ARMY SECURITY AGENCY

Washington, D. C.

HISTORICAL BACKGROUND OF THE SIGNAL SECURITY AGENCY

VOLUME THREE

Prepared under the Direction of the

ASSISTANT CHIEF OF STAFF, G-2

12 April 1946

WDGSS-13

HISTORICAL NOTE

When, in October 1944, plans were first made for the preparation of a comprehensive History of the Signal Security Agency, it was intended to include therein an account of the historical background of the Agency beginning with the earliest record of the use of cryptography by the United States Army. As the material was gathered together, however, it became increasingly clear that to do this would result in expanding the bulk of the History to such proportions as to discourage many readers. For this reason, the historical background has been prepared as a separate work in three volumes, as follows:

Volume One:	Codes and Ciphers prior to World War I	1776 - 1917
Volume Two:	World War I	1917 - 1919
Volume Three:	The Peace	1919 - 1939

Volumes One and Two of this series are provided with indexes covering the content of each respectively. The index in Volume Three, however, covers the text and footnotes of the entire series of three volumes.

It was not planned in the beginning to include any tab material in the Historical Background of the Signal Security Agency. After the work was finished, however, a number of documents were found which seemed worthy of note, and these were collected and arranged in a Supplement to volume Three.

HISTORIAN, ASA
20 April 1948

HISTORICAL BACKGROUND OF THE SIGNAL SECURITY AGENCY

VOLUME THREE: THE PEACE 1919-1939

Contents

Chapter

LIST OF TABS

HISTORICAL BACKGROUND OF THE SIGNAL SECURITY AGENCY

VOLUME THREE: THE PEACE 1919-1939

CHAPTER I. THE CODE AND CIPHER SECTION[1] 1919-1929

A. Distribution of Code and Cipher Work

Prior to World War I, responsibility for cryptographic systems used by the United States Army had been centralized in no single agency.[2] Distribution of and accounting for code books and cipher systems had been handled by the War College, The Adjutant General, the Military Intelligence Division, and, in some cases, by the Signal Corps. As a result, confusion arose as to which of these agencies was the proper authority to receive the necessary reports, requests, and recommendations. The War Department Telegraph Code 1915 had, for example, been prepared by the Chief Signal Officer and distributed by The Adjutant General, yet the Military Intelligence Division received many letters relating to it.[3]

A beginning had, however, been made towards the establishment of a definite policy in regard to the division of functions, and the Chief

---

1. Strictly speaking, no such section existed before 1921, but the functions were already being carried on prior to that time in the Office of the Chief Signal Officer.

2. On World War I, see Volume Two, especially Chapter II.

3. Memorandum to War Department, Chief of Staff from Assistant Chief of Staff, G-2, Subject: Preparation, distribution of, and accounting for code books, 27 January 1921, sec. III, par. 1-3 (SPSIS 311.5).

Signal Officer was charged with the "preparation and revision of the War Department Telegraph Code," while the printing, distribution, storage, and accounting for that code were the responsibility of the Adjutant General.[4] The Military Intelligence Division, nevertheless, had good reason to doubt the efficiency of the code compilation done in the Office of the Chief Signal Officer and established in its Cipher Bureau a special Code Compilation Subsection[5] which maintained its own system of accounting for the codes issued by the division. At the close of the War the functions of this unit were transferred to the Office of the Chief Signal Officer as a result of a conference held on 26 October 1920.[6] The agreement made at the conference, confirmed three days later,[7] was threefold in character and was destined to remain in force until May 1929.[8]

---

4. AR 1913, par. 1556.

5. On the work of this section, see Volume Two, chapter II.

6. Representing the Military Intelligence Division was Major Frank Moorman; the Signal Corps officers were Colonel Frank R. Curtis and Major John C. Moore.

7. Memorandum, Chief Signal Officer from Director of Military Intelligence Division, Subject: Code and cipher work by the Signal Corps, 29 October 1920 (MI no. 4131-607).

8. The new arrangement was incorporated into Army Regulations, 14 January 1922, par. 2e; changes no. 1, 20 October 1923; AR 105-5, 15 December 1926, par. 2e.

In accordance with this agreement, the Signal Corps was to undertake the compilation of such codes and ciphers as were required. Prior to their publication, however, all codes and ciphers were to receive the approval of the Military Intelligence Division. The reproduction, distribution, storage, and accounting were responsibilities still left with The Adjutant General. Though the solution of enemy codes and ciphers remained a function of the Military Intelligence Division, the Signal Corps agreed to give preference, in its search for officers qualified to supervise cryptographic compilation, to those who had practical experience in solution. Moreover, Signal Corps officers were to be instructed in the basic principles of cryptanalysis in order to make them fully aware of the need for avoiding in all cryptographic operations such blunders as render a system more vulnerable to the attack of enemy cryptanalysts.

This agreement did not embody principles fundamentally new at that time: the Signal Corps officers on duty with the American Expeditionary Forces in France had automatically assumed the functions allotted to them in this agreement. The chief change was the transfer of the functions of the Code Compilation Subsection maintained by the Military Intelligence Division to the Office of the Chief Signal Officer. Such transfer, however, was not immediately complete, since the Military Intelligence Division was still preparing tables of encipherment for

Military Intelligence Code No. 5 as late as 11 August 1921.[9]

B. Codes in Use at the Conclusion of World War I

The coming of the peace rendered the codes compiled by the Military Intelligence Division for combat units and for communications between high echelons of the Army both obsolete and unnecessary. One of these, the so-called Ideal Correspondence Code, as has been stated in Volume Two, had been printed in 1918 by the Government Printing Office, but bore on the title-page the imprint of a fictitious firm, the "Ideal Code Company," used only as a blind. The printer had used type and paper entirely unlike those used in ordinary government publications. By this time the Ideal Correspondence Code was believed to have been compromised[10] but continued to be used, at least by the Military Observer in Riga, as late as 12 March 1921.[11] This left only two codes in current use by the War Department. The first of these was the War Department Telegraph Code 1915, compiled by the Chief Signal Officer, which was currently in use to a limited extent

---

9. IR 4161: letter of Major Frank Moorman to H.O. Yardley, 11 August 1921.

10. Ibid.: letter of Major Frank Moorman to H.O. Yardley, 26 March 1921. So also a letter of the Chief of MI-5 to the Military Attaché in Peking, 21 April 1921 (IR 4324).

11. IR 4291: letter of Director of Military Intelligence Division, 12 March 1921.

but only for confidential communications. Concerning it the following paragraph is pertinent:

> The present War Department Telegraph Code was prepared with code groups which will not be accepted by the Cable Companies. It is therefore necessary to encipher all messages encoded by its use. The cost of clerical help for this purpose will in a single year amount to more than the cost of a new book.[12]

The language of this statement is misleading. The operation referred to as encipherment is merely a conversion of the code groups to make them pronounceable. This was effected by using a table, supplied with the code, for converting the serial number of each group to five letters forming a so-called "pronounceable word," i.e. five letters normally not a bona fide word but always pronounceable.

Furthermore, the code was constructed on insecure principles and it had by this time been used so long and with such heavy traffic that the probability of its having been compromised by cryptanalysis, was very great. Copies of the code were probably available to any government interested in obtaining one. In fact, The Adjutant General reported to the Chief of Staff on 28 July 1919 (IR 4296) that fifteen copies had been lost,[13] and it was almost certain the German Government had a copy.[14]

---

12. Memorandum cited in note 3, par. 6. Though the date of this memorandum (27 January 1921) was later than the preparation of the War Department Telegraph Code 1919, the quotation clearly refers to the 1915 edition which had not yet been supplanted by the 1919 edition, then still in the vaults.

13. Though it bore the imprint of the Government Printing Office, the book had been printed by a commercial firm in Cleveland.

14. See Volume Two, Chapter I.

The second code still in use was Military Intelligence Code No. 5 (MI-5), issued by that division in July 1918, and currently used for secret communications. Complete accounting for the copies of this code had been maintained, and the code itself was relatively more secure than the War Department Telegraph Code 1915, since it was never used without encipherment from tables issued by the division every two weeks.[15] During the summer of 1921 traffic in this code had declined to such an extent that it was believed desirable to lengthen the period during which a given table was valid to two months.[16] In the opinion of the chief of the New York office,[17] the fact that these tables were in uniform use throughout the world made them insecure and it was suggested that three different sets of tables be furnished holders of the code, one for each of three different divisions of the globe.[18]

Though this code had been based on more sophisticated principles than the War Department Telegraph Code 1915 (i.e. it was sent in enciphered form) and accounting had been more strictly maintained, the fact that it had been used for two years, not only for secret

---

15. At this time the tables were prepared by the unit of MID established in New York in 1919 (see letter of H. O. Yardley to Colonel A. G. Campbell, 15 July 1920, in IR 4158).

16. IR 4161: letter of Major Frank Moorman to H. O. Yardley, 2 August 1921.

17. On the work of this office, see Volume Three, Chapters II-IV.

18. IR 4161: letter of H. O. Yardley to Major Frank Moorman, 6 August 1921.

material but also for much that was nonsecret, made it seem highly probable that soon sufficient traffic could have been intercepted by foreign agencies to make solution of the code possible. Indeed, in December 1919 this code was believed to have been compromised by the French.[19] No steps were taken immediately to replace it because "nothing is being handled particularly that requires such a great amount of secrecy, especially with respect to this nation."

It was therefore very desirable to devise and distribute new systems to replace those in current use.

C. The Formulation of a Code Production Policy

In accordance with these considerations, the Military Intelligence Division approved a definite policy for the development of the code compilation work which had been charged to the Chief Signal Officer. The Adjutant General was requested to advise the Chief Signal Officer concerning the code books and cipher systems which should be compiled in the future. All duties relating to the issue and accounting for new systems were to be retained by The Adjutant General. Finally, it was requested that a War Department policy relating to the construction, issue and use of codes and ciphers should be announced to the service.[20]

---

19. IR 4157: Memorandum for Colonel Campbell, 30 December 1919. The information concerning the compromise had come from the Military Attaché in London.

20. Memorandum cited in note 1, sec. iv, par. 1-3.

The War Department Telegraph Code 1915 was accordingly withdrawn and the edition of 1919, then in the vaults of The Adjutant General, was issued in its place, effective 1 September 1921.[21] This met the requirement for a comprehensive code of 100,000 groups to be used for confidential communications. It had been compiled by Major Howard R. Barnes, who had previously been Officer in Charge of the Code Compilation Section, Signal Corps, American Expeditionary Forces in France.

Three editions of a War Department Staff Code were required. This was to be used for secret communications and was to contain 40,000 to 50,000 groups. To satisfy this requirement, the Military Intelligence Code No. 5, in spite of the fact that it was only one-part, had been used for two years and was open to the objections stated above, was to be regarded as the current edition of this War Department Staff Code. The Military Intelligence Code No. 9 (1918), then still in the vaults of the division, was to serve as the reserve edition for immediate replacement of No. 5 in the event of an emergency. Thus, without further compilation, two of the three editions requested were provided, and although these had been prepared during the War, they were both regarded as still serviceable. The third of the three editions was now to be prepared by the Signal Corps.[22]

---

21. It was suggested in a memorandum for Colonel McAndrews from Major W.K.Wilson, Chief, Statistics Branch, General Staff, 26 January 1921 (IR 4226) that the edition of 1915 be now used for training purposes, that the existence of reserve codes be kept secret, and that secret messages should be kept to a minimum.

22. IR 4161:memorandum of Major Frank Moorman to H.O.Yardley, 6 January 1921.

An Army Tactical Code, later[23] known as the Army Field Code, was to be prepared in three editions for confidential correspondence between divisions and higher tactical units. As directed for the War Department Staff Code, one edition was for immediate issue and current use, one edition for issue in an emergency,[24] and a third to be held in reserve, for issue in the event that the second edition should be compromised.[25]

Twelve editions of the Army Field Code, later[26] called the Division Field Code, were to be prepared. This was to be a confidential code for companies and higher tactical units, primarily for communication within the division. Of the twelve editions, each of which was to contain 3,000 groups, three were destined for use in the Philippine Department, three were for use in the Hawaiian Department, one for immediate issue to troops in the United States for current use and instruction, and the remaining five were to be held in reserve, for

---

23. This change was suggested in a Memorandum for War Department Chief of Staff from Assistant Chief of Staff, G-2 (Colonel S. Heintzelman) dated February 1922--the day is missing (IR 4226). The memorandum cited in note 21 recommends that this code be kept in reserve until the outbreak of war.

24. Doubtless this means that the process of distribution was to be begun so that no delay would be encountered in changing the code.

25. Memorandum cited in note 3, sec. iii, par. 9c.

26. See note 23.

issue as required. In each of the two departments mentioned, one edition was to be issued immediately, one held for an emergency, and the third held in reserve.[27]

Whether any other systems were approved at this time is not clear. A memorandum for The Adjutant General of the Army, Subject: War Department policy in reference to the use of codes and ciphers, 17 March 1921, signed by Brigadier General D. E. Nolan, then Assistant Chief of Staff, G-2, lists the following special codes and ciphers "to be prepared as required:"[28]

1. Signals between aeroplane and ground.
2. Supply catalogues.
3. Geographic codes.
4. Signal service code.
5. Meteorological data, etc.

D. Appointment of a Signal Corps Cryptanalyst

Although the Chief Signal Officer had been charged with the compilation of various codes, no regular staff had been appointed for such work in his office prior to the latter part of 1920. During the World War I, a Code Compilation Section, consisting of five Signal Corps officers and three enlisted men, had served under Major Howard R. Barnes at General Headquarters, American Expeditionary Forces in France. This unit had constructed various field codes for the front lines and for headquarters,

27. Memorandum cited in note 3, par. 9d.

28. IR 4226. The memorandum was first prepared on 27 January 1921, but issued on 17 March 1921. Whether all the provisions were definitely approved is not clear.

and had compiled the Staff Code for use in France.[29]

It was deemed desirable that the person chosen to prepare codes and ciphers for secret communications in the Army be chosen from among officers who had had practical experience in cryptographic or cryptanalytic units during the War. Furthermore, the person chosen should also be competent to assume the responsibility of training Signal Corps officers in the basic principles of cryptography and cryptanalysis through lectures and publications, and should understand thoroughly the operation of the printing telegraph cipher. Only two or three men in the United States possessed these qualifications; all of them had been officers in World War I engaged in some phase of code and cipher work.[30] That the Signal Corps was planning an appointment as early as 4 October 1920 is clear from an unsigned letter (probably from Colonel Marlborough Churchill) to H. O. Yardley which states that the Signal Corps at that date had no person qualified to engage in code compilation but was planning to form a unit for the purpose.[31] Prior to that time a policy of issuing contracts to qualified persons had been followed. Thus, on 4 November 1919 an order had been placed with Major Barnes, by this date again a civilian,

---

29. Memorandum for Executive Officer, Office of the Chief Signal Officer, from Edward Barnett, Civilian Assistant, 30 January 1939, sec. ii (SPSIS 311.5), p. 2, par. c. See Report of Code Compilation Section, General Headquarters, American Expeditionary Forces, December 1917-November 1918, a publication of the Office of the Chief Signal Officer (Government Printing Office, 1935). See also Volume Two, Chapter VII.

30. Memorandum for Administrative Section from Major J. O. Mauborgne, 13 October 1921 (SPSIS-201 W. F. Friedman).

31. IR 4158: Letter to H. O. Yardley, 4 October 1920.

for the revision of "a confidential staff code" which became, ultimately, the War Department Telegraph Code 1919. He completed this work on 29 April 1920 and was paid $1250 from Signal Service funds.[32]

This code, which was in use for purposes of economy in messages of low classification even later than 26 May 1941 (the date of the last sheet of instructions pasted in the copy in the Signal Security Library), used five-letter pronounceable groups with corresponding five-digit groups. The letter H was omitted and no groups began with Y or Z. The groups conformed to the patterns:

a. vowel-consonant-vowel-consonant-vowel
b. vowel-consonant-consonant-vowel-consonant
c. consonant-vowel-consonant-vowel-consonant

For each initial trigraph, 15 final digraphs were used. The plain equivalents were divided into the following sections:

I: dates (this is two-part in arrangement)
II: cardinal numbers, including fractions
III: organization and ordinal numerals
IV: ammunition, equipment, ordnance, etc.

The vocabulary began on page 59 with A = 10009 or ABAMI. The last group was 83,590, a blank. The vocabulary was assigned code groups, in general, according to the one-part principle, but inserted in it were the code groups which appeared in the four tables. There was a mutilation table and a thumb index.

---

32. Memorandum cited in note 30, par. d.

The work of compilation had proceeded to an advanced stage by 5 August 1919 when the Chief Signal Officer informed The Adjutant General concerning the project as follows:[33]

1. Herewith is submitted draft of a new War Department Telegraph Code.

2. This code has been in preparation since the signing of the armistice. A careful study of the telegrams of the American Expeditionary Force was made, the phraseology of more than 14,000 telegrams being studied at General Headquarters alone. Later an exhaustive study was made of the telegrams between Washington and the Philippines, Hawaii, Porto Rico, Panama and elsewhere. Particular note was made of the new phraseology coming into use through the adoption of radio. The new code contains approximately 65,000 words and phrases.

3. With the "Staff Code" of the A.E.F. as a basis the following codes were carefully studied and checked in the preparation of the new code: War Department Telegraph Code, 1915; The Greely Code; and three or four other of the largest commercial codes. In addition reference was had to the Tables of Organization, Signal Corps equipment, Q. M. supplies, makes of aeroplanes and motors, ammunition and ordnance, and War Department Orders and Bulletins. Provisions has been made for the spelling combinations of French, German, Spanish and Japanese as well as English. The names of towns and rivers in Alaska, Hawaii, Panama and the Philippines as well as the more important localities of the world have been listed. Special attention has been paid to Mexico.

4. This code, in accordance with modern practice, has been arranged alphabetically, the only deviation being in the arrangement of four tables in the fore-part of the book which set forth a comprehensive list of the organization of the Army; a series of numbers running to 6,000,000; a table of dates; and a list of miscellaneous supplies and equipment.

---

33. Memorandum now filed in IR 4296. This document contains a letter in which Yardley recommended to the Chief of the Positive Branch, Military Intelligence Division (13 August 1919) that the code be used in unenciphered form!

5. To insure accurate transmission of these tables the designating groups have been selected at random from the body of the code so that a great difference in sound and appearance exists and the danger of error materially reduced. Each of the words and phrases in these tables is found in the main body of the code in an indented line.

6. The book should be made of convenient size for office use and with a clear readable type which it is believed will further reduce the chances of error in operation.

7. Provision has been made throughout the code for the insertion at a later date of certain "Supplements" , or pamphlets, by which means all changes in phraseology relative to certain highly-specialized services of the Army or the introduction of new equipment or ordnance may be covered in a particular and convenient manner. Provision has also been made for an "Officers' List".

8. After careful consideration of the methods employed in the breaking-down of enemy codes and in view of the fact that it would be practically impossible to prevent the loss of a code of so wide a circulation, or at least to prevent its passing into the possession of unauthorized persons temporarily, therefore, in order to provide a rapid method of communication it is recommended that no form of encipherment be used with this code but that the designating groups be sent as they appear originally in the code. This is a deparature [sic] from the usual methods but it is believed that this method will answer all practical purposes of secrecy and at the same time provide a quick and economical means of communication. Special instructions may be issued from time to time under emergencies to provide for extraordinary conditions. There have been developed during the war methods of transmitting confidential information with a high degree of secrecy and it is believed that these methods should be resorted to for the transmission of information of that character.

9. It is further recommended that instructions be issued in a General Order that all persons using this Code follow the directions for its use as conscientiously in normal time as they would in time of war. Carelessness in the use of Codes should not be permitted at any time. The mere fact that the double work caused by any method of encipherment has been set aside temporarily in order to expedite the handling of code messages, by no means removes the obligation of the code operator to comply strictly with the instructions for care and secrecy.

10. The personnel of the Signal Corps Code Compilation Section are experienced code men and trained proof-readers, and it is desired that they be used to read the proof and make the final corrections for the printer. As their period of service is drawing to an end, attention is invited to the short time remaining for this special service.

11. Authority to print this Code is requested; this office to be advised of the approximate number of copies desired. It is believed that this Code could be finished by the Government Printing Office within a month after the receipt of copy.

Following the same policy of contracting for compilations in 1920-1921, a number of orders were placed with Mr. William F. Friedman who during the War had been a first lieutenant in the Military Intelligence Division, on duty with G-2, A-6, at General Headquarters, American Expeditionary Forces in France. About a year after he was demobilized, the Chief Signal Officer desired to grant Mr. Friedman a permanent commission in the Signal Corps,[34] but in the physical examination necessary for this commission it was reported that Mr. Friedman had "a functional heart disturbance."[35] As a result the Chief Signal Officer invited him to join the staff in a civilian

---

34. Upon demobilization Mr. Friedman had returned to the staff of Riverbank Laboratories, Geneva, Illinois, which he had left to enter the service. See Volume Two, Chapter I.

35. Personal statement of Mr. Friedman (1945). A re-examination (about a week later) was given him at the same station (Camp Grant) and he was pronounced physically fit but on receipt of the second report the Surgeon General refused to reopen the case.

capacity. A contract[36] was made on 6 December 1920 for the revision of the War Department Staff Code at a cost of $1800. An additional order was placed on 28 February 1921 for two field codes at a cost of $700. A third order was placed on 1 August 1921, providing for the revision of two special editions of the field codes, five emergency sets of cipher tables for use with the War Department Staff Code, at a total cost of $3,350.[37]

In order to carry out these contracts Mr. Friedman joined the Office of the Chief Signal Officer on 1 January 1921. He began at once on the preparation of the Staff Code. It was suggested that he have the advantage of possessing the cards then held by the New York office of the Military Intelligence Division.[38] These cards had already been used in the compilation of a code but did not embody the principle

36. This method of employment was selected with a view to facilitating a start on the work to be done. Its legality was later brought into question.

37. Memorandum cited in note 30, pp. 3-4, pars. F, G, and J.

38. IR 4161: memorandum of Major Frank Moorman to H. O. Yardley, 6 January 1921. The official request for the shipment of the cards was made on 10 January 1921. On 8 March 1921 Major Moorman wrote to Yardley that it had been definitely decided to use them. The code for which they had originally been prepared was Military Intelligence Code No. 9, made at a time when No. 5 was believed to have been compromised, i.e. December 1919 (see IR 4157: memorandum for Colonel A. G. Campbell from Colonel John M. Dunn, Chief, Positive Branch, MID, 30 December 1919)

of the two-letter differential which Mr. Friedman desired to employ. Considerable discussion took place concerning the adoption of this principle in the new code,[39] but it was finally decided to utilize the cards. The chief of the New York office, Mr. Yardley, was of the opinion that neither the War Department Telegraph Code 1919 nor the Military Intelligence Code No. 5 was sufficient for every contingency in which the military attaches would need cryptographic systems, and proposed that in addition to these codes, the attachés be furnished a cipher system for use when they were unable to maintain contact with their office safes. Such a system had to be easily portable and should require nothing more than a memorized key and pencil and paper. For this purpose he suggested a double transposition cipher, since "the only method we know of solving such ciphers is to have two messages of the same length in the same key." He also suggested that long messages be divided in parts, following the practice of the Germans during the war.[40] This would mean that the attaché would be supplied with the following systems:

39. Major Moorman, for example, favored adoption of a code group in which the second and fourth letters would always be consonants, the rest vowels (see his letter to Yardley, 3 February 1921, in IR 4161). This device would be chiefly valuable in preventing errors in transmission, since an operator who knew that a given letter had to be a vowel or consonant would be less likely to mistake it, and transpositions could be at once detected in garbled messages.

40. IR 4161: letter of Yardley to Major Moorman, 29 March 1921. See also Volume Two, Chapter IV.

a. War Department Telegraph Code 1919 for confidential communications;

b. Military Intelligence Code No. 5 (1918) for secret communications;

c. A cipher system for communications when neither code was available.

Apparently, Mr. Yardley rejected the possibility of issuing to the attaches the multiple disk cipher device (M-94), based ona principle invented independently by Thomas Jefferson, Commandant Bazeries of the French Army, and Colonels Parker Hitt and J. O. Mauborgne. Colonel Hitt had been responsible for the invention of the M-94, Colonel Mauborgne for its development as a practical device. That this device was under consideration is shown by a letter of Major Moorman to Colonel Locke, dated 19 September 1921 (IR 4295) in which it is stated that Mr. Friedman had described the M-94 as the best cipher ever used by the War Department prior to that time.

During the month of July 1921 Mr. Friedman went to Camp Alfred Vail, New Jersey, where he related some of his experience in code and cipher solution while on the staff at Chaumont (General Headquarters) and demonstrated the basic principles of the proper use of codes. Later in the same month he prepared a monograph on military cryptography and delivered a course of lectures in connection with instruction in

cryptography which had been inaugurated at Camp Alfred Vail.[41]

Finally, on 16 November 1921, steps were initiated to place Mr. Friedman on permanent tenure: a recommendation was submitted to the Secretary of War for his employment as Cryptanalyst, Signal Service at large, at a salary of $4,500 per annum. This recommendation was approved and he entered on duty in the Office of the Chief Signal Officer on 31 December 1921, having already spent a year there on the contract basis. Until 1930 he remained in charge of the Code and Cipher Section and carried on all work related to code compilation with the assistance of a single clerk-typist. His salary was increased by $700 on 1 July 1924 and by $400 additional on 1 July 1928.[42]

E. Code Compilation 1921-1929

Meanwhile a meeting of representatives of the various branches of the service to consider code compilation work had been called by the Chief Signal Officer on 12 February 1921. As a general policy, it was

41. Memorandum cited in note 30, page 3, pars. H and I. The monograph mentioned was the forerunner of the series of texts on cryptanalysis later prepared by Mr. Friedman. Mr. Yardley expressed considerable opposition to training of Signal Corps officers in cryptography (see his letter to Major Moorman dated 2 June 1922 in IR 4163). He seems to have feared for security in the event that much information about codes was made known to personnel not directly concerned with cryptanalysis, even when this was authorized and controlled.

42. Memorandum cited in note 30, p. 4, pars. K and L; and memorandum for Mr. William F. Friedman, Subject: Service record, 2 November 1944 (SPSIS 201-William F. Friedman).

agreed that letters were to be preferred to digits for code groups, that code books for communication within a division should be small enough to fit a man's shirt pocket, that mutilation tables need not be printed in the code books, and, finally, that general articles listed in storage catalogues should have a code designation affixed to them.[43]

On 21 March 1921 the list of codes required was approved by The Adjutant General and the Chief Signal Officer was directed to arrange for the compilation of three two-part codes. The War Department Staff Code was to contain from 40,000 to 50,000 groups, the Army Tactical Code (Army Field Code) was to contain from 12,000 to 15,000 groups, and the Army Field Code (Division Field Code) was to contain 3,000 groups. The compilation of the codes was to be completed as quickly as personnel and funds permitted.[44] In accordance with the policy previously determined by the Military Intelligence Division, it was decided to prepare the various editions of these three codes in the following order:

War Department Staff Code
Army Field Code: 3 editions
Army Tactical Code: 1 edition
Army Field Code: 3 editions
Army Tactical Code: 2 editions
Army Field Code: 6 editions[45]

---

43. Report of Conference, 12 February 1921 (SPSIS 311.5); Memorandum for Major Moorman from Major J. O. Mauborgne, 28 January 1921 (SPSIS 311.5).

44. Memorandum for Chief Signal Officer from The Adjutant General, Subject: Preparation of code books, 21 March 1921 (SPSIS 311.5).

45. Ibid.; Memorandum for The Adjutant General from Assistant Chief of Staff, Subject: Preparation of code books, 27 January 1921 (SPSIS 311.5.)

~~TOP SECRET~~

23 Jan 81 Request from FOIA/Privacy Office USA/INSCOM Anderson Attn: IACSF-FI Ft Meade Md 20755

(Request for Louis Kruh)

Declassified on 23 Jan 81 W. Winkler W. Huff at request of Larry Lough, INSCOM

1921 - SPSIS 311.5

Resume of Work of the Code and Cipher Section

1. Division Field Code No. 7 - prepared in ms., proofread, printed.

2. New code - "The General Address and Signature Code" was prepared, mimeographed, and distributed. To be used in abbreviating all addresses and signatures of radio messages handled by radio stations of the Army and certain stations of the Navy. Its use will facilitate traffic. Effective 1 November.

3. Army Field Code: vocabulary and code groups prepared. Ms. in preparation for printing. "It will be a code approximately three times the size of the Division Field Codes" - to be used for tactical field messages between units from Division upward.

4. Training Pamphlet 163 - Elements of Cryptanalysis written and now in press. To be standard text for instruction of signal officers in code and cipher work. Mr. Friedman at that time gave a two week course annually at the Signal School, Camp Vail.

5. Special code for airplane communication with ground stations in fire control and general reconnaissance work prepared. Being tested by units of VIII Corps Area, Hawaiian and Philippine Depts.

6. General method of solving so-called "Double Transposition Cipher", heretofore considered by all experts to be indecipherable, was devised and tested. 15 messages in as many different keys were solved.

7. By direction of Joint Board, a cipher for secret communication between Army and Navy was to be prepared. New cipher devised by W. F. Friedman approved by War and Navy Dept. "It requires only pencil and paper and is considered to be absolutely indecipherable without a knowledge of the key word, even though all the details of operating the cipher may be known to the enemy."

8. Many cipher systems and several cipher machines submitted by inventors examined and all rejected since they did not meet requirements regarding practicability and secrecy "an extremely ingenious electrical cipher machine is now being studied jointly with the Code and Signal Section " of Navy. Friedman directing investigation and Navy providing personnel for detailed work such as preparation of messages, tables, etc. "The results of my studies

SECURITY CLASSIFICATION CHANGED TO SECRET BY AUTHORITY Chief ASA CITE: 380-5-25 DATE: 22 July 52 BY: NAME: Historian G-2

~~TOP SECRET~~

so far seem to indicate that the messages produced by the machine are not nearly as secure as formerly believed by the Navy Department."

9. Study of telegraph alphabets in connection with Gen. Squier's new method of transmitting the alphabet. Aim to see whether certain fundamental changes in symbols will bring telegraph alphabet more in harmony with the requirements and results of modern traffic experience.

p. 31 note 57

10. "Some time has been devoted to the general problem of speeding up the methods of secret communication by the use of telegraph machines to which cipher devices may be applied. This is the coming development in cryptography".

pp. 28-29 note 52

W. F. Friedman
Cryptanalyst, Signal Corps

☆ U. S. GOVERNMENT PRINTING OFFICE: 1973—490-574

CLASSIFIED DOCUMENT ACCOUNTABILITY RECORD

For use of this form, see AR 380-5; the proponent agency is the Office, Assistant Chief of Staff for Intelligence.

DATE: 22Jan81

SECTION A - GENERAL

TO: National Security Agency
9800 Savage Road, ATTN: M6 (Mr. William Huff)
Door 3, SAB 2
Fort Meade, Maryland

FROM: Commander
USAIMSCOM
Arlington Hall Station
Arlington, VA 22212

DATE RECEIVED	ACTION OFFICE(S)	SUSPENSE DATE(S)	REGISTER OR CONTROL NO.
			0026

CONTROL, LOG OR FILE NO.	CLASSIFICATION	NUMBER OF COPIES	DESCRIPTION (Type, File Ref., Unclassified Subject or Short Title and Number of Indorsements/Incls)	DATE OF DOCUMENT	ORIGINATOR
	S	1	Ltr, Subj: Resume of Work of the Code and Cipher Section (SPSIS 311.5)	1921	Signal Corps
	S	1	SPSIS 201. W. F. Friedman, Memo from W. F. Friedman to The Chief Signal Officer, 12 Oct. 1928, Subj: Report of Arrival at London	120ct28	Signal Corps
//////////	//////////	//////////	///nothing follows/////wt//////////	//////////	//////////

SECTION B - ROUTING

TO	COPY NO.	DATE	PRINTED NAME	SIGNATURE
1.				
2.				
3.				
4.				
5.				

SECTION C - DESTRUCTION CERTIFICATE (Check appropriate block)

MATERIAL DESCRIBED HEREON HAS BEEN:

☐ DESTROYED ☐ TORN IN HALF AND PLACED IN A CLASSIFIED WASTE CONTAINER (AR 380-5)

OFFICE SYMBOL	DATE	PRINTED NAME OF CUSTODIAN OR REP.	SIGNATURE
DESTRUCTION RECORD NO.	DATE	PRINTED NAME OF CERTIFYING/DESTR. OFF.	SIGNATURE
PAGE OR COPY NUMBER	DATE	PRINTED NAME OF WITNESSING OFFICIAL	SIGNATURE

SECTION D - REPRODUCTION AUTHORITY

NUMBER OF COPIES TO BE REPRODUCED	AUTHORIZED BY	DATE

SECTION E - RECEIPT/TRACER ACTION (Check appropriate block)

☒ RECEIPT OF DOCUMENT(S) ACKNOWLEDGED ☐ DOCUMENT(S) HAVE NOT BEEN RECEIVED

☐ TRACER ACTION: SIGNED RECEIPT FOR MATERIAL DESCRIBED ABOVE HAS NOT BEEN RECEIVED.

DATE	PRINTED NAME, GRADE OR TITLE	SIGNATURE
Jan 23 1981	WILLIAM L. HUFF, CH M63	

COMMENTS

DA FORM 3964, 1 Nov 72 REPLACES DA FORMS 1203, 1 SEP 58; 1204, 1 JAN 60; 631, 1 MAR 62 AND 546, 1 OCT 63, WHICH ARE OBSOLETE.

SPSIS 201. W. F. Friedman

MEMORANDUM from W. F. Friedman to The Chief Signal Officer, 12 Oct. 1928

Subject: Report of Arrival at London

SRH-001 p. 42 Note 5

1. In Stockholm 1 October, conferences with Mr. Berlin, Chief Engineer of Aktiebolaget Cryptograph - Demonstrations of operations of their latest models of cipher machinery.

2. In London October 8 - Mil. Att. made arrangements for him to investigate a cipher machine made by Powers Adding and Calculating Machine Co. To be demonstrated tomorrow.

[This in connection with American Delegation to International Telegraph Conference at Brussels of which he was Secretary.]*

* W. F. Friedman to Chief Signal Officer, 11 Sept. 1928. SPSIS 701 - Freidman.

* Frank B. Kellogg to Major William F. Friedman, 28 June 1928. SPSIS 201 Friedman.

DOWNGRADE TO:

SECRET on:

CONFIDENTIAL on:

DECLASSIFY on: 25-3-75

CLASSIFIED by:

In order to insure the completeness of the vocabulary, it seemed desirable to study the text of a considerable body of actual messages. Accordingly, the files of telegraph messages transmitted by the First, Second, and Third Armies of the American Expeditionary Forces were borrowed by the Chief Signal Officer for study.[46] The whole program involved a large amount of work for a staff of two persons, working with limited funds. Nevertheless, progress in fulfilling the directive of The Adjutant General was rapid. By the beginning of 1924, the new edition of the War Department Staff Code was in manuscript, waiting to be checked. It consisted of 60,000 groups. The first seven of the Division Field Codes had been completed in the same period. During the next three years three more codes of this series were completed, printed, and held in reserve. These were smaller in size and were of immediate use in the Philippine and Hawaiian Departments, as well as in the continental United States, in connection with confidential communications and training.[47] By 1924 the first edition of the Army Field Code was being prepared, but this code was not so essential in an era of peace as the War Department Staff Code and the Division Field Code. In preparing these field codes an automatic procedure, utilizing obsolete printing

46. Memorandum for Major Larrabee from W. F. Friedman, 15 June 1921 (SPSIS 311.5) memo to The Adjutant General from Lieutenant Colonel C. A. Sloane, Subject: Data for completion of Army Field Codes, 1 May 1923 (SPSIS 311.5).

47. Memorandum for Colonel Voris from W. F. Friedman, 13 February 1924 (SPSIS 311.5), par 1c.

telegraph equipment in a novel manner, was devised. This was the first case of the use of automatic machinery for code compilation.

A number of other codes were also prepared. It was early recognized that addresses and signatures provide the cryptanalyst with much useful information. To disguise them, a special code was compiled: the General Address and Signature Code was distributed in mimeographed form for use in the abbreviation of all addresses and signatures of radio messages handled by the radio stations of the Army and certain naval stations, and was completed within the first year of the creatio of the Code and Cipher Section. The effectiveness of this code was carefully studied and the necessary changes incorporated in a revision prepared in 1924.[48]

Aircraft codes were prepared and tested in the Eighth Corps Area prior to their publication.[49] These employed panels of cloth or other material in signalling to aeroplanes from the ground. In 1926, Air-Ground Liaison Codes, for Infantry, Cavalry, Air Service, and Intelligence, and Air-Fire Control Codes for directing the fire of field and coast artillery, were compiled. These codes were printed on both sides of sheets of cardboard. While the Air-Ground Liaison Code was changed frequently for reasons of security, the Air-Fire Control Codes were standarized.[50]

---

48. Ibid., par. 1e; W. F. Friedman, Resume of work of Code and Cipher Section, 1921 (SPSIS 311.5).

49. Memorandum cited in note 5, par. 1f.

50. TR 162-5, Visual Signalling, 20 April 1926, pars. 26a, 30.

The Air Service also requested that a code for airways control traffic be prepared. In the course of the formation of a vocabulary for this code, a large file of messages was submitted and analyzed. The Meteorological Section of the Office of the Chief Signal Officer depended on the Code and Cipher Section for the required meteorological codes. The Radio Service Code was also prepared for technical signal messages, transmitted in the regulation of radio traffic. It was issued to all radio station and message centers, including battalions.[51]

In 1926 a Code Supplement was prepared for the Insular Bureau of the War Department, intended to be used with the War Department Telegraph Code. The Supplement was typewritten but the cover bore printed lettering. Each page had line symbols of vowel-consonant form and a variant of two-digits, with a hundred groups to the page. The pages were numbered consecutively from 850 to 1067.

F. Cipher Systems

In addition to the codes mentioned in the preceding section, much attention was given to the preparation of cipher systems operated by hand. Cipher machines had not yet been perfected though even in 1921 some time had been devoted to the general problem of speeding up the methods of secret communications by the use of telegraph machines to which cipher devices might be applied. It was correctly foreseen this early that in

51. W. F. Friedman, Code and Cipher Publications (1921)(SPSIS 311.5).

the field of machine ciphers lay the coming developments in cryptography.[52]

In 1923 there were three ciphers authorized for military use. The Double Transposition Cipher was a system designed to be used by all arms in an emergency when no other secret means of communication was available. It required, besides pencil and paper, only the knowledge of a word or phrase upon which agreement had previously been reached. Two transpositions were involved, controlled by numerical keys derived from key words or phrases.

The Cylindrical Cipher Device (M-94), composed of a series of metal disks mounted on a shaft bearing the letters of the alphabet on their circumference, was designed to be used within the regiment and issued as far forward in combat as the company command post. Instructions for the use of this device, had been issued in 1921 by the Code and Cipher Section in Signal Corps Training Pamphlet No. 2.[53]

A third military cipher authorized at this time was the Printing Telegraph Cipher. It consisted of a cipher system operated in connection with printing telegraphs and was to be used only between larger headquarters when the traffic was very heavy. Encipherment and decipherment were performed automatically at high speed. The machine had been

---

52. W. F. Friedman, Resume of work of the Code and Cipher Section, 1921 (SPSIS 311.5).

53. TR 162-5, par. 102; W. F. Friedman, Code and Cipher Publications (1921), par. 13.

developed by the Signal Corps and patented in 1918 by the American Telephone and Telegraph Company; it was employed for cipher purposes during the latter part of the war,[54] and became the basis for an interim teletype (double-tape) encipherment system in World War II, being used for the Military Intelligence net in the United States in 1942-3, and in certain overseas circuits, until it was replaced by the SIGTOT (single-tape) system.

G. Theoretical Work

In addition to the continuous supply of the necessary sets of cipher tables for use with current editions of the War Department Staff Code, the Code and Cipher Section also prepared at irregular intervals cipher tables for the Military Intelligence Code No. 5. These were compiled and multigraphed in the Office of the Chief Signal Officer.[55]

Though the basic assignment of this unit was limited to code and cipher compilation, the function of cryptanalysis being reserved for the Military Intelligence Division, the chief of the section realized that proper compilation theory and techniques could only be derived from a thorough knowledge of cryptanalytic theory and techniques. He therefore was deeply interested in the problems of cryptanalysis and

---

54. TR 160-5, par. 103; W. F. Friedman to The Adjutant General, Subject: Patents, 7 July 1922 (SPSIS 201-Friedman).

55. Memorandum for Colonel Voris from W. F. Friedman, Code and Cipher Publications (1921), (SPSIS 311.5), par. 8.

spent such time as his duties permitted on theoretical problems in cryptanalysis. A general method was devised for the solution of the Double Transposition Cipher, which had previously been considered indecipherable by all experts. As a test of this method, fifteen messages, each in a different key, were solved.[56]

In connection with a new method of transmission devised by the Chief Signal Officer a study was made of telegraph alphabets. The object of this study was to ascertain whether fundamental changes in the symbols brought the telegraph alphabet into closer harmony with the requirements of current traffic.[57]

Another of the responsibilities of the Code and Cipher Section was the examination of cipher systems and machines submitted by inventors to the Chief Signal Officer. Without exception, these were all rejected, since none of them met the requirements of practicability and security. One invention of this kind was a new type of electrical cipher machine which had been submitted to the Navy for purchase. The naval authorities regarded the system as highly secure and were about to spend what was then a large sum ($75,000) for some of the machines, when it was claimed by Mr. Friedman that the system was solvable.[58] A set of ten test messages submitted by the Navy as a challenge were solved by him in about two months. About six weeks were spent on the elaboration of

---

56. W. F. Friedman, Resume of Work of the Code and Cipher Section (1921) (SPSIS), par. 6.

57. Ibid. par. 9.

58. Ibid. par. 8.

a method of solution: afterwards, the test messages were solved in about two weeks.[59] This was, of course, before the days of statistical machinery: The chief value of this project was the discovery and establishment of principles of solution and the demonstration that traffic enciphered by rotating electrical commutator machines, such as the Hebern, could be solved. The principles and methods worked out then are still valid in 1945.

By 1924, an analysis of the Printing Telegraph Cipher had been completed and the Signal Corps Laboratory had undertaken work on apparatus designed to add certain complicating features.[60] The machine had been improved by the substitution of a new type of relay to obtain more positive action than had been possible in the conventional type previously used. Further experiments had been undertaken with the Morkrum teletype system and a cipher tape had been applied to it, resulting in more successful operation and greater simplicity than had been possible in the old "stop-start" printer.[61]

In 1925, two patents were issued to the Chief of the Code and Cipher Section. One of these, "Improvements in Printing Telegraph Systems"

---

59. Memorandum for Colonel Voris from W. F. Friedman, 13 February 1924, par. 2 a (SPSIS 311.5).

60. Ibid. par. 2b.

61. Annual Report of the Chief Signal Officer for the Fiscal Year 1924 (OCSigO 319.1), p. 34.

(No. 1530660), represented the result of a long period of work. The second, relating to the "Secret Signalling Systems" (No. 1516180) and also filed on behalf of the Government, was granted and issued to the section chief conjointly with a member of the Signal Corps Engineering Laboratory. Other patents were pending.[62]

By 1925, the Code and Cipher Section, in cooperation with the Signal Corps Engineering Laboratory, had made satisfactory progress in the development of automatic cryptographic apparatus. The work had already indicated that machinery for this purpose could be produced to fill a need long felt, particularly by centers transmitting a large amount of secret correspondence in a short time.

