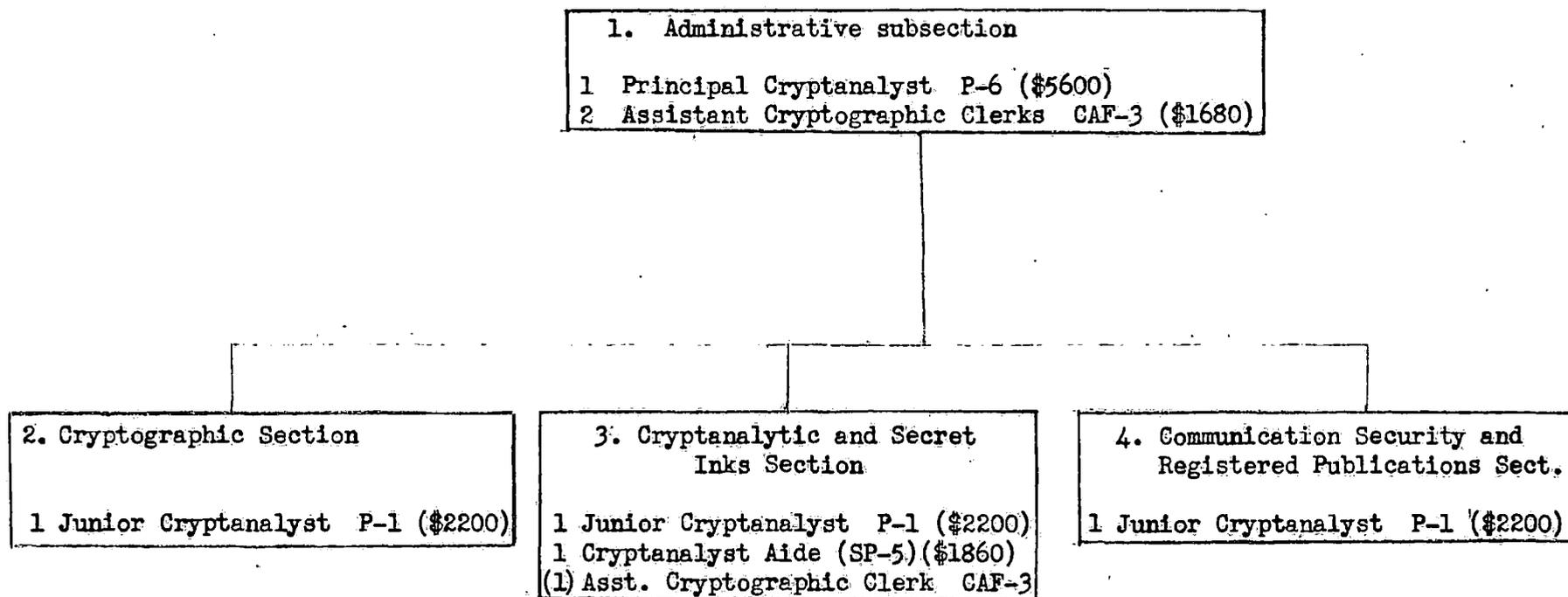
(1) Captain
 1 Asst. Cryptographic Clerk CAF-3
 (1) Clerk, typist CAF-2

Secret Inks and Secret
Signalling Section

1 Chemist-Physicist P-2
 (1) Clerk, typist CAF-2

~~CONFIDENTIAL~~

PRESENT ORGANIZATION OF SIGNAL INTELLIGENCE SECTION

~~CONFIDENTIAL~~

Total payroll: \$17,420 per annum.