Meanwhile certain developments in the art of cryptography were of extreme importance. It was predicted in 1925 that errors in transmission and reception, which had always constituted one of the most serious problems confronting cryptographers, would be entirely suppressed by telephotographic methods.

H. Secret Intercommunications between the Army and the Navy

One of the earliest cryptographic problems which had been presented to the Code and Cipher Section was that of devising a means

---

62. Annual Report of the Chief Signal Officer for the Fiscal Year 1925 p. 10, par. 14.

for secret intercommunication between the Army and the Navy. In 1921 a cipher for this purpose was devised and approved by the War and Navy Departments. It required only pencil and paper and was considered "to be absolutely indecipherable without a knowledge of the keyword, even though all the details of operating the cipher" might become known to the enemy. It had been devised after a long study of all of the known methods of secret communications and was the fastest and most secure of any then known.[63]

The Army-Navy Cipher No. 1 was authorized only as an emergency cipher. For regular communication between Army and Naval units the exchange of the War Department Staff Code and the Navy "A" Code was under consideration. Such a proposal, however, involved difficulties, principally connected with distribution. Both the Army and the Navy regarded the distribution of one of its most secret codes to the personnel of the other service as undesirable because of the threat to security derived from the increased number of holders. Neither of the two codes considered was adequate for joint operations. It was concluded, therefore, that a special code for secret communication should be compiled.[64]

---

63. W. F. Friedman, Resume of work of the Code and Cipher Section (1921) (SPSIS 311.5), par. 7; Memo for Colonel Voris from W. F. Friedman, 13 February 1924 (SPSIS 311.5), par. 2c.

64. Memorandum for Training Division from W. F. Friedman, 15 January 1926 (SPSIS 370.2).

The Joint Board also considered inadequate the means of secret intercommunication between Army and Navy forces engaged in joint operations. It recommended on 12 February 1926 that the Chief Signal Officer and the Director of Naval Communications jointly prepare a secret code for such operations. In the construction of this code it was further directed that the principles of simplicity and brevity should be observed, as far as was consistent with safety and secrecy,[65] a recommendation immediately approved.

The Chief Signal Officer acknowledged on 2 March 1926 the receipt of a copy of the Joint Board Report No. 317 from The Adjutant General, and agreed that the work on the code would be initiated at once. A fundamental cause for the inadequacy of previous attempts at radio intercommunication between the two services was the absence of a uniform method of radio procedure for both of them. It was recommended that the directive be expanded to include the preparation of a uniform radio procedure.[66]

Both the Director of Naval Communications and the Chief Signal Officer undertook studies relating to joint intercommunications and,

---

65. Memorandum to Secretary of War from Joint Board, 12 February 1926 (J. B. No. 317, serial no. 263).

66. Memorandum from The Adjutant General to Chief Signal Officer, Subject: Army and Navy secret intercommunication, 1 March 1926, (AG 311.5/4, 12 February 1926, Pub.); Colonel [illegible] C. Voris to The Adjutant General, Subject: [illegible] (OCSigO 461).

by the middle of May 1926 a plan had been formulated which provided for three classes of communications.

a. Between high commands by the exchange of liaison officers equipped with the necessary codes of their respective services.

b. Between intermediate commands by means of a specially constructed Army-Navy code.

c. Between small or detached Army units and individual vessels of the Navy by means of Cylindrical Cipher Device M-94.

The Adjutant General approved the plan as outlined[67] but it was not thought possible to put all parts of it into operation until the special code for the second class of secret communications was completed, and this would take two years. The actual work of compilation was assigned to a subcommittee of two persons.[68]

From June to September 1926 the Chief Signal Officer and the Director of Naval Communications prepared a draft of instructions on the basis of the approved plan.[69] This document, which was published after its

---

67. Chief Signal Officer to The Adjutant General, Subject: Army and Navy secret intercommunication, 15 May 1926 (OCSigO 461-CA and N Code) 1st Indorsement.

68. For the Navy Lieutenant H. McCoy Jones, USN, and for the Army the chief of the Code and Cipher Section. See Memorandum of Lt. H. McCoy Jones, Subject: Meeting of Representatives of Director Naval Communications and Chief Signal Officer, 14 June 1926. 24 June 1926 (SPSIS 370.26).

69. Memorandum for The Adjutant General from Chief Signal Officer, Subject: Secret intercommunication between the Army and the Navy, 11 October 1926 (OCSigO 461 Joint AN Code).

final approval on 15 November 1926, provided that the instructions for secret intercommunication between the Army and the Navy were to become effective on receipt of a telegraphic notice, issued concurrently by the Secretary of War and the Secretary of the Navy. To the three classes of communications upon which agreement had been reached, there was added a fourth class, aircraft, for which a code was to be designed.[70]

The actual work of preparing a system of secret intercommunication between the Army and the Navy had already been in progress for a period of five years but completion was delayed still longer. The distribution of the Cylindrical Cipher Device (M-94) had not been completed by the beginning of 1929 because the current supply of the device was exhausted. Delivery was then expected on an order which had been placed some time previously. Its execution had been delayed by the necessity of reconditioning dies and other tools involved in the manufacture of the devices.[71] By May 1929, however, the cipher devices were ready for distribution, and were distributed.[72]

---

70. Secret Intercommunication Between the Army and the Navy prepared Jointly by the Chief Signal Officer, U. S. Army, and Director of Naval Communications, approved by the Joint Board 11 November 1926, approved by the Secretary of War, 15 November 1926, approved by the Secretary of Navy 12 November 1926, Washington 1926.

71. The Adjutant General to Chief Signal Officer, Subject: Secret intercommunication between Army and Navy, 26 January 1929 (AG 311.55, 11 July 1927, Pub.).

72. Lieutenant Colonel J. E. Hemphill to The Adjutant General, 16 May 1929 (SPSIS 370.26).

Likewise, although the manuscript for the code for intermediate communications was compiled jointly in 1927-1928, it was still on file in the Navy Department in 1934. It had not been printed because funds had not been available and to print the code in 1934 would have required revision to bring it up to date. The only means available for secret intercommunication between the services remained the Army-Navy Cipher No. 1, the multigraphed edition of which had been distributed in 1925 with annual changes of the key word. The cipher was, however, considered unsuitable for the heavy traffic to be expected in an emergency.[73]

I. The Program for the Maintenance of Security

The experience of the United States Army in World War I had amply demonstrated that, however secure the secret means of communication, errors committed by code clerks might nullify the best work of the compilers. There were many examples in military history of defeat or disaster resulting from the interception by the enemy of plain-text dispatches or of cryptographed dispatches easily solved. Secrecy in the transmission of communications in time of war had been proved a vital necessity.

In themselves, codes and ciphers, however skillfully compiled, could not afford complete security. All systems had to be practicable, and, in actual combat where speed was essential, complicated methods could not be employed. The principal requirement for combat systems

---

73. Revised Code Production Program, 4 April 1935 (SPSIS 311.5), par. 4a.

was to delay the enemy in his endeavors to ascertain tactical movements and the disposition of forces until such time as the information was out-of-date. It was evident, therefore, that the system recommended for approval should present sufficient obstacles to the solution of messages transmitted in it, so that by the time the messages could be solved by the enemy, the information derived from them would be of little value in the tactical situation.[74]

It was incumbent upon the Chief Signal Officer to train Signal Corps officers in the proper use of codes and ciphers so that as few hints as possible might be given the enemy in the transmission of the message and the greatest delay possible imposed on its solution. The Code and Cipher Section therefore prepared rules for the use of codes and ciphers embodying the best cryptographic practices.

J. Training Activities

In addition to his other duties the chief of the Code and Cipher Section was also engaged in the devising and preparation of training literature. Before his employment on an official basis, he had given annually a two-weeks course of instruction for officers at the Signal School, Camp Alfred Vail, New Jersey. This course was continued until 1930 when it was replaced by correspondence courses in Military Cryptography and Military Cryptanalysis, available for those officers who chose

---

74. TR 160.5, par. 97.

to take them.[75]

War Department Document No. 117, Elements of Cryptanalysis, based on these lectures at the Signal School, was the first manual on cryptanalysis published by the War Department.[76] It was prepared in 1921[77] and revised in May 1923 as Training Pamphlet No. 3, and was designed primarily as a text for the instruction of officers in code and cipher work. The Navy requisitioned 500 copies for use in naval training.[78] A number of secret technical papers on cryptanalysis were also prepared.[79]

K. Miscellaneous Duties

From its beginning the Code and Cipher Section served as an advisor on methods of secret communications for other governmental agencies. The Navy Department, for example, referred the Intelligence Officer of the Coast Guard to the Code and Cipher Section for assistance in the solution of intercepted code messages.[80] In May 1927 the chief of the section was

---

75. Commandant, Signal School, Fort Monmouth, New Jersey, to Chief Signal Officer, 24 September 1930 (SPSIS 201-W. F. Friedman).

76. The only similar manual published under Army auspices was issued at the Army Service Schools, Fort Leavenworth.

77. W. F. Friedman, Resume of work of the Code and Cipher Section (1921), par. 4 (SPSIS 311.5).

78. Memorandum for Colonel Voris from W. F. Friedman, 13 February 1924, par. 3a.

79. Annual Report of the Chief Signal Officer to the Secretary of War, Fiscal Year 1926, (OCSigO 319.1), p. 54.

80. Memorandum for Colonel Voris from W. F. Friedman, 12 February 1924, par. 3.

sent to Fort Adams for ten days to form a Code and Cipher Section under the G-2 of the Blue Commander in the Joint Army and Navy maneuvers of that year.[81]

Instructions were also issued directing the Chief Signal Officer to assist other departments in the preparation of code and cipher systems. Among the federal agencies to which technical assistance was given by the Code and Cipher Section in the Fiscal Year 1925 were the Navy, the Coast Guard, the Department of Agriculture, and the Department of Justice.[82]

The chief of the Section also served as War Department technical adviser to the American delegation at the International Radio Conference at Washington in 1927, and was especially concerned with the proposed revision of the international regulations governing code-language communications and the revision of the International Code of Signals. He prepared a detailed report on the history of the use of code language which, as one of the documents of the conference, had a wide distribution, and a year later he served as secretary of and technical adviser to the American delegation to the International Telegraph Conference at Brussels.[83]

---

81. Memorandum for Executive Officer, Office of the Chief Signal Officer from Lieutenant Colonel J. O. Mauborgne, 5 May 1927 (SPSIS 201-W. F. Friedman.)

82. Annual Report of Chief Signal Officer, Fiscal Year 1925, p. 9, par. 11.

83. Annual Report of Chief Signal Officer, Fiscal Year 1928 (OCSigO 319.1).

At the conclusion of the conference he visited Stockholm where he conferred with the Chief Engineer of the Aktiebolaget Cryptograph firm and witnessed demonstrations of the operations of their latest models of cipher machinery. From Sweden he returned by way of London and investigated a cipher machine made by the Powers Adding and Calculating Machine Company.[84] Liaison was also maintained from time to time with the Cryptanalytic Unit in New York.[85]

L. Conclusion

In evaluating the work of the Code and Cipher Section it must be constantly remembered that this was a period when falling War Department budgets greatly limited the activity of the unit, and that at no time during these years (1920-1929) was the staff of the unit greater than one cryptanalyst and one clerk-typist.

The activity of the unit was therefore limited strictly to such code and cipher compilation as was absolutely necessary in a period of peace and a small amount of training in the field of cryptography. Such codes as were prepared during these years represented only modest expenditures. The War Department Telegraph Code 1919, prepared just the Armistice, represented an expenditure of $14,751.24, while the

---

84. Memorandum from W. F. Friedman to the Chief Signal Officer, 12 October 1928, Subject: Report of arrival at London (SPSIS 201-W. F. Friedman).

85. See below, Chapter II.

Military Intelligence Codes Nos. 5 and 9 (1918) cost $7,169.83 and $11,001.54 respectively. Military Intelligence Code No. 10, prepared by the Code and Cipher Section and completed in 1927, cost $3,000. The Division Field Codes were much smaller in size and only one of them (No. 4) cost more than $2,000, the actual cost being $2,178.71.[86]

In spite of the limited budget, a sure foundation was laid for the future. The codes essential for use in the event of war were prepared, the task of indoctrinating officers and cryptographers of the Signal Corps in the proper use of codes was begun, and experimental work on the development of electrical cipher machinery was undertaken which was to bear fruit in later years.

---

86. Memorandum for The Adjutant General from Chief Signal Officer, Subject: Fiscal Year 1932-Estimates for the printing and binding of codes, 27 March 1930 (SPSIS 311.5).

CHAPTER II. THE CIPHER BUREAU IN NEW YORK: ADMINISTRATIVE PROBLEMS

A. New Plans for MI-8

If the signing of the Armistice on 11 November 1918 had any immediate effect upon the activity of the Cipher Bureau other than to accentuate the knowledge that sooner or later a reduction in force would be imperative, it has left no trace in the records. Indeed, some of the more important achievements of MI-8 were accomplished in the first half of 1919.[1] There is, however, good reason to believe that following the Armistice there was a gradual exodus of members of the staff; some who left did so, of course, for personal reasons but there was a reduction in force caused by "the drastic demobilization order which called for a certain percentage of the clerks to be released each day."[2] The strength of the unit at its peak in November 1918 had been 18 officers, 24 civilian cryptographers, and 109 typists and stenographers. By 16 May 1919 there were only 15 officers, 7 civilian cryptographers, and 55 typists and stenographers, a reduction in force of almost fifty percent.[3]

---

1. For an account of the work of the Bureau prior to the summer of 1919, see Volume Two, Chapters I-VI. It should be pointed out that after the move to New York in August 1919, the designation "MI-8" was, when MID was reorganized, reassigned to another MID unit. Consequently, the present files of MID will contain under this heading much material not related to Yardley's unit.

2. IR 4157: Yardley to Campbell, 14 December 1919. The reduction in force order was already affecting MI-8 before Yardley's return from France in April 1919.

3. See Memorandum for the Chief of Staff from the Director of Military Intelligence, Subject: Plans for M. I. 8, dated 19 May 1919, a copy of which is now filed in IR 4366. Note that the decline in civilian cryptographers (24 to 7) was greatest, that of clerical help (109 to 55) next largest, while the number of officers was reduced by only about fifteen percent. Civilians were able to resign at will, whereas military personnel could not do so.

Between August 1918 and April 1919 the chief of MI-8, Captain Herbert O. Yardley,[4] was in Europe, during which time he visited the Radio Intelligence Section, General Staff, at General Headquarters in France; had conferences with personnel in a number of cryptographic bureaus of Allied Governments; and was for a time attached to the American Commission for the Negotiation of Peace (ANCP) in Paris. The primary purpose of this trip was to broaden the cooperation, originally established earlier in the War[5] by Captain J. A. Powell, between the Allied cryptographic bureaus and MI-8.

---

4. Records of The Adjutant General's Office (AGRD-W201 Yardley, Herbert O., 1st Ind., 28 August 1945) show that he sailed on 15 August 1918 and returned to the United States on 18 April 1919. He was promoted to the rank of major on 17 June 1919 and was honorably discharged on 1 October 1919. He remained a civilian until 28 May 1921, when he was commissioned a major in the Military Intelligence Reserve. This commission expired at the end of five years, but he was again commissioned at the same rank and in the same corps on 7 July 1927. His resignation was accepted on 1 April 1931. (For the details see below, Chapter IV, Sections C and D.) Therefore, for the most of the period covered by this chapter he was a major in the Military Intelligence Reserve and, as will be seen from the narrative, also was a civilian employee of the Military Intelligence Division.

5. See Yardley, The American Black Chamber, chapters ix-xii, pp. 197-238, for a highly colored account of the trip. See also the note of Lieutenant Colonel A. J. McGrail (in Mr. William F. Friedman's copy of the book) which confirms Yardley's story about the existence of British clerks in the code room of the military attaché in London. McGrail, then a first lieutenant, was one of the officers sent there to take charge of a code room manned by seven enlisted marines.

The earliest extant record of the coming reorganization of MI-8 is a statement made in a letter of F. W. Allen, chief of the Shorthand Subsection in New York, to Yardley in France, dated 2 December 1918[6] which says that General Churchill, the Director of Military Intelligence, had recommended to the Chief of Staff that MI-8 "be retained in toto". This probably meant that the organization was to be retained in all its functions, not that the strength be continued at the war-time level. The following paragraphs of Yardley's reply[7] are pertinent:

> Prince[8] as you probably know had charge of compiling codes. If I had it in my power to keep him I should do so, and I should continue the work that he has been doing. But what the General Staff will approve I can not say. I gather from Capt. Manly's cables[9] to me and from officers from MID on the Peace Commission that General Churchill asked Manly for a recommendation for the reorganization of M. I. 8 on a peace basis, and that Manly included Prince's section, which of course would include Prince. I can give you nothing definite for even General Churchill with whom I have talked several times since he came abroad knows nothing definite.

---

6. The letter is now filed in IR 4149. Much correspondence between Allen and Yardley is extant: the file is that kept by Allen, not by Yardley. For the period 1919-1929 there is available also the correspondence between Yardley and his superiors in Washington, but here again the extant files are those of G-2, not of Yardley. Yardley's own files are missing, probably taken by him in 1929 on the basis of a belief that they were personal, not public property.

7. IR 4149: Letter of Yardley to Allen (25 December 1918).

8. Captain A. E. Prince, formerly in the employ of the State Department, was in charge of Code Compilation in MI-8. (See Volume Two, Chapter I.) He had approached Allen in an effort to get a civilian job. Prince was not, however, retained.

9. During Yardley's absence in Europe, Captain John M. Manly was in charge of MI-8.

As a matter of fact I am not at all sure what will happen to me. Manly cables that he recommended a large permanent organization, and added that he wanted to get back to Chicago University as soon as possible but would hold on until I got back. He also recommended that I be retained as Chief of M. I. 8, Churchill wants to keep M. I. 8, and Harrison of the State Department tells me that Secretary Lansing wants to take it over.[10] There are many many questions to decide about the matter, Congress is in Washington and both Van Deman and Churchill are on the Peace Conference. Personally I feel that one of these men should be in Washington--so there you are. I of course can do nothing at all.

The situation is so uncertain that I have already written you about getting some sort of job with the American Code Company.[11]

In any case, after Captain Yardley's return to Washington in April 1919, plans were made for the establishment of MI-8 on a peace-time basis. A memorandum was prepared for the Chief of Staff by the Director of Military Intelligence.[12] Though signed by General Churchill, it was probably the work of Captain Yardley. After reviewing the accomplishments of MI-8 and the value which such work would have during peace, the memorandum draws conclusions and makes recommendations as follows:

---

10. No other mention of this desire is on record. As will be seen later, the State Department from 1919 to 1929 gave financial support to MI-8. Indeed, before Yardley's return in April 1919 "about twenty-five of the clerks in MI-8 had been told that they would not be subject to this drastic demobilization order... because funds had been received from the State Department and they would be placed on a separate roll." See IR 4157: Yardley to Campbell, 14 November 1919.

11. The letter is missing. Yardley later established a commercial code compilation business on the side.

12. Dated 16 May 1919. See note 3.

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 organization of skilled cryptographers[13] 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 <u>civilians</u> is indicated by the following facts:

a) After the demonstration afforded by the incident of the German withdrawal from Flanders[14]... 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.[15]

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.

---

13. As used here, this word undoubtedly meant cryptanalysts.

14. This was described in the preceding part of the memorandum. See Volume Two, Chapter IV, Section A.

15. This is not quite accurate. Such a policy was not in force at the beginning of the War.

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[16] 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 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
		$100,000.00

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[19] of $60,000.00 of funds pertaining to "Contingency Military Intelligence Division, General Staff" would make possible the execution of the plans outlined above.

These recommendations of the Director of Military Intelligence were first approved by the Acting Secretary of State, Frank L. Polk, on 17 May 1919, and three days later by the Chief of Staff, General Peyton C.

---

16. "Civilian officers" were civilians who had been given direct commissions.

17. Actually the rent, including heat, light and incidentals, during the first year amounted to $5500; during the second year $6500.

18. Of the $96,000 allotted for salaries only $45,000 was actually spent in the first year of operation.

19. The contingent funds were to be paid on vouchers not subject to review by the Comptroller General.

March.[20]

B. The Removal to New York City

Who originated the suggestion that the reorganized MI-8 be transferred to New York City does not appear anywhere in the records, but apparently the plan was already in existence before the recommendations for rent, heat, and light had been inserted in General Churchill's memorandum. Had the unit remained in Washington, it would doubtless have occupied Government space and no such item would have been needed in the budget. That the move was Yardley's idea seems highly probable: during the War the Shorthand Subsection under F. W. Allen had operated in New York, and Yardley's close friendship for the chief of that Subsection may have led him to think of setting up the new MI-8 in the same city.

From the perspective gained by a knowledge of what took place in New York, it is easy to see the disadvantages inherent in moving a Military Intelligence unit of the General Staff away from Washington. Close liaison necessary between the War Department, the State Department, and MI-8, was thus hampered. Supervision of the activities of

---

20. W. F. Friedman, A Brief History of the Signal Intelligence Service (29 June 1942), p. 3. This manuscript was prepared at the direction of the Chief, Special Branch, Military Intelligence Service, and is now in the files of the Director of Communications Research, Army Security Agency. Major Yardley communicated the news of the approval of the recommendations to his friend Allen on 5 June 1919 (see letter in IR 4150).

MI-8, was also made more difficult, since Yardley's unit was to have little or no contact with other G-2 activities in the New York area. On the other hand, the possibility of maintaining greater secrecy in a unit not ostensibly connected with War Department activities may have seemed to justify the unorthodox arrangement.

Captain Yardley went to New York to look over the properties available for his office and doubtless made contact with his friend, Mr. F. W. Allen, whose business was law reporting. After examining a large number of premises, most of which for one reason or another were rejected, Yardley recommended to General Churchill on 14 July 1919 that the building at 17 East 36th Street be rented by the Government.[21] At this point it developed that Mr. Allen himself had a property, which he either owned or controlled, at 3 East 38th Street. He was willing to rent this to the Government for the same sum as had already been agreed upon for the building on 36th Street. The cost to the Government for the basement, first, second and fourth floors was to be $5500 a year, and the Yardley family was to occupy the third floor as an apartment at a cost of $900 to be paid by Yardley out of his salary. Notwithstanding the fact that General Churchill had already approved the building on 36th Street, Mr. Allen's building was substituted for it without informing the general. Both properties were conveniently close to the New York Public Library on Fifth Avenue at 42nd Street.

---

21. IR 4150: Letter of Yardley to Churchill (14 July 1919).

Mr. Allen first prepared a lease which named the Military Intelligence Division as the lessee, but Yardley for reasons of security directed him to prepare another in which the lessee was named as Yardley himself, and then the latter signed the lease upon authorization of General Churchill.[22] Extensive alterations and decorations were to be made, and quarters for the guard established in the basement. The owner was to supply heat, light, and incidentals.[23] Thus, the new headquarters of MI-8 were provided.[24]

Each of the employees who was to continue to work in New York was handed a memorandum containing among other items the following:

> Where you work, and what you do is not a matter for discussion, but rather than appear mysterious you may say that you are employed by the War Department in its translation department.

The move to New York was expected to take place in the latter part of July 1919, so that MI-8 might begin its work in the new

---

22. It is interesting to speculate on what may have taken place had such a lease ever been the subject of litigation.

23. IR 4150: letter of Allen to Yardley (25 November 1919) complaining of high charges for electricity.

24. A post office box, No. 354, Grand Central Station, was engaged on account of the heavy amount of mail to and from Washington. Only one of Yardley's letters (14 November 1923-IR 4162) bears this box address but it was used throughout the New York period.

25. IR 4150: letter of Yardley to Allen (18 July 1919). This paragraph is interesting in the light of similar problems arising in World War II.

location on or about 1 August 1919,[26] but there is reason to believe that there was a delay of about two weeks.[27] John C. Meeth, who had been an Army Field Clerk at General Headquarters in France during the War, was taken on as Chief Clerk,[28] and was sent ahead to make arrangements. The office equipment and files were shipped by freight. On 26 August 1919 Yardley ordered locks put on all the doors,[29] so the new office was probably functioning by then. In order to conceal the true nature of its activity, the office was called "Code Compilation Company," a cover name for MI-8 but the real name of an incorporated business firm established by Yardley and Charles J. Mendelsohn, partners in the venture. This firm produced and sold, in fairly large quantity, a code called the Universal Trade Code.

C. Personnel and the Budget

The initial payroll of MI-8 in New York is not available.[30] The budget as recommended and approved in 1919 had provided for the chief,

---

26. IR 4150: letter of Yardley to Allen (21 July 1919).
27. See IR 4683.
28. IR 4150: letter of Yardley to Allen (1 August 1919).
29. Ibid.: letter of Allen to Yardley (27 August 1919).
30. It may be in the records of the Budget and Fiscal office, MID, access to which could not be obtained for the purpose of this work.

Major Yardley, at an annual salary of $6,000; ten code and cipher experts at $3,000 each, fifteen code and cipher experts at $2,000 each, and twenty-five clerks at $1,200 each; but since the total outlay for salaries in the first year came to only $45,000, less than half the amount approved ($96,000),[31] it is clear that many of the positions contemplated were never filled. The names of persons known to have been employed will be given later.

The unit had been operating in New York for only about ten months when Yardley proposed spending an additional thousand dollars for rent. The whole letter is of interest:[32]

S E C R E T

3 East 38th Street,
New York, May 4, 1920

Brigadier General M. Churchill, U.S.A.,
Director of Military Intelligence,
Washington, D. C.

Dear General Churchill

Referring to my letter[33] of today regarding my request for authority to pay an additional $1000 rent per annum, I wish to show briefly the amount of money now being spent to support this organization:

Rent	$ 5,500
Salaries	45,000
Incidentals	1,000
Total	$51,700

---

31. See IR 4157: letter of Yardley to Churchill (4 May 1920).

32. See the letter cited in note 31.

33. This letter is missing.

My original estimates for this bureau, as you will recall, were $100,000--$40,000 to be paid by the State Department and $60,000 by M.I.D. Figuring on the present basis we will have spent by July 1, $40,000 of the State Department and only $11,700 of the $60,000 appropriated by M.I.D.[34] The other $48,300 has been spent by M.I.D. for other purposes. You will recall the $60,000 was tacked on to theM.I.D. bill at the last minute; in other words, M.I.D. was able to get an appropriation of $60,000 more than it would have obtained had we not created this bureau.

With the $51,700 that we shall have spent by July 1, we have, briefly, accomplished the following:

(a) Compiled a new M.I.D. code.[35]
(b) Maintained an organization for the compiling of current secret cipher tables for M.I. 5 and M.I. 9 codes.[36] These tables are sent to the Military Attachés every two weeks.
(c) Broken four Japanese codes.[37]
(d) Broken two German codes.

---

34. Apparently the State Department was not informed of the fact that actual expenses were less than estimated in advance.

35. This was Military Intelligence Code No. 9. See Volume Two, Chapter II.

36. On these codes, see Volume Two, Chapter II.

37. The details on all solutions will be treated later.

My plans for the future, when greater confidence is established between us and the various cable companies, call for a bureau that can read messages of the following important governments, which I place in what I consider their order of importance:

(1) Japan

(3) Germany

In addition, of course, we shall keep up with

The request for increasing the rent was apparently approved: while no specific approval is found in the records, the unit did move some time in June 1920[39] to 141 East 37th Street. This move was necessitated, on Yardley's later testimony,[40] by the fact that the lease on the 38th Street property had been sold. If the 37th Street property is the one for which an increase in rent was necessary, the cost of housing was now $6,500 a year in rent, or

---

38. See below, Section D, on interception and the cable companies.

39. IR 4193: letter of Yardley to Campbell (1 July 1920).

40. Letter of Yardley to Frederick Sullens, who had been an officer in MID (not, apparently, in MI-8), had written Yardley a very sharp rebuke for publishing The American Black Chamber: Yardley's reply is characteristically rambling and does not even attempt to meet the main point made by Sullens that Yardley was a traitor to his country but it contains a number of statements about the New York office which he is not known to have made elsewhere.

056

about $542 a month.[41] On the 22nd Yardley wrote to Colonel Locke that he had "finally got a settlement on the lease yesterday for $1200." Just what this means is not certain: the presumption is that the lease with Mr. Allen had been cancelled for a consideration of $1200. If this surmise is correct, the Government was allowed to cancel its lease in return for about three months' rent. But if, as has been stated on Yardley's own testimony, the reason for the move was the fact that the lease had been sold, it is not clear why the Government should have had to pay for periods in which it did not occupy the building.

As the Fiscal Year 1920 drew to a close, the chief of MI-8 prepared a memorandum for the Director of Military Intelligence (June 1920) in which he recapitulated the record of MI-8, both in the Washington and New York periods. This memorandum, which was accompanied by a graph of the progress made,[42] was as follows:

---

41. The new building continued to be the headquarters of MI-8 only until November 1923: when on the fourteenth of that month, Yardley wrote Moorman, he did not use his street address, as always before and afterwards, but his cover address, Post Office Box 354, Grand Central Station, New York. See IR 4162: letter of Moorman to Yardley (14 November 1923) and letter of Yardley to Locke (22 November 1923).

42. Figure 1.

43. A copy is now filed in IR 4158.

Figure 1

058

SECRET

3 East 38th Street,
New York, June 5, 1920.

MEMORANDUM FOR THE DIRECTOR OF MILITARY INTELLIGENCE:

Subject: Number of alien codes and ciphers broken.

1. The principle [sic] codes and ciphers than [sic] can be read at present are as follows:

059

2. The greatest accomplishment during the fiscal year of 1920 was the breaking of four Japanese diplomatic codes.

3. Plans for the fiscal year 1920-1921 call for the breaking of the unsolved Japanese diplomatic, military, and naval codes.

In addition, it should be pointed out that the use of the word "codes" in this connection is highly inaccurate. No had at this time ever been solved by MI-8; a few codes had been compromised, but the great majority of the readable systems were ciphers, fairly simple ones at that.

44. See Volume Two, Chapter IV.

The unconventional status of Yardley's unit, existing, as it did, in a sort of quasi-autonomy, involved a number of administrative difficulties. For example, when Colonel A. G. Campbell assumed his position in the Military Intelligence Division as the officer by whom correspondence with Yardley was conducted, he was apparently impressed by the unusual character of the unit in New York and desired to see the official authorization. He wrote to Yardley:

> As a matter of fact, after looking through the safe this morning, my files, I find, are woefully deficient with reference to any authority for your work.[45]

He therefore requested, and no doubt received, a copy of the authorization mentioned. From time to time, also, other officers, not connected with Yardley's work, discovered the unit in New York, and not being aware of its secret nature, raised questions concerning it. General Grote Hutchinson, of the General Intermediate Depot in New York, learned in some way about Yardley's office and wrote a letter to the Adjutant General of the Army, reporting that space was being rented at Government expense while he himself was able to supply other quarters in a building at 39 Whitehall Street.[46] His letter came to the attention of Colonel Stuart Heintzelman, then in the Military Intelligence

---

45. IR 4158: letter of Campbell to Yardley (8 June 1920).

46. IR 4161: letter of Hutchinson to Heintzelman (23 November 1921).

Division, who wrote tactfully to the general, making it plain, however, that there was no possibility of moving Yardley to Whitehall Street.

The channel through which Yardley's supplies were drawn was the office of the Assistant Chief of Staff, G-2, Second Corps Area, Governor's Island, New York. A new Assistant Chief, Colonel J. R. Proctor, was asked to sign vouchers for Yardley and did so at first without question. Later he was disturbed by the lack of authority for his signature and wrote on 30 December 1921 for information.[47] Sufficient information was given him to assure him that Yardley's supplies were being used for Government purposes. Colonel Heintzelman's letter concludes:

> I know with this explanation that you will sign the vouchers in question and outside of this, hope you will forget about the existence of Mr. Yardley.

The employees at work in MI-8 during the first year of its existence included the following persons:

Herbert O. Yardley, chief of the section, salary $6,000.

---

47. IR 4163: Colonel Proctor visited Yardley's office, where he was received with courtesy but could learn little.

Frederick Livesey, who had been for eighteen months a first lieutenant in G-2, A-6, at General Headquarters in France. He was demobilized on 21 July 1919 and put on the MI-8 payroll the next day at a salary of $3000. He is said to have been able to work in Spanish, French, German, Russian, Italian, and Portuguese. Note that Japanese is missing from the list, though afterwards Livesey became MI-8's chief Japanese cryptanalyst and translator.[48]

John C. Meeth, formerly an Army Field Clerk in G-2, A-6, in France.[49]

Claus Bogel, Dorothea B. Jachens, Nellie A. Simpson, and Ruth Willson, all of whom had been formerly employed by MI-8 in Washington as civilian cryptographers.[50]

Robert Arrowsmith, who had been recommended by General Churchill, had passed all examinations, and was put on the payroll at $2500 on 14 July 1919.[51]

Charles J. Mendelsohn, who as a captain had been in charge of the German Code Solving Section of MI-8 in Washington. He was demobilized on 1 August 1919, returned to his work as Professor of History at City College, New York, but continued to spend part of his time in MI-8, being paid on an hourly basis.[52] His salary was at the rate of $3000 per annum.

---

48. See Memorandum for General Churchill, Subject: Personel Civilian Bureau, signed by H. O. Yardley as Major, undated but obviously prepared in August 1919. See Volume Two, Chapter VIII.

49. See Volume Two, Chapter VIII.

50. See Volume Two, Chapter I. Miss Willson was still on duty in MI-8 in 1929. Bogel's salary had been only $1500 but he was promoted to head the French work at a salary of $2000 on 1 August 1919.

51. See memorandum cited in note 48.

52. See memorandum cited in note 48.

Henry D. Learned, who was a lieutenant, demobilized 15 August 1919. "He is unusually equipped in German and is making rapid strides in code work." He was put on the payroll on 16 August 1919 at the rate of $2500 per annum.[53]

Victor Weiskopf, an employee of the Department of Justice on loan to MI-8 as a cryptographer. He also had participated in solution in the Washington period.[54]

I. H. Correll, a retired clergyman who had formerly been a missionary in Japan.[55]

Edna Ramsaier.[56]

---

53. See memorandum cited in note 48. Lieutenant Commander Learned, USNR, was a member of the Navy signal intelligence service during World War II.

54. See Volume Two, Chapter I. Weiskopf later was transferred to the MI-8 payroll and was still on duty in MI-8 in 1929.

55. See IR 4158: letter of Churchill to Yardley (18 December 1919), approving Correll's appointment as a Japanese translator for three months at the rate of $4,000 a year. Correll remained only six months, according to The American Black Chamber. His salary was $4000.

56. Miss Ramsaier was still on duty in MI-8 in 1929 and was one of the six persons then given a bonus, as will be described at a later point in the narrative. Sometime afterwards she became Mrs. Hackenberg and in 1939 or 1940, she applied for a position in the SIS. During the interview she gave no indication of any special devotion to Yardley. She had preserved silence on MI-8's activities, and was a competent clerk with a number of years of experience. She was therefore put on the SIS payroll. It later developed that she was corresponding with Yardley, then in China. Though this was an undesireable feature, she was not dismissed. Later, when Yardley himself was employed by the Canadian Government, she applied for a leave of absence to assist him. This was granted. When he terminated his work in Ottawa, she applied for reinstatement with the SIS but this was not granted, though officials of the SIS gave her some assistance in obtaining a position in New York. During World War II she became the second Mrs. Yardley.

Margaret C. Forrester, typist.[57]
Marguerite O'Connor, typist.
Isabelle V. DeForest, a file clerk.
Thomas K. Lomas, operator of the mimeograph machine.
Edith W. Hastings.[58]
Leah B. Andrews.
Serena B. Laning.[59]

The salaries paid some of these persons have been indicated; in the case of the others, salaries prior to 1 January 1921 can be inferred from a document shortly to be mentioned: eliminating any item for Mr. Weiskopf's salary, which at this time was not paid out of MI-8 funds, and any item for Dr. Mendelsohn, who worked only part time, the total cost to the Government for the services of the entire list would be less than $35,000 a year, yet it is known that the payroll for the first year (roughly Fiscal Year 1920) was $45,000. The conclusion is inescapable that other persons were at work in MI-8 but that their names have been lost.

---

57. Misses Forrester, O'Connor (later Mrs. J. C. Meeth), and DeForest, and Mr. Lomas, are mentioned in IR 4158: letter of Yardley to Campbell (15 July 1920), as then receiving a salary of $1100 a year.

58. Misses Hastings, Andrews, and Laning, were employed by MI-8 early enough to have merited a promotion of $120 a year on 1 January 1921. See IR 4161: recommendations of promotions dated 7 June 1921.

59. Although Miss Laning was not highly paid, she was described by Yardley as "a very clever girl . . . [who] . . . knows Japanese." See IR 4158: letter of Yardley to Campbell (7 July 1920). She had been an employee of the Office of Naval Intelligence in World Warl I, and much later, in World War II, she was an employee of the Signal Security Agency first as a Japanese translator and then as a French translator. She was born in Japan where her father was a prominent medical missionary. In June 1946 she described life in MI-8, her feeling, never completely suppressed, that somehow MI-8 was doing unethical work, and of the circumstances surrounding her dismissal in [redacted] were lacking.

In July 1920 Mr. Livesey received an offer of employment in the Far East at a higher salary. He was told by Yardley that "there was a real future in this bureau for him and that if he would reconsider his position I should immediately recommend an increase from $3000 to $3500."[60] The increase was approved. This arrangement saved Livesey's talents for MI-8 for a time. He had become the chief Japanese expert and also knew Spanish, Portuguese, French, German, Italian, and Russian, and was thus the most capable linguist MI-8 had. Some difficulity had been experienced in connection with him: what it was is not known, but there is an allusion to it in a Memorandum for the Director, Military Intelligence Division, which Major Moorman prepared on 9 November 1920, following a conference with Yardley.[61] The report is as follows:

MEMORANDUM FOR DIRECTOR, MILITARY INTELLIGENCE DIVISION.

Subject: Code and Cipher Work.

As the result of a conference with Mr. H. O. Yardley, I submit the following report on the above subject.

1. With the exception of some little difficulity with Mr. Livesey about which I talked with you the office seems to be well organized and functioning in a satisfactory manner.

---

60. See the letter cited in note 59.

61. IR 4158: Livesey is styled "Charles Mundy" in The American Black Chamber, chapter xv

Proper precautions to guard the secrecy of the work have been taken. Yardley is doing excellent work. His energy, loyalty and good judgment are exceptional. If the personnel is to remain exclusively civilians I would recommend no changes. I believe, however, that the nature of the work makes it desirable to have a [sic] military personnel either immediately available for or actually on duty in the office. I would suggest that this be accomplished by the detail of young officers from time to time for duty in Yardley's office and the gradual displacement of civilian personnel by such of these officers as show special ability and by intelligent enlisted men. Names of officers for above details can doubtless be obtained from service schools, especially the Signal Schools.[62] Yardley agrees that the detail of commissioned officers to his office is very desireable.

2. Request for increase in pay of some civilians was made by Yardley and forwarded to your office recommending approval. The question of pay for Livesey will be taken up at a later date.

3. Yardley fully concurs in the plan to have all codes prepared by the Signal Corps. This work will be gotten under way as soon as the Signal Corps can arrange for the neccssary personnel.[63]

4. As now arranged the code section is practically supported by the State Department.[64] The Department of Justice furnished one man.[65]

---

62. Major Moorman doubtless remembered the time when in 1916, as Acting Director of the Army Signal School at Fort Leavenworth, he had himself made a similar recommendation (see Volume One, Chapter VI).

63. At this time Mr. William F. Friedman had not yet been employed as cryptanalyst in the Office of the Chief Signal Officer. (See above, Chapter I.)

64. This was true because the entire State Department appropriation was used by MI-8; the War Department merely contributed additional funds to meet expenses.

65. Victor Weiskopf.

5. Just now it appears very desirable to arrange for the interception of as many messages as can be obtained in the Japanese Naval Code. This will enable a study and probable breaking of this code and will greatly simplify the work at a later date should it be necessary to read such messages for military or naval use. If this work is delayed until an emergency arises, it will require weeks—perhaps months—to make the first solution and during this time information of vital importance will be unavailable. If the Navy is requested to furnish the desired messages now they will naturally wish to know for what purpose and to what extent they are used. It is very desirable to confine information of this character to the fewest possible persons, but on the other hand it must be made known to some in order to make it useful.

6. Should the Navy organize a code and cipher section to work independently of ours, it would result in great duplication of effort. On the other hand a free exchange of information between the separate Army and Navy sections would facilitate the obtaining of valuable information by unauthorized persons.

7. In view of the above I wish to recommend a radical change in the relations of this office to the Navy Department. Objections offered by Major Collins and others, however, seem to indicate that such change is inadvisable at the present time. I am therefore forced to the conclusion that it will be better to make the best use of available Army facilities and await a more favorable time for gaining the cooperation of the Navy. I have prepared and filed in the office safe a proposed agreement with the Navy which will be submitted for your consideration should circumstances seem to warrent.

The recommendation made by Major Moorman in paragraph 1 of his report was carried out by the detailing of Major K. F. Baldwin about 1 December 1920.[66] While on duty in MI-8 Major Baldwin was promoted to Lieutenant Colonel[67] and left about 8 January 1921.[68]

---

66. IR 4158: letter of Baldwin to Collins (10 December 1920).

67. Unless Yardley is inaccurate in calling him "Colonel".

68. IR 4161: letter of Yardley to Nolan (8 January 1921).

There was no dissatisfaction with Colonel Baldwin's work, but he was a Japanese expert on temporary duty. Later, a Major McLean, was also at work in MI-8, but how long is unknown.

On 5 January 1921 Yardley addressed a letter[69] to Major Moorman in which he raised the question of an increase in salary for himself. The letter contains the following paragraphs:

> I think that I have outlined to you the difficulties I had in creating this bureau. When we started, the work on a peace time basis was purely an experiment. I gather from both you and General Nolan that my faith in the necessity for such a bureau in peace time has been justified.
>
> My ambition since the armistice has been to break enough codes to awaken the government to a sense of responsibility in this sort of work even in peace times. This I now feel that I have done, and in return I believe that I should be informed what the future holds for me, provided that I continue to be successful and provided that Congress supplies the funds.
>
> I am in this work because I love it. I developed many friends during the war who have offered to give me opportunities to make good in the business world, who tried to prevent me from remaining with the government. I did not stay with the government because there is money in this sort of work, but because I believe in it and enjoy it. At the same time I wanted a respectable living, and have got it. It isn't much as people speak of money today, but I can live decently on it, and I am quite content for I manage to find a little time for other things, and once in a while opportunities to pick up some money here and there.[70]
>
> However, Army Officers know pretty generally what the future holds for them financially, and of course have a feeling of security that a civilian can never enjoy. And I believe that my record deserves frankness on the part of the government.

---

69. IR 4161.

70. Probably an allusion to the code company with which he was affiliated. Later he also engaged in the real estate business.