~~CONFIDENTIAL~~

TOTAL PERSONNEL

Commissioned:

- 1 - Major
- 1 - Captain
- 1 - Lieutenant
- 3 - Total commissioned

Civilian:

| | | |
|---|---------------------------|-------------------|
| 1 Principal Cryptanalyst P-6 | (\$5600-\$6400) | (\$5600-\$6400) |
| 1 Senior Cryptanalyst P-5 | (\$4600-\$5200) | (\$4600-\$5200) |
| 3 Cryptanalysts P-4 | (\$3800-\$4400) | (\$11400-\$13200) |
| 1 Associate Cryptanalyst P-3 | (\$3200-\$3700) | (\$3200-\$3700) |
| 1 Assistant Cryptanalyst P-2 | (\$2600-\$3100) | (\$2600-\$3100) |
| 2 Junior Cryptanalysts P-1 | (\$2000-\$2500) | (\$4000-\$5000) |
| 1 Chemist-Physicist P-2 | (\$2600-\$3100) | (\$2600-\$3100) |
| 1 Cryptanalyst Aide SP-5 | (\$1800-\$2100) | (\$1800-\$2100) |
| 1 Senior Cryptographic Clerks CAF-5 | (\$2000-\$2500) | (\$2000-\$2500) |
| 2 Cryptographic Clerks CAF-4 | (\$1800-\$2100) | (\$3600-\$4200) |
| 4 Asst. Cryptographic Clerks CAF-3 | (1620-\$1920) | (\$6480-\$7680) |
| 2 Clerks, typist, CAF-2 | (\$1440-\$1800) | (\$2880-\$3600) |
| 1 Multilith-mimeograph-tabulating machine operator CAF-4 | (\$1800-\$2100) | (\$1800-\$2100) |
| 21 Total civilian | Grand total for salary | (\$52560-\$61880) |

~~CONFIDENTIAL~~

~~SECRET~~

COPY 2

SIGNAL INTELLIGENCE SERVICE

A BRIEF HISTORY
OF THE
SIGNAL INTELLIGENCE SERVICE

1942

BY

WILLIAM F. FRIEDMAN

ARMY SECURITY AGENCY

WASHINGTON, D. C.

~~SECRET~~

REF ID:A4148493

~~SECRET~~

| | |
|---|------------|
| Do NOT Destroy Return to the NSA Technical Library when no longer needed | |
| S-2049 | Copy No. 1 |

RECORD COPY
DO NOT DESTROY OR ALTER

~~SECRET~~

A BRIEF HISTORY OF THE SIGNAL INTELLIGENCE SERVICE

1. Prior to June 1917 no department of the Government conducted any cryptanalytic activities whatsoever. From June 1916 to about December 1920 a considerable amount of work along these lines was conducted purely as a patriotic enterprise and at his own expense by Mr. George Fabyan, whose Riverbank Laboratories at Geneva, Illinois, organized and provided elementary training for a small group of amateur cryptanalysts to work upon such codes and ciphers as were forwarded by the War, Navy, State, and Justice Departments. The group soon became somewhat proficient and grew in numbers, at one time reaching 30 persons. The undersigned directed the cryptanalytic operations and training at the Riverbank Laboratories from the time of the inception of this work until its close thereat in 1920, except for a period of a year (May 1918 - May 1919) when he was 1st Lieut., MID, serving at GHQ-ARF in the German code solving section.

2. a. In June 1917 the cryptanalytic activities of the War Department were initiated by Colonel Van Deman, G-2, with the commissioning of H. O. Yardley, a telegrapher at the State Department, who had taken some interest in cryptography, and was given two civilian employees to assist him. The work grew rapidly and by the autumn of 1917 the increased staff was organized as a section designated as MI-8, which was subdivided into six subsections:

- Subsection 1. Code and cipher solution
- " 2. Code and cipher compilation
- " 3. Training
- " 4. Secret inks
- " 5. Shorthand and miscellaneous
- " 6. Communications (for MID only).

b. The functions and duties of these six subsections may be briefly outlined:

(1) The code and cipher solution subsection was what would now be called the cryptanalytic subsection. It was the largest of the subsections of MI-8 and performed the cryptanalytic work not only for the War Department but also for all other Government departments, including Navy, State, Justice, and the two censorships--Cable and Postal, which were then separate organizations.