The last thing I want anyone to feel is that I am being overpaid as government salaries go. I do know however that many special appointees in Washington make from $8,000 to $10,000.[71]

I should like to have you compare my work with the work of these men and determine what I may hope for in the future. I started at $6,000 in October, 1919. If I am ever to be considered for a promotion, I feel that I should be considered now.[72] However, I wish to state very emphatically that I should prefer to continue as I am now than to have my superiors feel that a promotion would make me an overpaid employee.

I would add that Major Fischer's estimate of $46,000 as our present rate of disbursements is incorrect. My figures indicate that even with the promotions that you have already authorized, we will spend about $42,300 plus incidentals. This leaves a balance of about $6,000. Fischer's is incorrect due to the fact that several employees he had on his list have resigned.

The appeal for the increase in salary was successful, and not only Yardley but also all of the other employees except two (Barrie and Bogel)[73] were also promoted. The recommendations, as prepared by Yardley, were as follows:[74]

---

71. The closest existing parallel case was that of Mr. Friedman who was then receiving $4500, whereas Yardley never received less than $6000.

72. Only fifteen months had passed since he first was paid $6000.

73. Barrie had never received an increase in his salary, which was then $1440. Bogel had been increased from $2000 to $2500 on 1 January 1921, when eleven other employees had also received increases.

74. IR 4161 (7 June 1921).

Name	Salary	Last Increase	Recommended	Total
O'Connor, Marguerite	$1300	$100,1 Jan 1921	$100	$1400
Ramsaier, Edna	1300	100,1 Jan 1921	100	1400
Lomas, Thomas K.	1300	100,1 Jan 1921	100	1400
deForest, Isabelle V.	1300	100,1 Jan 1921	100	1400
Forrester, Margaret C.	1300	100,1 Jan 1921	100	1400
Barrie, William	1440	none	none	1400
Hastings, Edith W.	1520	120,15 June 1920	180	1700
Andrews, Leah B.	1700	180,1 Jan 1921	100	1800
Simpson, Nellie A.	1700	180,1 Jan 1921	100	1800
Laning, Serena B.	2200	200,1 Jan 1921	200	2400
Arrowsmith, Robert	2500	none	200	2700
Bogel, Claus	2500	500,1 Jan 1921	none	2500
Meeth, John C.	2500	400,15 Feb 1920	250	2750
Willson, Ruth	3500	500,1 Jan 1921	250	3750
Livesey, Frederick	4000	500, 1 Jan 1921	500	4500
Yardley, Herbert O.[75]	6000	none		

The recommended increases were approved in a memorandum prepared for the Finance Officer, Military Intelligence Division, by Major James L. Collins on June 1921.[76] Yardley was given a 15 percent increase as well, from $6000 to $6900 a year. At the same time, however, Yardley, and also the other employees, were informed by Major Collins that the limit had now been reached and it was suggested, politely but firmly, that if anyone in MI-8 were dissatisfied, he might make arrangements for employment elsewhere. To Major Collins' letter General Nolan appended a note, "This is office policy."

---

75. He modestly refrained from specifying the amount of the increase requested.

76. IR 4161 (20 June 1921).

Soon afterwards Yardley applied for a month's leave, stating that he had had, except for a day or two now and then, no vacation since about 1915. He had been an officer or civilian employee of the Government all that time.[77]

The value of the cryptanalytic unit prepared for use in connection with secret hearings before Congressional appropriations committees. It was necessary to defend the use of large sums for this purpose. The text is as follows:[78]

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 PUBLICALLY [sic] OR 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)[79] 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

---

77. IR 4161: letter of Yardley to Moorman (13 June 1921).

78. IR 4164.

79. Exhibit I in Yardley, Achievements, Part III.

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 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. Such a loss can only be made good by much work otherwise unnecessary. 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.

As an expression of appreciation of the hard work done by MI-8 during the Washington Disarmament Conference then in session, Christmas bonus of $998 was sent to Yardley to be distributed to the employees of MI-8 on a prorata basis: the report to Colonel Heintzelman of the distribution was dated 27 December 1921:[80]

Robert Arrowsmith	$72
William Barrie	39
Claus Bogel	67
I. V. DeForest	37
M. C. Forrester	37
E. W. Hastings	45
F. Livesey	120
S. B. Laning	64
Thomas Lomas	37
J. C. Meeth	74

80. IR 4161: letter of Yardley to Heintzelman (27 December 1921). Such a bonus was possible because MI-8 was supported out of secret funds on vouchers not subject to audit and review by the Comptroller General. (A precedent for this Christmas bonus had been established in the days of the early Papal cryptographers.)

M. O'Connor	$37
E. Ramsaier	37
Nellie Simpson	48
R. Willson	100
H. O. Yardley	184
Total	$998

As the Fiscal Year 1923 drew to its close the situation in MI-8 was such that a drastic reduction in force was necessary. This was doubtless caused by falling budgets and a decline of intercepts. In any case, several of the persons listed above as having received the Christmas bonus in 1921 were now about to be dismissed. The payroll at this time was the same as it had been at the time of the bonus, except that Victor Weiskopf, then an employee of the Department of Justice, was now on the MI-8 payroll.

Of the sixteen persons on the staff, nine were to be dismissed, but they were to be given at the same time a cash bonus[81] which in every case but one amounted to four months' salary. In the exception, the bonus amounted to six months' salary. The persons now dismissed were as follows:[82]

Name	Salary
Barrie	$1440
Forrester	1440
O'Connor	1800
Ramsaier	1400
Weiskopf	3660
Willson	3750
Yardley	6900
Meeth (1 Month)	229.16
Total	$20,579.16

81. This was in line with the idea that special consideration should be shown these people since they had no Civil Service status and could not use their talents in business or in other government work.

82. See the list in IR 4162.

It should be noted that this reduction in force affected some of the most competent personnel then at work in MI-8, and that Yardley gave assistance to several of them in their effort to find employment elsewhere. Misses Laning and Hastings were at first inclined to doubt Yardley's judgment in dismissing them, but the others are said to have accepted the reduction in force as inevitable.[83] Livesey was ultimately employed by the State Department, Bogel by the Navy, and Meeth by a business house:[84] the subsequent careers of the others are unknown.

The budget for the Fiscal Year 1924 thus became:

Bonuses	$ 7,508.31
Payroll	20,579.16
Rent	6,500.00
Office Expense	412.53
Total	$35,000.00

The following paragraphs discuss the budget:[85]

> The enclosure[86] will give you the entire story of salaries, expenses, bonuses, the 1923-1924 payroll, and the budget for 1923-1924. You will note that I have been obliged to make a slight change in the personnel. I have promoted Miss O'Connor from $1400 to $1800 and let Mr. Meeth go who was being paid $2750. However, I have asked him to remain until August 1st in order to give him plenty of time to break

---

83. IR 4162: letter of Yardley to Locke (5 May 1923).

84. IR 4162: letter of Yardley to Locke (14 May 1923), and to Moorman (26, 31 May 1923). Livesey rose to become Financial Adviser to the Secretary of State (1944); Bogel joined the Code and Signal Section of the Navy and remained there until about 1926, then went to the Library of Congress where he worked in the Reference Room until he reached retirement age (70).

85. IR 4162: letter of Yardley to Locke (5 May 1923).

86. This has already been discussed.

in Miss O'Connor and to consolidate our files so that we can reduce them and get rid of furniture that we shall not need. The total, as you will note, is exactly $35,000. In 1924-1925, if we retain the present personnel, we will be able to save the bonuses which amount to $7508.31, and $229.16 which we are paying Mr. Meeth for July, 1923--a total saving of $7737.47. This will reduce the $35,000 to $27,262.53 and if we can save $2,262.53 by moving to smaller quarters we will be able to maintain the present bureau during the year 1924-1925 on $25,000, or $10,000 cheaper than it is now costing us.

In 1919 our organization called for an expenditure of $100,000. This was reduced to something like $70,000, and then to $50,000; next year we are reducing it to $35,000 and if the plans outlined above are followed we shall, for the following year, reduce it to $25,000. This means that in the year 1924-1925 we will be spending only 1/4 of the money that was planned for this bureau when it was established in 1919, or a reduction of 75% in a period of five years.

According to our figures you will have something like $1700 left over from the appropriation for 1922-1923. It is respectfully suggested that instead of returning this to the State Department it be set aside for any emergencies that may arise.

Though the reduction in force was drastic, in November 1923 another clerk was dismissed, for what reason is not known.[87]

In the next month it was reported that though the budget for the Fiscal Year 1924 had been set at $35,000, Yardley had been able to reduce actual expenses to the point where only $1,875 was being spent each month ($22,500 a year), apportioned as follows.[88]

---

87. IR 4162: letter of Moorman to Yardley (3 November 1923).

88. IR 4162: Memorandum for Colonel Locke from Finance Officer, G-2 (15 December 1923). Yardley wrote again to Locke on 18 December 1923 (ibid): "What do you think of the chances of continuing next year and do you think we will begin to get the J material again?"

Salaries	
2 persons at $1400	$2800
1 person at $1800	1800
1 person at $3660	3660
1 person at $3750	3750
1 person at $6900	6900
Rent	3000
Incidentals	590
Total	$22,500

Cheaper rent had been found elsewhere, two or three rooms in a large office building at 52 Vanderbilt Avenue.[89] Plans for the Fiscal Year 1925 were drawn up with $25,000 as the maximum amount needed.[90] Of this sum, the State Department was prepared to supply $15,000, but Yardley was expected to cut his expenses below $25,000, if possible.[91] To this Yardley apparently replied with a request for an increase in his own salary and, surprisingly enough, in spite of falling War Department budgets, this was granted him.[92] The new salary was set at $7500, instead of $6900, and in addition he was to receive reimbursement for rent at $150 per month for eight months (a total of $1200). This was the last increase he received before leaving Government service in 1929.

---

89. In the letter to Frederick Sullens, 6 June 1931, already cited above, Yardley stated that the reason for moving to Vanderbilt Avenue was that the premises on 37th Street had been rifled by a foreign government. No other source confirms this statement.

90. IR 4160: letter of unknown (Milliken?) to Yardley (1 May 1924).

91. IR 4160: letter of unknown (Moorman?) to Yardley (10 May 1924). The new State Department representative was to be Arthur Bliss Lane.

92. IR 4160: Locke to Yardley (11 June 1924).

Miss Ramsaier, however, received an increase from $1400 to $1600 in January 1925.[93]

When in 1929 the unit in New York was amalgamated with the Code and Cipher Section, Office of the Chief Signal Officer, to form the Signal Intelligence Section, the payroll of MI-8 was as follows:[94]

Herbert O. Yardley	$7500
Ruth Willson	3750
Victor Weiskopf	3660
Marguerite O'Connor	1800
Edna Ramsaier	1600
Alice Dillon	1320
Total	$19,630

D. The Problem of Interception

Plans for establishing MI-8 on a peace-time basis in 1919 included no provision for the development of facilities for obtaining the necessary intercepted messages. A detailed account of the situation will be given shortly but at this point it will suffice to indicate that it was doubtless assumed that the cable companies would continue to supply copies of all messages passing through their offices and that the Signal Corps would continue its war-time intercept facilities which would be at the call of MI-8. These assumptions proved to be unwarranted. That no satisfactory solution for this problem was ever reached was one of the prime causes for

---

93. IR 4160: Yardley to Milliken (24 January 1925).

94. See note made by Mr. William F. Friedman at the bottom of the memorandum cited above in note 2. The information was derived from the fiscal records of the Military Intelligence Division.

the decline of activity in MI-8 in New York. It was also one of the factors which led to the absorption of the Bureau by the Signal Corps, an organization which could more easily develop intercept facilities.

The legal aspects of the problem of obtaining the necessary traffic for cryptanalytic studies caused great difficulty. During the War, the obtaining of cable traffic presented no problem and until the end of all cable censorship (1919)[95] all the messages entering or leaving the United States were at the disposal of MI-8. In 1919 the Radio Communication Act of 13 August 1912 was still in effect.[96] It had been enacted after the proclamation of the International Radio-telegraph Convention of 8 July 1913. Formulated and signed in London in 1912, this was the first international convention of its type to which the United States adhered. It provided that the Government would guarantee the secrecy of communications.[97]

> No person or persons engaged in or having knowledge of the operation of any station or stations shall divulge or publish the contents of any messages transmitted or received by such station, except to the person or persons to whom the same may be directed,

---

95. Cable Censorship on Far East circuits was ended 21 December 1918. Limitations on the use of codes were ended the next day. Later in the same month it was reported that the United States was willing to end all censorship but the British and French wished to continue. Early in 1919 censorship was dropped.

96. Statutes at Large, Volume 37, Part I (Washington, 1913), p. 307.

97. "International Radiotelegraph Convention signed at London, 5 July 1912, proclaimed 8 July 1913," Statutes at Large, Volume 38, Part 2 (Washington, 1915), "Service Regulations," Act X, Sec. 3.

> or their authorized agent, or to another station employed to forward such message to its destination, unless legally required so to do by the court of competent jurisdiction or other competent authority.[98]

This law was in effect until the enactment of the Radio Act of 1927, which empowered the Interstate Commerce Commission, under the Department of Commerce and Labor, later the Department of Commerce, to enforce its provisions.[99] Note that the law did not prohibit the interception of radio traffic but merely forbade the divulging or publishing of the contents of messages to unauthorized persons.

The Act of 1927, however, dealt with this matter more specifically and in much greater detail:

> No person receiving or assisting in receiving any radio communication shall divulge or publish the contents, substance, purport, effect, or meaning thereof except through authorized channels of transmission or reception to any person other than the addressee, his agent or attorney, or to a telephone, telegraph, cable or radio station employed or authorized to forward such radio communication to its destination, or to proper accounting or distributing officers of the various communicating centers over which the radio communication may be passed, or to the master of a ship under whom he is serving, or in response to a subpoena issued by a court of competent jurisdiction, or on demand of other

---

98. "An act to regulate radio communication," 13 August 1912, Sixty-Second Congress, Session II, ch. 287, Statutes at Large, Volume 37, Part I, p. 307.

99. This provision was incorporated in the codification of the laws of the United States in 1926. "The Code of the laws of the laws of the United States of American, of a general and permanent character in force December 7, 1925", Statutes at Large, Volume 44, Part 1 (Washington, 1926), p. 1554.

lawful authority;[100] and no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purport, effect or meaning of such intercepted message to any person; and no person not being entitled thereto shall receive or assist in receiving any radio communication and use the same or any information therein contained for his own benefit or the benefit of another not entitled thereto; and no person having received such intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that such information was so obtained, shall divulge or publish the contents, substance, purport, effect, or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto: Provided: That this section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication broadcasted or transmitted by amateurs or others for the use of the general public or relating to ships in distress.[101]

This act created the Federal Radio Commission of five members and also extended the definition of radio communication. It included within this category "any intelligence, message, signal, power, pictures, or communication of any nature" which was transferred "by electrical energy from one point to another" without the aid of any wire connecting the points, and any system by which this transfer of energy was effected. This provision remained in effect until the Federal Communications Commission was created in 1934.

---

100. Apparently this provision ("or on demand of other lawful authority") in the law was never used to justify interception of foreign diplomatic traffic. An interesting question is raised by the fact that no legal test has ever been made as to whether the act of interception, as distinct from the act of divulging the contents of an intercepted message, is prohibted by the statute.

101. "An act for the regulation of radio communications," February 23, 1927. Sixty-Ninth Congress. Session II, ch. 169, Statutes at Large, Volume 44, Part II (Washington, 1927) Sec. 27, p. 1172.

It effectually outlawed any intercept activities either in time of peace or time of war.

The effect of the Act of 1912 was to hamper, and that of the Act of 1927 to forbid, the interception of radio traffic of any kind, either in time of peace or time of war, though this could hardly have been the intention of the Congress in enacting these two laws. The purpose behind the legislation was of couse, the security of communications from the danger of interception by unauthorized persons who might have made use of the intelligence contained therein for personal profit. That the laws would also hamper Governmental agencies engaged in the production of intelligence upon which the safety of the United States might be based was probably far from the minds of the legislators. Indeed, prior to World War I, no such agency existed, and until 1931, the fact that one had existed during the war period was unknown either to the general public or to most officers in the Army itself.

On the other hand, inclusion in these acts of specific exceptions permitting the interception of radio communications for the purposes of military intelligence would have given notice to the world in general, and therefore to a possible enemy in particular, that cryptanalytic units were indeed operating. Such a course would have been highly undesirable. What solution this thorny problem could have had is not clear: the fact that no solution was ever reached constituted one of the greatest obstacles to the proper functioning of MI-8.

During World War I radio intercept of fixed station material in the United States by the Signal Corps was rudimentary. The task was, of course, a responsibility of the Signal Corps, but radio communications could hardly compete with cable and wire communications as a source of raw material because, not only did the large governments use cable in preference to radio, but also radio was then in its infancy as a means of communication between widely-separated fixed stations. The Signal Corps did have what were called "mobile transmitter" units stationed on the southern border, and these supplied considerable Mexican material. In late 1918 one large intercept station was established at Houlton, Maine, for the purpose of intercepting transatlantic radio messages. The large intercept stations maintained by the Signal Corps in France supplied a large quantity of which was forwarded as raw material to the Military Intelligence Division in Washington, but as soon as the War was over all these sources of intercept material were abandoned, leaving only the cable offices for this purpose. (The station at Houlton continued in operation during at least a part of 1920.) As long as the cable and wire services were operated under censorship, access to the messages was, of course, easy. It remained so for a year or two after censorship was discontinued by virtue of various secret arrangements made by the Director of Military Intelligence with the heads of the cable companies.[102]

---

102. This paragraph owes much to L. F. Hitchman, A Brief History of the Naval Intelligence Service (1942).

The story of how the negotiations _____ were made is contained in a later letter of Yardley, which includes the following paragraph:[103]

> I returned from France in April, 1919. At the time the State Department was trying to establish liaison with _____ During the following six months, it had no success and I finally suggested to _____ that he see _____ [sic] himself. Such a conference was arranged, _____ I saw _____ some time in September. After we had put all our cards on the table, _____ seemed anxious to do everything he could for us and instructed _____ to give us what we wanted with the exception of messages

A messenger was to call _____ each morning, pick up the messages available, "take them to the office[104] and return them before the close of the same day." _____ were the governments deemed most important for this purpose.

In the spring of 1920 negotiations were under way for the establishment of a channel through which intercepts could be gotten also from the _____ This company appears to have been less willing to cooperate _____ or at least to have been more disturbed by

---

103. IR 4161: Memorandum for _____ (5 April 1921).

104. The office of the Military Intelligence Division in Washington.

by the legal aspects of the problem. The files contain much correspondence on these negotiations[105] which were apparently carried on through an intermediary, a New York lawyer named [redacted]. Care was taken to phrase letters in such a way that no outside person would understand them. In one case [redacted] the latter's wife. For this reason, the steps by which the negotiations were carried on are not always clear. Later in the same year negotiations were also carried on to gain material from [redacted] who had been a commissioned officer in Military Intelligence during the War.

At this time intercepts were regularly received from both [redacted] in April 1921, for on the second of that month Yardley asked [redacted] to supply messages filed by an agent of [redacted] in whom MI-8 was then greatly interested.[107]

It developed, however, that there was opposition to extending any further favors to MI-8 and that this opposition was due to friction created by misunderstandings of a political and commercial

---

105. IR 4157: correspondence between Churchill, Yardley, and [redacted] (22, 23 March; 22 April 1920).

106. IR 4157: letter of Yardley to Campbell (15 April 1920).

107. IR 4161: letter of Yardley to Military Intelligence Division (2 April 1921).

nature between other departments of the Government

Yardley proposed that General Nolan have a conference with President

to see whether a modus operandi could not be worked out which would be satisfactory to both sides.[108] No further record on this subject appears in the files, continued to cooperate for about two years longer.

No real pressure was brought to bear upon the Signal Corps to establish intercept stations, though a few relatively weak efforts were made in this direction. For example, Major Moorman on 9 April 1921 prepared a memorandum for the Director of Military Intelligence in which he suggested that, as the Signal Corps had six men qualified to copy Japanese radio traffic,[109] these men be sent to the Philippines to establish an intercept station for MI-8 in the Islands. Nothing came of this; but four years later, after the cooperation of the cable companies had been largely curtailed, the Director of Military Intelligence recommended the establishment of "an efficient intercept station in the Far East."[110]

---

108. IR 4161: letter of Yardley to Nolan (5 April 1921). See the attached indorsement of Nolan to Hurley in the State Department, disclaiming some of the opinions expressed by Yardley.

109. IR 4161: Memorandum for the Director, Military Intelligence Division, Subject: Radio Intercept Operators, 9 April 1921.

110. Memorandum to The Adjutant General from the Assistant Chief of Staff, G-2, Subject: Japanese Telegraph Code, 26 March 1925 (SPSIS 322).

Meanwhile, Captain Fred G. Miller, Signal Corps, had recommended that four expert telegraphers be sent on a special mission to join the United States Army Forces in China. They were to study the Japanese language under a competent instructor and to acquire the ability to read the Japanese radio code, that is, become intercept operators. They were to be available upon their return, for assignment to G-2 and to the Signal Corps for the purpose of instructing others.[111] The Signal Officer of the Philippine Department considered operators trained to handle Japanese Morse code to be indispensable to efficient intercept work.[112] The Chief of Staff of the Philippine Department concurred promptly in the recommendation, as follows:

> The character of any future conflict in this part of the world will force both sides to depend largely upon the use of radio for the transmission of information. The need of American radio operators who can intercept and copy messages in Japanese code is apparent and immediate steps should be taken to provide a corps of operators in our forces skilled in this difficult business.[113]

---

111. Captain Fred G. Miller to Assistant Chief of Staff, G-2, Philippine Department, Subject: Japanese Telegraph Code, 6 January 1925 (SPSIS 322).

112. Ibid., 1st Ind. (no date), Department Signal Officer to Commanding General, Philippine Department.

113. Ibid., 2nd Ind., Headquarters, Philippine Department, to The Adjutant General, 12 January 1925.

The Chief Signal Officer declared he was ready to attempt the interception of "such Japanese radio signals as desired" and to "turn the results over to the designated official."[114] But no station was established in China, and finally in 1932, it was decided that, as "a matter of basic national policy," the establishment of a high speed recording station in China was not "deemed advisable." The then Chief of Staff (MacArthur) submitted the question to the State Department which disapproved of any such project as that contemplated. Why he should have seen fit to consult the State Department is not clear. In 1929 the Signal Corps had made other attempts to get Japanese traffic by radio interception in various corps areas but no success was obtained.[115]

To go back to an earlier attempt at interception, Yardley learned (in 1922) from a competitor[116] of the Radio Corporation of American, that there existed in the office of this competitor an automatic wireless-receiving set which was used to monitor the traffic of the Radio Corporation of America

---

114. Ibid., 5th Ind., The Adjutant General to Commanding General, Philippine Department, 26 October 1932; Captain John P. Ferriter to Department Signal Officer, Philippine Department, 1 August 1932, Subject: Report on Possible Location of Radio Intercept Stations in China. There is now on file in the Historical Unit, Signal Security Agency, a TOP SECRET document, Reminiscences of Lieutenant Colonel Howard W. Brown, the work of an officer who, as an enlisted man, was engaged in radio work in the Philippines at this period. Colonel Brown recounts vividly the struggles of Captain Ferriter and others in their efforts to establish the intercept station.

115. IR 4227 contains samples intercepted but no Japanese material was found.

116. He does not state the name.

for commercial purposes.[127] The intercepts were made on a tape which could then be read visually. It occurred to Yardley that, if he could acquire such a receiving set, he could do his own intercepting. The cost would be "practically nothing". This probably meant the cost of operation after the set was installed. Tests were actually made to see whether such a set, established either at Governor's Island or in Yardley's office, could intercept the San Francisco commercial station which, it was believed, was broadcasting Japanese diplomatic messages. These tests were a failure, however, and the project was abandoned.[118]

E. Operations and Commendations

The modus operandi in MI-8 was as follows: Yardley maintained liaison with the Military Intelligence Division by means of ordinary and registered mail and by personal conferences, when necessary. Usually these conferences were held in Washington and were officially ordered. The text of messages when solved and translated was sent to Washington in a "bulletin" which then became available for intelligence purposes in both the War and State Departments. Contact was made with the State Department through a specially

---

117. IR 4163: letter of Yardley to Moorman (22 November 1922).

118. IR 4162: letter of Yardley to Moorman (3 January 1923). A week later Yardley reported that it seemed probable that results would not be obtained from these tests for some time. See also letter of Yardley to Moorman (27 February 1923); Memorandum from Colonel Locke to Assistant Chief of Staff, G-2, Second Corps Area, 2 March 1923.

appointed official , there who would pass the information on to the proper office without revealing the source. Copies of messages were regularly prepared for the State Department, beginning with the following stereotyped phrase: "We learn from a source believed reliable that . . ." and then would follow the text of the message translated faithfully but in indirect discourse. Such a message could be passed to any division of the State Department without compromising the source.

The Secretary of State (Charles Evans Hughes) in a letter to Senator James W. Wadsworth, Jr., wrote on 24 May 1922 with reference to the withdrawal of military attachés from some foreign capitals:

> 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.

The reference to military attachés was a blind. The funds requested were really for MI-8.

From time to time Yardley received letters of commendation from his superiors. For example, Colonel A. G. Campbell, the first of the long line of officers who handled the correspondence with Yardley's unit, wrote that both General March and Assistant Secretary of State Polk had the greatest of admiration for the results obtained.[119] An unknown officer (probably Colonel Campbell) wrote on 1 March 1920 that the solution of a Japanese

---

119. IR 4157: letter of Campbell to Yardley (29 January 1920).

system[120] was the "most remarkable accomplishment in the history of code and cipher work in the United States."[121] A letter of commendation came from General Churchill on 12 May 1920.[122] General Churchill's successor as Director of Military Intelligence, Brigadier General D. E. Nolan, wrote a letter of commendation on 21 January 1921, and a second on 14 April 1921, the text of which is as follows:[123]

April 14, 1921.

To Mr. H. O. Yardley:

Dear Sir:

As a result of your work as Major, Military Intelligence Division, during the World War, the code and cipher service of the War Department was placed on a basis of real efficiency. It is much desired to maintain the standard set by you and, with this in view, I would much appreciate any information in regard to new developments which may from time to time come to your notice.

It may be of interest to you to know that your work has been very highly appreciated, and that your treatment of this science--so little known before the War--is regarded as of the greatest value by the War Department.

In the event of another war[124] it is hoped that the Government will be able to avail itself of your expert knowledge and ingenuity in the compilation of codes and ciphers, and in the examination of them.

---

120. Specific details of solutions will be given in subsequent sections.

121. IR 4157: letter to Yardley (1 March 1920). The doubt as to the writer of the letter is caused by the fact that the carbon copy is unsigned.

122. Ibid.

123. IR 4161.

124. Yardley himself prevented this hope from fulfillment.

Assuring you of my personal appreciation of the invaluable service rendered by you, I am

Very sincerely yours,

D. E. Nolan,
Brigadier General, General Staff,
Assistant Chief of Staff.

The Distinguished Service Medal was later presented to Major Yardley in recognition of his services during the War. The award was published officially in War Department General Order No. 56, 13 December 1922, but apparently the medal was not presented to Yardley until some time in the next month.[125] Statements in The American Black Chamber make it appear that the medal was presented "not long after . . . (Yardley) returned from Arizona," where he had gone for his health after a severe illness.[126] This trip, as is clearly shown by the letters written by Yardley to Washington during his absence,[127] took place between March and May 1922.

---

125. IR 4162: Yardley to Moorman (10 January 1923) mentions that Yardley had just been notified. A letter of Moorman to Yardley (12 January 1923) states that the award would be presented in Washington. To his credit Yardley immediately recommended that Captain Manly be given the same recognition but Manly received the medal.

126. Black Chamber, pp. 321-323. (He had contracted a mild tuberculosis of the lungs).

127. IR 4163.

CHAPTER III. THE CIPHER BUREAU IN NEW YORK: SOLUTIONS

The Cipher Bureau in New York continued the cryptanalytic activity begun in Washington, but as a result of the negotiations with the Signal Corps already described in Chapter I, it soon abandoned code compilation. No work in secret ink was ever done by MI-8 in New York, despite certain statements made at a later date by Yardley[1] but the

were studied and, in many instances, were solved. These systems will be discussed in turn.

A. Japanese Solutions[2]

By far the most important achievement of MI-8 in New York was the solution of Japanese diplomatic, military attaché, and naval attaché codes, which thus made available to the State Department the valuable intelligence contained in the messages, particularly at the time of the Washington Disarmament Conference (12 November 1921 to 6 February 1922).

According to Yardley's testimony,[3] while he was in France in 1918 and 1919 some work had been done on the solution of current

---

1. These will be discussed in Chapter IV, Section E.
2. See Japanese Codes and Ciphers 1917-1930, a paper of the Historical Unit, Army Security Agency, now (April 1946) in preparation.
3. IR 4157: Yardley to Churchill, 15 December 1919; Black Chamber, 252.

Japanese systems but this was discontinued because there seemed little hope of solution.[4] MI-8 had then many cryptanalysts of sufficient competence to solve difficult systems but probably no one with adequate knowledge of Japanese. With the close of operations in Washington, however, interest in the Japanese problem was revived, for some time during the summer Yardley promised General Churchill that he would solve the code in a year or resign. He based this promise, as he later said, "merely on my theory that anything can be read.[5] In any case, Yardley began an attempt to solve the code which was, however, not successful until five months had past. For a time Yardley apparently entertained the naive idea that a Chinese expert would be useful. He gave up the idea when he "learned that there is no resemblance between Japanese and Chinese.[6]

In December 1919 Yardley attempted to find an entry into the Japanese code then being studied by means of ulterior assistance. On the first of that month he wrote a letter to General Churchill in

---

4. IR 4157: letter of Yardley to Churchill, 15 December 1919.

5. In this case Yardley's theory turned out to be correct, for he was able, in spite of his ignorance of Japanese, to solve the simple system and apparently without much help, but as a general proposition his statement is founded upon incomplete knowledge and inexperience.

6. The Japanese written language, to be sure, was actually derived from Chinese characters, but in vocabulary and structure, as well as in many other important respects, Japanese and Chinese are extremely divergent languages. See IR 4157: letter of Yardley to Churchill, 9 December 1919.

which he included the following paragraph:[7]

> The following may not be practicable, but will serve as a lead for some other subject matter. Get the name (from MID, San Francisco) of someone who has recently come to the United States from Tokio, for example a Russian. (As I can think of no Russian names offhand, I will use my own name.) Now address a note to the Japanese Military Attaché: Confidential. Any information that you or the Japanese War Office may have regarding political activities while in Tokio of one Hubert Charnley or Hubert Yardley, a Russian subject, reported as sailing from Yokohama to San Francisco on November first, is urgently requested. Please consider name confidential.

It was hoped that the Japanese Foreign Office's reply would be intercepted, that repetitions within it could be equated with the name of the Russian, and that solution would thereby be facilitated.

The suggestion was acted upon, and Colonel A. B. Coxe, then Chief of the Negative Branch,[8] wrote to Lieutenant Colonel R. I. McKenney, then Assistant to the Director, MID, on 29 January 1920 as follows:

> MEMORANDUM FOR COLONEL McKENNEY: Subject: Russian Agent.
>
> 1. A Russian, who claims to have been the Private Secretary of Seminoff, has recently arrived in San Francisco. He has certain information that he wishes to sell to this Government, but before making any business arrangements with him we would like to know whether or not he was employed in a confidential capacity by Seminoff, as he claims.

---

7. IR 4157: a letter marked "Personal and Confidential" and also "Secret."

8. The Military Intelligence Division was organized into a Positive Branch (intelligence), a Negative Branch (counter-intelligence), and a Geographical Branch.

2. It is understood that he has spent several months in Japan, where he was associated with one GORTINSKI. It occurred to me that the Japanese Government might have some information regarding this man that would indicate whether or not his claim to have been Seminoff's Secretary is warranted by facts.

3. This man's name has been reported as being VLADISLAUS FILOFEI and also as WENCESLAUS FILOFY.

4. I would appreciate it if you would ask the Japanese Military Attache to ascertain, confidentially, from his Government whether or not they have any information regarding this man. As the matter is urgent, it is requested that you take this up with as little delay as practicable.

NOTE: Gortinski was Seminoff's agent in Tokyo.

The Japanese Military Attaché, then Major General K. Inouye, of the Imperial Japanese Army, fell into the trap. His reply was as follows:

MILITARY ATTACHE
IMPERIAL JAPANESE EMBASSY
WASHINGTON

CONFIDENTIAL

February 26, 1920

Lieut. Colonel R. I. McKenney, General Staff,
Assistant to the Director,
Division of Military Intelligence,
War Department, Washington.

My dear Colonel McKenney:

Replying to your inquiry of the 29th ultimo, as to the identity of VLADISLAUS FILOFEI or WENCESLAUS FILOFY, for the use of the Chief of the Negative Branch of your office, I have the pleasure of hastening to convey hereby cable advice received today from the General Staff, Tokio, as follows:

"VLADISLAUS FILOFEI was a chaplain to the Seminoff Army, but never Seminoff's Secretary as he claims. Upon visiting Japan with Dertinski (cablegram reads DERTINSKI instead of GORTINSKI) he contemplated establishing a Russian newspaper in Tokio, but did not succeed, owing to insufficient capital. Due to misconduct, being unable to procure employment, he came to this country for a living."

Assuring you of my highest esteem, I remain, my dear Colonel,

Very sincerely yours,

/s/

K. Inouye, Major General, I. J. A.,
Military Attache
Imperial Japanese Embassy.

But before the information was received in February 1920, it was no longer needed. The letter in which success was reported to General Churchill is as follows:[9]

The work on the Japanese code has now progressed so far that it will not be necessary, as requested in my recent letter, for you to send a message through the Military Attache. I am also informing Major Strauss that he need not attempt to get me any information.

While engaged during the past five months[10] on the Japanese code, I have passed through various periods of confidence and

---

9. IR 4157: letter of Yardley to Churchill, 15 December 1919. Yardley later (Black Chamber, 268) pretended that MID had been unable to find a real case that would fit. The story was included in the book because it showed that Yardley was ingenious but he did not want to leave the impression that he really needed to have such assistance. Even without it, he was able to solve the code.

10. He must therefore have begun the work while still in Washington. See comment by William F. Friedman (Black Chamber, 252): "Yardley's difficulties with these messages were entirely due to his ignorance of the language. As a problem in cryptography, it was of the simplest order. Had he gone about the matter scientifically, he could have accomplished the results in 5 days instead of five months."

depression but it was not until Saturday morning about One A. M.,[11] that I locked my safe, and with it the correct solution of the code. Of course the solution is not complete. I cannot read the messages. Only a thorough Japanese scholar can do that. But there is now absolutely no doubt about my identifications.[12] I have identified enough groups to know that I have the correct system.

I shall take your time with only a short explanation of the work that has been done.[13] Later, if you should care to go into the subject thoroughly, I shall be immensely pleased to carry you through the entire analysis.[14]

While I was in France some little work was done by M. I. 8 on the Japanese code, but was discontinued because it appeared impossible of solution. Last July when I promised you the solution within a year, I knew nothing about the code and made the statement merely on my theory that anything can be read.

During the last five months in addition to running the office[15] I worked incessantly on this code. After about a month's

---

11. Yardley (Black Chamber, 271-272) states that he had gone to bed, had awakened about midnight by getting the inspiration of Airurando, as mentioned later in the letter. As a matter of fact, both Airurando and Dokuritsu were suggested to Yardley by Livesey (see the latter's note on p. 270).

12. As will shortly appear, by the time this was dictated, Yardley and Livesey had spent a day confirming the early identifications.

13. This is, however, the longest report on a single Japanese system in the MI-8 files.

14. Doubtless he would have omitted only Livesey's contributions.

15. Livesey (Black Chamber, 250) states that even at this period Yardley was dividing his time between official and private business, the latter being code compilation for the Tannery Council.

analysis, I decided that it was a two letter code.[16] Some 8000 groups were then indexed. In order to get a Japanese frequency, I split the clear text messages which are written in Roman letters into one-, two-, three-, and four-letter combinations.[17] Some 7000 syllables were thus indexed.[18] It did seem like a foolish and profitless task and I was laughed at a bit.[19] However, though the Japanese use about one hundred "kana", including accented letters, my frequency showed that Japanese is like any other language in at least one respect—it has distinct characteristics. Thus no word can begin with the kana for N, though a large percentage of the words end in I and N.

I was handicapped by my ignorance of Japanese, but I could find no available Japanese scholar and the weeks were gradually slipping by. Then, too, mixing of code and cipher[20] confused

---

16. A correct assumption though we should now call this a syllabary. Cf. Livesey's note (Black Chamber, 260): "The code texts were in 10-letter groups—see page 251. We found the sequence 'ba il ly' beginning with the 1st, 3rd, 5th, 7th, or 9th letter in a group—strongly indicating that a 2-letter group was the unit of the code. The word was, I think, 'no n dai.'" Cf. also Friedman's note on the same page: "Y always calls this a code. But technically the J messages were in cipher, with a few groups representing whole words." to which Livesey added: "I doubt this. Consider 'yu' at top of page 263."

17. On this statement, see Livesey's note (Black Chamber, 255): "Miss Willson [whose specialty was Spanish] and I, having bought Japanese dictionaries, went over these texts and divided them as best we could. Even with dictionaries we could not translate these plain text messages—Japanese is very hard to read when transliterated into our alphabet." Yardley exaggerated this action into work by "a corps of typists."

18. The plain and cipher frequencies should therefore be roughly equal.

19. By whom? The thought is repeated in Black Chamber, 260.

20. A fatal error in cryptography. Yardley said later (IR 4163: 18 February 1922) that at times a word would be sent partly in code and partly in plain!

the frequencies in no small manner. There were however a few bright spots. A frequencey of the endings of messages disclosed that probably EN meant STOP.[21] The highest code ending was OK, and one of the high text endings was RI. The presence of the group ASFYOK near the end indicated also that it probably meant period. This I took for the Japanese word OWARI. Then the group OWAG occurred in such a position as to lead me to believe that it meant stop. This I later identified as SUE, the Japanese word for conclusion.

By analysis I assumed that IL equaled N and UB equaled I; also that WI YE PO probably equalled respectively A NO RU. I also had several other theories. I did not see how I could be entirely wrong, but I was beginning to doubt the correctness of any of my identifications, when at last I identified[22] Airurando which means Ireland or Irish. This led immediately to Dokuritsu which means Independence, which in turn led to JOOIN for Senate; Ketsugian for resolution; heiwa Jooyakuan[23] for peace proposal; Kaigi for conference; Teishutsushi for introduced; Teishi for withdrawn....[24]

---

21. On this cf. Yardley (Black Chamber, 261): "one of the most striking points that these charts revealed was that the code group en occurred only 11 times, and that its position was, in most cases, in the last ten letter group of these messages. Now one of the reasons that I had been uncertain of the possibility of a two-letter code was the fact that the last code word always contained 10 letters. As the reader can see, in a two-letter code there is only one chance in five of the message ending in letters divisible by 10." He came at length to the easy explanation that nulls were added to fill up the last group! But Livesey (note on p. 262) says: "I don't remember any punctuation. Certain terminal inflections indicate the end of a sentence." Yardley then goes on to state that he later discovered that en really stood for p and that ab meant STOP.

22. As a result of Livesey's suggestion, according to the latter; as the result of a midnight inspiration, according to Yardley himself.

23. This word and Jooin were both identified by Livesey; see below.

24. Here he included a list of the identifications he had made, thirteen in all, two of which had been made by Livesey.

I did not want to write to you until I was sure, and to be quite frank I was not sure until Saturday.[25] With the aid of a good Japanese scholar there is no doubt but that I can have the Japanese code complete for you and probably some important messages before you go to Congress for the M I D appropriation. I may, because I am so interested in this code, overestimate its value, but I cannot but feel that if you go before an executive committee with this information, you will have no small argument for M I D.

I am sure you will overlook the tone[26] of this letter, if it seems over zealous. With the exception of clerical assistance I have worked practically alone,[27] and it is the first thing that I have ever done which I really feel proud of.[28]

What happened after the original success is best told in Livesey's words:[29]

Yardley called me in the morning after his inspiration and we spent the morning writing in his eleven[30] guesses under the code texts. We found no place where they were near together and no confirmations until, just as I was going to late lunch, I

---

25. Strictly true. It was on Saturday afternoon that certainty came.

26. Cf. Black Chamber, 272: "I shouldn't wonder but that this letter sounded a bit youthful. Even yet, the memory of those exciting days thrills me."

27. Cf. Livesey (Black Chamber, 263): "Yardley kept these speculations pretty much to himself—avid for the credit of breaking the code—which always looked easy. I was engaged in preparing . . . [other] . . . material." Yet Yardley even wrote to Captain John Matthews Manly, formerly in MI-8, about his discouragement. Apparently, Manly gave sympathy rather than help.

28. One year later Yardley's opion of this solution is indicated by his statement that it was "a simple code" fatuously intermixed with plain text. See IR 4163: memorandum for Major Moorman, 18 February 1922.

29. Black Chamber, 272.

30. In the list there are thirteen but these include two by Livesey.

found three of them spelling 'ku a u.'[31] I knew just enough Japanese to prefix 'joo' making the words 'jooyakuau'—'draft treaty' and a moment later found 'jooin'—'senate.' That proved all the previous identifications. Not till then was Yardley sure he was right. By night we had seven or eight more identifications.[32]

This is the only Japanese system, the solution of which is clearly to be attributed to Yardley. Even in this case he had help from Livesey.

General Churchill sent his congratulations and approved the appointment of the Rev. I. H. Correll, a former missionary in Japan, as a Japanese expert, for three months at the rate of $4,000 a year. This was the highest salary rate ever paid to any employee of MI-8 except Yardley. The search for a suitable man had taken five months, and Correll was the only positive prospect. He had wanted $5,000 a year, but he apparently accepted the lower figure.

The work went on rapidly, and on 4 May 1920 Yardley was able to claim the solution of four Japanese codes.[33] These were the codes designated by the short titles JA, JB, JC and JE.[34] In July Yardley

---

31. Curiously enough, none of these appears in the list.

32. None of these appeared in the report of Monday, 15 December 1919.

33. IR 4157: letter of Yardley to Churchill (4 May 1920).

34. These were codes of the syllabary type, that is two-letter code groups stood for two-letter plain equivalents. There could thus be no more than 676 code groups but probably there were only about half that many. Consequently, solution was not difficult for one who knew Japanese. The solution should have been particularly easy, for the text consisted of [illegible] ruthlessly intermixed with plain text—Yardley's own statement.

reported that there was material on hand for the solution of other codes which had not yet been solved. These included one diplomatic code (JH) believed to have 100,000 code groups, a Naval code (JD ?) and a military attaché code (JF).[35] The diplomatic code used five-digit groups and was at times enciphered, at other times unenciphered. A thousand groups had been identified, and it was possible to tell the subject matter of a message and occasionally to read the entire message. Work was soon to begin on the military and naval attaché codes.

The military attaché code (JF) had, however, been solved several months before Yardley reported the solution,[36] no messages having been found of outstanding interest. A few days earlier than 13 September 1920, code JK, the current military attaché system, was solved and the first translations were forwarded on that date.

In December and January Major K. F. Baldwin, who had been a "language officer" (student of Japanese) in Tokyo, was temporarily on duty with Yardley, assisting in the solution of another military code (JM).[37] Yardley reported on 3 January 1921 that Major Baldwin had made the code readable.[38] Colonel Baldwin, who had been advanced

35. IR 4158: letter of Yardley to Campbell (7 July 1920).

36. IR 4158: letter of Yardley to Cook (13 September 1920).

37. IR 4158: letter of Baldwin to Collins (10 December 1920).

38. IR 4161: letter of Yardley to Nolan (3 January 1921).

in rank while in MI-8, left on 8 January 1921, and Yardley asked for the assistance of another Japanese expert Major McLean, of whom nothing else is known than that he did work for a time in MI-8.[39]

In March 1921 it was learned that JH had only about half as many groups as originally thought and that the code was in the English language.[40] This code was used in unenciphered form, in enciphered form using digits, and in enciphered form using letters. By the end of March, about 2,000 code groups had been identified, all the encipherments had been solved, and, after a few days' study, almost any message could be read. If the code had as many as 50,000 groups and only 2,000 had been recovered, this claim of readability is surprising.[41]

At the same time JL also was reported as based on the English language and in use for diplomatic traffic. The code groups were words (e. g. AFFECTED, BUCHILLE, PLANXIMUS, RACINOLANO, etc.). The size of this code was also estimated to be about 50,000 groups.

---

39. IR 4161: letter of Yardley to Nolan (8 January 1921).

40. IR 4161: Yardley to MID (31 March 1921).

41. An experienced cryptanalyst would be inclined to consider the estimated size of the code as still far too high. Usually codes are not readable until twenty percent of the groups have been recovered.

Attempts at solution failed until it was discovered that the alphabetical progression of the code groups ran in the reverse direction to that of the plain equivalents.[42] About 200 groups of JL had been identified.

JG was found to be a Japanese-language code with groups of two and three letters, as Yardley says. Other witnesses say the extra groups were tetragraphs, not trigraphs. Previous codes of the syllabary type had proved to have only about 250 groups, but this one was thought to contain 1,000 groups;[43] consequently, it was the most difficult problem yet encountered. Solution was, however, nearly completed by the spring of 1921.

Another code (JI) made up of five-letter groups, was used by the Japanese naval authorities, presumably for messages in Japanese. The tentative estimate of the size of the code was about 25,000 groups, and Yardley was far from sanguine concerning the possibility of solving a Japanese code of this size. Work on the preparation of frequency studies was in progress and soon an attempt would be made to solve. Yardley wrote:

---

42. Presumably, all the codes discussed hitherto were one-part affairs, a point confirmed by the speed of solution.

43. Though a digraphic code can have only 676 groups at a maximum this code had in addition a few groups which were tetragraphs. the compiler may have thought that a mixture of digraphic and tetragraphic groups would delay solution. Actually it would not, but Yardley thought so and wrote a paper on the idea—a plea for departing from a fixed-length code group.

Aside from the obvious interest to the foregoing it proves probably for the first time that a code can be successfully attacked without knowing what language it is written in. In conclusion, the writer should like again to emphasize the type of intelligence we have in the Japanese Department.[44]

The method used in MI-8 at this time is described in a memorandum which Yardley sent to Washington on 3 June 1921:[45]

All of the material that we had in JI comprised about 25,000 five-letter code words. These were first typed, for purposes of indexing, filling about 800 pages. Each code-word with its two prefixes and two suffixes was then typed on a card. This work required 25,000 cards which were then alphabetized. The data on these cards was [sic] then typed in manuscript form which required about 1100 pages.[46] Next in order to try to discover the system upon which the five-letter code-words were constructed, which if possible would give us the exact size of the code, each code-word with the number of times it appeared was copied in manuscript form in alphabetical order. This required about 200 columns of code-words.

All of this work of course was required before any attempt was made to make identifications. So far we have discovered the days of the months, numerals from 1 to 50, Roman alphabet from A to Z, and quite a number of the more frequently used Japanese words. As an example of the importance of the wireless messages that you send us, I cite the following. You sent us a copy of a Japanese plain text wireless message from Tokio to Washington stating that message number 34 had been received. This was evidently in response to a wireless message that had been sent by Washington as a test. This single unimportant plain text wireless message led to the identification of the number 34 which in the code is represented by ODWOK.

---

44. At this time the "Japanese Department" consisted of Correll and Livesey.

45. IR 4161: Yardley to Military Intelligence Division (3 June 1921).

46. Such a manuscript would now be called an index of occurrences.

Ordinarily the Japanese spell English words according to the Japanese phonetic spelling but now and then they follow the English spelling. In the latter case they are required to use a five-letter code-word for each letter. In examining our manuscript carefully we ran on to one curious repetition which turned out to be p--r--o--t--o--c--o--l (note the repetition of the letter 'o'). The discovery of this identified the entire Roman alphabet.

In a code containing from 30 to 50,000 Japanese words and phrases, numerals, dates, etc., it would seem the foregoing identifications are relatively unimportant but it is these little things that finally lead to a solution. It will probably be somet time before we can read any messages in this code but we are making identifications now every day.

There is another Japanese five-letter naval code which appears to have so few repetitions that we are as yet undecided just how to attack it. When anything definite is discovered I shall so inform you.

On 18 July 1921 the first message was received in a new code (JP) used for important diplomatic traffic. Though the attempt to solve this code was intense, work being carried on after hours and on Sunday, on 8 August[47] no success had been achieved, but three days later Yardley had discovered that the reason for the failure was the fact that JP was in reality "24 different small codes instead of the usual 1."[48] Translations would be ready soon, as progress was now rapid. The first translation was ready on 23 August, when only about fifteen messages had been received.[49] The code was also much larger than those previously studied and it was apparently two-part; moreover

---

47. IR 4161: letter of Yardley to Cook (8 August 1921).

48. Ibid., letter of Yardley to Cook (11 August 1921).

49. IR 4161: Memorandum for MID (25 August 1921).

it was used in enciphered form.

In November 1921, during the Washington Disarmament Conference, considerable interest was shown, of course, in the naval attaché codes. Work in both JI and JJ was carried on simultaneously, but solution of the latter was difficult owing to the great size of the code (estimated to be 30,000 to 50,000 groups). No success in solving JJ was obtained at this time.[50]

While the Conference was still in session, however, Yardley, a month later, prepared a report for General Heintzelman in which appeared the following paragraphs, chiefly concerned with Japanese Military Attaché solution:[51]

> (a) Army [Military Attaché Systems]--Until the first of this year 1921 we solved the Japanese Army Codes with comparative ease.[52] During the last of December, 1920, we received a warning that beginning the first of the year of 1921 a new system would be installed by the Army. Since that time until the present, nearly a year, we have been unable to read a single army message.
>
> (As you already know, our methods of attack are similar to that used by the decipherers of Babylonian and Assyrian inscriptions; we assume the meaning of the group from the frequency with which it occurs, its position in the message, and its association with other groups. This statement, of course, is not entirely accurate but it can be generally stated that the foregoing principles underlie all solutions.)

---

50. IR 4161: Yardley to Military Intelligence Division (19 November 1921).

51. IR 4161: Memorandum for General Heinzelman [sic] (23 December 1921).

52. Probably in a message intercepted and read.

During the following months we made quite a collection of army messages but up until the last few weeks we had made not a single discovery. Out of a count of some 10,000 groups we found as many of one kind as another. From this of course it was obvious that we were dealing with a system that changed at various intervals or with one that automatically broke up the frequencies and repetitions.

We shall not go into all of the systems that we tried over a period of many months without any success; but shall give below only the method that at last gave us an inking of what was being done to equalize the frequencies[53] . . . .in any case it may be said that it was learned that the cycle contained 11 different codes and that the encoder, by the use of an indicator codeword, proceeded from one code to the next in a cycle at intervals, which though irregular averaged a little less than four lines. If this indicator had occurred in the message as an indicator only, we would have discovered the foregoing many months ago; but the indicator in Code No. 1 that means to change to Code No. 2 stands, in Code No. 2, for something entirely different; so that the indicators occur quite as often as any other group.

We now discover that from January until the first of November of this year the [Japanese] army used two differerent sets of 11 codes and that beginning November 1st they started with another set of 10 codes and perhaps more. The last digit of the sum of the figures in the number of a message indicates the code with which the message starts. From then on it runs in a cycle; thus, No. 331 will start with Code No. 7 as the sum of the number is 7; and No. 93 will start with Code No. 2 as the sum of 93 is 12, the last digit of which is 2. Beginning with November they have evidently started even a different system as a good many of the messages are not numbered; but it is believed that we shall shortly learn the system as we now know how their minds run.

Of course all of these codes are by no means solved but we can now classify the messages and in time will break all of the 32 or more codes which are being used.

---

53. At this point the description becomes technical and has therefore been omitted. The result of much study convinced the cryptanalysts that the "message is encoded in a cycle of 10 [really, 11] different codes changing at an interval of every four lines."

(b) Navy. [Naval Attaché Systems]—The Navy has made no changes and is still using two 5-letter codes of the approximate size of M. I. 5. In one of them several hundred words have been identified and the other has not as yet been attacked. Reading codes of this size is of course a long and tedious task. However, once having got the vocabulary of one code it will not be so difficult to break the others when they change.

(c) Diplomatic.—Beginning July 1 of this year all the diplomatic Japanese codes were changed and a few new ideas introduced but they were not of a kind that puzzled us very long.

They have, however, in one of their English codes, adopted a rather ingenious method of sending repetitions of phrases in the same message. For example, suppose the encoder notes that the phrase "Sub-committee No. 1 on Far Eastern and Pacific Questions" occurs more than once. The first time it occurs he will encode it in the regular manner and surround it by a blank code-word, say "xalaf"; this means that the next time "xalaf" occurs in that particular message it stands for "Sub-committee No. 1 on Far Eastern and Pacific Questions". It is possible that such a system might be profitably used by our own Communications Section. As far as I know it is entirely original with the Japanese and certainly presents a very difficult problem to the cryptographer.

The Washington Disarmament Conference ended on 6 February 1922 and gave MI-8 a chance to get caught up on work which had been suspended during the conference. Yardley wrote:

> There are at least four (4) different unsolved J Army systems which contain at least ten (10) codes; also two (2) unsolved J Naval codes of approximately 25,000 words.[54]

A few days later he sent a longer report on current work:[55]

---

54. IR 4163: letter of Yardley to Moorman (13 February 1922).

55. IR 4163: Memorandum for Major Moorman (18 February 1922).

We have no information which would confirm or disprove the authenticity of this alleged German-language Japanese military correspondence[56] among [sic] Tokio, Vladivostok and Harbin. All our information is fully shown in our translations and reports.

We have no evidence of the Japanese using German-language codes nor have German texts been transmitted in any code. French diplomatic texts from Paris have been transmitted in JE which is primarily an English language code, having special groups for "the", "and", etc.

In the matter of military codes, the Japanese technique has shown a rapid improvement. In 1918, 1919 they were using a simple code, fatuously intermixed with plain text,[57] sometimes sending a word part in plain and part in code. In 1920 they used three codes without this intermixture, JF, JK and JM, simple codes which were solved with no great difficulty. During the past year they have been using several codes which superficially resemble these latter but which when compiled in two-letter groups yield a baffling frequency as every possible two-letter group is used in a single long message and one group is used about as frequently as any other. By analysis it has been determined with some certainty that these current codes each comprise ten or eleven distinct keys. The material is being compiled for study on this basis. So far only one of the codes has been thus compiled. It has been under study for a few days, so far without success on account of the paucity of material in each key, but there is no reason to believe that it is other than Japanese language.

The current codes are really clever and effective to a degree and there would be no particular reason for the Japanese staff to use a German-language code but it is not impossible that they may have been in the habit of doing so in some instances before the recent development of their own codes and that the alleged correspondence may have used German code books in the hands of the officers conducting it. The Japanese language written in our alphabet for telegraphic transmission is often obscure because many syllables and words have a multiplicity of meanings distinguishable only by their ideographs. The use of German would therefore be easily explainable.

---

56. Moorman's letter, now lost, must have discussed the correspondence referred to.

57. A fatal cryptographic error.

It is expected that with a reasonable amount of study we may hope to solve some or all of the current codes. In the meantime we shall bear in mind the possibility of the use of the German language.

This memorandum was followed in March by a further recapitulation of the situation in regard to Japanese solution:[58]

> The situation here as to the progress of the work is briefly as follows. The Japanese diplomatic codes are all broken and the naval codes are all carded[59] and are being worked on. Two of the army codes, JM and J?, have been carded and are being worked on and JM is now in the hands of the typists. There is still another Japanese army code that has not been identified.[60] This will have to wait until I get back[61] as no one except myself understands how to identify the indicators (you will no doubt recall that I have already written explaining the details of this rather difficult system)."

Up to this time it is apparent that no Japanese message had been intercepted by electrical means: those messages which had been studied had all been received from the cable companies. But Major Moorman received from an unspecified source[62] in January 1923 a radio intercept

---

58. IR 4163: letter of Yardley to Locke (10 March 1922).

59. This means that an index was prepared on filing cards.

60. Though preliminary research had been begun, no conclusions had been reached.

61. Yardley's health had broken and he was about to leave for an extended trip in the Southwest.

62. Actually, this was Mr. Friedman. About this time the U. S. Coast Guard was really getting under way in radio intercept work against rum runners. Mr. Friedman had good contacts with the Coast Guard through Mrs. Friedman, a cryptanalyst employed by that service, and thus learned of the Japanese intercepts. A few samples were turned over to Major Moorman with the suggestion that they might be of interest to MI-8, since Mr. Friedman was well aware that MI-8's source of raw material had dwindled greatly.

of a Japanese message sent from station JAA (Funabashi, Japan) to station NII (Kokohead, Hawaii), and when Yardley returned a translation of the text he raised the question of whether it might not be possible to intercept radio traffic regularly.[63]

Work in MI-8 had by now lessened, as the result of difficulties in interception, to such an extent that the Japanese cryptanalytic staff was able to process a good deal of older material which had lain in the files for want of time to study it.

MI-8 copies of all material which was on hand when MI-8 established its relation with the telegraph companies in 1919, and this included traffic dating from the period of the War and the Peace Conference.

Summaries of the first hundred of these messages were forwarded for information on 25 January 1923[64] and translations were made of 45 of them. The reasons for processing this material were two:

a. There was a possibility that some of the messages might contain material of some historical value.

b. The staff in MI-8 needed the evidence of the older messages as to Japanese vocabulary.

63.

64. MR A162: letter of Yardley to Moorman (25 January 1923).

Not until 15 August 1924 was any further mention made of Japanese solution in any extant document. On that date Yardley wrote to

68. It is the height of cryptographic security to transmit as small a volume of messages as possible in a system.

69. This probably reflects the fact that the best [illegible] experts were now gone. Who was doing the translations is not known.

70. Presumably [illegible] messages sent from [illegible] territory.

71. MR 4162: letter of Yardley to Locke (13 December 1923).

115

Washington as follows:[72]

> Mr. Lane[73] no doubt has told you something of our progress with the J (he was here about an hour a couple of weeks ago). Since then we have broken into the J English code (a great deal of it has been identified) as well as into "Ju", one of the new Japanese language codes.
>
> All of the material that you have sent us is in new codes which we have arbitrarily called
>
> JU J language
> JV " "
> JE J English
>
> As stated above, Ju and Je are coming along nicely. Jv is about the same size as Ju. Work will be started on Jv as soon as Ju is completed. The first JU message was translated and forwarded on 22 September 1924.[74]
>
> JV, another J language code, has not been started on yet. We thought it better to complete one and send you the decoded messages rather than divide our time on two codes.
>
> The new English language J code, called JE, is nearly completed. This code, we learn, is changed every two months, and they will hereafter be referred to as Je4, Je5, etc. Je4 is nearly completed.

Code JV was more difficult that JU. Evidence is clear that traffic was still being received at this time from the cable companies but from 19 August to 16 October 1924 none had come in.[75] On 7 November

---

72. IR 4160: Memorandum for MID (15 August 1924).

73. Arthur Miles Lane, the representative of the State Department who had succeeded W. A. Hurley as liaison officer for MI-8's affairs.

74. IR 4160: Memorandum for MID (22 September 1924). JU and JV were used for Japanese language messages, while JJ was used for English messages.

75. See IR 4160: Memorandums for MID (6 October 1924; 15 October 1924).

1924 Yardley wrote that the subject matter in the JV messages was proving to be more interesting than those in JU.[76] The problem was still the acute lack of adequate traffic intercepts.[77]

The first messages, six in number, in a new Japanese code (JX) were received early in January 1925,[78] but this system was never solved. In 1925 or perhaps a little later Miss Willson prepared a technical paper[79] describing the methods of solution used in attacking three Japanese codes: JU, JV, and JX, in use for diplomatic traffic between 1 April 1924 and 18 March 1925.

The first JWa message was translated on 16 January 1925.[80] The solution had been partly the work of Miss Edna Ramsaier: her lack of knowledge of Japanese did not hinder her work, as the code was in English. At the end of the month Yardley wrote an interesting paragraph to Major Milliken:[81]

---

76. See IR 4160.

77. See Memorandum for MID (12 December 1924).

78. Japanese U-Type Codes, copy now filed in IR 4876. This is a photostat of the 167-page manuscript.

79. IR 4160: letters of Yardley to Milliken (12 January 1925).

80. IR 4160: letter of Yardley to Milliken (16 January 1925).

81. IR 4160: letter of Yardley to Milliken (30 January 1925).

> The Japanese seem to think that the only way we can break their codes is by comparing texts of messages handed the State Department with the original code messages, which would indicate that they feel that their other codes are insoluble and that they are utterly in the dark as to modern methods of breaking codes.[82]

In the autumn of 1926 it was believed, at least for a time, that a satisfactory source of intercept material had at last been found. Some intercepts were received from the Signal Corps between 28 October and 15 November, but the average volume was about one message every other day. It was hoped that the Signal Corps would continue to intercept and that the volume would increase, but this hope was not fulfilled.[83]

In Yardley's Brief Summary of Work During Last Year[84] a short paragraph describes all solution of Japanese systems in 1926 as follows:

> Only 11 radio intercepts received and these are in several different systems; material still too scant to admit of a solution. Have solved thousands of Japanese messages and can solve these with more material.

The record for 1927 was somewhat better.[85] The following is a tabulation of the intercepted material:

117 JY messages received; 75 returned; 42 on hand.[86]

---

82. This happy state of affairs ended when Yardley, by publishing The American Black Chamber, informed the Japanese of the truth.

83. IR 4159: letter of Yardley to Milliken (1 December 1926).

84. IR 4159. The date was 3 February 1927.

85. See Brief Summary of Work During 1927, dated 14 January 1928 (IR 4159).

86. The word "returned" here means "translated."

112 JAA messages received; 70 returned; 42 on hand.

44 JBB messages received; none returned. This code is under study and 122 identifications have been made.

60 JCC messages received; none returned. This code is under study.

18 JZ messages received; none returned. This code is under study.

8 JDD messages received; none returned. This code is under study.

9 JW messages received; 2 returned; 7 on hand.

18 Naval messages received; none returned. This code is too large to solve without more material.

6 Army code messages received; none returned. This code is too large to solve without more material.

36 Miscellaneous Japanese messages received through 9th Corps Area; 3 returned; 33 on hand. Those on hand are too badly garbled to identify.

Total number of Japanese messages received 428; total number returned 150; total number on hand 278.

Number of different codes completely solved 3; partly solved 1; 3 under study.

In recapitulation, it should be stated that MI-8 had studied a total of thirty-one different Japanese systems in the period 1917-1929, designated by the short titles JA to JZ and JAA to JEE. Of these, nothing at all is known of one (JD), but the others were to be classified as follows:

a. Diplomatic:—JA, JB, JC, JE, JG, JH, JO, JP, JU, JV, JW (four types), JX, JY, JAA, JBB, JCC, JDD, and JEE, a total of twenty-one. Of these, one was a one-part code of fairly large size (JH), the rest all being syllabaries. JE, JH, and the four types of JW were all used for English-language messages, the others for Japanese texts. Except for the latest codes in the series, used at a time when interception was particularly difficult, all of these were solved, being relatively easy cryptanalytic problems. The most difficult diplomatic code was JP which was solved in about three weeks.

b. Treasury:—only one system was known to be used by the Japanese Treasury (JL), a one-part code.

c. Naval attaché:—JI, JJ, JS, JT (unsolved), and JZ. JI and JJ were large one-part codes. JS was a one-part code in English; JZ was a syllabary and code similar to the diplomatic syllabaries.

d. Military attaché:—JF, JK, JM, JN, JQ and JR. Of these JF and JK were probably simple syllabaries not unlike the diplomatic syllabaries. JM was an enciphered system, using eleven different keys, each message being entirely in a single key with an indicator. JN, JQ, and JR, were enciphered syllabaries but messages could change key with a switch group to show this.

In the ten years of its existence in New York City, MI-8 prepared approximately 10,000 translations, most of them diplomatic in character. A total of 1600 were forwarded during the Washington Disarmament Conference.[87]

The solution of these Japanese systems was not comparable to the vastly more difficult problems in cryptanalysis which the experts of

87. The evidence is contained in the files of the "J Series" and contradicts Yardley's statements in the Black Chamber (252, 318) that about five thousand messages were sent in that period. It was for their work during the Conference that the MI-8 employees received a Christmas bonus (see Chapter II).

SSA were forced to solve in World War II, yet, in spite of the difficulties of intercepting sufficient material to make solution possible, which was the main reason for failure to solve JT at all and some of the later codes completely, the percentage of success was high. Had not Yardley publicized exaggerated claims for the work of his New York office, the reputation of the group at work there would today be far greater among American Governmental experts in cryptanalysis than it is. The MI-8 cryptanalysts should not be belitted because in their day their Japanese opponents had not yet reached cryptographic sophistication. They were sufficient for the tasks which they faced and who knows that, had they faced more difficult systems, they would not have proved themselves superior even to these?

[redacted]

C. German Solutions

The German solutions accomplished by members of the staff of MI-8 in New York consisted in part of a study and completion of reconstructions which came from a source known as "the Dutchman." The man was probably not Dutch at all, but in April 1919 he had approached American

---

101. See [redacted] Cryptographic Systems prior to 1917, par. 29.

officials then in Holland with an offer to sell to the United States Government a considerable body of cryptanalytic information pertaining to German systems. His identity was never made known to the cryptanalysts in MI-8 who consequently referred to him simply as "the Dutchman." It is clear, however, that he had been a member of a cryptanalytic bureau which had access to a considerable body of German diplomatic intercepts and had been successful at least partially, in reconstructing several codes.[102] That the man who supplied this material had been a member of a cryptanalytic bureau maintained by the Imperial Russian Government is at least a possibility. He wrote English fluently, though not perfectly, but his handwriting was not like any of the Western scripts.

The material was not immediately brought to Washington, but in December 1919 it was submitted for examination by MI-8, photographed, and returned as "not wanted."[103] In this material were found reconstructions of a code known as 2500, with tables for converting this code into three other forms, known as 37000, 29000, and 18400. Upon examination 18400 proved to be identical with 18470, a code already reconstructed by MI-8 in Washington.

---

102. See German Cryptographic Systems during the First World War, a paper of the Historical Unit, Signal Security Agency (IR 5096), par. 18.

103. See note of the late Dr. Charles J. Mendelsohn to Mr. William F. Friedman, dated 8 May 1931, in IR 4763.

The information from "the Dutchman" helped to fill out lacunae in the story of German diplomatic cryptography as then known by MI-8, and in addition supplied data concerning a number of other codes not previously known to MI-8. These included code 2970, from which code 14000 was "derivated" as "the Dutchman" said. Codes 9700 and 5300 were basically the same two-part code. Code 1219 was an enciphered form of 9700.

The following paragraphs are taken from a letter of Yardley to General Churchill, dated 22 September 1919, when MI-8 had been in New York for only about a month:[104]

> 1. Some time in June I informed you that M.I.8 had broken the German diplomatic code used between Berlin and Madrid.
>
> 2. We have now broken three of the codes, having identified approximately one thousand words in each. Hundreds of messages are partly deciphered but it is only now and then that we find a message that we can decipher completely. I am enclosing two such messages.
>
> 3. Work is progressing rapidly and it should not be very long before we are able to decipher all of the messages.

The German section of MI-8 compiled a pamphlet of about 100 pages recounting the story of the solution of German codes, but no copy has survived.[105] The work was nearing completion in March 1920.

In his Memorandum for the Director of Military Intelligence, dated 5 June 1920, Yardley reported the readable German systems as follows:

---

104. IR 4157.

105. IR 4157: letter of Yardley to Churchill (2 March 1920).

Code 13040[106]
Code 26040-9[107]
Code 5950[107]
Code 18470-9
Code 12444[108]
Code 1777[108]
Code 2310[108]
Code 50874
Code 84668
Code 83203
Code 2815
Code 3009[109]
Code 3090
Code 3900
Code 0039
Code 0390
Code 5030[110]
Code 5300
Code 0053
Code 0530

Although there are twenty codes in this list, the first eleven were certainly solved before the move to New York. Of these eleven, there were in reality only three or at most four different basic codes, each basic having several derivatives, and of the basic codes, the British had given MI-8 one in early 1918. The remainder, ostensibly nine in number, are really only two, one which used the variant discriminants 3009, 3090, 3900, 0039, and 0390, and another which used 5030, 5300, 0053, and 0530. In each case only a single cryptanalytic problem was involved.

The final reference to German systems in Yardley's correspondence

---

106. A copy of the British reconstruction, partially completed, was received by MI-8 early in 1918.

107. These were derivatives of 13040 and were described by the British in forwarding their partial reconstruction of that code.

108. Derivatives of 18470.

109. This and the next four codes were really all one: a single code with five indicators varying so little that a good cryptanalyst should have at once suspected the essential unity, as no doubt the staff of MI-8 in Washington had recognized.

110. This and the next three codes were also a single code with slightly varying indicators.

is a letter dated 23 December 1921:[111]

> During the war the A.E.F. intercepted German diplomatic messages between Berlin and Madrid. We have read a good part of these messages but gave up the work shortly after we came to New York as we were receiving no current material. However, several months ago the State Department began sending us a few messages intercepted in Russia and we have managed to keep in touch with what the new German Government is doing. The messages we receive are badly garbled, fragmentary and not in sufficient volume to make it worth while to try to read them; but we managed to reconstruct what they call their diplomatic "Nummerheft" which is a small five-letter code of some 1500 groups containing telegram numbers, dates, and the usual words of reference that begin messages. Out of a very few groups we reconstructed the . . . mutilation table for their "Nummerheft", and as each message bears a number and date in this code it did not take us long to fill it out.

No work was done thereafter on German systems by MI-8.

---

111. IR 4161.

112. See Volume Two, Chapter IV, [illegible] 1917-1923, a paper of the Historical Unit, Signal Security Agency (AH 5093), par. 7.

113. IR 4157: letter of Yardley to Campbell (17 May 1929).

114. If more were available, they are no longer on file.

CHAPTER IV. THE CIPHER BUREAU IN NEW YORK: REORGANIZATION IN 1929

A. Plans for Reorganization

Readers of the preceding two chapters will have seen that, as War Department funds available for cryptanalytic activity gradually decreased in the decade 1919-1929, there was likewise a parallel decline in the volume of traffic intercepted, accompanied by a gradual loss of interest in the day-to-day solution activities on the part of the officers in Washington who were Yardley's superiors, as well as similar decline of interest in such matters even within MI-8 itself.

In the summer of 1929 Major O. S. Albright, a Signal Corps officer who had been assigned to G-2 to supervise and coordinate the activities of the cryptographic[1] and the greatly curtailed cryptanalytic[2] sections of the War Department, made an extensive study of the situation. After a careful appraisal of the cryptographic work of the Signal Corps, the cryptanalytic work of MI-8, and the printing, distributing, and accounting work of The Adjutant General, he concluded that a complete reorganization of code and cipher work done by the War Department was necessary.[3]

---

1. The Code and Cipher Section, Office of the Chief Signal Officer. See above, Chapter I.

2. MI-8. See above, Chapters II-III.

3. W. F. Friedman, A Brief History of the Signal Intelligence Service, p. 7. His paper is the source for many of the statements in this chapter.

MI-8 had been publishing a "bulletin" every few days, but this was of primary interest to the State Department, and the War Department had only a secondary interest in the material contained in it. Major Albright concluded that the principal interest of the War Department in cryptanalytic studies in peace, as distinct from war time, was to use them as a means of training personnel for immediate effectiveness at the outbreak of hostilities. MI-8, with its limited staff, although already experienced theoretically as well as practically[4] in the science of cryptanalysis, either could not or would not conduct any training. Indeed, it is doubtful whether the need for training was even contemplated. Moreover, all except one member of the staff were then of such an age as to make their potential usefulness for any war that might arise extremely doubtful.[5]

---

4. Most of the staff of MI-8 has actually participated already in cryptanalytic activity during one war, either in MI-8 in Washington or in the Radio Intelligence Section, General Staff, in France. Only two members of the staff later again entered the service of the War Department. One (Mrs. Edna Ramsaier Hackenburg, afterwards Mrs. Herbert O. Yardley) ceased to be an employee before the outbreak of hostilities. The other was Mrs. Serena B. Laning Slocum.

5. As it actually happened, when, after an interval of peace which lasted roughly 22 years, World War II began, the Signal Security Agency was able to command the services of only four persons who had done cryptanalytic work during the earlier conflict. The Director of Communications Research, Mr. William F. Friedman, had been a first lieutenant in the Radio Intelligence Section, General Staff, in France. Two of the Army Field Clerks in the same unit were later on duty in the Signal Security Agency. These were Captain (later Lieutenant Colonel) Leonard Bickwit and Captain Edward J. Vogel. The fourth person was the late Lieutenant Colonel A. J. McCrail, Chief of the Laboratory Branch, who had been in charge of the Secret Ink Laboratory in 1918.

The fact that the office of MI-8 was maintained in New York, remote from any direct supervision that might be exercised by the War Department or G-2, resulted in a state of affairs in which no one in the War Department actually knew very much concerning what was being accomplished, except for the information contained in the "bulletin" received at irregular intervals. No one in G-2 knew how the office was being administered. Actually, perhaps to give the cover name the verisimilitude which it suggested, Yardley devoted a part of his time to two or three private enterprises. He had engaged in commercial-code compilation, acted as consultant for commercial firms in code matters, and was a licensed broker in real estate,[6] at that period undergoing a great inflation.

As already stated, Major Albright concluded that it was highly desirable, if not necessary , to place all of the cryptographic and cryptanalytic work of the War Department under the control of a single agency. This would end the threefold separation of code and cipher matters which had prevailed: the compilation of codes and ciphers by the Signal Corps; the printing, storage, issue, and accounting of codes by The Adjutant General; and the solution of foreign communications by Military Intelligence.

B. Changes in the State Department

Before any reorganization could be effected, a new and very disturbing factor appeared in the affairs of MI-8.

---

6. See Friedman, op. cit., p. 8.

The full details cannot now be determined with confidence: there are many points on which the testimony of firsthand and reliable witinesses is lacking. Yet it seems probable that the following statements are true.[7]

In March 1929 a new President (Herbert Hoover) had been inaugurated and a new Secretary of State (Henry L. Stimson) had assumed direction of foreign affairs. The officials in the State Department who knew of the existence of MI-8 did not at once bring its product to the attention of the new Secretary. In May, however, it was deemed a propitious time to share the secret with Mr. Stimson[8] and a few translations of Japanese messages were laid on his desk. His reaction is said to have been immediate and violent. The Secretary was of the opinion that the activity of MI-8 was highly illegal[9] and he directed that State Department funds[10]

---

7. Ibid., and Yardley, Black Chamber, chapter xx.

8. In 1922 Secretary Hughes seems to have been well aware of what was going on.

9. Much can be said to support his view. See above, Chapter II, Section D.

10. The State Department had contributed to MI-8 a total of $230,404.

no longer be used for this purpose.[11]

It was necessary for the Assistant Chief of Staff, G-2 to exert a considerable amount of pressure before the Secretary of State was dissuaded from this sudden and drastic course. Its immediate application might have had serious consequences as a result of summarily casting the six people concerned out of employment.[12] These six employees had highly specialized training and experience in a field that had little value in commercial, industrial, shipping, or banking business, and had no counterpart in educational institutions; and as regards the possibilities for employment in other governmental agencies, aside from the Signal Corps, the Code and Signal Section of the Navy, and the Intelligence Office of

---

11. Later, Yardley told Mr. Friedman that the fundamental objection to the policy of MI-8 arose from the attitude of President Hoover, rather than from that of Secretary Stimson. The real reason, therefore, remains obscure. It should be pointed out that the strong attitude shown by Secretary Stimson at the time of the first Japanese aggression against China in 1932 supports the view that Mr. Stimson himself may have been less opposed to such activity than his decision no longer to support MI-8 would seem to indicate. In view of the fact that ten years later Mr. Stimson, in his capacity of Secretary of War, was daily the recipient of the product of the cryptanalytic activities of the SSA, it would be of great interest to know the truth in this connection. As Secretary of War, his enthusiastic support of these activities was never lacking.

12. The severe economic depression which began in October 1929 was not yet clearly foreseen, but the consequences of the ultimate closing of MI-8 in New York some months later, with its resultant effect upon the income of Yardley himself, was one of the factors which ultimately helped to justify, in Yardley's mind at least, his publication of The American Black Chamber in 1931.

the U. S. Coast Guard, these were very small indeed. Even did they exist, time would be required to make financial provision therefor in the Budget—and this took at least one year. The situation was also complicated by the fact that none of these people had any status in Civil Service.

An arrangement was finally made which provided that the actual work of the office should end immediately, but that the personnel should be retained on the payroll during the period of reorganization. This took about two months, and in June 1929 the six employees of MI-8 were given three months' pay in advance to tide them over a period when they might be jobless. They had been paid out of confidential funds and since, as noted above, they had no Civil Service status, they had no retirement benefits and were ineligible for transfer to other government positions.

The chief objection to the dissolution of MI-8 arose from the possibility of dissatisfaction on the part of the ex-employees with the abrupt manner in which they were being dismissed:[13] their financial position in a period of severe economic depression. There was every reason to fear that sudden dismissal might result in indiscretions which could be embarrassing to the Government and produce serious consequences as regards efforts to maintain an adequate national defense.

---

13. It is probable that the volume of intelligence produced by their activities was then so negligible that its absence was hardly felt in the State Department. In this period the unit was producing three or four Japanese translations every few days and nothing more.

Yet all but one of the discharged personnel proved loyal and discreet and adjusted themselves to their new situation as best they could.

C. Publication of "The American Black Chamber"

The exception was the chief beneficiary of the funds appropriated for MI-8, Herbert O. Yardley, himself.[14] Refusing an offer of temporary employment[15] in the reorganized cryptanalytic activities, he appears to have begun to prepare secretly for a series of revelations of the cryptanalytic work of the United States with which he had been intimately associated since 1917. These revelations appeared first in a series of illustrated articles in Volume 203 of The Saturday Evening Post:

"Secret Inks"	4 April 1931 (pp. 3-4, 140-145);
"Codes"	18 April 1931 (pp. 16-17, 141-142);
"Ciphers"	9 May 1931 (pp. 35, 144-149).

The articles had originally been offered to Collier's but no satisfactory agreement could be reached on the amount of payment, and then Yardley approached The Saturday Evening Post. The material in the articles formed

---

14. At the time of the dissolution of MI-8 he was being paid exactly twice the salary of the next highest paid employee: Yardley was paid $7500 a year, Miss Willson, $3750. At no time in the history of MI-8 in New York was Yardley ever paid less than twice the salary of the next highest-paid employee. Between 2 October 1919 and 31 October 1929 he had received as salary a total of $71,183.34.

15. It required serious effort on the part of the Chief Signal Officer to extend the offer, which was also made to the other employees. None of them accepted. Mr. Weiskopf had a private business in York City (stamps); the women employees had husbands and families in that city and were unable to leave.

part of the sensational book known as The American Black Chamber[16] published by Bobbs-Merrill later in 1931. It is alleged that Yardley was assisted in the writing of the book by a man named Clem Koukul, an engineer employed by the American Telephone and Telegraph Company, who was paid $1,000 for his work.[17]

The fact that the book was obviously intended for wide popular perusal, coupled with Yardley's own egotism, resulted in a large number of inaccuracies, rendering it a very untrustworthy record of the events it pretends to describe. Its failure, too, to speak of many important phases of the work of MI-8 throws the whole account out of balance. Nothing is said, for example, of the difficult reconstructions of the German diplomatic codes, while much is made of such achievements as the solution of the Waberski cipher, which is depicted as having been accomplished overnight whereas, in fact, it remained unsolved from 7 February to 18 May 1918, a period of over three months. Yet, the fact that there are serious inaccuracies in the book did not in any way

---

16. The title was, of course, derived from the soubriquet of the French cipher bureau, "la Chambre Noire," but the United States Government never officially or even unofficially used a similar term.

17. Lieutenant Colonel McGrail is the source for this item: he made the statement to Mr. Friedman, "on excellent authority." Whether the "ghost-writer" or assistant was actually Mr. Koukul or not is unimportant, but to judge from Yardley's official correspondence, there is good reason to believe that he did have assistance in writing The American Black Chamber. Literary analsis of his subsequent novels tends to confirm this belief. His mystery novel, Crows are Black Everywhere (Putman's, 1945) was written in collaboration with Carl Grabow (on the title-page).

minimize the unfortunate effects its publication had as regards our national security.

The amicable relations of the United States and Great Britain were seriously threatened. The British were rightly resentful of the fact that Yardley disclosed information which he had obtained from them as a commissioned officer.[18] Even more serious was the effect which the publication had upon the Japanese, with whom relations were already exceedingly precarious. Some 30,000 copies of a Japanese translation of the book, possibly subsidized by the militarists in Japan, were sold in Tokyo in less than a month.[19] An officer now on duty at Arlington Hall Station,[20] who in 1931 was a teacher in Japan , well remembers the sensational effect which the book had and the wave of anti-American feeling it stirred up among all classes of the Japanese people. The Japanese were particularly bitter because of the revelations concerning the interception of messages to and from their representatives at the Washington Disarmament Conference, which had convened on 12 November 1921 and closed on 6 February 1922.

---

18. Yardley was employed by the Chinese Government in 1937; later by the Canadian cryptanalytic bureau (the Examination Unit at Ottawa) in the early months of World War II until the British refused to collaborate with the Canadians as long as Yardley remained in Ottawa. Naturally, upon the termination of his contract, renewal was not made.

19. Mr. Friedman, who is authority for this statement, received it from Commander (later Captain) Ellis H. Zacharias, USN, who was a language officer in Tokyo when the translation appeared on sale.

20. Lieutenant Thomas F. Fawcett.

Whatever changes in Japanese public opinion or foreign policy may have directly resulted from the publication of the book, it is certain that from that date the Japanese began extensive development of their cryptographic bureau in an effort to devise much more secure systems.[21] Had they been allowed to believe that the systems in use between 1917 and 1929 were indecipherable, they might have continued to use the same principles, with the consequent possibility of solving the newer systems with much less difficulty than was actually experienced. It is not too much to say that in the field of Japanese cryptanalysis alone, the publication of the book has cost the United States millions of dollars in expense and probably the loss of many thousands of lives.

It will not be amiss at this point to digress for a moment to discuss the theory and need for secrecy as applied to the technical processes and fruits of signal intelligence operations. Revelations of all cryptanalytic successes should be rigorously suppressed, since whenever it becomes known or even suspected that a specific system has been solved, its users will inevitably effect as soon as possible as many changes in the cryptographic elements as they can.

---

21. It would be interesting to read the telegrams to and from Tokyo for the first few months after The American Black Chamber was published—but with the closing of Yardley's office and the hiatus that ensued for several years, the traffic is not available for this purpose.

Such changes, which may vary from merely replacing the keys used with a basically unchanged system to a complete abandonment of the system itself and its replacement by a radically different system, are naturally limited by the difficulties of distribution of the new materials. In time of peace, such difficulties are relatively minor in character: the system of diplomatic pouches used by all governments then provides a safe method of distribution, and all governments may be presumed to have distributed to their diplomatic representatives reserve systems which can be put into effect at any moment. In war, however, distribution is complicated by a vast increase in volume of traffic, in number of holders, and in the frequency of routine changes. Furthermore, the materials themselves must be transported securely over great distances, often through or around enemy or neutral territory, subject to constant danger of capture by enemy espionage agents.

From the technical point of view, the introduction of radical changes as the result of an indiscreet revelation either vitiates or completely nullifies the work of the most brilliant cryptanalysts over a considerable period of time. Moreover, until sufficient traffic has been accumulated to make possible a new solution, the production of intelligence is greatly hampered, if not suspended entirely.

Thus far we have been discussing this problem purely from the point of view of its bearing upon the cryptanalysis of specific traffic transmitted by a specific government.

There is, however, a larger aspect to the question, namely, the fact that publication of any cryptanalytic success not only gives notice to all governments that cryptanalytic techniques have been devised which have made possible the reading of certain types of cryptography, but also gives clues to the extent of the progress that has been made in the cryptanalytic art. If, for example, a government which has been unsuccessful in its attempt to read certain traffic learns that another government has been successful, it will renew its efforts to solve that traffic and will almost certainly make changes in its own communications systems to prevent solution of the type it knows has been accomplished. Thus, a success in one direction, if revealed, may have unfortunate results in another. It may indeed be said that in World War II as well as in World War I the most secret "secret weapon" possessed by the British and the United States Governments was not a physical piece of equipment. It was a far less tangible thing—a mere fact, together with certain associated ideas, the complete hiding of which was more important than even the atomic bomb, viz, the fact that they could and did read practically all of the cryptographic communications of their avowed enemies. Associated with this great secret fact were also the facts relative to the astonishing extent to which progress had been made technologically in the signal intelligence field. Had this fact not been successfully hidden, the effect, sooner or

later, would have been to arouse these enemy powers from their lethargy, "educate" them and give them knowledge that leads to sophistication in the cryptographic field.

Finally, and this is an aspect of the problem likely to be forgotten by cryptanalytic technicans, the validity of information derived from signal intelligence activities depends upon the existence of a serene confidence upon the part of the users of a system that it is impregnable to cryptanalytic attack. Only thus will it be used for authentic communications from which may be derived valuable information. The more disillusioned a government becomes concerning the possibility of devising a cryptographic system which is "absolutely indecipherable," the more careful will it become not only to improve its techniques but also to keep out of its traffic the most important secret information which it possesses.

That solutions have nevertheless been possible does not minimize the fact that the additional cost to the Government in time and money has been incalculable.

Another equally disastrous effect was the development on the part of high government officials of a lack of enthusiasm for cryptanalytic activity. Funds became even more difficult to obtain; and this was especially serious, since the State Department, which had most to gain by the continuance of cryptanalytic activity, not only no longer made any contributions for this purpose but was hostile towards it. In 1919 the State Department had been fully aware of the need for cryptanalytic work, but having relied on the War Department for information in the period 1919-1929, the State Department had developed no facilities for carrying on the work. It at this juncture apparently regarded the whole business as unethical--which it would be, if nations based their dealings on ethics.