(2) Despite the fact that under Army regulations the compilation and revision of codes was a function of the Chief Signal Officer, compilation activities under the Signal Corps were apparently in a moribund state. Information having been received that the Germans possessed copies of the War Department Telegraph Code, MI-8 deemed it advisable to establish a code compilation subsection, and that subsection produced several codes

~~SECRET~~

such as Military Intelligence Codes No. 5 and No. 9, small pocket codes for secret agents, and the like.

(3) In addition to training our own personnel, MI-8 trained the majority of the personnel sent overseas for cryptanalytic duties with field forces, both AEF and Siberia. It must be mentioned, however, that approximately 85 officers were trained at Riverbank Laboratories, where a six-week training course in cryptanalysis was given these officers prior to their shipment overseas.

(4) A laboratory was established for the preparation of invisible inks for use by our own agents. It also examined letters for secret writing and an average of over 2000 letters per week were examined for the military and postal censorship from July 1, 1918 to February 1, 1919.

(5) The shorthand subsection was organized to handle captured documents and texts in various shorthand systems, especially German, which had to be deciphered. This was in fact the first subsection organized in MI-8, when censorship began sending (October 1917) letters and documents supposed to be in cipher but which turned out to be in shorthand. In June 1918 the AEF requested 15 expert stenographers who could take down verbatim examination of German prisoners. The required number was found and shipped. This subsection also provided trained linguists for MI-8 and the AEF.

(6) The communications subsection was established in MI-8 for handling messages to and from military attaches and intelligence officers serving abroad. In a period of nine months it sent and received about 25,000 such messages, practically all in code.

3. At the height of its development, which was reached in November 1918, MI-8 was, for those days, a rather large unit, consisting of 18 officers, 24 civilian cryptographers and cryptanalysts, and 109 typists and stenographers. The time had come for the establishment of a definite policy for the future. Now, the guiding heads of Military Intelligence at that time fully recognized the high importance and value of the services rendered by the MI-8 cryptanalytic bureau, because they had been in positions where the products of the daily activities of the bureau came directly to their notice and they could not fail to note the influence and bearing which the work had, not only upon the military and naval, but also upon the diplomatic, political, and economic phases of the conduct of the war. They therefore had practical experience in the matter and could bring the weight of their position of influence and their actual experience to bear upon those in charge of the purse strings, with the result that they were able to obtain funds sufficient to keep a fairly large organization intact for a year or two. An annual appropriation of \$100,000 was recommended in a memorandum for the Chief of Staff from the A. C. of S., G-2, dated May 16, 1919, (Tab A attached) to be used as follows:

~~SECRET~~

~~SECRET~~

| | | |
|----------------------------|-----------|---------------|
| Rent, light and heat | \$ | 3,900 |
| Reference books | | 100 |
| Personnel: Chief (Yardley) | | 6,000 |
| 10 code and cipher experts | @ \$3,000 | 30,000 |
| 15 code and cipher experts | @ \$2,000 | 30,000 |
| 25 clerks | @ \$1,200 | 30,000 |
| | | <u>30,000</u> |
| | | \$ 100,000 |

The item for "rent, light, and heat" is explainable when it is noted that the bureau was to be moved from Washington with a view to hiding its existence. Of the \$100,000 recommended, the State Department was to provide \$40,000 and \$60,000 was to be provided for expenditure by the A.C. of S., G-2 on "confidential memoranda" against funds pertaining to "Contingency Military Intelligence Division" — that is, by vouchers not subject to review by the Comptroller General. The paper containing the recommendations made by the A. C. of S., G-2 to the Chief of Staff was "OK-ed" and initialled by Acting Secretary of State Polk on May 17, 1919, and within three days of the initiation of the paper (May 19) it was approved by the Secretary of War over the signature of General March, Chief of Staff. (see top sheet of Tab A). Next came the question of actually obtaining the funds. Just how difficult this turned out to be I do not recollect, if I ever did know. (I don't think there was much difficulty. I was offered a very good position in the organization but, for reasons not pertinent to this paper, was forced to decline.) However, the necessary funds were obtained. The plan was put into effect, the bureau was installed in a private house at 22 East 38th Street, New York City, and all personnel together with existing records were moved thereto.

4. The foregoing funds took care of the bureau for the FY 1920, but when in June 1920 it came time to set up the budget for FY 1921, the purse strings were already beginning to be pulled tighter. Many of the "old-timers" in G-2 had gone to other assignments; those remaining and the newcomers in G-2 apparently did not have the background of the story, nor the foresight and the influence to press the matter so far as the War Department was concerned. The appropriation was at once cut in half, that is, to \$50,000, of which the State Department share still continued to be \$40,000. It is possible that the G-2 thesis was that since the work done by the bureau was primarily, if not solely, for and of interest to the State Department at that period in our affairs, all or nearly all of the funds should be provided by that department. The War Department overlooked some very important points in the situation — points which will be brought up and emphasized later in this summary. Near the close of FY 1921, when it appeared that a further contraction in funds could be anticipated, an attempt was made to obtain State Department support before Congressional appropriations committees, and

~~SECRET~~

~~SECRET~~

the A. C. of S., G-2 succeeded in getting the Secretary of State to write a letter to the Chairman of the Senate Appropriations Committee. A copy of this letter is attached as Tab B. The A. C. of S., G-2 also presented his views before the committee in closed session, during which open reference to and exhibits of cryptanalytic work were made, as evidenced by a memorandum attached to Tab B. The showing made must have been impressive, for there was not, in FY 1922, another sharp decline in funds allotted for cryptanalytic work. However, in order not to break the continuity of the history at this point, will merely be stated that year by year the funds provided for the maintenance and operation of the bureau became more and more constricted until by the autumn of 1929 the following tabulation, based upon a letter dated July 17, 1929 from Major G. S. Albright, G-2, to the Chief Signal Officer (General Gibbs), shows how the bureau had been permitted to deteriorate:

| | |
|--|-----------|
| Rent | \$ 3,000 |
| Books, postage, travel and transportation, misc. | 2,370 |
| Personnel: | |
| 1 Chief (Yardley) | 7,500 |
| 1 code & cipher expert | 3,660 |
| 1 translator (Jap) | 3,750 |
| 1 secretary | 1,800 |
| 1 clerk-typist | 1,600 |
| 1 clerk-typist | 1,320 |
| | <hr/> |
| | \$ 25,000 |

5. Of the total appropriation of \$25,000, the State Department furnished \$15,000, the War Department \$10,000. The activities of the bureau had by this time become so reduced that it was sending in only occasional translations of a few Japanese and a few Mexican diplomatic messages. No research whatsoever was conducted in cryptanalysis; there were no training activities, no intercept, no direction-finding studies, no secret ink work. The personnel consisted of six persons all told and 37% of the total payroll went to one man, who had little interest other than to continue as long as possible to maintain himself in the sinecure into which he had been permitted to establish himself. He not only had his well-paying Government position but was engaged commercially in other activities.

6. In the summer of 1929 Major G. S. Albright, Signal Corps, was assigned to G-2 to serve on the staff of the A. C. of S., G-2, to supervise and coordinate such of the cryptographic and cryptanalytic activities of the War Department as remained. After a careful study of the situation and an appraisal of how the existing cryptanalytic bureau was and was not serving the functions for which it had been or should be intended, Major Albright came to the conclusion that the entire picture was wrong. He felt that the product ("bulletin") which the bureau was turning out only intermittently was indeed of primary interest for its own sake to the State Department, and while the War Department had only a secondary interest in the "bulletin" for the information it gave, the primary interest of the War Department in