The question now arises as to what, if anything, was done to punish Yardley for his grave indiscretion in publishing the articles and the book. The answer is that nothing was done. Yardley had taken steps to protect himself from legal prosecution by resigning his commission as a major in the Military Intelligence Reserve Corps. The resignation took effect on 1 April 1931, just before the publication of the first article

in The Saturday Evening Post (4 April 1931).[22] The resignation had originally been tendered directly to the Secretary of War but for some reason Yardley was required to submit it again through channels, which meant, in this case, that the resignation had to be submitted to Captain M. F. Shepherd, Unit Instructor, Headquarters, 333rd Infantry, Room 11, City Hall, Vincennes, Indiana. He therefore wrote a petulent letter to Captain Shepherd on 24 February 1931 in which he complained of having to go through channels after having written thousands of letters directly to the War Department. This letter contains the following statement as to his reasons for resigning:

> However, my reason for resigning is that I do not approve of the policies of the Military Intelligence Division and therefore no longer wish my name identified with this division. My resignation is unconditional and without rancor of any sort.

Information had, indeed, come to the Government that Yardley was about to make his disclosures several weeks before publication. The possibilities of suppression of the proposed publications and punishment of Yardley were discussed but high Government officers felt not only that the Government was powerless, in the absence of an adequate legal basis for suppression but also that prosecution of Yardley either

---

22. Since the magazine, dated on Saturdays, was at that period put on sale on news stands on Thursday, he protected himself by only two days' grace. The publishers of the periodical, however, were in the habit of shipping copies to distributors many weeks or even months in advance of publication date, and undoubtedly the first article was in print long before the resignation was tendered.

as a Reserve Officer or as a civilian could not be conducted in camera, and that prosecution in open court would be most compromising and embarrassing to the Government.

After the publication of the disclosures responsible officers in the War Department took the attitude that, however regrettable the publication of the book was, nothing could be done to prosecute Yardley, and even if steps of this sort could have been taken, the damage was already done and could not be repaired. In a subsequent imminent and similar episode, again involving Yardley, something was done to prevent publication, as will be later noted.

D. Ethical Aspects of Yardley's Indiscretion

The ethical aspects of Yardley's action are interesting. Had Yardley really been officially informed of his duty to maintain silence regarding his activities? Was he under oath? Did he realize the serious consequences his action might have? These questions may all be answered affirmatively: there is abundant evidence in the records to prove the facts.

Though Yardley had been at General Headquarters, American Expeditionary Forces in France, for only about two weeks in December 1918, yet he was included in a list of former personnel of the Radio Intelligence Section, General Staff, to whom was sent a copy of a letter from the Director of Military Intelligence (Brigadier General Marlborough Churchill) to the Assistant Chief of Staff, G-2, in France (Brigadier General D. E. Nolan),

written on 16 April 1919.[23] The text of the letter is interesting:

April 16, 1919.

From: Director of Military Intelligence.
To: Assistant Chief of Staff, G-2, G. H. Q., American Expeditionary Forces, France.
Subject: Preservation of Secrecy in regard to Code and Cipher Work.

1. In M.I.D. it has been understood by all that the preservation of secrecy in regard to the code and cipher work done during the war is not to be relaxed by the armistice or even by the signing of peace.

2. Adequate reasons for this view are the following:
   a) Any stimulation of general interest in this subject would result in the production of so large a number of ingenious and difficult ciphers as to require in time of war the services of an inordinately large staff of expert deciphererers.[24]

   b) Foreign governments now using codes and ciphers of little security would be warned and would

---

23. The preparation of such a letter would ordinarily be the responsibility of the chief of MI-8. It therefore would be interesting to know whether in this instance the letter was originally prepared by Yardley himself. The original documents, now filed in IR 4154, do not show his initials on General Churchill's letter. The letter was, however, written just two days after Yardley's return to Washington from France and it may be that this was his first official act upon his return. He may well have been the source of the information mentioned in paragraph 3 of the letter.

24. As a matter of fact the personnel of the Signal Security Agency in World War II reached a maximum of more than 10,000, including the personnel of the Second Signal Service Battalion used in intercept activities. This figure does not include the immense number of Army personnel not directly under the control of the Commanding General, Signal Security Agency, but subordinate to theater commanders, of whom there were more than 15,000, nor any personnel of the Navy or Allied cooperating centers.

procure new ones that could be deciphered only at the expense of much time and labor.[25]

c) The limitations of modern methods of code and cipher attack would be revealed, and the means of constructing impregnable codes and ciphers would be indicated.

d) So much information in regard to code and cipher attack during the war was received from our British and French allies that discussion of our own methods and results--even if desirable--could hardly occur without a violation of the confidence which they reposed in us: and they are strongly opposed to any revelation of either methods or results.

3. Recent conversations with officers[26] formerly connected with G-2, A-6, American Expeditionary Forces, France, indicate clearly that some of the officers of that organization not only are not aware of the policy of the Military Intelligence Division in the matter, but on the contrary are definitely of opinion that what has been done in attack on alien codes and ciphers should be made known to the public, and some of them even contemplate publishing these facts.[27]

4. Inasmuch as such publication would demonstrably be contrary to the best interests of the Army, it is requested that secrecy in regard to this subject be enjoined upon every officer, field clerk and enlisted man, now or formerly a member of G-2, A-6.

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

---

25. Warned by Yardley's book, these governments did so.

26. This strongly suggests that Churchill's letter was at least proposed by Yardley.

27. No information is available as to who these men were. Had Yardley been one of them, it is hardly possible that he would have been allowed to remain in charge of MI-8. As it was, no officer in G-2, A-6, save Yardley himself, ever published any disclosures.

The question arises: did Yardley receive a copy of this letter, if, indeed, he did not read it before it was sent? When General Nolan received the original in France, he prepared a cover letter, a copy of which was sent, together with a copy of General Churchill's letter, to eighty officers, field clerks, and enlisted men, who had formerly been in G-2, A-6, Yardley included. Yardley's own copy may never have reached him, but General Nolan reported what he had done to General Churchill, and General Nolan's letter, now filed in IR 4154, clearly bears Yardley's initials. It was he who ultimately received General Nolan's letter for permanent filing!

In November 1919, Dr. Paul B. Altendorf, who had during the War worked in Mexico for the Military Intelligence Division, created a serious disturbance in MI-8 by unfortunate revelations concerning the Waberski cipher.[28] Just where these revelations were published is not clear. A letter from Dr. Manly, then back at his work at the University of Chicago, makes it appear that the article or articles had appeared in Harper's Monthly Magazine, the editors of which had also approached Manly for one or more articles on cipher[29] but a diligent search of that periodical has failed to locate any

---

28. On this cipher, see Volume Two, Chapter IV.

29. How the editor knew of Manly's connection with MI-8 is not clear, but the fact that MI-8 personnel included several people of literary fame affords a clue.

article by Altendorf.[30] Manly felt it unfair to permit Altendorf to "exploit our stuff while we must remain silent." Yardley wrote his friend, F. W. Allen, that Altendorf has been"A-1 in MID" but that nothing could be done about punishing him since he had not been required to take an oath.[31] He also reported the matter to General Churchill, as follows:[32]

> I have written to Captain Manly that the Altendorf articles were written and published without the consent of M.I.D., that both you and Colonel Van Deman are still opposed to the publication of work done by M. I. 8, but that in the case of the

---

30. No article by Altendorf appears in any set of Harper's in the Library of Congress, nor is any article by him listed in the Readers' Guide to Periodical Literature for the period in question. Altendorf did give an interview to a New York Times reporter which was printed in the issue of 30 December 1919 (p. 17). In this interview he urged the execution of Waberski but did not mention the solution of the cipher. In the September 1919 issue of Harper's (vol. 139,pp. 510-524) there is, however, an article by Heber Blankenhorn, formerly a Captain in MID, entitled "The War of Morale: How America 'shelled' the German lines with paper." This article deals with the topic of psychological warfare but does not mention any activity of MI-8. It may be that Manly's memory was confusing this article with the newspaper interview given by Altendorf.

31. IR 4150: letter of Yardley to Allen, 7 November 1919.

32. IR 4322: letter of Yardley to Churchill, 8 December 1919.

Waberski cipher M.I.D. was helpless.[33]

General Churchill then wrote a letter to Dr. Manly which explained the exact situation:[34]

> Major Yardley has shown me a quotation from a recent letter which you wrote him concerning Altendorf's disclosure of the Waberski cipher.
>
> I understand that Major Yardley has already informed you that neither Colonel Van Deman nor myself knew anything about this disclosure before it was too late. It must be obvious to you that the only safety-valve which will stop this sort of thing is character on the part of ex-officers and employees, who are too highminded to traffic in confidential and secret information. There is no legal hold over them whatsoever.
>
> No one could regret this disclosure any more than I do, or regret that, if conditions permit the disclosure of the Waberski cipher, you, who were responsible for its decipherment, should not receive the credit and anything else that goes with it.

Dr. Manly's reply to General Churchill, dated 18 December 1919, was as follows:

> I have your letter of December 11th in regard to Altendorf's publication of the Waberski.
>
> I hope you understand that I am, as I always have been, entirely in sympathy with the policy of M.I.D. in the matter of

---

33. The reason for this statement as regards the Waberski case was, of course, that the trial was in open court and the testimony was of public record.

34. IR 4322: letter of Churchill to Manly (11 December 1919).

35. IR 4322.

> secrecy. My paragraph to Yardley was occasioned by Altendorf's publication of a decipherment and translation which he must have secured from some official source, as he was himself unable to make the decipherment. The publication suggested that Military Intelligence had changed its policy, and I felt that if this was the case, I should know it. In the light of what you say, I, of course, understand that the policy has not been changed and that Altendorf must have received his information from some source outside of Washington. I should presume that the San Antonio office had furnished him with a copy of the decipherment. The translation he seems to have made himself.

Through the whole of this correspondence there is nothing in Yardley's conduct which suggests that in any way he failed to share the general policy of the Military Intelligence Division in regard to preserving inviolate the record of the achievements of MI-8.

Another breach of security occurred in the same month (November 1919) which might well have endangered the future of MI-8.

who had been a clerk in MI-8 in Washington, was reappointed and assigned the task of copying traffic received from

She apparently revealed the nature of her position to unauthorized persons, and she was never allowed to enter on the duties for which she had been employed. The story can best be told by presenting a secret letter from Yardley to Colonel A. G. Campbell:[36]

> It is needless to say that your secret letter of November 13 was a distinct shock.
>
> In the fall of 1917 while I was organizing at the War College what later became M. I. 8, who was then employed in the

---

36. IR 4157: Yardley to Campbell, 14 November 1919.

Record Section was pointed out to me as a girl who was extremely capable. She was later transferred to M. I. 8 and placed under [redacted] Under [redacted] direction she practically [redacted] until he left for Siberia which was a year after her transfer to M. I. 8. During these twelve months she gained the well-earned reputation of being not only discreet and efficient, but a girl who had unusual executive ability.

In the fall of 1918 I was ordered abroad and a few months later she was sent to [redacted] to work in the [redacted]

[redacted] was in New York Monday and Tuesday and stopped in several times and talked with a number of the clerks[97] late Tuesday afternoon I gather indirectly that she was uncertain of her status and, seeing an opportunity to retain in M. I. 8 one when I had come to regard as both discreet and efficient, I dictated the letter that has brought up the present situation.

She came to me about an hour later and told me that [redacted] had informed her that I had written in her behalf and asked whether she was to carry the letter. I replied that the letter would be mailed to you and upon her arrival in Washington she was, pursuant to instructions she already had, to report to the Military Intelligence Division for disposition, and if you cared to follow my recommendation you would no doubt get in touch with her.

I did not know until I received your letter that she had been informed of the nature of the work that I had outlined in my letter. This information was given to her by [redacted] to whom I dictated the letter.

[redacted] has proved himself to be unusually discreet and his action in this case though wrong, can be understood, for his opinion of her was that held by everyone before her departure for [redacted] and he felt that she was sufficiently on the inside to be informed of the nature of her work. His action of course was based on the incorrect premise that my recommendation would be carried out and that the girl must sooner or later learn of the work that she was to do.

Her statement that she was to be paid from the State Department can not be explained.

---

97. Apparently Yardley's office rules in New York permitted free access to the premises.

When I came back from Europe in April I learned that about twenty-five of the clerks in M.I. 8 had been told that they would not be subject to the drastic demobilization order which called for a certain percentage of the clerks to be released each day, because funds had been received from the State Department and they would be placed on a separate roll. Although the money was not received until three months later, a fact which has never been mentioned, it has been a natural conclusion of those in this office who came from Washington that the State Department was helping to finance this bureau. I have taken particular care that this belief can be based only on what was learned before my arrival, for since then both Mr. Winslow and General Churchill have impressed on me the necessity for keeping such information secret.

I have repeatedly told the clerks in this bureau that if any of them had any reason to believe that they understood the organization of this bureau, they were to forget it and under no circumstances even discuss it among themselves.

How learned of the connection the State Department has with this bureau is beyond me. I shall immediately take steps to find out what was said in her conversation with different clerks and let you know the result.

I feel that I should take some of the responsibility for recommending for I hardly talked to the girl, assuming that she was as discreet and as competent as she was when she left for London. Aside from the information contained in your letter I learned that her conversation while here would lead one to believe that her experience abroad had turned her head. I believe that her statements to other people about her work were prompted by wishing to appear important in the eyes of her associates; and that her trip to Europe has so turned her head that she has lost all sense of discretion.

I heartily approve of your decision not to employ her. Sooner or later, however, because of her many friends in Military Intelligence she will learn your real reason for not employing her.

If I were you I should call her to Washington and tell her frankly why she is not being employed. I should also tell her that when she divulged this information she was under oath[38] and that if she

---

38. If was under oath, certainly Yardley was also.

did not put some restraint on her tongue, action would be taken against her, and I should say this in such a manner as to leave no doubt in her mind as to your sincerity. I should also warn her that because of her many friends in Military Intelligence and their connections with her friends, sooner or later any further indiscretion on her part would come home.[39]

While I was in the State Department such a case as this occurred and the law was examined with a view to ascertaining whether civil action could be taken against an employee under oath who divulged confidential information. Of course I realize that in this particular case no action really could be taken, but I think that if such a possibility were outlined to her, she would think twice before she talked. As a matter of fact this is the reason that we insist that, though not on a regular payroll, all employees take an oath. To make the matter particularly impressive I think that I should hand her a copy of the oath and let her read it before I talked to her.

If you decide to follow my suggestion and I am sure that you will feel that I have written the foregoing merely as a suggestion, please inform me so that I can cite to the clerks in this office the example of as a strong plea for greater discretion.

As I have no one in mind who can do the work which I had outlined for it will be necessary, as suggested in the last paragraph of your letter, for you to find someone in Washington.

When Yardley prepared the exhibits included in his Achievements (Part Three), he appended to the individual exhibits warnings of the need for secrecy. These were as follows:

SECRET! Making known a single message in a foreign code will destroy all our work covering many months. To make known that a code book is being reconstructed at all, leads to absolute discontinuance of its use.[40]

---

39. Apparently an empty threat of criminal action. See below in the letter.

40. IR 4611.

> SECRET! If enemies learn that we can decipher their present codes, they will try to devise more difficult forms. Let's keep them ignorant of our success.[41]

> SECRET! Remember that making public a single code message deciphered by M.I. 8 may lead to discontinuance of the code and thereby nullify the labor of months.[42]

An unknown officer in the Military Intelligence Division wrote this paragraph in a letter to Yardley dated 1 March 1920.[43]

> No one, who is in the least interested in finance or partisan politics, should ever even know that we are able to do this kind of work.

This was doubtless an allusion to the need for keeping information concerning solution activities from anybody who might, for the sake of financial recompense or for purely partisan political reasons, use the information to the national disinterest.

When Colonel George Fabyan, of Riverbank Laboratories, wrote in March 1920 asking for information concerning new developments in the field of diplomatic solution, Yardley wrote to General Churchill.[44]

> The distribution of our information may compromise the secrecy of our work and would not give us a sufficient return to warrent the risk.

A little later he wrote to Colonel Campbell:[45]

---

41. IR 4619.

42. Ibid

43. IR 4157; the writer may have been General Churchill.

44. IR 4157: Yardley to Churchill correspondence (2, 10, 18, 27 March 1920). General Churchill was more willing to conciliate Colonel Fabyan than was Yardley.

45. IR 4157: Yardley to Campbell (19 May 1920).

> If the Japanese should learn that we can read their messages they may make such a violent change in their new codes that we could never read them.

As early as 1924 Yardley was of the opinion that no future war was possible.[46]

> I am hopeful of our being together again but not in the next war—you old pessimist—there won't be any more in our day.

A passage in a letter of Colonel Locke written in the same month is illuminating:[47]

> Of course it is like working in a prison for one is not permitted to talk about one's work and we are all vain enough to like to talk about the things we do.

In October of the same year Yardley again expressed his conviction that divulging the secrets of MI-8 would be disastrous:[48]

> Ever since the war I have consistently fought against disclosing anything about codes and ciphers. My reason is obvious: it warns other governments of our skill and makes our work more difficult.

On 12 October 1920 Yardley wrote a very long secret letter to Major Moorman as the result of a telephone conversation with the latter occasioned by the fact that Childs (obviously, Lieutenant J. Rives Childs, who had been on duty in G-2, A-6 in France) had written to the Secretary of War asking permission to publish his book on codes and ciphers. Yardley was asked for an opinion on what should be done.

---

5. IR 4160: letter of Yardley to Moorman (5 June 1924).

. IR 4160: letter of Yardley to Locke (ca. 10 June 1924). This letter asked for a raise in salary.

IR 4160: letter of Yardley to Milliken (22 October 1924).

He began his reply by quoting at length from several earlier letters (about the Altendorf case) which have already been cited and then continued:

On March 6 I received the following letter from Colonel Campbell:

> "Attached herewith is a memorandum from Lieutenant Colonel Frank Moorman, enclosing copy of letter to the Director, Infantry Journal, Washington, D. C., on the subject of Code and Cipher work. Please look this over and give me your views as to whether or not there is any objection to its publication."

On March 11th I replied as follows:

> "Your memorandum of March 6, - 4131-576 - requesting me to give my views as to whether or not there is any objection to the publication in the "Infantry Journal" the enclosed article written by Colonel Moorman, has been received and given a great deal of thought.
>
> "Since the creation of the Cipher Bureau, I have steadily maintained a position of secrecy and non-publication of any information dealing with codes and cipher. General Churchill is familar with both Captain Manly's and my stand; it seems to me that it is a question of policy which, if changed, will inevitably lead to an explosion. I am besieged on all sides by letters and personal requests from ex-members of the A. E. F. and M. I. 8, asking me to use whatever influence I may have to obtain permission for publication in magazines or in book form of articles or long treatises dealing with the history and development of codes and ciphers as they learned it from the French, British and American General Headquarters in France and what information they picked up in Washington.

"It is hard to lay down a 'thumb rule' regarding this subject: One article may be harmless on its face but once we establish a precedent I am certain that we can not prevent the avalanche of publications that will follow.

"I am sure that an article of the type of the enclosure to be published in the 'Infantry Journal' is written, and, if published, is published to awaken an interest in the Army regarding this subject and not for personal gain. Granting that this course of procedure is sound, on what grounds can the War Department protest against the writing of code and cipher articles or books for publication by responsible publishing houses for personal gain?

"When I was in France Colonel Moorman said that he was not in sympathy with my views regarding secrecy and non-publication after the war. In drafting your reply to Colonel Moorman you should, it seems to me, give proper weight to his views."

I was later informed by Colonel Campbell that my position was overruled and the article published.

That I predicted that we should have to face such a situation as Childs has brought up is no consolation, but the foregoing is written to show that I have done everything I could to avoid it.

I do not think that we can consistently refuse Childs permission to publish this book, but consistent or not, I think that permission should be refused.

Childs is a very good friend of mine and has told me repeatedly that he is afraid that his book will get lost in the files of the War Department[49] and that in the next war

---

49. The fear was well-founded but as it happened, the book was not lost but is now (1946) in the Library of the Army Security Agency.

we shall have to learn this subject all over again.[50] Aside from that of course he would like to make some money out of his book as well as a name for himself.

In drafting a letter for the Secretary's reply I should thank and commend Childs for this pamphlet,[51] assure him of its value by stating that it will be one of the principal texts for the training of future cryptographers in the army and point out that the pamphlet is too secret for publication. I think that you should also point that, aside from our own reluctance to inform the world of our knowledge of complicated codes and ciphers, we must consider the attitude of France and Great Britain for it should be remembered that our knowledge of codes and ciphers is linked very closely with the information which the French and British gave us in confidence.

If Childs is permitted to exploit the work he did in France I can confidently predict requests for permission to publish a treatise on diplomatic codes and ciphers and if he is permitted to publish his book I am not sure that our refusal to consent to the publication of a book on diplomatic codes and ciphers will stop its publication for the authors will feel that they are being discriminated against.

In conversation with Mr. Friedman some time in 1933, when asked why he made his disclosures, Yardley simply said that his family needs left him no other recourse.[52] He had, as a result of the economic

---

50. While this fear was not wholly realized, it was Yardley's own action in publishing The American Black Chamber that gave such a tremendous stimulus to the cryptographic art that much that would have been adequate against the type of cryptography prevalent thirty years ago would have been wholly unsuccessful in World War II.

51. Yardley had never seen the book: it contains 211 pages.

52. In the letter to Frederick Sullens, dated 6 June 1931, he had claimed that an unnamed foreign government had offered him twice his MID salary and expenses for himself and family if he would found a cipher bureau for that government. This may be put down as fiction for Yardley's character was such that he could never have refused such an offer. He later worked for the Chinese Government and still later for the Canadian Government.

collapse in 1929, lost heavily in his real estate ventures, the sales of the Universal Trade Code were practically nil, the depression made it impossible to obtain a new position, etc. Besides, the War was long past and he could not see how it was detrimental to national defense to have published what he did. Moreover, and this he apparently sincerely believed, it was necessary to make clear to the American people the bureaucratic stupidity which, by closure of his bureau, resulted in depriving our Government of its most reliable source of secret information. He seems to have become convinced that there could not be any transfer of the activity to the Signal Corps, since the Secretary of State had decided the work was unethical or illegal. The sincerity of his belief in this regard leads to taking a bit more charitable view of his actions, for his patriotism in other respects has never come into question.

During the Senate debate, to which reference will be made in Section E, Senator Robinson (of Indiana), who claimed that Yardley, as a resident of Indiana, was one of his constitutents, introduced and read a telegram from Yardley himself which is among the most remarkable of his statements:[53]

---

53. Congressional Record, Senate, 10 May 1933, pages 3179-3180.

Please refer to your telegram in which you ask that I give you my defense for my publications, since they seem to have inspired the new bill.

I presume that you refer to "The American Black Chamber." The American Cipher Bureau, which intercepted and deciphered foreign code messages, was created by me in 1917 and directed by me until 1929, when the Government ordered it disbanded on the theory that it was unethical to read foreign code messages.

My justifications for publishing The American Black Chamber, in which my activities are described, are:

(1) It could not injure this Government, because it proved to foreign nations that we would no longer stoop to this sort of espionage.

(2) It could not offend any foreign government, because it contained no material about their machinations in this country.

(3) It would, I hoped, awaken the conscience of the State Department, so that they would revise their own code systems and render American diplomatic secrets invulnerable to attack by clever foreign cryptographers.

(4) I assumed that the United States Government belonged to the American people, and since this Government had washed its hands of secret diplomacy I saw no reason why the people should not to know [sic] about the world in which we live—a world in which we are too unconcerned to follow the espionage practices of all great nations, a world in which we are so unconcerned about our own diplomatic secrets as to use unsafe codes.

One press dispatch carries the story that the bill is to protect our own codes. Just to keep the record correct I wish to say that I have been very careful not to publish a single word about our own codes except to say a year or so ago that they were decipherable. If our codes have since been revised and are now indecipherable by master cryptographers of foreign nations, the publication of The American Black Chamber was not in vain.

This Government's fear of the unpublished manuscript now in its hands is, in my opinion, due to false sensational rumors originating in New York. It is a dull treatise for scholars and students of history. The ordinary person would fall asleep while reading it. Whether it is published or not is of no consequence to me. As a matter of fact, I am too busy in my laboratory completing my experiments on a commercial invisible secret ink for children and adults to write their letters with to be at all concerned about anything else.

Herbert O. Yardley
Worthington, Ind.

E. Secrets of Japanese Diplomacy

Reference has already been made (in Section C) to a second occasion on which Yardley planned to publish further revelations of the signal intelligence work of MI-8. Early in 1933 the authorities learned that he had prepared the manuscript of a book entitled "Secrets of Japanese Diplomacy" and that this was to be published in New York by Longmans, Green and Company. The manuscript was, however, furnished by the prospective publisher to the Government and it was never published. Meanwhile, this experience led to an attempt to prevent such types of publication in the future by the enactment of special legislation. At the instigation of the State Department, Representative Hatton W. Sumners, Chairman of the House Judiciary Committee, introduced, on 27 March 1933, H. R. 4220 ("For the preservation of Government records"). This bill was reported favorably by the Judiciary Committee as amended and was passed without opposition by the House on 3 April 1933. The bill

That whoever, by virtue of his employment by the United States, having custody of, or access to, any record, proceeding, map, book, document, paper, or other thing shall, for any purpose prejudicial to the safety or interest of the United States wilfully and unlawfully conceal, remove, mutilate, obliterate, falsify, destroy, sell, furnish to another, publish, or offer for sale, any such record, proceeding, map, book, document, paper, or thing, or any information contained therein, or a copy or copies thereof, shall be fined not more than $2,000 or imprisoned not more than three years, or both, and moreover shall forfeit his office and be forever afterwards disqualified from holding any office under the Government of the United States.

Sec.2. Whoever shall wilfully, without authorization of competent authority, publish or furnish to another any matter prepared in any official code; or whoever shall, for any purpose prejudicial to the safety or interest of the United States, wilfully publish or furnish to another any matter obtained without authorization of competent authority, from the custody of any officer or employee of the United States or any matter which was obtained while in process of transmissions from one public office, executive department, or independent establishment of the United States or branch thereof to any other such public office, executive department, or independent establishment of the United States or branch thereof or any matter which was in process of transmission between any foreign government and its diplomatic mission in the United States; or whoever shall for any purpose prejudicial to the safety or interest of the United States, wilfully, without authorization of competent authority, publish, or furnish to another, any such matter or anything purporting to be any such matter, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

Sec.3. In any prosecution hereunder, proof of the commission of any of the acts described herein shall be prima facie evidence of a purpose prejudicial to the safety or interest of the United States.

When the press became aware of the fact that the House had passed this bill without debate, a great cry went up that this was an abrogation of the freedom of the press and contrary to the First Amendment.

Accordingly, when the Senate considered the bill, a sub-committee did much to remove the objections of the press. The bill was passed by the Senate on the Monday preceding 10 May 1933 but it was moved that reconsideration be given to the bill and on 10 May 1933 the Senate devoted several hours to debate on H. R. 4220. In general, the Democratic senators supported the bill but there was some opposition from Republicans. In the end, however, H. R. 4220 became Public Law No. 37, 73d Congress, as follows:

> AN ACT for the Preservation of Government Records.
>
> Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That whoever, by virtue of his employment by the United States, shall obtain from another or shall have custody of or access to, or shall have had custody of or access to, any official diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, and shall wilfully, without authorization or competent authority, publish or furnish to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.
>
> Approved, June 10, 1933.

During the Senate debate serious objections had been raised by Senator Bronson Cutting of New Mexico to the wording of the bill. There were, however, other objections to the measure as passed by the House, which did not receive attention by the Senate.[54] It covered

---

54. See Memorandum for the Assistant Chief of Staff, G-2, from Lieutenant Colonel J. H. Van Horn, Signal Corps, Executive Officer, 13 April 1933 (OCSigO 032 Legis.), copy now filed in the Office of the Director of Communications Research.

code but not cipher; it covered diplomatic traffic, not military and naval as well; it covered traffic in transit to and through the United States but not traffic between foreign points; it did not cover plain text; and, finally, the word "furnish" was not sufficiently clear. The memorandum cited therefore suggested the following version in place of that originally passed by the House:

> That whoever being or having been in the employ of the United States shall wilfully, without authorization or competent authority, disclose, publish, or furnish to others any official code or cipher of a foreign government, or any official secret communication exchanged between officials of a foreign government, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

A much more serious objection to the bill as passed by Congress was that it offered to the Government only partial protection: it forbade the publication of information obtained from any code message of this or other governments but it did not forbid the publication of collateral information, the revelation of which might have just as damaging an effect upon the future of signal intelligence. For example, a person who had been trained in Governmental signal intelligence units might publish a text on cryptanalysis and still not violate this law. A further attempt was made much later, during World War II, to enact really stringent legislation designed to prevent the publication of any kind of book or article or related topics. This bill was actually passed by the Senate but was recommitted on motion of Senator Homer Ferguson of Michigan, who having been absent when it was passed, regarded

it as an attempt on the part of the executive branch to prevent giving of testimony to the Pearl Harbor Congressional Investigation.

F. Reasons for the Failure of MI-8

The most obvious reason for the failure of MI-8 lay in the fact that its principal support was derived from a department of the Government which reflected political changes and the temper of the times more directly than does the War Department. It was, in fact, a change in administration which produced a change in policy that led to the withdrawal of this support.

Internally, however, were two other reasons which contributed to the failure of MI-8: the location of the unit and the choice of its Chief. The isolation from direct supervision as a result of its transfer to New York produced neither the desired secrecy nor the attention that it should have had from the War Department. The Cipher Bureau accepted the support offered, assumed a clandestine existence, and slowly declined. Too few persons knew of its official status,[55] and when those who were acquainted with this connection became preoccupied with matters of peace or where transferred to new

---

55. While Mr. W. F. Friedman, then Chief of the Code and Cipher Section, Office of the Chief Signal Officer, was well aware of the existence of MI-8, he had no official connection with the New York unit and could establish liaison with it only through Yardley's superiors in the Military Intelligence Division.

assignments, the lessons learned in World War I were ignored or forgotten.[56]

The man most responsible for the secrecy imposed by necessity on MI-8 was the only one who violated it. He had demonstrated a certain amount of cryptanalytic ability during the War and had achieved within the War Department a reputation as a cryptanalyst, but in a position of authority in time of peace he had neither the incentive nor foresight to build MI-8 on a firm foundation. Even had it been practicable—which it was not, because of the clandestine situation into which he had maneuvered the bureau—all training was ignored, while he profited from real estate activities; his enthusiasm for cryptanalysis lagged as he became a consultant in more profitable code production activities for commercial firms. Then, when his own position was abolished, he divulged information of the highest secrecy and made himself notorious in the annals of cryptology.

Nevertheless, if potential enemies had learned lessons from the experience of MI-8, the War Department had also learned its lesson. It was obvious that the separation of cryptanalysis and cryptography was a mistake of the worst sort; that the two should be integrated under a single agency in order that each might profit from the knowledge gained by the other. It was equally evident that training

---

56. With one exception (Major Frank Moorman) the officers who were Yardley's superiors were without technical experience in cryptological matters. The only other technical expert then employed by the War Department (Mr. Friedman) was a Signal Corps civilian employee.

should be the principal objective for this agency in an era of peace, so as to prepare for immediate expansion in time of war. These lessons were well learned, and measures were already taken to rectify the errors of the past.

CHAPTER V. THE FORMATION OF THE SIGNAL INTELLIGENCE SERVICE

A. Steps toward the Establishment of Unified Responsibility

The primary result of the investigation conducted by Major O. S. Albright for the Military Intelligence Division,[1] though it was not at once fully achieved,[2] was the unification[3] of responsibility for all cryptological work carried on by the Army in a single organization. It was peculiarly fortunate that this movement began when it did, for in the same year (1929) the Nation faced the most severe economic depression it had ever experienced, with the result that funds for military purposes, though by no means abundant in the first decade of the Peace, were much more restricted in the second. At a time when Government revenues fell off, it was inevitable that such money as was available should be spent for more pressing needs than preparation for a war which to most people then seemed remote, if not impossible. The unification of responsibility made it possible for those concerned with cryptology to present a single request for funds, with the result that a proper balance could be maintained between cryptographic and

---

1. See Chapter IV, Section A.

2. Not until 1934 was responsibility for printing, storage, and issue, assigned to the Chief Signal Officer.

3. A step in this direction had been taken during World War I when the Military Intelligence Division assumed some of the cryptological functions formerly carried on by the Signal Corps, but even then the unification was by no means complete. See Volume Two, particularly Chapter I.

cryptanalytic activities. Had the diversity of responsibility longer continued, it is doubtful whether sufficient funds could have been obtained to carry on adequate preparations for war.

That the responsibility should be unified in the interests of efficiency was a fact that does not appear to have needed much discussion. The experience of the preceding decade when no such unity had existed convinced all concerned of the need for a reorganization in this direction. The factors which ultimately justified the placing of the unified responsibility within the Signal Corps were these:

a. The Signal Corps had already established a code compilation section which had done satisfactory work.

b. The chief of this section was a competent cryptanalyst.

c. He had already participated in training programs, as the author of training pamphlets, as instructor in Army camps, and as a participant in maneuvers.

d. The Signal Corps was better equipped to develop necessary intercept facilities than any other Army organization; in fact, it was the only such organization.

e. The Signal Corps could develop secret ink facilities as well as any other organization.

f. The Military Intelligence Division had no training program; in fact, it had borrowed the services of the Signal Corps cryptanalyst for such limited training exercises as had been possible.

g. The Military Intelligence Division had lost the financial support formerly received from the State Department.

h. Internal difficulties within MI-8 made a radical reorganization imperative.

i. It was believed desirable to remove the operation of solution and detection services from the General Staff and to place it within an existing operating branch.[4]

Accordingly, it appeared logical "that the Signal Corps should be charged with all phases of this work", to the end that it might "be properly coordinated as an organized entity, and still remain as at present under the General Staff control and supervision of G-2."[5] Such a concentration of the entire responsibility in the Signal Corps would eradicate, it was believed, the existing difficulties. Training could be coordinated through the assignment of personnel for technical training, and, in time, qualified personnel would be available for maneuvers.[6]

In order that the Signal Corps might assume the duties of solution of codes and ciphers and the detection of secret inks, in addition to those formerly held, certain changes were recommended in existing Army Regulations. The pertinent paragraph in the Communications Section of the Handbook for War Department General Staff (October 1923)[7] was amended to read as follows:

---

4. See Memorandum for Colonel [S. H.] Ford from Lieutenant Colonel W. K. Wilson, 18 March 1929; Memorandum for the Chief of Staff from the Assistant Chief of Staff, G-2, Subject: Responsibility for the Solution of Intercepted Enemy Secret Communications in War (no date, approved 5 April 1929), sec. 2, par. 3.

5. Memorandum for the Chief of Staff from Colonel Ford (5 April 1929), sec. 2, par. 4.

6. Memorandum for Colonel Ford from Lieutenant Colonel Wilson (18 March 1929), par. 4.

7. Chapter iii, pp. 21-22.

> 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 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.[8]

Among the duties of the Chief Signal Officer as then currently prescribed by Army Regulations 105-5, 15 December 1926, was the following:

> e. The preparation and revision of the War Department Telegraph Code and other codes and ciphers required by the Army.

This paragraph was amended on 10 May 1929 as follows:

> e. The preparation and revision of 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.[9]

Though the responsibilities of the Chief Signal Officer in the field of cryptography and cryptanalysis were considerably expanded on this change, responsibility for printing, storing, issuing and accounting for cryptographic materials were not yet a function of the Chief Signal Officer but continued to remain with The Adjutant General until 1934.

B. The Creation of the Signal Intelligence Service

As a consequence of the transfer of these functions from the

---

8. Memorandum for the Chief of Staff from Colonel Ford, 5 April 1929, sec. iii, par. 2.

9. Ibid., par. 3. Changes No. 1, 10 May 1929, to AR 105-5, 15 December 1926.

Military Intelligence Division, a conference, attended by Lieutenant Colonel John E. Hemphill, Major William R. Blair, Major O. S. Albright, and Mr. William F. Friedman, was held in the Office of the Chief Signal Officer on 19 July 1929. The conclusion was reached that the primary function of the newly formed Signal Intelligence Service[10] was one of training personnel for utilization in war and of establishing the necessary organization to accomplish the training missions of the respective sections of the Signal Intelligence Service.[11]

It was proposed that the Signal Intelligence Service should consist of four sections, organized in a unified manner and administered by the Office of the Chief Signal Officer. These were to be:

a. Code and Cipher Compilation
b. Code and Cipher Solution
c. Intercept and Goniometry
d. Secret Ink[12]

The function of the Compilation Section was to continue the policy formulated ten years previously. Codes and ciphers were to be produced for use in peace, but a certain number of reserve codes and ciphers were

---

10. The term "signal intelligence" had been coined a few days previously by Mr. Friedman. Though the new agency was known officially as the Signal Intelligence Service, a designation it was to retain until 1942, it appears on various Tables of Organization of the War Plans and Training Division, Office of the Chief Signal Officer (e.g. 15 October 1934—SPSIS 320.3; 2 March 1937—ibid.) as the "Signal Intelligence Section," a designation which was also used in the title of some of the technical papers published by the organization prior to 1937.

11. Memorandum (minutes of the Conference—SPSIS 320.3), p. 1.

12. Ibid.

to be kept ready for immediate use in time of war. The peacetime mission included the training of cryptographic personnel who would be able to function properly in the field during war.

The Code and Cipher Solution Section was to be trained and organized for a war emergency in order that in a crisis it could solve enemy codes and ciphers. Thus its work was to be primarily the establishment of a training program, not immediate interception and solution of the communications of foreign armies or governments. If, however, in the course of the training program, foreign messages were intercepted and solved, and they were found to contain material of potential value as intelligence, G-2 would be glad to have the information obtained, but this was to be regarded as a by-product of the training work, not a normal function of the service in peacetime.

In war the principal function of the Intercept and Goniometric Section was to be interception of enemy communications and location of enemy transmitting stations by goniometric means. In peace, its principal objective was to be the organization and training of units which could function effectively in war. Similar aims were assigned to the Secret Ink section. It was to devise and develop secret inks for the use of G-2 personnel and to detect secret inks in enemy documents. Its peacetime mission was likewise one of research and training for operations in war.

It was contemplated that sections of the Signal Intelligence Service would be organized in the Panama and Hawaiian Departments, where training maneuvers and exercises were frequently conducted. These sections were to be manned by enlisted personnel. It was decided that higher authority would be requested to determine the advisability of establishing such a section in the Philippine Department. The departmental intercept stations were to be organized solely for training purposes. Intercepted material would be analyzed only if there were available a section devoted to solution. The intelligence derived would be submitted to the Department G-2 or to the Department Signal Officer, for transmission to the Department G-2.

The establishment of sections of the service outside of the continental limits of the United States emphasized even more the need for intensive training. It was estimated that it would take a minimum of two years to train personnel who would be capable of acting as independent cryptanalysts and engaging in solution activities at the departments indicated. It was contemplated, however, that material which proved insoluble would be forwarded to the Office of the Chief Signal Officer for further study. The training for both intercept and goniometric work and the study of secret inks was to be conducted at Fort Monmouth.

C. The Closing of MI-8

This transfer of activities involved the dissolution of MI-8 and an abandonment of its mission except insofar as the SIS assumed the function. MI-8 had been designed to "obtain information of present, immediate value" and as Major Albright had discovered, had devoted little attention to training for war. There remained the problem of the disposition of the personnel of MI-8, which was made especially difficult by the withdrawal of all financial support by the State Department. War Department funds were not available to cover the loss of the State Department's contribution. Until ways and means could be worked out to obtain an increase in War Department annual funds, it was suggested that the Chief of MI-8 (Herbert O. Yardley) be offered a temporary position in the Signal Intelligence Service at a salary considerably lower than that which he had previously received,[13] and that other personnel of MI-8 should also be offered temporary positions, the total expenditure to be within the available funds of $10,000. It was considered highly probable that the offer to Mr. Yardley would not be acceptable to him, in which case a reorganization without "entanglements from the past" would be possible.

---

13. His salary in 1929 was $7500 a year. Mr. Friedman in the same period was being paid $5600 a year. It should be remembered that at this time Yardley had not yet become *persona non grata* to the signal intelligence services of the Government. He did not publish *The American Black Chamber*, as described in the preceding chapter until 1931, more than a year afterward.

If this proved to be the case, four young men were to be employed and given thorough training in the Signal Intelligence Service for their future development, with the ultimate object of organizing the Signal Intelligence Service in the departments. They were to be college graduates and great care was to be taken in their selection. It was also anticipated that they should qualify as reserve officers so that, as holders of Signal Reserve Commissions, they would be competent to act independently as heads of advanced Signal Intelligence Service Sections, wherever these might be established.

It was estimated that with the funds available from the Military Intelligence Division, which amounted to only $10,000,[14] and the $7,160, paid by the Signal Corps to the two persons in the Code and Cipher Section, only $1,720 of additional funds would be required. Thus, the total sum of $18,880 would be necessary for the salaries of the four cryptanalysts and three clerks who would serve under Mr. W. F. Friedman, the Civilian Chief of the Service. The section would be assigned to the War Plans and Training Division of the Office of the Chief Signal Officer to which the Code and Cipher Section had also belonged. The lease and salaries of MI-8 were terminated 1 November 1929 and in October, Mr. Friedman was sent to New York to take over the files and records, which had been packed, and to

14. After the State Department had withdrawn its support.

The SIS about 1935: Seated, Mrs. Louise Newkirk Nelson; Standing, Left to Right: Mr. H. F. Bearce, Dr. Solomon Kullback, Captain Harrod G. Miller, USA, Mr. William F. Friedman, Dr. A. Sinkov, Lt. L. T. Jones, USCG; and Mr. Frank B. Rowlett. Mr. John B. Hurt was ill when the picture was taken. Photograph through the courtesy of Colonel Frank B. Rowlett.

supervise their transportation to Washington. He also made offers of employment in the Signal Service at Large to two of the persons who had worked in MI-8. Mrs. Ruth Willson,[15] then the Japanese expert of MI-8, was unable to accept a position because it involved her moving to Washington--she had a husband and child in New York. Another employee, Mr. Victor Weiskopf, had a rare-stamp business in New York and he, too, refused to move to Washington. The clerical employees were not technically trained and could not be transferred to the Signal Service at Large, because they had no Civil Service status. An offer of temporary employment was made to Mr. Yardley, but he refused it.[16] Eight months later (1 June 1930), a second tender of appointment as a Cryptanalyst at $312.50 per month was made to Mr. Yardley, but this also was declined.[17]

D. The Signal Intelligence Service Officially Established

By order of the Secretary of War, The Adjutant General officially notified the Chief Signal Officer of the changes in War Department

---

15. In the available records she is always referred to as "Ruth Willson"--No reference to her as a married woman is extant.

16. W. F. Friedman, History of Signal Intelligence Service, p. 11.

17. Memorandum for the Executive Officer from Edward Barnett, Civilian Assistant, 30 January 1939, Sec. II, p. 7. The salary offered Yardley was fifty percent of what he had been getting in 1929.

policies relating to codes, ciphers, secret inks, radio interception, and goniometry. The text of this letter was substantially that drafted by Major Albright and Mr. Friedman and is so important that it should be quoted in full:[18]

SUBJECT: Codes, Ciphers, Secret Inks, Radio Interception and Boniometry

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.