~~SECRET~~

~~SECRET~~

cryptanalytic studies in peace time was that it was intended to engage in research and to provide a means for training specialized personnel for immediate war-time effectiveness. Major Albright found that not only was there very little if any training being conducted but also that all persons in the bureau, except for one clerk receiving the least pay, were "getting along in years"--their potential usefulness for possible wartime service practically nil. Moreover, the bureau was now hidden away in a public office building in New York (under cover of the "Code Compilation Company" for alleged purposes of security) and far away from direct supervision of anybody connected with the War Department or of G-2, so that nobody knew what was going on, how the office was administered, etc. Yardley devoted most of his time to two or three private enterprises, (commercial code compilation, real estate brokerage, consultant in code matters to commercial firms) and he was having a "field day" at Government expense. There were, in addition, several other weighty factors which motivated Major Albright in preparing a G-2 study [(Tab C)] recommending that the bureau be taken out of G-2 and its functions transferred to the Signal Corps. Chief among these was the desirability, if not necessity, of placing all cryptographic and cryptanalytic work of the War Department under one agency, rather than distributing it among three (The Adjutant General, for printing, storage, issue, and accounting of codes; the Chief Signal Officer, for compiling codes and ciphers; Military Intelligence, for solution of codes and ciphers). A memorandum on the same subject was prepared by Lieut. Col. W. K. Wilson of the War Plans and Training Section of G-2, [and is also attached hereto (Tab D).] The reasons given in the G-2 study and in Colonel Wilson's memorandum were apparently deemed valid by the Chief of Staff, for Major Albright's recommendations were approved in April 1929 and steps were soon initiated by G-2 and the Chief Signal Officer to put them into effect. The recommendations carried with them merely the wording of changes to be made in AR 105-5, specifying the duties of the Chief Signal Officer, these duties being enlarged to include the printing, storage, distribution, and accounting of codes and "in time of war the interception of enemy radio and wire traffic, the geometric location of enemy radio stations, the solution of intercepted enemy code and cipher messages, and laboratory arrangements for the employment and detection of secret inks."

7. However, before anything could be done actually to transfer the activity, a new and very disturbing factor entered into the picture. In March 1929 a new administration took office, in which Mr. Stinson became Secretary of State. For a few weeks no "bulletins" from the cryptanalytic bureau in New York were given him, the intention being to "go slow" until he had become sufficiently well oriented in the duties of his office to warrant bringing to his attention the highly secret (and in the then current view, highly "unethical") activities engaged in by War and State Departments by means of funds provided in large part by the latter Department. Early in May 1929, however, the time was deemed ripe for this measure, and,

~~SECRET~~

~~SECRET~~

(according to Yardley) it was with some trepidation that a few translations of Japanese code messages were placed on Mr. Stimson's desk. There seems to be some reason to believe that his reaction was violent and his action drastic. Upon learning how the material was obtained, he characterized the activity as being highly unethical and declared that it would cease immediately, so far as the State Department was concerned. To put teeth into his decision he gave instructions that the necessary funds of the State Department would be withdrawn at once⁽¹⁾. It was only after considerable pressure by the A. C. of S., G-2 that he was dissuaded from this course, which might have had serious consequences by suddenly throwing out of employment the six people concerned, at a time of severe economic depression. For these workers had only special training in a field wholly *useless to commercial, industrial, shipping or banking firms, or to other government departments, or to educational institutions.* An arrangement was therefore made to close the office immediately so far as active work was concerned but to keep the personnel on the payroll for the time necessary to wind up affairs and get the files in shape ready to turn over to the Signal Corps. This took a couple of months, and at the end of June 1929 the employees were given three months' pay in advance in a lump sum, to tide them over the period in which they might be jobless. Since they had been paid out of "confidential funds" they had no civil service status and no retirement benefits; moreover, they were ineligible for transfer to other Government positions. Of course, the danger was that their dissatisfaction with what must have appeared to them as high-handed, arbitrary action on the part of a new official, and that their helplessness in the serious personal situation created for them in the midst of a serious economic depression by this drastic action might lead them to indiscretions which might prove most embarrassing to the Government and have serious consequences upon national defense. It turned out that whatever their private feelings, all the discharged personnel, except the chief beneficiary of the old regime, remained loyal and did the best they could to find jobs.

8. In October 1929 I was sent by the Chief Signal Officer to New York to take over the boxed up records and files of the defunct bureau and to oversee their transportation to Washington. The cryptanalytic activities, research, and training now being under the Chief Signal Officer, immediate steps were taken completely to reorganize the bureau and its work. The funds available were, of course, very slim -- only what remained of the War Department's contribution of \$10,000 for the FY 1930 was available, because the remainder of the State Department's share of \$15,000 had already been withdrawn by the State Department, as indicated above. An offer of employment was made to Mrs. Wilson, the Japanese expert with Yardley, but she was unable to accept, since it involved moving to Washington and she

(1) A number of years later (1941) Yardley told me that he had been misinformed as to Mr. Stimson's attitude and that it was really the President (Mr. Hoover) who "killed" the bureau, not Mr. Stimson. There may be some grounds for believing this, and it would be interesting to know the truth.

had a husband and child in New York. Another employee, Mr. Victor Weisskopf, had a business in New York and refused to move to Washington. The female clerical employees were deemed unsuitable for our purposes and, moreover, having no civil service status, they could not be taken on by transfer. An offer of temporary employment was made to Yardley but he refused the tender. Instead, he proceeded secretly to prepare a book which first appeared in the form of articles in the Saturday Evening Post, and later appeared in much expanded form under the title, "The American Black Chamber." The book and articles were highly sensational and made damaging disclosures concerning the most secret activities ever conducted by the Government. Before the appearance of the articles and book, however, he had taken certain steps to protect himself from possible prosecution for his disclosures, among which was to resign his commission as Major in the Military Intelligence Reserve. Of course, had the authorities understood the real purpose of his resignation they might have prevented it so as to retain some hold on him. But being in doubt or in ignorance of his real motives and deeming it just as an act of pique, the resignation was accepted. The unfortunate consequences attendant upon the publication of the book need no elaboration herein. Suffice it to say that our amicable relations with the British, who resented the disclosure of certain information obtained from them by Yardley as a commissioned officer, were disturbed; much more serious, our precarious relations with Japan were brought to a boiling point when about 30,000 copies of the Japanese translation of The American Black Chamber were sold in Tokyo in a period of less than a month (perhaps the book was subsidized by the Japanese Government itself). The bad odor into which all cryptanalysts and cryptanalytic activities fell, as a result of the difficulties which the publicity given the matter by Yardley's disclosures occasioned high government officials, had a bad effect upon the attempted reorganization of the cryptanalytic bureau by the Chief Signal Officer. Funds were hard to get, and State Department support was lacking, if not in the other direction altogether. The most serious consequences of Yardley's disclosures, however, came ten years later, and their effects can hardly be estimated. I refer here to the jolt which his book gave the Japanese cryptographers, leading them out of their blissful ignorance and causing them to develop really complex methods which are now giving us so many difficulties. The same is true probably as regards the German and Italian cryptographers -- their education has been entirely at Uncle Sam's expense and the final consequences of Yardley's work can not yet be foreseen. They may well turn out to be disastrous.

9. Without delay, as indicated in the beginning of the last paragraph, the Chief Signal Officer proceeded, as energetically as possible under the circumstances, to carry out the mission assigned to him. The reorganized code and cipher solving section was placed under the War Plans and Training Division, since the code compilation section was already there. A rather detailed directive, which was prepared by G-2 and approved by the Secretary of War (Tab E), became the guiding plan of the reorganized service, which was now named the Signal Intelligence Service. Its personnel, consisting of myself and one or two clerks, soon was augmented by a half dozen more