---

18. Quoted from the copy on file in the Office of the Director of Communications Research. This bears the stamp of the Office of the Chief Signal Officer dated 1017 hours, 24 April 1930. See File AG 311.5 (4-14-30) Pub.

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, and 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[19] is responsible for the printing of codes 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.

---

19. That is, the Office of The Adjutant General.

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 disguisement.

b. At General Headquarters:

(1) The preparation of field codes and ciphers which are employed 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 of disguisement.

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 peace time organization and training of this activity should contemplate, first, training personnel, and second, furnishing specialists to large commands for peace time maneuvers after personnel has been sufficiently trained. To accomplish this end it would seem that, at the present inception of this new service, its peace time 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 peace time 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 peace time 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 peace time maneuvers of large commands. It is also a possibility that during peace time 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.

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 objectives 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 objectives 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:

/s/ Alfred J. Booth
Adjutant General

In accordance with the directive from the Secretary of War a draft was immediately formulated for Army Regulations to cover the functions and duties of the Signal Intelligence Service. Five types of signal intelligence units were to be organized, (1) in the War Department, (2) in the corps areas and departments, (3) at General Headquarters, (4) with the field armies, and (5) Radio Intelligence Companies which might be assigned to any of the spheres of activity outside of the War Department.[19]

While the War Department Signal Intelligence Service was designed to operate directly under the control of the Chief Signal Officer, general staff supervision of its activities was exercised by the G-2 division of the War Department General Staff. The signal intelligence units in the corps area or departments were established at the direction of the War Department, but operated under the direct control of the local Signal Officer, under general staff supervision by the corps area or department G-2.[20]

The General Headquarters organization included a Signal Intelligence Service and several Radio Intelligence Companies under its supervision

---

19. Organization and the Duties of the Signal Intelligence Service (SPSIS 322) par. 2, pp. 5-6.

20. Ibid. pars. 16-17, pp. 11-12.

and direction. Since its sphere was in a theater of operations it was to study captured enemy documents relating to enemy signal service which were forwarded to it by the G-2 division of the General Headquarters general staff. It was composed of four sections, devoted to administration, radio intelligence, security, and secret inks, the compilation of codes and ciphers, and the solution of enemy codes and ciphers.[21]

The Signal Intelligence Service at General Headquarters was to be interested primarily in such tactical operations as enemy radio organization, the location and types of enemy radio stations, the relief of units and their changes in frontage, increases or decreases in the number of enemy transmitting stations, and enemy aerial activity. It was also to coordinate the work of the General Headquarters and Army Radio Intelligence Companies and in its security work to study violations of communication security and radio operating regulations.[22]

The Army Signal Intelligence Service was to consist of a headquarters section, with one or more Radio Intelligence Companies operating under its direction and supervision. The duties of this unit were restricted to the combat zone, including interception, goniometry, the translation of messages with the assistance of information supplied by General Headquarters the supervision of radio and wire traffic to subordinate units in the field army concerned, and maintenance of communication security within the combat zone. The four sections of the Army

21. Ibid., pars. 18-19, pp. 13-14.

22. Ibid., par. 19, p. 14.

unit were engaged in administrative, solution, radio intelligence, and security activities.[23]

In its solution of enemy codes and ciphers, the Army service was to prepare plans and orders for radio surevillance of enemy radio stations and interception of the traffic of the required type. Intercepted traffic was to be clarified, indexed, and filed, and documents and messages were to be translated. It was to exchange the information promptly with General Headquarters and adjacent armies.[24]

The Radio Intelligence Section was to issue orders for the radio surveillance of its sector of the combat zone for interception and the location and grouping of enemy stations by goniometry. Intercepted traffic was to be submitted to the code and cipher section for translation and for transmittal to General Headquarters for study and solution. This section was also to correlate, evaluate, and submit in proper form all information obtained concerning the location and grouping of enemy radio stations, call signs, operating frequencies, transmitting and operating characteristics to permit useful inferences to be drawn therefrom. It monitored United States Army communications for security reasons and supervised the training and operation of the Army Radio Intelligence Company.[25]

---

23. Ibid., pars. 21-22, p. 18.

24. Ibid., par. 23, p. 19. It is to be noted that evaluation and dissemination were at that time contemplated as part and parcel of the assigned functions of the SIS—a very important point, since these functions usually belonged to Military Intelligence.

25. Ibid.

The principal aim of the Security Section was to intercept communications from friendly radio stations in order to discover violations of cryptographic security rules and regulations. Radio camouflage was to be used for the deception of the enemy. It was to maintain surveillance to prevent the tapping of our important wire lines and to tap enemy wire circuits. Reports concerning violations of cryptographic and communication security were to be submitted as required and information gleaned from tapping enemy wire circuits was to be compiled for forwarding.[26]

The fifth Signal Intelligence Service unit was the Radio Intelligence Company. It was "equipped to perform intercept and goniometric functions for both limited and long range enemy transmission." The proper disposition and location of personnel and equipment for satisfactory interception was considered a matter of critical importance. Its coordination by the Army Signal Officer was essential, but considerable latitude and freedom of action on the part of the operating personnel were highly desirable in order that interception might be timely and accurate.[27]

In all cases the general mission of the Radio Intelligence Company consisted of the interception of enemy radio traffic, the location of enemy transmitting stations, and the surveillance of our own radio transmissions for purposes of security; but its principal mission depended on

---

26. Ibid., par. 23, p. 20.

27. Ibid., par. 24a, p. 21.

the purpose for which it was employed. It was not organized to intercept enemy wire or visual signal traffic. Its organization, training, and equipment were under five categories:

(1) As a unit of the GHQ Signal Service;
(2) As a unit of the Field Army Signal Service;
(3) In coastal frontier defence;
(4) For border surveillance;
(5) For interior surveillance.[28]

In organization, at war strength, the Radio Intelligence Company consisted of a headquarters and three operating platoons. The headquarters platoon consisted of an administrative section for company administration and mess; a supply and transportation section, which also repaired radio equipment; and an intercept section. The latter was to operate in two teams, each composed of four intercept stations. Its primary function was to intercept enemy traffic and to monitor Army communications, and to report enemy identifications and frequencies.[29]

The operating platoon was to consist of an intercept section, a control section, and a position finding section. Their operations were interrelated so that the entire platoon operated as a team primarily for the purpose of intercepting and locating enemy radio transmitting stations. The intercept section operated four radio receiving stations and located targets by direction finding and served as an intercept unit. The control section assigned missions to the

---

28. Ibid., par. 24b, p. 21.

29. Ibid., par.24c, p. 21.

intercept and position finding sections and consolidated information and transmitted it to the company command post. It also installed and maintained the telephone systems required by the platoons, providing the tie lines necessary to connect them with the company and higher headquarters. The position finding section operated four direction-finding stations to locate enemy radio transmitting stations by radio goniometric methods.[30] The duties of the various platoons varied with their assignments.[31]

E. Personnel of the Service

Although the official sanction of the transfer of the functions of MI-8 to the Chief Signal Officer was embodied in the change of Army Regulations dated 10 May 1929, the actual termination of MI-8 as a distinct organization did not occur until 1 November 1929, and the Chief Signal Officer was not officially advised as has been stated, of the policies that had been formulated until he received The Adjutant General's letter of 22 April 1930. Meanwhile, however, steps had been initiated to employ the necessary personnel after the appropriations from the Military Intelligence Division became available. On 16 December 1929, the sum of $6,666.68 was allotted by the Assistant Chief of Staff, G-2, to the Chief Signal Officer for the payment of personnel engaged

---

30. Ibid.

31. Ibid., par. 25, p. 22.

in code and cipher work.[32]

Provision had already been made for the cryptanalyst and the clerk authorized for the Code and Cipher Section of the Chief Signal Officer. It was necessary, however, to select and employ the personnel who were to be trained as permanent members of the Signal Intelligence Service. On 4 January 1930, the Secretary of War was requested by the Chief Signal Officer to authorize the employment of four Junior cryptanalysts (P-1) at $2,000 a year and one assistant cryptographic clerk (CAF-3) at $1620 a year in the Signal Service at Large, Washington, D. C. They were to engage in the preparation of codes and ciphers, because it had been concluded that there should "be established during peace time a small section of code and cipher specialists who will be under constant training in these sciences." These experts were to keep abreast of progress in this field and would serve as a nucleus in the initial phases of any emergency for the expansion of the Signal Intelligence Service into a much larger organization for war time. This recommendation was approved by the Secretary of War 13 January 1930.[33]

The four junior cryptanalysts were to complete a special course of instruction in cryptanalysis. After the initial states of their instruction had been completed, they were to assist in the technical

---

32. P/A MID P 5205A 1110-0. Cf. Memorandum for the Executive Officer from Edward Barnett, Civilian Assistant (30 January 1939), p. 4.

33. Ibid., 4-5; Memorandum for the Secretary of War from the Chief Signal Officer, 4 January 1930; 1st Ind., 13 January 1930.

phases of the work of the Signal Intelligence Service: compiling codes, preparing ciphers and cipher tables, conducting research in new cryptographic methods and machinery and in the solution of codes and ciphers, and participating in field training exercises in the war-time operation of code and cipher solution units. The assistant cryptographic clerk was to perform similar duties under more immediate supervision.[34]

A restricted budget demanded that the Signal Intelligence Service be organized with a small staff. It was essential, therefore, that the four persons to be trained be carefully selected. The principal qualifications required included a thorough training in mathematics and languages, embracing an understanding of French, Spanish, German, and Japanese. Eight candidates were recommended by the Civil Service Commission, but only three of these were appointed. The three were Frank B. Rowlett,[35] appointed 1 April 1930; Abraham Sinkov,[36] appointed 10 April 1930; and Solomon Kullback,[37] appointed 21 April 1930. Miss Louise Newkirk (later Mrs. Nelson) had been appointed to the clerical vacancy on

---

34. Memorandum for the Secretary of War from the Chief Signal Officer, 4 January 1930.

35. Colonel Rowlett was Chief, General Cryptanalytic Branch, SSA, from 1943 to 1945 when he became Chief, Intelligence Division, afterwards the Operations Division, Army Security Agency. He reverted to inactive duty on 1 May 1946.

36. Colonel Sinkov was Assistant Director, Central Bureau, Brisbane, from 1942 to 1945, when he returned to this country and became, in 1946, Chief, Security Division, Army Security Agency. He was still on active duty in June 1946.

37. Colonel Kullback was Chief, Military Cryptanalytic Branch, SSA, from 1943 to 1945 when he became Chief, Research and Development Division, Army Security Agency. He reverted to inactive duty on 1 June 1946.

1 March 1930,[38]

On 30 April 1930 authority was requested to employ a cryptanalyst aide (CP-3) at $1,800 a year, Signal Service at Large.[40] This recommendation was approved by the Secretary of War on 1 May 1930 and two weeks later, on 13 May 1930, Mr. John B. Hurt,[41] was appointed to this position. The Civil Service Commission had no eligible mathematician who also knew Japanese and waived the usual procedure for employment in this case, permitting the War Department to fill the position with Mr. Hurt whose knowledge of Japanese was outstanding.[42] One additional vacancy remained to be filled and on 2 September 1930

38. Executive Officer, Office of the Chief Signal Officer, to Secretary, Fourth U. S. Civil Service District, 25 February 1930; Memorandum for the Executive Officer from Edward Barnett, Civilian Assistant, 30 January 1939, p. 6.

39. The misconduct consisted of forging a physician's signature to several sick-leave certificates.

40. Several years earlier Mr. Friedman had, jointly with the Chief of the Code and Signal Section of the Navy Department, drawn up a schedule of job descriptions, in order to keep both services aligned in respect to qualifications, grades, rates of pay, etc., of cryptographic and cryptanalytic personnel. This far-sighted move was to become quite important later on.

41. From that date Mr. Hurt remained an employee of the SIS or of its successors, during World War II having worked at different times in the Military Cryptanalytic Branch or the Language Branch.

42. Memorandum for the Executive Officer, Office of the Chief Signal Officer, from Major W. H. Crawford (29 April 1930).

Lawrence Clark[43] was appointed assistant cryptographic clerk (CAF-3) at $1,620 a year.

The work of the Signal Intelligence Service was performed by Mr. Friedman and these six assistants on a budget of from $17,060 to $17,400 a year from 1930 to the conclusion of the Fiscal year 1937. There were some changes in clerical personnel during this period but the total remained constant. When Lawrence Clark was transferred to the Navy Department in 1935, he was replaced on 1 January 1936 by Herrick F. Bearce.[44] When Dr. Abraham Sinkov was transferred to Panama in 1936 and Dr. Solomon Kullback was transferred to Hawaii in 1937, they were replaced, respectively, by Robert O. Ferner[45] and M. A. Jones.[46]

---

43. Lieutenant Colonel Clark was on the staff of Colonel Sinkov in Australia and later became Assistant Chief, Security Division, Army Security Agency.

44. Lieutenant Colonel Bearce served with signal intelligence units in North Africa, Italy, France and Germany during World War II, and is at present (April 1946) chief of one of the large sections of the Intelligence Division, Army Security Agency.

45. Mr. Ferner continued to be employed as a cryptanalyst throughout World War II, being at present a member of the Research and Development Division, Army Security Agency. Mr. Jones and Mrs. Nelson were the only employees of this early period who did not remain throughout the War.

46. Memorandum for the Executive Officer from Edward Barnett, 30 January 1939, p. 7.

The five years 1933-1938 marked a period of severe economic depression not only in the Nation at large but in the Signal Intelligence Service in particular. Promotions were not made and salaries were cut. As a result, morale was extremely low.

In the Fiscal Year 1938, as the tension in a militant Europe became more obvious, the authorization for personnel in the Signal Intelligence Service was increased to eleven, including two additional junior cryptanalysts and two more clerks. The budget was raised to $24,360 for that year.[47] After the Munich crisis, when a conflict appeared even more inevitable, the authorization for the Fiscal Year 1939 was increased to fourteen persons.[48]

F. Conclusion

The unification of the units engaged in the solution of secret means of communication with that assigned to the task of compilation marked a progressive step in the development of cryptological activity in the War Department. Training for war had become the fundamental objective of the Signal Intelligence Service. Even that training, however, as well as the other essential work of the organization, was handicapped by the program of economy imposed upon the War Department

47. For the first time in the history of the Signal Intelligence Service the budget approximated the lowest sum spent by MI-8 in any year. It should be mentioned that this increase for additional personnel for signal intelligence work was the very first in the War Department preparations for expansion and possible war.

48. Memorandum for the Executive Officer from Edward Barnett, 30 January 1939.

in a period of economic depression and budgetary restriction. This policy continued even after the depression relaxed because of governmental preoccupation with internal problems.

In October 1931, during the preparation of the budget for the Fiscal Year 1934, it was recommended by the Chief Signal Officer that the personnel for the solution of codes and ciphers should be increased by four. Such an expansion was deemed necessary for the proper discharge of this function if the Army was to have trained Signal Intelligence personnel available for the mobilization of the necessary sections on M-day. The proposal would have increased the personnel to eleven and the budget to $24,740 by 1934, but the actual authorization for this increase was not obtained until 1938.[49]

The entire burden for the support of the Signal Intelligence Service was thrown upon the Signal Corps in the Fiscal Year 1932 when the Military Intelligence Division allotment was withdrawn. The Signal Corps therefore increased its allotment for the service by $9,600 to make up for the loss of the G-2 appropriation, but the Signal Corps had many other operations to support, although the importance of the Signal Intelligence Service was fully appreciated.[50]

---

49. Memorandum for The Adjutant General from Executive Officer, OCSigO, Subject: Signal Intelligence Service, 14 October 1931 (SPSIS 311.5).

50. Ibid., Inclosure.

In 1935 the Chief of the Signal Intelligence Service recommended that the time had come to organize the Signal Intelligence activities of the Chief Signal Officer upon a more extensive basis, "in order that personnel for efficient operation may be available when the situation will require their services." It was also considered essential to provide opportunities for advancement for the personnel already employed, in order that a restricted field might be attractive to them. Otherwise, the Signal Intelligence Service would "become merely a training ground for other departments."[51]

A five-year expansion program was recommended, which would increase the total personnel to 21 by 1942, with a total budget of $54,660.[52] Various obstacles impeded the immediate approval of this plan. In the first place, any proposal for an increase in the salaries of the personnel in the Signal Intelligence Service was held to be objectionable. For several years, owing principally to measures of economy imposed by the President and Congress, it had not been possible to provide administrative promotions for any Signal Corps employees. In addition, the President had directed that no promotions were to be included in the 1937 budget.[53]

---

51. Memorandum to Major Rumbough from W. F. Friedman, 19 August 1935 (SPSIS 320.2).

52. By that date, war had been declared and the budget increased many times the figure requested.

53. Routing and Work Sheet, 19 December 1935, Action 2, Fiscal Officer to Executive Officer, OCSigO, n. d. (SPSIS 320.2).

A second obstacle was that the personnel and equipment assigned to the Signal Intelligence Service fully occupied its available space and because of the critical shortage of office and storage space in the District of Columbia no additional space was likely to be secured for the expansion of that organization. It was suggested that additions to the existing force would overcrowd the area and be detrimental to health and comfort as well as impair the performance of their duties.[54]

This request for personnel was not approved and the four additional positions had to be deleted from the estimates. One of the contributory factors which necessitated this was the lack of support received from representatives of G-2. Assurance had been obtained from G-2 in advance that it would cooperate in defense of the item, but its representatives "failed to appear at the hearing when held."[55]

It was the opinion of Major W. S. Rumbough, Officer in charge of the War Plans and Training Division, of which the Signal Intelligence Section was a part, that such "a serious shortage of trained personnel exists in the Signal Intelligence Service" that it could not "full perform its peace-time mission." If this shortage should "be allowed to continue, no Signal Intelligence Service worthy of the name will be available during the early phase of an emergency when the most valuable results should be expected from this agency."[56]

---

54. Routing and Work Sheet, 19 December 1935, Action 3, Civilian Assistant to Executive Officer, OCSigO, n. d. (SPSIS 320.2).

55. Memorandum for the Chief Signal Officer from Major W.S. Rumbough, Subject: Increase in Personnel for the Signal Intelligence Service, 18 February 1936 (SPSIS 320.2).

56. Ibid.

CHAPTER VI. CRYPTOGRAPHIC PROGRESS 1930-1939

A. The Code-Production Program 1930-1934

The policy regarding the production of codes, which had already been formulated by the Code and Cipher Section[1] in the twenties, was continued by the Signal Intelligence Service in 1930. In general, the goal was to keep an initial M-Day issue of every code in readiness for an emergency and two reserve issues in secret storage. Every effort was made to attain this aim as soon as funds and personnel available permitted.[2] To accomplish it, a schedule of priorities for code production was prepared.

In 1930 it was planned that all codes required for a war emergency, together with the necessary reserve editions,[3] would be published within the succeeding ten years. The amount to be expended for printing and binding the codes in any fiscal year never exceeded $7,600, while the number of codes to be printed in any single year varied from one to seven.[4]

Within a year, however, it became necessary to formulate a new program which would reflect the reduced budget for printing and binding upon which the compilation unit was forced to depend. The schedule of

---

1. See Chapter I.
2. Memorandum for Lieutenant Colonel O. S. Albright from Major D. M. Crawford, 5 April 1930 (SPSIS 111).
3. That is, sufficient systems for the beginning of a war.
4. See note 2.

seven codes to be printed in 1931 had not been fulfilled. One code which was already compiled was printed, but no new codes were published. Consequently, in the revised schedule for 1932, eleven codes were listed. Many of these were revisions of codes which were relatively low in production costs, so that the estimated expense for 1932 was $5,000. This was a five-year program, in which the estimated annual costs varied from $4,100 to $5,100.[5]

It was evident by March 1932 that the personnel assigned to the Service were insufficient in number to accomplish the tasks required in compilation. The urgency of the work required to compile the 12 authorized editions of codes that had yet to be prepared was such that practically all other activities would have to be suspended until the section had caught up with this work. It was then estimated that it would take a single team of two junior cryptanalysts and one assistant cryptographic clerk three years to compile the manuscripts. If an additional code was authorized an additional year would be required.[6]

Therefore, as early as 1933, an official revision of the code production program was considered necessary. It was submitted to the Chief of Staff and approved by Major General Hugh A. Drum, Deputy Chief of Staff, on 22 March 1933. This program required the publication of 10

---

5. 1st Memo. Ind. for The Adjutant General from the Chief Signal Officer, 28 April 1931 (SPSIS 111).

6. Memorandum to the Chief Signal Officer from Major D. M. Crawford, March 1932 (SPSIS 311.5).

codes in the Fiscal Year 1935 and postponed the printing of the more voluminous War Department Staff Codes No. 2 and No. 3 until the Fiscal 1936 and 1939, respectively. Four other codes were scheduled for the Fiscal Year 1936 and three for the Fiscal Year 1937. Consequently, the estimated costs were decreased gradually from 1935, when they totalled $12,850 to $9,000 for the single volume of War Department Staff Code No. 4 to be printed in 1939.[7]

Two additional paragraphs, requesting that The Adjutant General include the funds necessary for printing and binding the required codes in his estimates and that two additional clerks be added to the staff, failed to receive the concurrence of the Assistant Chief of Staff, G-4. The latter objected that the project would cost $13,650 per year for five years and he could not concur unless this sum could be absorbed by The Adjutant General or the Chief Signal Officer in their budgets.[8]

The revision of the program was carried even farther in the latter part of 1933. The Code Production Program of 22 March 1933 anticipated that Army Field Code No. 2 and Division Field Code No. 11 would be printed in the Fiscal Year 1934 at a total estimated cost of $5,000. Special funds became available to The Adjutant General toward the close of the Fiscal Year 1933. As a result, the Signal Intelligence Service

---

7. Memorandum for the Chief of Staff from the Assistant Chief of Staff, G-2, Subject: Program for Code Production, 7 March 1933 (SPSIS 111).

8. Memorandum for the Assistant Chief of Staff, G-2, from the Assistant Chief of Staff, G-4, Subject: Program for Code Production, 10 March 1933 (SPSIS 111).

was asked to print the available codes as rapidly as possible. It was possible to print both Division Field Codes No. 11 and No. 12 as well as Military Intelligence Code No. 11, at a total cost of $3,228 from 1933 funds. Division Field Code No. 12, however, was not scheduled to be printed until 1935 and a change in program was necessary.[9]

A further change was made in September 1933, when The Adjutant General notified the War Plans and Training Division that no funds would be available for printing codes in the Fiscal Year 1934. It had been estimated that $5,000 would be required, of which the sum of $3,800 was necessary for the publication of Army Field Code No. 2. Although this code was then 25 percent complete, its publication had to be postponed until the funds could be secured.[10]

On 28 May 1934 The Adjutant General advised the Chief Signal Officer of a new peacetime policy relative to War Department codes. It was directed that, as funds became available, the Chief Signal Officer would always have in his possession, ready for immediate distribution, one edition of each authorized confidential and secret code. Cipher tables and two reserve editions of such codes and cipher tables in printed form would be held in reserve.[11]

---

9. Memorandum for Major S. B. Akin from Captain H. L. P. King, 26 February 1934 (SPSIS 311.5).

10. Ibid.

11. Memorandum to the Chief Signal Officer from The Adjutant General, Subject: Codes, Ciphers, Secret Inks, Radio Interception and Goniometry, 28 May 1934 (AG 311.5 (5-25-34)Pub.); Annual Report of Signal Intelligence Section, Fiscal Year 1934 (SPSIS 319.1), par. 1a.

The fairly wide distribution of all of the secret codes increased the possibility of the compromise of one or more codes through loss, capture, or exposure as a result of carelessness in safeguarding and handling codes and messages. Even if no compromise occurred, experience had demonstrated that the life of a secret code varies with the volume of messages sent and received and the size and type of construction of the code book. Consequently, the safest of secret communications required the substitution of a new code before the maximum permissible number of groups had been transmitted. It was necessary to insure the safety and continuity of secret communications by keeping at least two reserve editions on hand at all times.[12] In conformity with this policy, the Signal Intelligence Service concentrated its efforts upon the compilation and production of the required editions of all authorized secret or confidential codes.

B. The Unification of Code Production, 1934

By 1934 it had become obvious that the complete centralization of responsibility for the production of codes and ciphers in the Office of the Chief Signal Officer was necessary in order that this work might be discharged more efficiently. The preparation of cryptographic communications involved three phases of activity. First, the Chief Signal Officer had for the past 14 years been charged with

---

12. Memorandum to the Assistant Chief of Staff, G-2, from Executive Officer, OCSigO, 27 February 1933 (SPSIS 111).

devising and developing codes, ciphers, and cipher devices for use by the Army. The second phase was assigned to The Adjutant General. He directed the publication, storage, distribution and accounting of codes and ciphers. The third phase, the actual transmission of the secret and confidential messages through their preparation and translation, was handled in each headquarters and command by personnel assigned these duties by the commander. In Washington this work was done within the Cable Section of The Adjutant General's Office, a unit which had been transferred to his jurisdiction from the General Staff in August 1921. There was nothing to be gained by making any changes in regard to the third phase but as regards the first and second, the division of responsibility for correlated duties between two unrelated operating agencies was unsound, with an attendant loss of efficiency and security.[13]

Funds for the publication of codes and ciphers were never specifically allocated for this purpose, but were taken out of a lump sum allotted to The Adjutant General in accordance with the practical exigencies of the moment.[14] Such an arrangement did not facilitate the establishment

---

13. Draft Memorandum to Major Wogan, G-2, Subject: The Unification and Coordination of Cryptographic Work in the Military Establishment, 1933 (SPSIS 311.5); Memorandum for the Chief of Staff from Brig. Gen. Alfred T. Smith, Subject: War Department Policies with reference to Codes and Ciphers, 18 December 1933 (SPSIS 311.5).

14. Draft Memorandum to Major Wogan, Par. 6a; Memorandum to the Chief of Staff from Brig. Gen. Smith, Sec. II, Par. 1c (2).

and execution of any well conceived and consistent program for initial issue of the authorized codes and ciphers or for subsequent replacements of those which had grown obsolete.

The printing of codes and ciphers differed in technique from that of the majority of the other War Department documents which were published by The Adjutant General. To insure the necessary security only a very limited number of personnel could be entrusted with the work in all of its stages, including the preparation by mimeograph or multigraph in the Office of the Chief Signal Officer.[17]

This assumption of additional responsibility was necessary but it was also unauthorized. In time of war, when cipher tables and cipher alphabets would have to be replaced at very frequent intervals, this work would be extremely important. It constituted a responsibility that should be covered by appropriate regulations in a definite assignment of duty.[18]

After their publication, the codes and ciphers had to be properly stored or distributed to authorized holders. Periodic accounting was also essential. A publication costing thousands of dollars to produce might be rendered entirely worthless by the loss or compromise of a single copy in an edition of a thousand or more.[19]

---

17. Draft Memorandum to Major Wogan, par. 6c.

18. Ibid.

19. Ibid., 6d.

For adequate security the storage facilities for such secret documents must be carefully considered. The Adjutant General then had no vault or storage space which provided the required security. Certain secret codes and ciphers had had to be stored in space under the control of the Chief Signal Officer. While this vault in the Munitions Building was superior to the space available to The Adjutant General, it was neither secure nor sufficiently large for the storage of the secret codes. It was employed for the storage of other secret documents relating to signal intelligence work. Although the Chief of the Signal Intelligence Section was the only person who knew the combination of the vault, access to it was granted of necessity to some of his assistants.[20]

The Chief Signal Officer was not responsible for storage and could not initiate a proposal for a new vault. Since The Adjutant General did not actually store all of the codes, he could not defend a project for a new vault. His storeroom, on the top floor of the State, War and Navy Building was adequate in size for storage as the reserves were published, but it was considered unsafe because it had a wooden door without a combination lock and two skylights which could easily be broken, although they were fastened down.[21]

---

20. Ibid.

21. Ibid., Memorandum for the Chief of Staff from Brig. Gen. Smith, Sec. II, par. 1d.

These storage arrangements complicated the distribution of code and cipher publications. The Adjutant General, the officer authorized to control storage under Army Regulations, had to call on the Chief Signal Officer to supply the copies desired. The Signal Intelligence Service was acquainted with the agencies and means of signal communication available to the various units and knew those which should be provided with specific codes and ciphers. Distribution also involved accounting, which is exceedingly important in the case of secret codes. The existing arrangement, with its divided responsibility, involved a duplication of operations. It was not only considered illogical, but from the point of view of economy of effort and of communications security, it was believed to be untenable.[22]

As already mentioned, the third phase of cryptographic work in Army communications involves the handling of codes and ciphers in the transmission and reception of messages. Other operations are merely preliminaries to the provision of means for assuring secrecy in communications, the real purpose of codes and ciphers. Experience gained in war and peace had already demonstrated that even the most efficient codes and ciphers could not provide security if the cryptographic personnel was inefficient, careless, or untrained.[23]

---

22. Memorandum to Major Wogan, par. 6e.

23. Ibid., 7a.

In the field units the responsibility of cryptographing and decryptographing messages was a function of the message center according to Army Regulations. This insured a certain amount of training in the use of authorized codes and ciphers for message center personnel, but additional training would have been valuable. Even in permanent headquarters, such as Corps Areas, Departments, and the War Department itself, such messages were handled by personnel to whom other and more pressing duties were also assigned and no special training was provided. In one corps areas, the work might be performed by G-2, while in another it might be handled by G-3 or G-1.[24]

In headquarters where secrecy of communications was most often desired and security was most essential, the absence of properly trained personnel was conducive to a reduction of security. Blunders in cryptography that might be of value to enemy cryptanalysts were not necessarily caused by carelessness. Lack of technical knowledge which could be acquired only through special training and experience in cryptanalysis,[25] was the fundamental cause.

The procedure for routing secret and confidential messages also involved difficulties. In Washington the plain text was typed and forwarded to The Adjutant General's office by messenger with the request that it be sent in the appropriate secret code. In that office, it was turned over to the Cable Section where personnel, with no

24. Ibid., 7b.

25. Ibid.

training in cryptanalysis, cryptographed the message. The cryptographic version of the message was then carried by messenger to the War Department Message Center. After transmission it might be decryptographed by one of several staff officers, as designated by the local commander. Under such circumstances, the control of literal versions, or of those which were paraphrased or in code could be only superficial, resulting in a constant threat to security. Serious blunders might be undetected because, in this routine, a trained cryptanalyst could not observe the cryptographic clerks in actual operation.[26]

A further objection to the existing procedure was that it prevented the code-producing agency from determining the practicable suitability of the existing code system because that agency had no opportunity to observe any system in operation. As a result, any improvements in a system were based on purely theoretical considerations and it was possible "that potential enemy cryptanalysts" had access to "better data on the cryptographic idiosyncrasies of the U. S. Army" than did the Army's own code compilers.[27]

If, as was confidently anticipated, the cryptographing and decryptographing of communications at the larger headquarters were to be accomplished by automatic machines, which would require trained technicians for operation and maintenance, these technicians ought to

---

26. Ibid., 7c.

27. Ibid.

be Signal Corps specialists, performing their work at a message center under Signal Corps control.[28]

A final consideration in effecting such a transfer in control lay in the responsibility for the coordination and supervision of secret communications exercised by the Military Intelligence Division. This became more difficult to fulfill with the complicated distribution of such activities. In matters pertaining to the solution of enemy codes and ciphers, G-2 had only the Signal Corps to consider, but, in matters relating to United States Army communications, it had to supervise and coordinate several different agencies: the Signal Corps, The Adjutant General, the corps area and departmental staffs. This situation presented a constant threat to security and impaired the efficiency of operations with no compensating advantage in economy of either time or effort.[29]

In accordance with these considerations, it was recommended to the Chief of Staff that the publication, storage, distribution, and accounting of codes and ciphers should be transferred to the Signal Corps. The Chief Signal Officer was to include in his annual budget the necessary funds for printing and binding codes and ciphers, prepared in accordance with the approved program of code production. The Cable Section of the Office of The Adjutant General was to be

---

28. Ibid., 7d.

29. Ibid., Par. 8.

transferred to the Office of the Chief Signal Officer.[30]

On 21 March 1933 the Chief of the Signal Intelligence Section had been designated as the contact representative of the War Department for code production at the Government Printing Office.[31] This arrangement, however, did not eliminate the objections to the control of the funds for printing and binding codes and ciphers as exercised by The Adjutant General, and recommendation for the transfer of the control of such funds to the Chief Signal Officer was made on 6 February 1934.[32]

The Assistant Chief of Staff, G-4, objected to this recommendation on the ground that it was a mistake to isolate a single item. The reduction of funds allotted to code and cipher work could not be compensated by the use of funds in a general pool and flexibility in the use of such funds would be lost. He recommended that, beginning with the Fiscal Year 1936, the Chief Signal Officer should be directed to prepare an estimate for the required funds for printing and binding codes and ciphers, in accordance with the approved program of code production. The Adjutant General would then be directed to omit this

---

30. Memorandum to the Chief of Staff from Brig. Gen. Smith, Sec. III, par. 1, 3, 5.

31. The Secretary of War to the Public Printer, 21 March 1933 (SPSIS 311.5).

32. Memorandum to the Chief of Staff from Brigadier General Smith.

item from his estimates.[33] With this amendment the recommendation was approved on 28 May 1934.[34] The responsibility for the work was transferred to the Chief Signal Officer and the estimates for printing and binding codes and ciphers were included with the regular Signal Corps printing and binding estimates for 1936.[35]

On 21 August 1934 the transfer of the control of the publication, storage, distribution, and accounting of all codes and ciphers from The Adjutant General's Office to the Signal Intelligence Section, Office of the Chief Signal Officer, was officially approved and the corresponding change in Army Regulations published.[36] When these duties were actually transferred some 20,000 publications, with all records pertaining to them were inventoried and moved from the storage rooms in the State, War and Navy Building. They were either placed in the vaults of the Chief Signal Officer or shipped to Brooklyn for storage in the Signal Corps Depot. The operation was performed without the loss of a

---

33. Memorandum for the Assistant Chief of Staff, G-2, from the Assistant Chief of Staff, G-4, Subject: War Department Policies with reference to Codes and Ciphers, 16 February 1934 (SPSIS 311.5).

34. The Adjutant General to the Chief Signal Officer through the Chief of Finance, Subject: War Department Policies with reference to Codes and Ciphers, 28 May 1934 (SPSIS 311.5).

35. Memorandum to the Budget Officer for the War Department from the Acting Chief Signal Officer, Subject: Revised Estimates, Printing and Binding, Fiscal Year 1936, 18 September 1934 (SPSIS 111).

36. Changes No. 1, to AR 105-5, 15 March 1933, 21 August 1934 AG 311-5 (5-25-34).

The change in the control of cryptographic work in connection with messages in the War Department was also approved and effected in accordance with the recommendation to the Chief of Staff. The Code and Cable Section was transferred from The Adjutant General's Office to the War Department Message Center and the Chief Signal Officer became responsible for all cryptographing and decryptographing in the War Department. Signal officers assumed the same responsibility in corps area and departmental headquarters. On 1 September 1934 Army Regulations were issued to provide instructions for the employment of codes and ciphers and indicate the transfer of the several functions from The Adjutant General to the Chief Signal Officer.[39]

The responsibility for the Cable Section was assumed by the Chief Signal Officer but sufficient personnel was not transferred to provide for 18-hour operation and for such emergencies as leave and illness. The Signal Intelligence Service was requested to assist in training additional personnel for the efficient operation of the Message Center.[40]

C. The Introduction of Tabulating Machines

One of the most important achievements in code production by the

---

39. AR 105-25, Signal Corps, Telegraph, Cable, and Radio Service, 1 September 1934.

40. Secret Supplement to the Annual Report of the Chief Signal Officer, 27 August 1935 (OCSigO 319.1) par. 7.

single document.[37]

The transfer of storage, issue, and accounting to the Chief Signal Officer involved numerous clerical details. Army Regulations required semi-annual reports from holders of systems to be made on 30 June and 31 December. Each report had to be checked against the records to verify its accuracy and to ascertain whether all holders had reported. The name of the custodian and the date of the report had to be entered on the records. This work entailed much correspondence since some holders failed to submit reports or omitted some of the items which had been issued to them.

In the Fiscal Year 1935, a new system of accounting for code and cipher publications was instituted. Several new blank forms were adopted, printed, and distributed. Better security was thus established for these important documents both in Washington and in the field. The system of accounting for registered documents by assigning short titles to the publications, in accordance with Paragraph 3, AR 330-5, was inaugurated in the latter part of 1934, and was adopted as the standard for the whole War Department. Two storage vaults for codes were also rearranged and a system of guarding and inspecting instituted. These new duties were assumed and the improvements made without additional personnel.[38]

---

37. Secret Supplement to the Annual Report of the Chief Signal Officer, 27 August 1935, (OCSigO 319.1) Sec. II, Par. 1a.

38. Ibid., passim.

Signal Intelligence Service was the introduction of an automatic method of compilation, using IBM tabulating machinery as a labor-saving device. The story of how the machines were first obtained is interesting. Another branch of the War Department (Office of the Quartermaster General) had been using machines for tabulating purposes for some time, when a change of officer-in-charge brought about a decision to stop using the machines. Although the rental contract could have been terminated at once, the Chief of the SIS was able to persuade the OQMG to allow the SIS to use the unexpired time, amounting to several months. The machines were therefore moved to SIS quarters, thus permitting the Signal Intelligence Service to employ the machines for its own purpose during the balance of the period for which the machines had been rented.

The experiment proved so successful that when the year's lease was about to expire, it was requested that funds be made available so as to continue the lease for at least another year. A routing slip still extant in the files of the Machine Branch, Signal Security Agency, contains the following note accompanying the request for the funds:

> Major Akin: In many years service here I have never once "set my heart on" getting something I felt desirable. But in this case I have set my heart on the matter because of the tremendous load it would lift off all our backs. The basic idea of using machinery for code compilation is mine and is of several years standing. The details of the proposed system were developed in collaboration with Mr. Case, of the International Business Machines Corporation. I regard this as one of my most important and most valuable contributions to the promotion of the work for which we are responsible. Please do your utmost for me. If you do, we can <u>really</u> begin to do worthwhile <u>cryptanalytic</u> work. F.[41]

41. The date was 30 October 1934

The machines were to be rented from the International Business Machines Corporation at an annual rental of $600 which would provide a single set (punch, sorter, and tabulator). The installation of the machines as an official charge against the budget of the Signal Intelligence Service took place on 1 February 1935.[42] Thus began the use of IBM machinery for cryptological purposes. While in World War II the use of such machines was greatest in cryptanalytic activities, it should be pointed out that in 1935 the personnel of the SIS were primarily interested in using the machines for cryptographic purposes. The machines were obtained to eliminate the huge amount of drudgery attendant upon code compilation by hand methods, a task so great that it had absorbed a disproportionately large portion of the time and energy of the entire staff. With the machines on hand, it was expected that most of the members of the section would have more time to engage in cryptanalytic activities by hand methods, for at this period the amazing possibilities of machine aids for cryptanalytic statistical work were as yet not clearly understood. This whole incident furnishes an example of how a scientific development motivated by a specific need becomes useful in providing for problems of quite a different sort.

The system, as is well known to the general public, employed perforated cards on which the contents of all authorized codes were punched

42. See Secret Supplement to the Annual Report of the Chief Signal Officer, 27 August 1935 (OCSigO 319.1), par. 2; Revised Code Production Program, 4 April 1935.

so that new editions could be prepared on short notice. Code manuscripts could be prepared by this method in very much less time than was required by the old hand methods. The Signal Intelligence Service was enabled to complete a heavy code compilation program within a few months which would otherwise have required at least three additional years. By using this system a code formerly requiring the services of four compilers for a period of six weeks could be prepared in two days by one operator. For example, the Division Field Code had required 136 man-hours of labor to produce under the old method. The first edition using machines could be produced in this way in 50 man-hours and subsequent editions in eight man-hours. In addition, the automatic method could be adapted very readily to the reproduction of copies by lithography, thereby eliminating the necessity of proofreading.[43]

In general, this method of code production was considered as "the most important development" for practical use, that had ever taken place in cryptographic compilation. It established a procedure for the efficient production of codes with a minimum personnel in time of war. The problem of producing tactical codes in the field during actual war had thus been satisfactorily solved. Code production was streamlined to function readily in conditions of mobile warfare and to produce the necessary codes to serve rapid electrical encipherment, transmission,

---

43. Secret Supplement to the Annual Report, 27 August 1935; Revised Code Production Program, 4 April 1935.

and to withstand attack in an age of expert cryptanalysis. Not only was the code production program accelerated and hastened to completion before an actual emergency arose, but also improvements were devised for the adaptation of the tabulating machines to many cryptologic usages. For example, a method of scrambling a set of ordered cards to produce a random arrangement, by means of a device invented by the Chief of the SIS and his first assistant, greatly increased the amount of time saved through the use of the machines.[44]

D. Code and Cipher Compilation 1930-1939

As a result of the revision of the code production program and the transfer of the control of the funds for printing and binding to the Chief Signal Officer, the sum available to the Signal Intelligence Section for this work was greater than had originally been anticipated. The estimates, however, were never realized in the actual allotment of funds. Although it was understood that the War Department Budget Officer had approved $12,000 for this purpose for the Fiscal Year 1935, the amount actually transferred to the Chief Signal Officer from the allotment of The Adjutant General was only $10,500.[45] By the autumn of 1934, the status of the code production program, as approved 22 March 1933, and revised by later changes in the system of secret and confidential cryptographic communication, was very different from that which had

---

44. Revised Code Production Program, 4 April 1935.

45. Memorandum for The Adjutant General from the Executive Officer, OCSigO, Subject: Printing and Binding Funds for Codes, 17 July 1934 (SPSIS 111).

originally been devised.

The War Department Staff Code No. 1 (WDSC-1), was printed originally in 1932 in an edition of 300 copies at a cost for printing and binding of $14,768.29. It was a two-part code in two volumes. Ten months were required for printing and binding this code, while its compilation in manuscript form had required the services of four cryptographers and two typists for over ten months. The entire edition was in secret storage.[46]

The War Department Staff Code No. 2 (WDSC-2) had been compiled and printed in 1919[47] as Military Intelligence Code No. 9 (MI-9) in an edition of 208 copies at a cost of $11,001.59. It was also a secret, two-part code, of which five copies had been issued to the military attachés in London, Paris, Berlin, Rome, and Tokyo. According to the report of the Military Attaché in Tokyo, his copy had been destroyed[48] in the earthquake and fire of 1923 and the other four were recalled in 1930. In 1932 its title page was changed to War Department Staff Code No. 2 and a supplement, covering new terms, names of persons and places,

---

46. Memorandum for Major John H. Lindt from Major S. B. Akin, 24 September 1934 (SPSIS 111); Memorandum to Assistant Chief of Staff, G-2, from Executive Officer, OCSigO, 27 Feburary 1933 (SPSIS 111).