employees. Training literature and courses in cryptanalysis and cryptography were prepared and put into good usage at once. A great deal was done in expanding our cryptographic work also, by preparing reserve editions of existing codes, compiling and devising new codes and ciphers, developing cipher apparatus, and so on. Cryptanalytic work was put on a firm basis of research and training, with emphasis on the latter, for there existed no intercept service and the raw material could not be obtained. (Yardley had been able to get a small amount of material from the cable companies but this source had practically "dried up" by 1929 due to fear on the part of the companies.) Hence an intercept service now was organized and grew very slowly. All phases of signal intelligence were unified under one service and taken under study and action. Moreover, important cooperation with the Navy in the same type of work was also initiated. How the activity has expanded since then requires no comment at this time. However, a few words about relations with the Navy are pertinent.

10. Cryptanalytic activities in our Navy Department were practically non-existent until after the close of the last war, during which, as was noted above, whatever problems they had in cryptanalysis were referred to MI-8. But in 1921 the Navy, recognizing the important role which cryptanalysis was bound to play in the future, began building up a large unit in the Navy Department, with echelons afloat. Whereas the Army placed emphasis upon civilian training, the Navy placed emphasis upon officer training; and for each dollar the Army was able to obtain for cryptanalytic and cryptographic work the Navy was able to obtain three to five dollars, until by 1939, as far as concerned numbers of officers and civilian personnel engaged in these activities, amount of equipment on hand, and funds available for research, the Navy had considerably outstripped the Army. However, it may be said, with some justifiable pride perhaps, that while they were ahead of us in quantity, we were ahead in quality, for all the important developments in both the cryptographic and the cryptanalytic fields must be credited to Army personnel. At first, cooperation between the two services was intermittent and at times very indifferent -- the usual mutual suspicions and jealousies pervaded our relationships. But, happily, for the past four or five years cooperation has been much more wholehearted, with the result that it may now be said without reserve that, as regards their cryptographic and cryptanalytic activities, technical cooperation between the Army and Navy in these fields is so close as to be the same as though they were under one head. This, of course, is as it should be and must be in order to gain the desired result from such activities.

11. It would be of utmost value to the winning of this war if the Government were now in a position to read the codes and ciphers of all the foreign powers whose actions and probable intentions are of interest and importance in our prosecution of the war. It could have been in this fortunate position had it given to cryptanalytic studies the attention

which they deserve during peacetime and had provided funds for their continuity on a scale sufficient for the purpose for which they are intended. The matter can be summarized very succinctly in this statement: Actual or physical warfare is intermittent but signal security warfare, especially cryptanalytic warfare, is continuous. It is vital that this be understood by those who exercise the control over such studies.

12. There are four basic reasons why this continuity in cryptanalytic studies is so important. They will be discussed briefly:

(1) [It must be realized that cryptanalytic activities have no counterpart in civil life. Therefore, on the outbreak of war there is no important source from which trained, experienced personnel can be drawn for immediate usefulness. Since skill in cryptanalysis can hardly be developed in a short time and cryptanalytic units capable of producing quick results can not be improvised in a hurry, unless there is a good-sized nucleus of such trained and experienced personnel no good cryptanalytic operations can be conducted in the early phases of a war; that is, just at the time when results can usually be obtained most easily and when such results are extremely important. Moreover, it is in the upper strata of cryptanalytic brains that continuity in studies is most important. It is possible, under pressure, to obtain large numbers of recruits of high intelligence from colleges and universities, but until they have had at least five years actual experience and training they are wholly unprepared to attack the more difficult problems encountered in modern, up-to-date secret communications.] Consider the present "Purple" system, for example. It required almost two years of concentrated effort to break down this system and it was indeed fortunate that this had been accomplished by September 1939. If we had only been able to start this study in December 1941 it would not have been possible to read those messages short of two years' study, if at all, because the problem is so difficult to begin with, and moreover, the volume of traffic available for analysis would be so small compared to what it was shortly before December 7, 1941. Moreover, if we did not have the two years' experience with the ordinary "Purple" the task of reading the special "Purples" now occasionally employed would be extremely more difficult, if it could be done at all before too late to be useful. Again, our present difficulties with Japanese military systems are in large part occasioned by our failure to devote sufficient study to these systems over the past few years; but it must be realized that limitations on funds and personnel made such studies impossible, because with the small staff of SIS personnel from 1930 to 1940 it was all that this personnel could do to keep abreast of the Japanese diplomatic systems, for which G-2 was clamoring. - 1940