47. See Volume Two, Chapter II.

48. Because the destruction of this copy could not be proven beyond a shadow of doubt the edition was not reissued but held in reserve until a replacement (WDSC-3) could be prepared and printed.

and types of equipment, to make the vocabulary current was prepared in June 1938, at a cost of $231.44 and inserted in the original edition. The entire edition was placed in secret storage in the Office of the Chief Signal Officer, as an emergency reserve for WDSC-1 until WDSC-3 could be printed.[49]

The old Military Intelligence Code No. 5 (MI-5)[50] of which an edition of 800 copies had been printed in 1918 at a cost of $7,169.83, was still used by corps area and department commanders and military attaches in War Department communications. It also served for the exchange of military intelligence. The Adjutant General had destroyed 121 copies as unserviceable and 600 copies were still in storage in 1934. The edition was then revised for conversion into War Department Confidential Code No. 1 (WDCC-1) and provided with a new title page and supplement. The copies outstanding were recalled and the new cipher device (Type M-138), was issued for cryptographing secret messages between corps area and department commanders and the War Department. It was planned that when WDSC-3 and WDSC-4 were printed, the first distribution of WDCC-1 would be made.[51] WDCC-1 had been authorized under the revised plan for the distribution of codes and ciphers. The converted code was designed for use with a cipher system then being devised. This system operated by means of frequently-changed key words,

---

49. Memorandum for Major John H. Lindt from Major S. B. Akin, 24 September 1934; Inclosure: Revised Code Production Program, Par. 1.

50. See Volume Two, Chapter II.

51. See note 49.

which could be issued in the form of a single sheet at quarterly or semiannual periods.[52]

Military Intelligence Code No. 10 (MI-10) printed in 1927, in an edition of 120 copies at a cost of $3,000, was another secret, two-part code. The entire edition was stored awaiting initial distribution when a revised plan was effected. Military Intelligence Code No. 11 (MI-11) had been printed in 1933 at a cost of $1,474.12 for 200 copies. It was stored as the first reserve edition. In 1934 Military Intelligence Code No. 12 (MI-12) was in the process of being printed and delivery was expected by the end of January 1935.[53]

All three editions of the Army Field Code (AFC) were nearly completed. AFC-1 had been compiled in 1925, but was not printed until 1932, at a cost of $3,382.92. Both AFC-2 and AFC-3 were in the press in 1934. AFC-2 was to be delivered by the middle of December 1934, while delivery on AFC-3 was expected by 1 March 1935.[54]

The Philippine editions of the Division Field Code (DFC) were incomplete in 1934. The edition of DFC-5, printed in 1922 at a cost of $940.52, was compromised ten years later, when the loss of one copy in the Ninth Corps Area was discovered. All outstanding copies were then recalled and the edition was stored for use in special

---

52. Ibid., Par. 6.

53. Ibid., Par. 2b.

54. Ibid., Par. 3.

exercises or joint maneuvers. The reserve edition (DFC-9) was distributed for use in the department, following this compromise. It had been printed in 1926 at a cost of $1,116.68. All but 270 of the 2,070 copies printed were issued to the Philippine Department, to the Hawaiian Department, to United States Army troops in China, and to the Ninth Corps Area. DFC-11, printed in an edition of 2,000 copies in 1933, at a cost of $806.78, became the first reserve edition in storage. The second reserve edition (DFC-13) was scheduled for production in the Fiscal Year 1935 and was completed and printed in that year. The number of reserve editions required by current war plans was then complete.[55]

The three editions destined for use in the Hawaiian Department had also been completed. DFC-6, printed in an edition of 2,000 copies at a cost of $776.43 in 1922, had been distributed to the pertinent centers employing that code. DFC-10 was printed in 1926, in an edition of 2,000 copies at a cost of $1,301.03. It was a reserve edition in secret storage. The second reserve, (DFC-12) was completed in 1933 at a cost of $947.06.[56]

Two of the continental editions of this code had been printed. DFC-7, printed in an edition of 5,000 copies in 1923 at a cost of $1,227.33, had been distributed to the communication centers in the Panama Canal Department and the Eighth Corps Area. Some 4,950 copies

55. Ibid., par. 6.

56. Ibid., par. 7.

of this edition were still in storage. A second edition (DFC-8) of which 5,000 copies were printed in 1924 at a cost of $1,250 was still in secret storage. In accordance with the production schedule DFC-14 was published in the Fiscal Year 1935.[57]

The Air-Ground Liaison Code (AGL) was another of the authorized codes, the production of which it was necessary to expedite. AGL-2, printed in 1930 in a confidential edition of 14,000 copies at a cost of $136.85, had been partially distributed for training purposes, but some 6,500 copies were still in secret storage. This code and Fire Control Code No. 2 (FC-2) were printed on the obverse and reverse faces of the same sheet of cardboard. Under the revised plan, however, these codes were printed independently. AGL-2 had been authorized as a confidential code and was subject to frequent change, which demanded new editions. FC-2, on the other hand, had been revised and improved in 1931. It was for official use only and was well standardized. Four editions of the AGL Code, which had also proved to be satisfactory, were scheduled for publication in the Fiscal Year 1935. It was decided, however, to prepare only one edition in the new form, because of the pressure of other work and the desirability of trying out the new vocabulary prior to printing the reserve editions.[58]

An Air Force Command and Liaison code was considered necessary for use by aircraft engaged in distant reconnaissance and tactical

---

57. Ibid., par. 8.

58. Ibid., par. 9.

missions. It had not yet been approved for use, but was listed in the Tentative Cryptographic Security Manual. Four editions of this code were scheduled, but it was not authorized.[59]

Two editions of the General Address and Signature Code, authorized several years previously, had been produced. They worked satisfactorily enough, reducing telegraphic expenses considerably, but when the War Department in the interests of governmental economy, extended its telegraphic services to other departments, the code proved to be unsuited for this type of traffic. As a result, the General Address and Signature Code was abandoned by 1934. This was definitely a step in the wrong direction, for security in time of war is greatly enhanced by such a code.

The Radio Service Code had first been prepared and published in 1922, in a confidential edition of 7,000 copies at a cost of $1,550. Of this edition, some 1,600 copies had been distributed for training. By 1934 it was considered unsatisfactory and it was recommended that it be revised or recalled.[60]

The old War Department Telegraph Code 1919 was still in service but was no longer used for secret messages. Some 600 copies had been issued to the various posts and stations and additional copies were

---

59. Ibid., 10

60. Ibid., 14-16.

distributed as required.[61]

Meanwhile the necessity for a publication contained the most important data relative to authorized codes and ciphers had been recognized. The Military Intelligence Division had prepared a manuscript in 1931 but before funds for printing it could be appropriated, it had been necessary to make certain important changes in the system of codes and ciphers for use within the Army and therefore to revise the manuscript. This project was authorized in 1932 and undertaken toward the close of the Fiscal Year 1933.[62] By 1934 a tentative edition of the Cryptographic Security Manual (CSM-1) had been distributed to all holders of secret codes.[63]

The purpose of the manual was to give the minimum information essential to the protection and proper handling of all secret and confidential codes and ciphers at all times, whether the nation was at peace or war.

The increased international tension in the latter part of the decade and the necessity for concluding the code production program in time to meet any emergency were the principal factors that caused an increase in the printing and binding estimates after 1934. The

---

61. Ibid., 14; see Chapter I.

62. Supplement to Annual Report, 1933, p. 7-8.

63. Ibid., Revised Code Production Program, 4 April 1935, par. 16.

The estimate for the Fiscal Year 1935 was $20,618 and that for the succeeding year rose to $30,000. Yet the printing of WDSC-3 and WDSC-4 had to be postponed because the funds allotted for 1936 amounted to only $8,700. The original edition of this code had cost $14,768.29 in 1932 and it was estimated that each of the two volumes required for the remaining two would cost $9,000.[64] By 1935 it was evident that the principal reason for the failure to adhere to the approved code production program was the fact that sufficient funds to cover the annual requirements under the program had never actually been made available. Consequently, the shortages had to be made up in succeeding fiscal years.[65]

From year to year codes scheduled to be printed were postponed. Estimates were made, allotments were cut, codes were rescheduled. In 1935 it was estimated that $21,400 would be required for the Fiscal Year 1937 and in the succeeding years $35,050 would be sufficient to complete the entire program.[66] In 1937, the sum of $17,400 was available. A reduced estimate of $19,600 with a balance of $10,450 was required to complete the program. The sum available for 1938 was $15,000 a reduction from the $16,400 allotted. By 1939 the estimate was $24,600 with which it was proposed to print all of the remaining codes excepting

64. Estimate for Printing and Binding, Fiscal Year 1936, 18 September 1934 (SPSIS 111).

65. Revised Code Production Program, 4 April 1935.

66. Memorandum for Colonel Stanley from Major H. L. P. King, 18 October 1935 (SPSIS 111).

WDSC-4. By this time the rapid progress made on the Converter M-134 indicated that it would serve the purposes for which WDSC-4 was intended and that the production of that code might be deferred.[67]

The publication of authorized codes was not the only item in the estimates for printing and binding and their preparation was not the only cryptographic burden on the personnel of the Signal Intelligence Service. In addition to authorized codes, which were expanded in number as M-Day appeared more imminent, cipher keys, cipher alphabets, and pamphlets of instructions for the codes, cipher systems, and cipher devices had to be prepared, published, and distributed.

E. Secret Army-Navy Intercommunication

The only means for secret intercommunication between the Army and Navy in joint exercises in 1934 was the old Army-Navy Cipher No. 1, the multigraph edition of which had been distributed in 1925.[68] This was unsuitable for heavy traffic.[69] In 1931 in collaboration with the Code and Signal Section of the Navy, a cipher system had been developed for use between the two services. It was used with the Cipher Device (Type M-94), which was finally recommended by the Joint Board as a substitute for the code book which had been authorized and compiled but never printed.[70]

---

67. Estimates for Funds for Code Production for the Fiscal Year 1939, 27 July 1937 (SPSIS 111).

68. See Chapter I.

69. Revised Code Production Program, 4 April 1935, Par. 4.

70. Supplemental Report to Annual Report of the Chief Signal Officer, Fiscal Year 1931 (SPSIS 319.1), p. 2.

It was concluded that a cipher device was better adapted for the purpose than a code and experiments were initiated by both the Army and the Navy to develop a more practical instrument. An improved model of Type M-94 was constructed and tested to determine its adaptability. It was found to be superior to the old one, although further modifications were desirable for increasing the speed of operation.[71] After the development of the M-138 it was substituted for the M-94.[72]

Cooperation between the two services had also included joint experiments with aircraft codes. In 1933 an experimental edition of an aircraft code, Tentative Aircraft Code No. 1, for use in joint Army-Navy operations, was authorized by the Joint Board. It was prepared in an edition of 500 copies at a cost of $89.15 from Signal Corps funds and distributed by the Signal School to certain headquarters where joint exercises were conducted at frequent intervals. After service tests the necessary modifications were made in a second edition.[73] An equivalent code, Tentative Aircraft Signal Book No. 4, was produced and issued by the Navy. Both codes were used side by side to determine their relative merits.[74]

---

71. Supplement to the Annual Report of the Chief Signal Officer, Fiscal Year 1933, Codes and Ciphers, (SPSIS 319.1), p. 8.

72. Supplement to the Annual Report of the Chief Signal Officer, Fiscal Year 1936, 31 August 1936 (OCSigO 319.1), p. 21.

73. Supplement to the Annual Report, Fiscal Year 1933, p. 7; Revised Code Production Program, 4 April 1935., par. 13.

74. Revised Code Production Program, par. 13.

F. The Development of Cryptographic Machinery

One of the activities of the Code and Cipher Section, Office of the Chief Signal Officer, was, as has been related in Chapter I, concerned with the development of automatic cryptographic machinery. This initial experimentation was continued by the Signal Intelligence Service after 1930 and work was also done on the improvement of the hand-operated cipher devices.

The Cipher Device Type M-94 had been used extensively since 1923 and an improved model was produced in 1931. As originally developed, this device had been based on cryptographic principles worked out by Colonel Parker Hitt[75] which had been adapted to practical use by researches conducted by Lieutenant Colonel Joseph O. Mauborgne when Chief of the Engineering and Research Division, Office of the Chief Signal Officer, during World War I. Essentially, the device was a series of disks fastened together on a central shaft, with the possibility of rearranging the order of the disks at will. On the circumference of the disks were stamped mixed cipher alphabets. In the model as originally adopted, these disks were made of metal and the alphabets could not be changed without manufacturing new disks. In the improved model an attempt was made to paste strips of paper on the circumference, so that the cipher alphabets might be changed more readily.

A new device, Type M-138, was developed, procured in limited quantity, thoroughly tested, and finally approved in 1935. It employed

---

75. On the relation of M-94 to devices by Thomas Jefferson and Bazeries, see Chapter I

changeable paper-strip alphabets, which for the purpose of encipherment were inserted in channels on a metal base. Attempts were made to get the Aluminum Company of America to manufacture these devices but they were unable to do so. In the end, Price Brothers, a small firm in Frederick, Maryland, was induced to attempt to make the devices and succeeded by using laminated bakelite.[76] The first thirty of these devices were manufactured at a cost of $15 each and delivered in April 1935. The security of the device was very high, since the cipher alphabets could be changed in relation to the volume of the traffic. A pamphlet of instructions was issued to all holders and the system was placed in operation on 1 July 1935. This device was also employed by the Navy.[77]

By 1938, a new cipher device, Type M-161, was being developed to provide a small machine for use in combat operations. It was, however, never put into production and for it the M-209 (Hagelin) machine was substituted before the outbreak of the War. The first mention of the development of the M-161 in the files is contained in a statement by

---

76. Later, the Aluminum Company of America did manufacture metallic boards. The first channels were made by fastening cylindrical rods about one-eighth inch in diameter to the metal base, but the strips had a way of sticking or getting bound within the channels at the tangents. Ultimately, the solution of this practical problem was reached by making grooves in the base.

77. Secret Supplement to the Annual Report, Fiscal Year 1935, Par. 3; Supplement to the Annual Report, Fiscal Year 1936, p. 21; Revised Code Production Program, par. 17.

Major S. B. Akin:[78]

> It is of the greatest importance that early efforts be devoted to the production of a means of rapidly encoding, cryptographing and decryptographing messages for:
>
> Aviation
> Mechanized units
> Front line (infantry-artillery liaison) units.
>
> Has the field been fully explored for a rapid mechanized means of the required size and weight? I consider this far more important at this time than machines for the use of rear elements. . .

To this, Mr. Friedman replied in a first indorsement: "We have nothing but Cipher Device M-94, and Air-Ground Liaison Code No. 2."

The next item in the file is a memorandum from Major Henry L. P. King to Mr. Friedman, dated 28 September 1935:

> Please let me have a written report on the status of the device for cryptographing and decryptographing messages for aviation, mechanized units and front line units that Col. Akin directed you to devise in his April 24th memo.

The reply (30 September 1935) was as follows:

> At the time of my 1st ind. to Col. Akins' memo of April 24 was written, I had in mind a small device which, however, did not produce a written record. I understood that a device which does not produce a written record will not be considered, because of impracticability of having to write down by hand the results of operation of the device.
>
> I think this case should be considered as a phase of project recently set up under title Converter Type No. M-161.
>
> By Oct. 5 I expect to hand in draft specifications and drawings covering a modified Converter Type M-134-T-2[79] which will[80] become the basis of Converter Type M-161. It can readily be used as a basis for discussion with R & D with Labs.

78. R&W, Major S. B. Akin to William F. Friedman, 24 April 1935.

79. On this machine, see below.

80. A note by Mr. Friedman (27 January 1938): "It did not, however."

Action 3 of the paper just quoted (by Major King, 1 October 1935) asked the question: "Will the device mentioned in paragraph 3 above meet the military characteristics of the M-161?" Action 4 gives the reply:

> One form of the device will meet the military characteristics of M-161. The cryptographic principle is such that a machine for large fixed installations is merely an extension of parts of a basic assembly. The principal difference between a machine for small, mobile stations (M-161) and one for large, fixed stations (M-134-T-3) lies in the printing or recording mechanism. For the M-161 we must have a very small, simple device not necessarily a page printer. For M-134-T-3 we must have a large, sturdy, electrically operated typewriter like the electromatic. The small printer must be worked out, and I have what I think are practical ideas along this line.[81]

Action 5 (Major King to Mr. Friedman, 1 October 1935) is as follows:

> Please note 2nd par Col Akins basic memo--all work in a modification of the M-134-T-2 must be suspended if the work interferes with the development of the M-161. I consider the development of the M-161 to be the most important project now before your section.

Action 6 dated 3 October 1935 and signed by Mr. Friedman is as follows:

> There is <u>nothing</u> about what I am now working on in connection with project of Converter M-161 which will in any way interfere with the projection of the two M-134-T-2 models. And I absolutely concur with your statement that the development of M-161 is <u>the</u> most important project before my section at the present time. I am pushing this as fast as possible and am most anxious that a start be made. I would like very much to talk the various designs over with the LABS, and am going to hand in draft specs and drawings by October 5, for your action.

81. See Mr. Friedman's note in the margin (27 January 1938): "This describes a machine which did <u>not</u> become M-161 but is now assigned the No. SISDE-11." A more recent note underneath (3 August 1944) says: "Became M-134-C SIGABA." See below.

The Military Characteristics of the proposed cipher machine, to which the nomenclature M-161 had been given, were set up as follows:

1. This machine should be designed for the fundamental purpose of enciphering and deciphering messages with speed, accuracy, and security equal to that of the present Division Field Code or better.

2. It should consist of a single unit, combining a 26-element keyboard and an indicating device making a printed or written record, either in tape or page form.

3. The weight of the machine including its carrying case should not exceed 15 pounds. It should be rugged in construction, capable of withstanding the jarring incident to its being carried and used in the vehicles for which intended.

4. The apparatus should be mechanically operated so far as possible, but electrical circuits for effecting the cryptographic substitution are admissible. The record may be made by mechanical, electrical or chemical agencies not requiring the use of carrying of liquids for development.

5. The minimum speed of operation in enciphering and recording or deciphering and recording should be approximately 60 characters per minute; the optimum speed would be 150 characters per minute.

6. The device should be operated in any position and should require the services of a single operator for maximum operating speed. The operation should be simple enough so that an average enlisted man can be trained to operate the device efficiently after one day's instruction.

These were forwarded to the Laboratories by Lieutenant Colonel Roger B. Colton for the Acting Chief Signal Officer on 10 September 1935. Though a letter of Major W. S. Rumbough to the Research and Development Division dated 8 November 1935 stated that the Secretary of War had approved the military characteristics and that the papers were being

forwarded to the Signal Corps Laboratories for study and comment, the papers were not actually so forwarded until 6 April 1936,[82] and before that date the sum of $250 had been allotted to the Laboratories for preliminary work on the M-161 and the design submitted by Mr. Friedman was being studied by the Patent Section.[83]

The matter was now in the hands of the Signal Corps Laboratories and work was progressing there but upon what lines the Signal Intelligence Service did not know: compare the following quotation from a routing and work sheet dated 10 September 1936 from William F. Friedman to the Chief, War Plans and Training Division:

> 1. In connection with development of automatic cipher machinery, about 1 1/2 years have gone by since this section submitted sketches of a machine which offers great possibilities not only for fixed station message centers but also for small, mobile units. This case has been assigned the type number M-161. Funds were established in current budget for its development but I do not think anything has yet been done on it.
>
> 2. Is it possible that this development could be let by contract to a commercial firm like WE or GE? In this connection I would like to point out that the Navy has given up trying to develop apparatus of this kind at their labs or shops and are committed to policy of outside development.

Action 3 on this was as follows:

> Comments of SCL are attached. It appears there is little if anything to gain, by farming out this development, even if funds were available, and they are not without discharging a portion of the staff.

---

82. Marginal note by Mr. Friedman.

83. Chief, Research and Development Division, to the Chief Signal Officer, 22 January 1936, first indorsement to letter of Major Rumbough to the Research and Development Division, asking what action had been taken.

Nearly a year later, the Signal Intelligence Service had still not learned much about the work on the M-161 in the Signal Corps Laboratories:[84]

> In connection with the development of Converter Type M-161 it is understood that this project has been assigned B priority and that work has been initiated and is progressing on same in the Signal Corps Laboratory. Informal attempts on our part to ascertain the lines upon which the development is based have been unsuccessful. It is believed highly desirable that the Signal Intelligence Section be given an opportunity to examine the proposed scheme and basic cryptographic principle before any further work is done on the project; otherwise it may develop that considerable time and effort will be wasted.

This stimulated a letter to Lieutenant Colonel William R. Blair at the Laboratories dated 30 July 1937, signed by Lieutenant Colonel Louis B. Bender, as follows:

> The War Plans and Training Division[85] is getting a little concerned about the progress of Project 104, and without any cooperation on their part. If I am correctly informed, you are pursuing on this project a somewhat different plan than was originally intended. That fact does not appear from the reports to date, but it is my impression that I was so informed on some visit to the laboratory. I believe that the original plan contemplated some sort of electrical mechanism, for which you have since found what you think is an acceptable mechanical solution. I should like to be set straight on this subject in some detail.
>
> I fear this project may become a bone of contention between the laboratory and the War Plans and Training Division. Naturally, they feel that they have all the available knowledge on the subject of ciphers and cipher machines. That being the case they feel that advantage should be taken of their experience and knowledge of this subject. On the other hand, you probably feel that you should be free to use any design that appears to be most suitable to obtain the objectives that division may set up.

84. R&W from W. F. Friedman to War Plans and Training Division, 15 July 1937.

85. That is, by the Signal Intelligence Service which was a part of the War Plans and Training Division.

Colonel Blair replied on 3 August 1937 as follows:

I regret that the War Plans & Training Division is concerned about the progress of project 6-a on Converter M-161 and do not understand why they should feel that their ideas and suggestions are not being given consideration at the Laboratories. The idea that we are pursuing this project in a different manner than was originally intended is erroneous.

The military characteristics for Converter M-161 are contained in a letter from OCSigO to The Adjutant General dated October 22, 1935, file OCSigO 413.52 (M-161) subject "Military Characteristics for Converter, Type M-161" from which is quoted par. 1 d as follows: "The apparatus should be mechanically operated so far as is possible but electrical circuits for effecting the cryptographic substitution are admissible. The record may be made by mechanical, electrical or chemical agencies not requiring the use or carrying of liquids for development."

The 2nd indorsement to the above-mentioned letter from the OCSigO to Director, Signal Corps Laboratories, dated November 13, 1935, file OCSigO 413.52 (M-161) 10-22-35, contained the following instructions. "Your preliminary investigations of this project will be conducted with a view to arriving at a solution by the use of a strictly mechanical device or devices and without the aid of any electrical features."

The investigation directed by the 2nd indorsement mentioned above resulted in the conception of several mechanical solutions. These ideas were not sufficiently developed at the time Mr. Friedman last visited these Laboratories to justify discussion and presentation. It was felt that a number of details should be proved in drawing layouts and in construction form prior to discussion.

Work on the construction of the first service-test model has been intermittent due to personnel being required for work on projects of a higher priority. Active work on project 6-a was not started until completion of the Converter M-134-C. In this connection, see 1st indorsement, OCSigO to Director, Signal Corps Laboratories, dated July 14, 1936, file OCSigO-111-FY 1937 (7-8-36). Work on the Converter M-134-C was not completed until June 1, 1937.

A preliminary proposal for a converter M-161 dated April 6, 1935, was submitted by Messrs Friedman and Rowlett by letter from OCSigO to Director, Signal Corps Laboratories, dated April 6, 1936,

subject "Inventions of Cryptographic Mechanisms—Messrs Friedman and Rowlett" with the statement "This is for your information, file and such use as you may care to make of it. Acknowledgement of receipt by indorsement is desired." The device described in the practical counterpart of the Converter M-134 without the tape transmitter but substituting therefore control commutators. This proposal was given consideration but was not deemed a mechanical solution as outlined in the military characteristics and directive contained in second indorsement of November 13, 1935, mentioned above.

The drawings for the building of the first service-test model of the Converter M-161 are about 75% complete. Some construction work of minor parts for the service-test model has been completed and it is the plan of these Laboratories to have the first service-test model completed for service test about April 1938.

We would be pleased to have Major Rumbough, Mr. Friedman or any other representative of the War Plans and Training Division visit the Laboratories and acquaint themselves with the drawings and layouts and the progress which has been made on their development to date. It must be understood, of course, that our development work is definitely guided and limited by the military characteristics set up. Any discussion of the project not falling within the military characteristics set up or that does not come to us as a directive or an authorized modification of the military characteristics, while it may be helpful, may not properly be incorporated in the design. In view of the work that has been done on this project in accord with present directive and the great probability that an entirely successful mechanical device will result, I should regard a change in directive at this time as unfortunate indeed. It would not only delay the project but would set aside a large amount of good work that we could ill afford to waste in this way. However if it appears wise to you to authorize a change in the military characteristics of this device, the sooner they are changed the better.

In accordance with the suggestion contained in the letter just quoted at length, Major Reeder and Mr. Friedman visited the Laboratories on 1 October 1937 and as a result of this conference, "two devices

representative of the cryptographic possibilities of the Converter M-161" were sent to the Signal Intelligence Service.[86] On 29 April 1938 the Director of the Signal Corps Laboratories wrote as follows:

> The construction of the subject machine [the M-161] has reached the stage where preliminary and improvised tests are feasible. In these tests it is found that the machine functions satisfactorily in the encipherment and decipherment of messages but that certain modifications and refinements are desirable . . ."

To this a second indorsement dated 13 June 1938 reports that "Converter M-161 and the tape numbering machine are being delivered." Three days later the Laboratories reported[87] that prior to that date a total of $10,025.90 had been spent on the development of the M-161 and that it was estimated that M-161-T-2 would require an additional $7,413 in the next Fiscal Year (1939).

A security study of the M-161 as developed by the Signal Corps Laboratories could now be made. It was assumed that the enemy had captured one of the machines and therefore knew of its construction. Two messages were prepared with indicators enciphered by a system unknown to the cryptanalysts who made the study. The probable-word method was used as a point of attack: it was assumed that the word "infantry" appeared in both messages. In the first message the word was not found but it was found, in 30 minutes' time, in the second.

---

86. Letter of Director, Signal Corps Laboratories, to the Chief Signal Officer, dated 7 October 1937.

87. Director, Signal Corps Laboratories to Chief Signal Officer, 16 June 1938.

Having found the assumed word, the correct initial setting of the machine was determined in 15 minutes and the rest of the message was deciphered by means of the machine itself. Solution of the other message required approximately three hours, owing to the number of probable words tried. "The degree of security afforded by this machine is considerably less than that afforded by our present cipher device Type M-94."[88]

Before this security study was made, however, the Signal Intelligence Service had begun negotiations which ultimately led to the adoption, with modifications, of a cipher device originally invented by the Swedish inventor Hagelin. Because it was believed that the Hagelin device might offer a better solution to the problem than the one which had been developed by the Signal Corps Laboratories, the Laboratories were directed[89] on 17 August 1938 as follows:

> In view of that report [i.e. the security study] no further development work will be undertaken on this project pending results obtained with the Hagelin Cryptographer type B-360, for which you are negotiating purchase. The funds remaining to the credit of this project after that purchase will be reallocated to other projects on your program following your recommendations on this subject.

Meanwhile, in January 1933, a model (M-134-T1) of an automatic cipher device was completed. In this machine the stepping of the code

---

88. Letter of Lieutenant Colonel L. B. Bender to the Director Signal Corps Laboratories, 12 July 1938, inclosing the security-study report.

89. First indorsement to letter of 16 June 1938.

wheels was very irregular[90] and under the control of a keying tape. Electric control had thus made its first appearance![91] Tests demonstrated that this machine was reliable but certain limitations in the speed of its operation—it used only one rotor, the keying element being external and supplied by a tape which could be fed into the machine as desired—indicated that further improvements were needed. The design was modified and submitted to the Signal Corps Laboratories for further development. The necessity for such a device had become extremely urgent, because the time required to encode and decode messages had become a bottleneck in practically all headquarters.[92]

After further modification, a very efficient automatic cipher machine (Type M-134-T2) was completed in May 1934. A five-rotor arrangement was installed, the external tape being still used for supplying the keying element. The device was designed to be connected directly to an electrical typewriter. Primarily for field use, it combined an electrical and a mechanical device for automatic encipherment and decipherment: the manual operation of a keyboard acted to print a cryptographic resultant. The machine attained a speed of from 30 to 40 words per minute in encipherment and decipherment. This speed was far more rapid than had been

---

90. In a cryptographic device or machine, security is directly proportionate to the degree of irregularity in the keying element.

91. On 25 July 1933 the Chief Signal Officer filed a patent application (Serial No. 682,096) on behalf of the inventor, Mr. William F. Friedman.

92. Supplement to the Annual Report of the Chief Signal Officer, Fiscal Year 1935, Par. 1 h, p. 8; Annual Report of the Signal Intelligence Section, Fiscal Year 1935, par. 1e.

achieved by the use of any code book. In addition, the cryptographic principle of the machine provided the highest degree of security.[93]

A contract was placed with the firm of Wallace and Tiernan, Belleville, New Jersey, a relatively small and inadequately-equipped manufacturer, for these converters.[94] Shortly before 15 June 1935, while this contract was being negotiated, Mr. Frank B. Rowlett, then principal assistant to Mr. Friedman, conceived the idea which constitutes the basis of the

in the design, despite urgent recommendations by Mr. Friedman that he do so. The Chief Signal Officer took the position that in view of the approaching emergency, it was better to be supplied with actual machines of somewhat inferior design than to have no machines at all.

Shortly after this, in October 1935, Lieutenant J. N. Wenger, USN, of the Code and Signal Section of the Navy, approached the Signal Intelligence Service with a request for assistance in designing the cryptographic principles of a new machine, the Navy being then dissatisfied with the degree of security afforded by their Mark I machine. With approval of his superiors, Mr. Friedman revealed[95] the principles of the Rowlett-Friedman invention to the Navy, but at that time these principles were apparently[96] of not sufficient interest to the Navy

95. This was done to various Naval officers on three occasions: the dates were 21 October, 31 October, and 1 November 19 .

96. According to a document by Captain L. F. Safford, USN, one of the officers who later became acquainted with the record of the Rowlett-Friedman invention, shortly to be cited, this was true at the time.

Having permitted ourselves this digression, we must now return to the continuation of the story of the M-134-A at the point where we left off on page 252: the letter of the contract to Wallace and Tiernan. In 1937, when a few of the M-134-A machines had been completed, two were placed in the Signal Intelligence Service and two were taken by Mr. Friedman to Panama. Service tests were made, establishing the fact that these machines were successful. When more machines had been completed, additional installations could be made. Accordingly, the Quartermaster General was requested to ship seven Converters M-134-A in the strong room of the United States Army Transport Republic on 15 November 1938. Two were to be delivered in Panama, one in

San Francisco and four in Honolulu. Two of the latter would be later shipped to Manila by the United States Army Transport Grant on 6 March 1939.[99] Mr. Friedman accompanied these converters as far as Honolulu. In Panama, San Francisco, and Honolulu, he set up the converters and tested them.

G. Revision of Cryptographic Plans 1938-1939

As the possiblity of a general European war became more imminent, the Signal Intelligence Service carefully reexamined its means of cryptographic communications in order that the best methods might be available in the event of war.

It was found that the secret systems were too few and not distributed widely enough. Since secret means of communication could not be extended to a great number of holders, lest the entire system be jeopardized through increased traffic and the greater possibility of error, it was necessary to prepare more secret systems and give at least one of them a wider distribution.[100]

There was only one confidential system. The inevitable increase in traffic after the outbreak of war would enhance the possibility of solution. A compromise occurring at a single station would also involve the confidential communications of all stations to which the system had been

---

99. The Chief Signal Officer to the Quartermaster General, Subject: Shipment of Converters M-134, 10 October 1938 (SPSIS 320.3).

100. Memorandum for The Adjutant General from the Chief Signal Officer, Subject, Codes, 28 April 1938 (SPSIS 311.5) par. 2a.

issued. It was decided therefore to increase the number of confidential systems.[101]

The majority of the systems were still too slow. Electrical communications had become so rapid that any means of cryptographing and decryptographing that did not afford a speed at least commensurate with that of the telegraph was too slow for practical purposes. Impatient commanders, unwilling to brook a delay, might direct that messages be sent in the clear, which would compromise secret systems. The most immediate need, despite the success of the cryptographic device M-138, was a more adequate means of cryptographing and decryptographing messages automatically. Without such means it was believed that communication could not be secret and meet the speed demanded by modern warfare.[102] The early adoption of a suitable device (M-161) was recommended.[103] Danger to cryptographic security lay in the fact that no centralized agency controlled security procedures. It was recommended that someone in each headquarters be designated as Cryptographic Security Officer with the duty of supervising secret and confidential communications, noting violations of regulations, etc.

---

101. Ibid., 2b.

102. Ibid., 2c.

103. Ibid., 2d.

Thus, it was concluded that sufficient new systems should be authorized, so as to prevent the accumulation of large bodies of intercepted traffic in any one system by foreign cryptanalytic bureaus. It was believed that this could be accomplished by the adoption of a relatively small number of basic cryptographic procedures or devices, variability being provided by the issue of different keys to each group of users.[104]

For communication between the War Department and corps areas, Cipher Device M-138 would be used until the Converter M-134 could be introduced with individualized keying procedures. A similar secret system would be used between the War Department and overseas departments and another between the War Department, corps areas, and overseas departments where more than one unit was concerned.[105]

Another secret system would be used between a larger group of holders including lower headquarters which at that time used the Army Field Code in unenciphered form. It was expected that the M-134 would be used in the future with individualized keying and the Army Field Code would be held in reserve. Messages to be repeated to posts, forts, camps, arsenals, and depots would require a different

---

104. Ibid., 3.

105. Ibid., Plans for codes, Par. 1-3.

system because the possibility of compromises was too frequent under the existing arrangement. The M-138 was recommended for this type of traffic. Though it was slow, the volume of traffic was not considered sufficiently large to necessitate a more elaborate device.[106]

It was planned to use the M-138 with the existing Military Intelligence Code and an individualized keying procedure for secret communications between the War Department and military attaches. Secret communications of the Military Intelligence Division and between the Army and Navy would continue to use the M-138. The double-transposition system would be used as an emergency secret system.[107]

For confidential communications, the Cipher Device M-161, then being developed, was recommended. The M-94 would be used in such messages with the Navy and Coast Guard. No change was contemplated in the Air Ground Liaison Code.[108] For restricted communications, the War Department Telegraph Code and Fire Control Code were still in use and no changes were contemplated.[109]

---

106. Ibid., Par. 4, 6.

107. Ibid., passim.

108. Ibid.

109. Ibid.

H. Conclusion

Confronted with a restricted budget and the difficulty of assuming expanding responsibilities with limited personnel, the Signal Intelligence Service, building on the old code-production program, had by 1939 placed the development of military cryptography on a sure foundation. The code-production program, in spite of revisions and postponements, was completed by the outbreak of World War II. Yet sufficient flexibility had been retained, and critical analysis of the program enabled the Service to adapt itself to the rapidly accelerating pace of military cryptography and its demands in an age of electrical communication. The security of the secret communications of the United States Army was well protected.

The demands of secret traffic for General Headquarters of Armies and for divisions had likewise been satisfied. Each had the means of communication for warfare both within the continental United States and in the overseas departments. The demands for speed and accuracy in the intensity of modern, mobile warfare had also been anticipated. Tabulating equipment had reduced the length of time and the number of personnel required for the production of codes in the theaters of operation. Improvements in automatic cipher machinery through the introduction of electrical devices had made it possible to predict with confidence that cryptographic operations would not delay the transmission of important secret and confidential communications.

Indeed, the success of the Signal Intelligence Service appears not to have been unheralded abroad, despite the confidential nature of its work. In August 1935 the Code and Signal Section of the Navy and representatives of the Office of the Chief Signal Officer conferred on the matter of Japanese representatives who were visiting foreign countries to study cryptography and cryptanalysis. Their aim was to improve their own system of communications, stimulated no doubt by the revelations of The American Black Chamber. Measures were undertaken to prevent the visitors from learning anything about the secure cipher machines made by Hebern[110].

110. Edward Hebern was an American inventor who had patented a cryptographic device using rotors. This had been used by the Navy in modifications of Hebern's work, developed by collaboration between the Navy and Hebern himself.

CHAPTER VII. SOLUTION AND TRAINING ACTIVITIES 1930-1939

A. The Training Program

One of the basic reasons for the transfer of solution activities from the Military Intelligence Division to the Signal Corps had been the desire to concentrate more effectively on the training of personnel in cryptanalytic work. It was indeed, precisely in the sphere of training that MI-8 had been most deficient. The limited amount of training which had been carried on under War Department auspices was the result of Signal Corps activity, not that of MI-8.

The change in emphasis from solution of immediate value in the production of information also reflected the relatively lower interest which the War Department has in such information in a time of peace. In the period 1919-1929, when the War Department had with State Department support maintained MI-8, the chief value had been gained by the State Department, so that when the latter withdrew its support in 1929, the true level of interest in the War Department was revealed. The difficulties encountered in establishing facilities for adequate interception may have contributed to the result, though had this been the only factor, doubtless these difficulties could have been surmounted by the Signal Corps.

As a matter of fact, the science of cryptography had been making rapid strides since 1919. The experience of World War I had sharpened

the interest of most governments in increasing the security of their communications and the growing cryptographic maturity of the United States was probably only typical of what had taken place in most of the larger countries.

Moreover, American technological advances in the use of machinery and electricity during the War and in the first decade of the peace, had made training which was adequate for the tasks confronting cryptanalysts in 1918 wholly inadequate for those which were likely to be involved in another conflict.

In addition, it was probable that after Yardley published The American Black Chamber in 1931, even those governments which had hitherto been backward in the art would adopt new methods for preserving the security of their communications and develop better cryptographic bureaus. Action by the Japanese Government was certainly to be expected since in Yardley's book the solution of Japanese systems was easily the most sensational disclosure.

Thus, it had now become imperative that an adequate force of cryptanalysts be trained for a future war. Since this training could not be obtained without contact with practical problems, it was out of the question for the Signal Intelligence Service to look for its specialists outside the War Department.

B. The Training of Cryptanalysts

The four young cryptanlysts who had been employed under Civil Service regulations in 1930, Messers Rowlett, Kullback, Sinkov, and Hurt, began, under the tutelage of the Director of the Signal Intelligence Service, their extended training in the various aspects of the work of the Signal Intelligence Service.[1] They gave early promise of ability and their progress in cryptanalysis was particularly encouraging: by 1932 they were already prepared to conduct independent research in this field.[2]

The training which they received in cryptanalysis was at first largely theoretical, but a great many practical problems were supplied by the large number of cipher systems which were submitted by persons from many different parts of this country, and even from foreign countries. Increased interest in cryptography had been aroused by the appearance in the public press of various books and magazine articles dealing with the subject. Amateur cryptogram societies were organized and syndicated cipher contests were conducted in various periodicals and daily newspapers.

---

1. One of them (Rowlett) recalled in 1945 that owing to the stringency of space he was at first given a table in "the vault", a room in the Munitions Building in which the existing stocks of reserve codes were stored.

2. Supplemental Report to the Annual Report of the Chief Signal Officer, Fiscal Year 1931 (SPSIS 319.1), p. 5.

The Signal Intelligence Section examined all codes, ciphers, and cipher apparatus submitted to the War Department for consideration and possible adoption in the military service. Of the many submitted every year, only an extremely limited number (not over five) possessed sufficient merit even to warrant serious consideration for military use. In fact, the probability that persons outside the military service might invent cryptographic systems better than those actually in use became more then ever remote. The principal reason for this lay in the fact that the majority of the inventors had never had any experience in military cryptography and were not conscious of the many difficult requirements that had to be fulfilled by systems adapted to military usage. The invention of cryptographic systems became a profession in which only the highly skilled specialist could succeed.[3]

In the event of an emergency the Signal Intelligence Service would not be able to find in civil life trained specialists in either cryptography or cryptanalysis in sufficient numbers to meet the requirements of the anticipated expansion. Consequently, it was necessary to conduct courses of instruction for carefully selected personnel who, as a result of the training, would be available for such duty in time of war.[4]

---

3. Ibid., p. 4; Data for Annual Report, War Plans and Training Division, 2 August 1932 (SPSIS 319.1).

4. Supplement to the Annual Report, 1933, p. 5.

In recognition of the necessity for training some members of the Signal Intelligence Section in the Japanese language, a special course of instruction was begun in September 1932. Mr. John B. Hurt, who was the Japanese expert of the section, taught this course until the end of April 1933, three hours per week being devoted to it. Mr. Hurt became ill in May and a competent civilian instructor had to be located to take his place.[5] A former colonel in the Imperial Russian Army, Mr. W. Ayvazoglou, now an American citizen, took charge of the course on 1 June 1933.[6]

C. The Signal Intelligence School

In the thirties, the major portion of the training of a reservoir of qualified military personnel, for eventual service in time of an emergency, was conducted through the Signal Intelligence School, attached to the Signal Intelligence Service and directed by Mr. William F. Friedman. The school grew out of provisions for the detail of a Regular Army officer to the Signal Intelligence Service, but before it was established a start had been made in the direction of training by the preparation of manuals.

Using as a basis his earlier lectures on cryptography[7] and cryptanalysis in the Signal School at Camp Vail (after 1925 Fort Monmouth),

---

5. Memorandum to the Assistant Chief of Staff, G-2, from the Executive Officer, Office of the Chief Signal Officer, 13 May 1933.

6. Memorandum to the Assistant Chief of Staff, G-2, from the Executive Officer, Office of the Chief Signal Officer, 20 May 1933.

7. See Chapter I.

Mr. Friedman prepared training manuals in these subjects which by 1930 were used in connection with Army Extension Courses, offered primarily to reserve officers with a cryptological interest. For the first time in cryptological literature these courses presented the basic principles and methods of cryptography in a logically ordered form and represented pioneer work in cryptographic instruction. The texts prepared were Elementary Military Cryptography (1930) and Advanced Military Cryptography (1931). They became the standard treatises on the subject and were offered to the Army at large.[8]

In 1935, the Army Extension Courses were carefully revised to keep them abreast of the latest research in cryptology, and new problems were added. They were sent to The Adjutant General for publication but were proofread by the staff of the school. The manuscript of two special texts, covering the first two of a series of ten subcourses in cryptanalysis, were also written in the same year. They were designed to form the basis for lesson assignments in this subject and were, when published (1938), the only texts of their kind. They were much more complete and detailed than Training Pamphlet No. 3 then used by the Army, Navy, and Coast Guard, and represented fifteen years of cumulated experience and research in

8. Annual Report of the Chief Signal Officer, 1930; Supplemental Report to Annual Report, 1931, p. 5.

crytanalysis.[9]

A second objective of the training program of the Signal Intelligence School was to give junior officers in the Signal Corps actual instruction and experience in all phases of signal intelligence work. In addition to the two-week course for officers, which the Chief of the Signal Intelligence Section conducted at the Signal School, Fort Monmouth , a similar course in cryptography was conducted in 1920 for reserve officers in the Signal Intelligence School in the Office of the Chief Signal Officer. It was attended by 13 carefully selected Signal Reserve and Military Intelligence Reserve Officers and one special student assigned to the course by the U. S. Coast Guard.[10]

In the next year, authority was requested for the annual detail of one specially selected junior Signal Corps officer as a student in

---

9. Signal Intelligence Section, Major Accomplishments, Fiscal Year 1935, Par. 6. The following texts were prepared.

   1. Elements of Cryptanalysis (1924).
   2. Elementary Military Cryptography (1935, 1943).
   3. Advanced Military Cryptography (1935, 1943).
   4. Military Cryptanalysis, Part I (1938, 1942).
   5. Military Cryptanalysis, Part II (1938, 1941, 1943).
   6. Military Cryptanalysis, Part III (1939, 2nd ed., 1939).
   7. Military Cryptanalysis, Part IV (1941).