(2) [Continuity in cryptanalytic studies also requires continuity in intercept work, for without the basic raw material no studies at all can be conducted on actual traffic and purely theoretical studies may be

~~SECRET~~

far off the real target altogether, no matter how successful. Continuity in intercept work means, of course, that the equipment and personnel of the intercept service have to be maintained and thus, these are available at the outbreak of war, for immediate, useful work. Unless cryptanalytic studies are pursued the need for the maintenance of adequate intercept stations soon disappears, for it presently begins to look as though the work done by the intercept personnel is useless and funds for this activity are withdrawn.

(3) Continuity in cryptanalytic studies is necessary because cryptanalysis is not a static science or art -- it must progress as cryptographic science progresses. In the past few years great strides have been made in the latter, especially as regards the development of complex electrical and mechanical cryptographic devices and machinery. Moreover, the cryptanalytic work done during the last war has been publicized. As alluded to above, "The American Black Chamber" in particular has exercised a wide influence in putting certain nations which had been quite backward in their cryptography on their guard, causing them to engage in studies and developments for the improvement of their codes and ciphers. The result is that the cryptographic systems of these nations have become more and more difficult to analyze. It is important to note that improvement in cryptography usually comes in successive small steps, and if the opposing cryptanalyst can keep in step with these progressive increases in complexity he can, as a rule, be in a position to read the new systems almost as fast as they are put into usage. If there is much of a lag in the cryptanalysis the cryptographer gets too far ahead for the cryptanalyst to catch up quickly; in some cases catching up becomes impracticable or impossible.

(4) Finally, it may be noted that continuity in cryptanalytic studies brings improvements in our own cryptographic systems and methods, without which we may be lulled into a false sense of security and remain blissfully ignorant of what some foreign cryptanalytic bureau may be doing with our supposedly secret communications. It can be said that the greatest blow that can be dealt to signal security work is loss of continuity in cryptanalytic studies, for it means that a disastrous blow has been delivered to technical efficiency of both the cryptographic and cryptanalytic services for war-time functioning.

15. It may be pertinent to add that the British Government began its cryptanalytic activities in 1914 and never desisted from them for even a month since then, though of course on a smaller scale than was reached at the height of these activities in 1918-1919. However, it was on a scale sufficient to enable them to keep up with the diplomatic traffic of most of the governments of any consequence in the world in which they had an interest. The British built up a corps of about 35 to 40 able cryptanalysts, including Army and Navy officers permanently assigned to cryptanalytic

~~SECRET~~

~~SECRET~~

duties. They maintained cryptanalytic units in London, India, Africa, China, and so on -- the officers being transferred from one unit to another but constantly staying in cryptanalytic work. The result is that today, while our SIS has solved and can perhaps again solve more difficult individual problems, in overall coverage of the field the British organization is considerably ahead of ours. It is clear that no country is too small for them to have an interest in that country's secret communications, and they are today able to read the traffic of most countries on which they have had continuity since the last war.

14. Finally, if we are not to repeat once more the mistakes made at the close of the last war in respect to signal security work, every effort should be made to place the present organization on the most firm, permanent foundation it is possible to erect. The service should not be considered as merely an appendage to the functions performed by the Signal Corps only in time of war but as a permanent service that operates on a large scale in peace-time as well as in war-time.

William F. Friedman,
Director of Communications Research.

Originally written
and dated June 29, 1942.
Minor changes made on
April 2, 1943.

Attached:
5 Tabs, A to E, incl.

~~SECRET~~