10. Annual Report, 2 c (2), p. 6.

the Signal Intelligence School. This request as approved by The Adjutant General[11] on 11 October 1930, was as follows:

1. Reference is made to your letter of August 22, 1930, subject: Honor Courses in Service Schools [(A. G. 352.01) (8-18-30) Misc. (c)], in which, under Paragraph 6, there appears as one of the suggested study courses that of "codes and ciphers".

2. So far as this office is aware there is no civilian or military institution in this country at which special courses are conducted in the compilation, application, handling, or solution of military codes and ciphers. It is true that at certain of the service schools some instruction in code work is given, but this is very fragmentary and nowhere is there given adequate instruction in either compilation or solution of codes and ciphers. It is also true that from 1922 to 1929, inclusive, there was given annually at the Signal School, Fort Monmouth, a subcourse in Military Cryptography covering approximately twelve hours of lecture and class room work and fifteen to thirty hours of home work, but this subcourse is no longer to be given. At best it could cover only some of the broad and more general features of code work but could not go into detail on account of the limited time available.

3. A recent change in Army Regulations (Change No. 1, A. R. 105-5 of May 10, 1929) assigns to the Chief Signal Officer very important responsibilities in connection with the solution of codes and ciphers and the preparation and detection of secret inks. As a result of this added responsibility there has recently been organized in this office a Signal Intelligence Service under which all work connected with secret communications is concentrated. Among these activities is that of instruction of military personnel and civilian personnel of the War Department in cryptography and allied subjects.

---

11. The Chief Signal Officer to The Adjutant General, Subject: Detail of Officers for Instruction in Cryptography, 2 October 1930 (AG 352.01, 10-2-30, Misc.; AGO, 10-4-30 to G-3). This letter was signed by Colonel G. E. Kumpe, Executive.

Regular courses of instruction are to be conducted for Reserve Officers and certain of the Army Extension Courses are to be administered and conducted directly by this office. In order to accomplish this instruction efficiently, much time and labor has been expended in the preparation of training courses.

4. While a certain amount of valuable instruction in these subjects can be conducted by the correspondence method, the time required to become at all proficient with the administrative and technical details of the operation of an efficient Signal Intelligence Service is far beyond that available to officers engaged in other work. Moreover, much of the more complicated material is of such a nature that it does not lend itself readily to absorption by the correspondence method. It should also be recognized that the training of commissioned personnel for duty in this important service ought not be left a matter of individual inclination or idiosyncrasy. During time of war, sufficient experienced commissioned personnel at least to administer this service in an efficient manner, if not to engage in its technical control, will be unavailable unless a logical program for their instruction is established and conducted in the same manner as is the case with other military subjects.

5. This office has given considerable thought to this matter and submits the following recommendations:

(1) That one Signal Corps officer, not above the grade of 1st Lieutenant, be detailed annually to this office for full year's instruction in the compilation of codes and ciphers, the solution of codes and ciphers, the operation of radio intercept and radio goniometric organizations, and the preparation and detection of secret inks.

(2) That the officer so detailed should not be considered as an addition to the quota of commissioned personnel assigned to the Office of the Chief Signal Officer, but solely as a student on the same basis as other officers attending institutions of learning in the capacity of students. He should have no duties other than those connected with his studies.

(3) That, if this project be approved, the first officers selected for this duty be chosen in time to commence instruction by June 1, 1931, the course to be completed by June 1, 1932.

First Lieutenant Mark Rhoads, Signal Corps, was the first officer to be so detailed.[12] He reported on 8 September 1931, for a year's training. Meanwhile, arrangements had been made for the assignment of First Lieutenant J. C. Sherr,[13] Signal Corps, as a language student in Japan for four years. He sailed in August 1931. The plan was that he should upon completing his studies in Japan return to the Signal Intelligence School for cryptanalytic training. This plan was carried out.

By the conclusion of the Fiscal Year 1932, it was evident that one year was hardly sufficient to provide the required instruction and authority was requested to extend the course to two years. The basic document is as follows:[14]

---

12. In 1935 Captain Rhoads was sent to the Philippines but soon afterwards contracted an illness which forced his retirement from the Army. He ultimately recovered from this illness but in spite of repeated requests for a return to active duty, both by Captain Rhoads and the Signal Intelligence Service, no change in status was permitted by the Surgeon General. In January 1944, however, Captain Rhoads became Assistant Director of Communications Research in the Signal Security Agency with the status of civilian employee.

13. Colonel Sherr served during the early part of the War in the Philippines but was killed in September 1943 as a result of an airplane accident while on temporary duty in India.

14. Acting Chief Signal Officer of the Army to The Adjutant General, Subject, Detail of Signal Corps Officers for Instruction in Cryptography (OCSigO 210.6 Gen), approved in 1st Indorsement, 29 April 1932 (AG 350.01, 4-23-32, Misc. C.).

Reference is made to a letter dated October 2, 1930 from this office, subject as indicated above, and to your indorsement dated October 11, 1930, [A.G. 352-01 (10-2-30) Misc. C.] in which approval was granted for the establishment of a one-year course of instruction to be given at this office in the various phases of the work of the signal intelligence service. In accordance with the aforementioned authority, 1st Lieut. Mark S. Rhoads, Signal Corps, was selected as the first student for this one-year detail and he began the course on September 6, 1931.

2. The above-mentioned officer has proved to be an apt student and this office considers his selection as having been thoroughly satisfactory. Despite a most consistent application to duty, however, it has become apparent that one year is hardly sufficient to cover the ground contemplated by this office when the course was projected and authority to establish it as a one-year course was requested. The seven months that have been spent by this student officer in the pursuit of the course have been devoted thus far only to a study of the various types of cipher systems, and these have by no means yet been covered in a manner considered adequate by this office. No time has been devoted to the analysis of any code systems, which represents a most important phase of modern military cryptography; neither has there been any time as yet for the study of radio intercept and goniometric operations, nor of the preparation, use and detection of secret inks. It is obvious that the failure to make a closer approximation of the time required to cover the ground is occasioned by the fact that this course has never been given before, and that no course even remotely similar to it is to be found at any civilian institution in this country.

3. It is estimated that at least two months' additional time should be devoted to the study of cipher machines; six months to the study of code systems; two months to the study of radio intercept and goniometric operations, and one month to the study of secret inks. Such a schedule would require the present student's continuation on this duty until about April 1, 1933, allowing for no leave of absence whatever. It is felt, however, that the nature of the work and the degree of concentration required are such that no officer should be expected to subject himself to this type of mental strain for more than nine consecutive months, without a rest period of at least one month. Hence, allowing for one month's leave, the present student could be expected to cover the ground intended by about May 1, 1933.

4. In view of the foregoing situation, this office requests authority to extend the present course until about May 1, 1933, and to establish it as a regular two-year course on the same basis as the two-year courses pursued by officers attending civilian institutions. The course should commence in September, should allow for one months leave of absence during the next summer, and then reopen to continue until about the following May.

5. In view of the short period of time now available for decision as to the subjects to which the remainder of the present student officer's time should be devoted, it is requested that action on the recommendations made in paragraph 4 be expedited. No additional funds are involved.

Lieutenant Rhoads was continued as a second year student in the school and a second student officer, First Lieutenant W. Preston Corderman, was selected as the first year student.[15] It was proposed that upon the completion of his second year, Lieutenant Rhoads would be replaced by another student. Thus, there were always two officers pursuing this special course, one in his first year, and the other a second year student.

The experience of Lieutenant Rhoads in his two years of training reflected the variety of training in all aspects of signal intelligence work which was offered in the school at that time. He spent seven months on 61 cipher problems, six months on code problems, four months in the study of cipher machines, three and a half months in

---

15. Colonel W. Preston Coderman served as Chief, Signal Security Agency, and as Commanding Officer, Second Signal Service Battalion, from 1 February 1943 to 31 March 1946. For much of this period he was also Chief, Signal Security Branch, Office of the Chief Signal Officer, and Commanding Officer, Arlington Hall Station, and he held the temporary grade of Brigadier General from 18 June 1945 to 31 March 1946.

16. Data for Annual Report, 1932 [illegible]

code compilation and administrative problems, and two weeks on secret inks. During his second year, he studied Japanese with Mr. Hurt for three hours a week for eight months and took an elementary course in Russian at the Department of Agriculture for two hours a week for eight months.[17]

In addition to the two Signal Corps officers trained in the Signal Intelligence School, reserve officers also attended the school between 1929 and 1933. During this period Signal Reserve Officers, Military Intelligence Reserve Officers, and one Coast Guard Officer were ordered to active duty for a period of two weeks. The number in attendance each year was as follows:

Year	Signal Reserve	Military Intelligence Reserve	United States Coast Guard
1929	5	5	
1930	8	8	1
1931		No funds available	
1932	3	2	
1933	3	2	

The number of personnel completing the Extension Subcourses from 1931 to 1933 was as follows:

Year	Sig. C.	Sig. Res.	Nat. Guard	M. I. Res.	Other
1931	2	3	-	-	-
1932	3	6	1	-	-
1933	2	15	-	2	4

17. The Chief Signal Officer from First Lieutenant Mark Rhoads, Subject: Report Covering Course in Codes and Ciphers, 28 July 1933 (SPSIS-201 Mark Rhoads).

Until the summer of 1934, instruction in cryptology was conducted by civilian personnel of the Signal Intelligence Section, in addition to other duties, but by November 1933, it was already considered desirable for more of their time to be devoted to current research activities. The assignment of a Regular Army Officer as an instructor was requested for this reason and because it would permit the expansion of the extension and resident courses. Finally it was hoped that the assignment of Regular Army personnel would render the Signal Intelligence Service less dependent on civilian personnel.[18] In July 1934, a Regular Army Officer (First Lieutenant W. Preston Corderman) was detailed as instructor and the school was formally organized as a separate and distinct unit. War Department restrictions limited the number of officers assigned to duty in Washington and only one officer was detailed as a student in the Fiscal Year 1935, and it was recommended that as increase in the number of student officers be authorized.[19] In 1935 the number was increased to two, in addition to the instructor, but appointments were to be made every two years, instead of annually as before, so that the average number of officers per year was still only one. This move made it possible to give identical courses to both officers, instead of

---

18. Memorandum for Major John B. Wogan, G-2, 4 November 1933 (SPSIS 353.16).

19. Secret Supplement to the Annual Report, 1935, Sec. III, Par. 1.

a first-year course to one and a second-year course to the other.[20]

The material studied by the students of the Signal Intelligence School from 1934 to 1936 included formal courses, special lectures and conferences, and visits of inspection. The schedule of courses was as follows:

4 September 1934 to 4 April 1935
Analysis of cipher problems, with special emphasis on the applications of mathematics to cryptanalysis.

5 April 1935 to 23 December 1935
Analysis of code problems, consisting of both one-part and two-part codes with superencipherment. The security of the Division Field Code was studied. Some familiarity with the adaptation of International Business Machines to code problems was imparted.

2 January 1936 to 29 February 1936
Analysis of cipher devices and mechanisms, including the Wheatstone Device, the M-94, the Kryha Machine, and the IT&T Machine.

Two courses were given in the Japanese language.

15 March 1935 to 30 June 1935
Two hours per week

1 September 1935 to 29 February 1936
Six hours per week

Dr. Abraham Sinkov, Dr. Solomon Kullback and Lieutenant Mark Rhoads expanded the curriculm with lectures on the application of mathematics to the solution of transposition ciphers (nine lectures); permutation tables (three lectures); statistical methods in cryptanalysis (16 lectures);

20. Supplement to the Annual Report, 1936, p. 22; The Adjutant General to the Chief Signal Officer, Subject: Quota of Students at the Cryptographic and Signal Intelligence School, 8 October 1935 (SPSIS 352)

and the work of the Provisional Radio Intelligence Detachment,[21] 1933-1934 (one lecture). Visits of inspection were made to the Accounting Division, Public Works Agency, to witness the operation of business machinery, 9 November 1934, and the United States Coast Guard Monitoring Station, Fort Hunt, Virginia, on 16 November 1934

In this period First Lieutenant W. Preston Corderman served as Instructor and First Lieutenant Harrod G. Miller,[22] Signal Corps, and Lieutenant (j. g.) Leonard T. Jones, USCG, were the regular students. In addition, Captain Edward J. Vogel[23] and First Lieutenant Ulrich S. Lyons[24] of the Military Intelligence Reserve, and Captain J. B. Mathews,[25] Captain Ware, and Captain Cooper of the Signal Reserve received instruction in the analysis of cipher problems during their two-week tours of active duty in May and August. Three other persons, two staff-sergeants, and Mr. Pickering, of the Department of Justice, received instruction in cryptography.[26]

---

21. On this topic, see below.

22. Colonel Miller served in Europe during World War II.

23. Captain (afterwards major) Edward J. Vogel was from 1943 to 1945 Officer in Charge of the Special Examination Unit, Signal Security Agency, except for a period of detached duty in the European Theater.

24. Captain Lyons (afterwards Major) served in t he Signal Security Agency in 1942 and 1943.

25. Lieutenant Colonel J. B. Mathews was Administrative Officer at Arlington Hall Station until 1 February 1943.

26. Signal Intelligence School during period September 4, 1934-February 29, 1936 (SPSIS 352).

Some of the students were exchanged with the Federal Bureau of Investigation, which afforded Signal Intelligence personnel facilities and instruction in document examination. In return FBI personnel received instruction in cryptography and cryptanalysis. This cooperation was found to be mutually advantageous.

The question of the removal of the Signal Intelligence School from Washington to Fort Monmouth was considered first in 1934. While the school was located in Washington, it was not a part of the Office of the Chief Signal Officer, but rather an activity conducted under his supervision, "because of the impracticability of providing elsewhere adequate facilities in the way of secret material and qualified personnel."[27] Hence, it was considered advisable, in 1934, that the Signal Intelligence School should be kept in Washington "until actual, working signal intelligence units" were established elsewhere.[28]

Following the establishment of a signal intelligence detachment at Fort Monmouth however, the question of moving the school to Fort Monmouth appeared no more feasible. It was considered to be functioning satisfactorily at that time in the Office of the Chief Signal Officer,

---

27. Memorandum for the Chief of Staff from Brigadier General Alfred T. Smith, Subject: Cryptographic and Signal Intelligence School, 11 September 1933 (SPSIS 352).

28. Memorandum on Signal Intelligence School, 23 February 1934 (SPSIS 352).

and its removal would be detrimental to the training of the students and instructor,[29] but the plan of the Chief Signal Officer to augment the Signal Intelligence School made it necessary finally to remove it to Fort Monmouth, where it could also train enlisted personnel. Therefore, on 7 September 1939 The Adjutant General approved its transfer from Washington, effective during the Fiscal Year 1941.[30] The training of officers was retained in Washington as a responsibility of the Signal Intelligence Service. The list of officers in the Signal Intelligence School is as follows:

The Signal Intelligence School
Officers in Attendance[31]

Dates	Students	Instructors
Sept. 1931 - June 1933	First Lieutenant Mark Rhoads	W. F. Friedman
June 1932 - June 1934	First Lieutenant W. Preston Corderman	W. F. Friedman
Sept. 1934 - June 1936	First Lieutenant Harrod G. Miller Lieutenant Leonard T. Jones	First Lieutenant W. Preston Corderman
Aug. 1936 - June 1938	First Lieutenant George A. Bicher First Lieutenant Charles B. Brown	Captain H. G. Miller

29. Memorandum for the Chief Signal Officer from Major W. S. Rumbough, Subject: Location of the Signal Intelligence School, 6 February 1936 (SPSIS 352).

30. The Adjutant General to the Chief Signal Officer, Subject: Signal Intelligence Service, 7 September 1939 (SPSIS 352).

31. This list is based on material in SPSIS 201, and SPSIS 352.16.

Dates	Students	Insturctors
Aug. 1938 - June 1940	First Lieutenant J. C. Sherr First Lieutenant H. G. Hayes	Captain G. A. Bicher
Aug. 1940 - 7 Dec.1941	Captain Harold Doud First Lieutenant E. F. Cook Lieutenant Rhoads, USCG	Captain H, G. Hayes

D. The Army Amateur Radio System

Since 1925 the Office of the Chief Signal Officer had conducted training of and maintained close connections with the American Radio Relay League. In 1924 the Signal Corps School recommended that the members of this leading organization of amateurs should be affiliated with the Army. The plan was approved 28 September 1925 and a net control station was set up at Fort Monmouth in charge of an Army liaison officer. An amateur in each Corps area was to initiate the plan, organize a net, and keep records of its activities. Many members resigned after the initial enthusiasm had diminished, but the plan was revived in January 1929. The Army net control station was moved to Washington. The Army Amateur Radio System rendered valuable assistance in relief in disasters, cooperating with the American Red Cross. Starting with a small membership, the number of those interested increased steadily until, in 1939, there were 1,700 members.[32]

---

32. Courtney R. Hall, Development of the Office of the Chief Signal Officer, Part 1, 1917-1943. (Control Approved Symbol SPSEO-100, Project D-1. Historical Section Field Office, Special Activities Branch, Office Service Division, Office of the Chief Signal Officer), p. 22.

This organization also proved its value in experimental work and tests, under the War Plans and Training Division. News of these activities was reported in the Signal Corps Bulletin and QST, the organ of the American Radio Relay League. Instruction in the use of codes and ciphers was added to the training aspect of this program in 1930. This had a decided value as a war time training measure and increased the interest of the Army amateurs in their avocation. A special cipher system was prepared for use by the amateurs in conducting regular communications. The venture was so successful that further training along these lines gave early promise of becoming an important part of the regular activities.[33] Some of the amateurs were enrolled in the extension courses and demonstrated considerable ability in cryptanalysis. A greater number were issued "Cipher Busters" certificates for solving cryptograms during the Fiscal Year 1937.[34] Captain Norman L. Baldwin, who had taken practically all of the cryptanalytic course in addition to his regular duties while stationed in the Office of the Chief Signal Officer in 1931-1934, was in charge of this work.

---

33. Annual Report, 1930.

34. Colonel Stanley L. James to Chief Signal Officer, Subject: Army Amateur Cryptanalysts, 24 February 1938 (SPSIS 311.5).

E. Cryptanalytic Research and Solution

When the civilian cryptanalysts became sufficiently expert in the subject, special research in cryptanalytic theory and procedure was conducted. The result obtained were embodied in classified technical papers for reference purposes and for the training of personnel. Some of these papers represented important advances in the application of complex statistical methods. Procedures were devised for the solution of the difficult double transposition cipher and for the scientific construction of permutation tables for code compilation.[35]

Studies were also made of various codes devised by the Code Compilation unit to determine the degree of their security. In one investigation it was concluded that the addresses and signatures of tactical messages should either be omitted or be cryptographed by a system other than that used for the text of the messages. Steps were taken to eliminate this threat to cryptographic security.[36]

By 1935 a series of 20 technical papers on cryptography and cryptanalysis had been published for a restricted distribution.[37] The manuscripts of all of them were edited and a number of them were written by the Chief of the SIS.

---

35. Supplement to the Annual Report, 1933, p. 8; Annual Report, 1933, p. 8.

36. Annual Report, 1934, par. 2.

37. Signal Intelligence Section, Major Accomplishments, 1935, par. 5.

The series was as follows:

a. Analysis of a Mechanico-Electrical Cryptograph, Part 1 (1934). Prepared by William F. Friedman.

b. General Solution of ADFGVX Cipher (1934). Based on Elements of Cryptanalysis, Signal Corps Training Pamphlet No 3 and a paper by First Lieutenant J. Rives Childs, Report on German Military Ciphers.

c. Permutation Tables Involving a Feature of Non-Transposability (1934). Prepared by Dr. Abraham Sinkov.

d. Existence of Alphabets Having No Internal Repetitions (1934).

e. General Solution for the Double Transposition Cipher (1934). Prepared by Dr. Solomon Kullback, based on earlier research going back to 1921.

f. Permutation Tables for the Most Important Commercial Codes (1934).

g. Principles of Solution of Cryptograms Produced by the I. T. & T. Cipher Machine (1934). Based on the solution of messages of the model installed in the Department of State, 1931.

h. German Military Ciphers from February to November 1918 (1935). Based on report of First Lieutenant J. Rives Childs, prepared in 1918.

i. The Principles of Indirect Symmetry of Position in Secondary Alphabets and their Application in the Solution of Polyalphabetical Substitution Ciphers (1935). Prepared by William F. Friedman.

j. The Index of Coincidence and Its Application in Cryptanalysis (1935). Prepared by W. F. Friedman.

k. Field Codes Used by the German Army during the World War (1935). Prepared by W. F. Friedman.

l. Statistical Methods in Cryptanalysis (1935). Prepared by Dr. Solomon Kullback.

m. Principles of Solution of Military Field Codes Used by the German Army in 1917 (1935). Based on a brochure by a British Officer of the Code Solving Section, General Headquarters, British Expeditionary Force , 1918..

n. Course in Cryptography Translated from the French Work of General Givierge (1934). Translated by John B. Hurt.

o. Notes on the Liaison Service and the Liaison Intelligence Service of the German Army during the World War (1935). Based on a report of Captain Philip B. Whitehead, F. A., prepared in 1919.

p. Analysis of a Mechanico-Electrical Cryptograph, Part II (1935). Prepared by William F. Friedman on the basis of tests conducted in 1932.

q. Report of Code Compilation Section, General Headquarters, American Expeditionary Forces (1935). Prepared by Captain Howard R. Barnes, SigC, in March 1919.

r. Final Report of the Radio Intelligence Section, General Staff, General Headquarters, American Expeditionary Forces. Prepared by Lieutenant Colonel Frank Moorman, General Staff Corps.

s. The Contribution of the Cryptographic Bureaus in the World War (1935). Prepared by Yves Gylden and reprinted from the Signal Corps Bulletin, 1933-1934

t. Further Application of the Principles of Indirect Symmetry of Position in Secondary Alhabets (1935). Prepared by Frank B. Rowlett, based on work begun by William F. Friedman in 1923.

In the next quadrennium four other papers were added to this list:

a. Studies in German Diplomatic Codes Employed During the World War (1937). Prepared by Dr. Charles J. Mendelsohn, formerly Captain, Military Intelligence Division, General Staff, based on work in Washington (1918-1919).

b. An Encipherment of the German Diplomatic Code 7500 (1938). Prepared by Dr. Charles J. Mendelsohn.

c. The Zimmerman Telegram of January 16, 1917 and its cryptographic background (1938). Prepared by William F. Friedman and Dr. Charles J. Mendelsohn.

d. Statistical Methods in Cryptanalysis (revised, 1938). Prepared by Dr. Solomon Kullback.

In addition to the service rendered other governmental agencies in the construction of special codes and ciphers adapted to their needs, assistance was also given them in the solution of many code and cipher messages and in testing cipher machines which they were considering for adoption. In 1930, for three months, all of the personnel of the Signal Intelligence Section collaborated with the Code and Signal Section of the Navy Department in an attempt to solve certain Russian code cablegrams. These had been passed between the Amtorg Trading Corporation in New York and to headquarters in Moscow, and had been

38. Supplement to the Annual Report, 1936, p. 22.

submitted by the Chairman of the House Committee engaged in the investigation of Communist propaganda in the United States. The Naval unit had already devoted three months to the study, without success, before the assistance of the Signal Intelligence Section was requested.

There was a similar lack of success in the joint efforts. Not a single code telegram in the Russian language, passing between officials of the Foreign Office of the Soviet Union, had been solved at this time. On the basis of authentic information, the code and cipher systems employed by the Imperial Russian Government were considered among the most complicated and effective in the world. The Soviet Regime had inherited and improved on these methods. It was considered doubtful, in 1931, whether any of these code telegrams could be read with the information available.[39] Later it was learned that these messages were all sent in "one-time pad" encipherments of code groups taken from a large code. For this type of encipherment, properly prepared and properly used by cryptographic personnel, no general solution is as yet known (1945).

In 1932 another project was undertaken at the request of the Navy Department. For seven years the Code and Signal Section of the Navy had been engaged in the development of a cipher machine which it was hoped could be adopted for use throughout the service. The device had been designed by personnel of the Code and Signal Section in collaboration

39. Supplemental Report to Annual Report, 1931, pp. 6-7.

with personnel at the Navy Yard in Washington and a civilian inventor of long experience in the field, Mr. Edward Hebern. The naval experts were considerably impressed with the security of their device and challenged the Army to solve a set of test messages. The machine was furnished and keying instructions but not with the key list (daily settings) itself. The cipher texts of 55 messages were also furnished, together with their corresponding plain texts. In addition, the cipher texts of 110 other messages, all of the same cryptographic period as the 55 above-mentioned messages, were furnished, but without the plain texts. The Signal Intelligence Service personnel were challenged, even with all the foregoing material in their possession, to produce the solution to any one of the 110 cipher messages. In other words, it was intended that the experts in the Signal Intelligence Service would be presented with conditions even better than those usually present in attempting to solve the intercepted traffic of a single day's operations. This suggests that the Naval experts were extremely confident in the security of their new machine, for they permitted the test to be made under unusually favorable conditions.

The Signal Intelligence Service experts were successful in meeting this challenge. The indicator system was solved and a number of these messages read.[40] As a result of this test, the Navy continued

40. See Analysis of a Mechanico-Electrical Cryptograph, Part II (1935), p. 7, for the details.

to experiment with its machine in order to improve it.

A second project was also undertaken in 1932 at the request of the State Department. A highly complicated but well-built printing-telegraph cipher machine had been developed by Colonel Parker Hitt, a retired Army officer who for many years had been regarded as one of the leading experts in the field of cryptography and cryptanalysis.[41] The machines had been produced by the International Telephone and Telegraph Corporation and installed in the State Department for a test. The Secretary of State, not having any cryptanalytic staff, officially requested the Secretary of War to make suitable cryptanalytic studies to ascertain the cryptographic efficiency of the new machine. In order to provide material for the studies, ten cipher messages enciphered by the machine with settings not indicated were provided. The messages were solved in some cases after only thirty minutes' work and it was concluded that practically any of the messages enciphered by the machine could be solved within a few hours. The insecurity of the machine was thus adequately demonstrated. It was also obvious to the International Telephone and Telegraph Corporation that the machine was not secure and further work on it was abandoned.

The cryptanalytic skill of the Signal Intelligence Service was put to another test in 1935. The German inventor, Kryha, had constructed a

---

41. On Colonel Hitt's undeniable contributions to the science of cryptology in the early period, see the index to this and the two preceding volumes.

cipher machine which had been officially adopted by several governments. Aboard it had been heralded as absolutely indecipherable and was brought to the attention of the Chief Signal Officer in February 1935 by an American firm which had purchased the American rights to the machine for a considerable sum of money. After some correspondence, a test message was submitted by the purchaser as a challenge of the accuracy of certain contentions made by the Signal Intelligence Service. Solution was accomplished by a team of three cryptanalysts in a little more than one hour and was in the mail within three hours of the receipt of the cryptogram. The method of solution was embodied in a technical paper.[42]

Considerable assistance was also given to the Department of Agriculture in 1932, in supplying the Crop Reporting Board with a set of code words with three-letter differences for telegraphic accuracy. The Department of Commerce was given cooperation in the solution of commercial messages referred to it by business houses. Continuous aid was given to the Coast Guard, Treasury Department, in the solution of difficult cryptograms.[43]

F. Intercept Activity 1929-1939

The Radio Act of 1927, in its regulation of radio communications in the United States through the Federal Radio Commission, effectively

---

42. Revised Code Production Program, Individual Mention of Machines, par. b; Supplement to the Annual Report, 1933.

43. Annual Report, 1932 p. 9.

outlawed the interception or divulging of information relating to the contents of messages. In 1934, when the Federal Communications Commission was created and assumed the functions of the Federal Radio Commission, the new legislation which was enacted did not relax the rigid prohibition of intercept activity. The Communications Act of 1934 contain the following provision:

Unauthorized publication or use of Communications

> No person receiving or assisting in receiving, or transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person other than the addressee, his agent, or attorney, or to a person employed or authorized to forward such communication to its destination, or to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, or the the master of a ship under whom he is serving, or in response to a subpoena issued by a court of competent jurisdiction, or on demand of other lawful authority; and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person; and no person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by wire or radio and use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto; and no person having received such intercepted communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that such information was so obtained, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto: Provided, that this section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication broadcast, or transmitted by amateurs or others for the use of the general public, or relating to ships in distress.[44]

---

44. Communications Act of 1934, Sec. 605, 48 Stat. 1103.

Nevertheless, it was essential for purposes of training and the development of improved equipment that intercept work should be undertaken. Even more important was the necessity of having certain fixed stations available in an emergency to undertake the interception of enemy messages. Toward the end of the Fiscal Year 1931, the construction of an experimental intercept station was begun at Battery Cove, Virginia. It was located in the vicinity of Washington, in an area where remotely controlled receivers of radio station WAR served the War Department Message Center in the Munitions Building. Its primary objective was to study the performance of certain recently developed high-speed radio receiving equipment, but it was also to gather actual intercept material for the cryptanalytic practice of personnel of the Signal Intelligence Service.[45]

In the same period also Colonel Joseph O. Mauborgne, then Signal Officer in the Ninth Corps Area, established an unofficial intercept station in the basement of his home in California. He possessed an automatic recording outfit which recorded the intercepted texts on a tape which was then mailed to Washington. Some intercept activity was also carried on in the Eighth Corps Area, the Panama Canal Department, and the Philippine Department by very small radio intelligence

45. Supplemental Report to Annual Report, 1931.

detachments, but these provided the Signal Intelligence Section with only "a fair amount of material for research." Many of these messages were also solved.[46]

Mention should also be made of the establishment in 1933 of a Provisional Radio Intelligence Detachment at Fort Monmouth, First Lieutenant Mark Rhoads, Commanding. While relatively little traffic was intercepted much research and development in the field of radio intelligence was carried on.[47]

By the close of 1937 it was evident that such intercept resources as the United States had developed might shortly be called upon to render actual service in war. In November of that year, it was proposed that a radio intercept station be established in Washington to be used for monitoring the radio channel carrying the bulk of the diplomatic traffic between Washington and New York City, during the twelve of fifteen hours of the day when the most interesting traffic was being handled.

---

46. Major Accomplishments, 1935, par. 10; Supplement to the Annual Report, 1936, sec. III, par. 5.

47. See Report on The Provisional Radio Intelligence Detachment for the Period October 1, 1933 to October 17, 1933, a copy of which is now on file in the Office of the Director of Communications Research, Signal Security Agency. During maneuvers in September 1934, Lieutenant RHoads served as a signal intelligence unit (there were no others involved) for the Black Side. He succeeded in solving most, if not all, of the messages intercepted. This was the first example of a signal intelligence unit at work in the field since the First World War, as the Provisional Detachment was the first radio intelligence unit to operate since 1918.

The proposal involved the installation of receiving sets at Battery Cove and the War Department Message Center, the installation of the necessary equipment in the Message Center, and the transfer to Washington of two radio operators of suitable qualifications.[48]

The War Plans and Training Division of the Office of the Chief Signal Officer, however, did not concur in the recommendation. The value of the proposed station at Washington was deemed not sufficient to justify the expense which would amount to $5,408.20 initial costs and a rental of $72 per month. The Signal Intelligence Section was by this time receiving from other sources more intercept material than it could handle, and had indication of increased activity for which there was insufficient personnel. The establishment of an intercept station at Fort Monmouth was already being contemplated and it was anticipated that it would be able to monitor the circuit suggested for the Washington station. Consequently, it was recommended that the plan for establishing a station at Washington be dropped, at least until the possibilities of a station at Fort Monmouth had been determined.[49]

By 28 February 1938 the Signal Intelligence Service was operating six intercept stations.

---

48. Memorandum for the Chief Signal Officer from Major W. S. Rumbough, Subject: Proposal for Establishment of a Radio Intercept Station in Washington, 19 November 1937, par.1.

49. Ibid., 4-5.

The installation of the station at Fort Monmouth had been completed. Two other stations were set up within the continental United States; one in the Ninth Corps Area, was located at the Presidio of San Francisco, California, another was established at Fort Sam Houston in the Eighth Corps Area. Authority had been obtained in 1935 for the establishment of signal intelligence detachments at these stations and in overseas departments. As soon as the increase in Signal Corps personnel permitted the organization of such detachments they were established in each of the three overseas departments; one at Quarry Heights in the Panama Canal Department;[50] one at Manila, in the Philippine Department;[51] and one at Fort Shafter, in the Hawaiian Department.[52] The intercepted messages were transmitted to Washington for analysis by registered secret mail in weekly batches.[53]

On 26 January 1938, the Signal Intelligence Detachment at Quarry Heights, Canal Zone, had been directed to attempt 24-hour intercept activity.

---

50. Dr. A. Sinkov was stationed there as cryptanalyst. See Section H for fuller details.

51. This station had no expert cryptanalyst.

52. Dr. S. Kullback was the cryptanalyst here.

53. See Memoranda to each of these Stations from the Chief Signal Officer, 28 February 1938 (SPSIS 320.3); W. F. Friedman to Captain Mark Rhoads, 10 October 1935 (SPSIS 201-Mark Rhoads).

It was to give first priority to Japanese and Italian diplomatic traffic from Rome to Tokyo, with a secondary emphasis on the same type of traffic transmitted from Berlin to Tokyo. It was also directed to monitor Japanese diplomatic traffic between Tokyo and the Central and South American Countries.[54]

The location of the Signal Intelligence detachments in Hawaii, Panama, and the Eighth and Ninth Corps Areas, however, did not permit the Signal Intelligence Service to take full advantage of the "golden opportunity" to obtain Japanese Army radio traffic presented by the Japanese penetration into China. It was highly desirable that the Japanese Army methods of enciphering and deciphering be studied in order that the code and cipher solution section of the Signal Intelligence Service might have some experience in the analysis of this material. It would prove, of course, of inestimable value in the event of hostilities.[55]

In 1935 the War Department, with the foregoing purpose in view, had established an intercept station at Fort Hughes in the Philippines, with Captain Mark Rhoads as officer-in-charge, but he was taken ill a few months thereafter, and was shortly forced to retire from the Army. He was not replaced until March 1938 when Captain Harrod G. Miller,

---

54. Memorandum form the Chief Signal Officer to The Adjutant General, Subject: Intercept Activity of Signal Intelligence Detachment, 26 January 1938 (SPSIS 320.3).

55. Chief Signal Officer to The Adjutant General (through G-2), Subject: Radio Intercept Activity in the Philippine Department 9 February 1938 (SPSIS 320.3), par.1.

who had been graduated from the Signal Intelligence School and afterwards had served as instructor in that school, was sent to the Philippines.

No effective use of officers of similar experience and training had been made in the Philippine Department. Instead, officers equipped by skill and training for the task had been placed on routine Signal Corps work (e.g. Captain W. Preston Corderman became a Signal Officer, not a Signal Intelligence Officer). It was requested that a specific directive be issued to the Commanding General, Philippine Department. Unless the necessary men and equipment were provided for Captain Miller, the effort to activate radio interception through him would prove abortive. Ten enlisted personnel were considered necessary to accomplish the desired monitoring.[56] The Radio Intelligence Company at Fort Monmouth was also directed to concentrate on Japanese Government traffic from New York to Tokyo, Rome to Tokyo, and Berlin to Tokyo.[57]

By the end of March 1938, the plans for increased intercept activity, which was still prohibited by the Communications Act, required official approval by higher authority in order that it might proceed

---

56. Ibid., par. 3-4

57. Chief Signal Officer to Commanding Officer, Fort Monmouth, Subject: Intercept Directive of Radio Intelligence Company, 10 Eebruary 1938 (SPSIS 320.3).

unimpeded. It was necessary to protect the War Department and its personnel with a record of official authorization for such activities, applicable, incidentally, to the Navy as well.[58] A memorandum was therefore transmitted to the Chief of Staff, recommending that authority be granted to the Chief Signal Officer, under the direction of the Assistant Chief of Staff, G-2, "to maintain and operate in time of peace under strictest provisions to insure secrecy, such radio intercept and cryptanalytic services" as were "necessary for training and for national defense purposes."[59] (The operation of the Signal Intelligence Service had been of value to the Military Intelligence Division. In two instances it had obtained information which indicated that two foreign powers were "using their diplomatic codes for the transmission of information prejudicial to" American preparations for national defense).[60] This recommendation was approved by the Secretary of War, 30 March 1938.[61]

The intercept activity of the Signal Intelligence Service was consequently accelerated in 1938.

---

58. Memorandum for the Chief of Staff from the Assistant Chief of Staff, G-2, 26 March 1938.

59. Memorandum for the Chief of Staff from the Assistant Chief of Staff, G-2, Subject: Radio Intercepts, 26 March 1938 (SPSIS 676-3).

60. Ibid.

61. Ibid., indorsement by Deputy Chief of Staff.

On 6 April 1938 the Chief of the Signal Intelligence Service, Major W. O. Reeder,[62] summarized this activity as follows:

> Six months ago only two stations were operating effectively and the mission of these was somewhat general. We are now operating four with good efficiency and one is coming along gradually. The first steps in organizing the work has been to assign channels to each station. Obviously, we cannot cover all the air, and therefore those channels which are currently the most interesting have been assigned. These assignments are not fixed but were made solely as a point of departure. Of course some of these assignments may be found to be beyond the capabilities of certain of the stations. In that event, no greater service can be given by that station than prompt report of its difficulties.[63]

By the end of June 1938, it was evident that the location of the intercept station at Fort Monmouth was unsuitable. It had been operated by the reorganized detachment of the 51st Signal Battalion, the Provisional Radio Intelligence Company. The site, however, was not well-suited for 24-hour radio reception and in addition the occurrence of man-made radio interference made the functioning of the monitoring station difficult. Surveys were made to find a site better adapted to interception and a part of the Fort Hancock, New Jersy, reservation was found to be "vastly superior to any part of Fort Monmouth

---

62. In view of the growth and greatly increasing importance of the activities the Chief Signal Officer deemed it advisable to assign a Regular Army officer as head of the Signal Intelligence Service; Mr. Friedman remained as the principal assistant and chief technical adviser.

63. Memorandum to the Commanding Officer, Provisional Radio Intelligence Company, Fort Monmouth, 6 April 1938 (SPSIS 320.3).

as a site for a monitoring station."[64]

It was requested that the 18 Signal Corps enlisted men, First Lieutenant Earle F. Cook, commanding, should be transferred to Fort Hancock from Fort Monmouth not earlier than 1 September 1938. The station would continue its operation under the direction of the Chief Signal Officer. The estimated cost of this transfer was $2, 618.80.[65]

By the autumn of 1938, preparations to send to the overseas departments the necessary cryptographic equipment had been undertaken. It was now possible to supply these units the Converter M-134A which had recently been developed. Meanwhile, the Tenth Signal Company in the Philippines had been strengthened far its prospective intercept activity by the transfer of four qualified radio operators from Fort Monmouth.[66]

G. Cryptanalytic Solutions

Throughout the period under discussion (1930-1939) attempts were made to solve certain diplomatic traffic within the limits of available staff and facilities, and whenever sufficient volume was available to

---

64. Memorandum to The Adjutant General from the Chief Signal Officer, Subject: Establishment of Monitoring Station at Fort Hancock, N. J., 23 June 1938 (SPSIS 212,2 Fort Monmouth).

65. Ibid.

66. Third indorsement, The Chief Signal Officer to The Adjutant General 24 June 1938 (SPSIS 320.3).

justify hope of solution. The government which received the greatest attention was, of course, the Japanese. The cryptanalysts of the Signal Intelligence Service had the benefit of the records of solutions made by MI-8 in the preceding decade,[67] but not until 1933 was any serious attempt made to resume the attack on Japanese systems. In that year Dr. Kullback and Mr. Hurt were assigned some Japanese encoded messages consisting of two-and-four-letter substitution groups of a Japanese syllabary and small vocabulary. It was not long before they could read them. Although these messages and others provided information of no real value as intelligence, they did provide a basis for a study of the type of vocabulary, the grammatical forms, frequencies, and cryptographic habits to be expected in other Japanese traffic. Typical of the solution activities of this period is that of a system known as "J-6", a three-and four-letter code, which was solved by March 1934.[68]

Between 1933 and 1935 five Japanese diplomatic systems were used in rotation at intervals of three months. These systems, solved and read, were all of the two-and four-letter type of code with syllabary and

---

67. See Chapter III.

68. A description of the steps leading to solution is now filed in IR 5010-50-12, together with the traffic and worksheets. The date is 5 March 1934.

vocabulary. By 1938 nine Japanese diplomatic systems had been read by the Signal Intelligence Service. The appearance of new systems and the increasing complexity observed in them during the thirties is believed to be the result of the publication in 1931 of Yardley's book, The American Black Chamber.[69]

Japanese systems known to the Signal Intelligence Service during the ten years before World War II include the following:

Digraphic substitution	Dates effective
AW	July 1932 to December 1934
CA	November 1936
YO	September 1938

Polygraphic substitution	
XA	1931-1932
XB	?
DA	October 1932 to 15 October 1935
EG	January 1933 to 15 October 1935
WI	April 1933 to October 1934
IK	December 1933 to October 1934
J-6	15 October 1935 to 28 February 1938
J-7	1 January 1936 to 26 February 1936
J-8	1 July 1936 to 31 October 1938
J-9	1 July 1936 to 31 October 1938
J-10	1 November 1938 to 9 April 1939
K-I	1 November 1938
J-II	10 April 1939 to 1 January 1940
KO	April 1939
J-12	2 January 1940 to 31 May 1940
J-13	1 June 1940 to 15 July 1940
J-14	15 July 1940
J-15	15 July 1940
P-I	15 July 1940
J-16	15 August 1940 to 30 November 1940

69. See Chapter IV.

The Japanese introduced transposition as an encipherment of various codes. Usually the transpositions had to be designated in the traffic by an indicator. The following systems were known: ALYTA, ETOME, FIPUF, one without indicator, YMMBO, XUMFO, POSTA, BYWDE, VOSAI, KALNY, VERDI. Transposition was applied to the various codes as follows:

Code	Effective
XA	1931
K-1	19 January 1939 to 1 July 1940
K-2	19 January 1939
K-3	1 July 1940
K-4	15 July 1940 to 15 November 1940
K-5	15 August 1940 to 30 November 1940
K-6	1 December 1940 to 28 February 1941
K-7	
K-8	1 March 1941
K-9	11 March to 25 April 1941
K-10	23 June 1941 to 15 August 1943

The following spelling tables were also used:

JE English Spelling
English Spelling and Vocabulary
French Spelling and Vocabulary
HE Code
EX Code
OG Code
UJ Code
CH Code
B Table
PA English Spelling
CA English Spelling

It will be recalled that the furnishing of texts of translations was not expected by G-2 in the early days of the Signal Intelligence Service. When translations became possible, they were for some time not forwarded to G-2 at all but were kept within the Signal Intelligence Service, although occasionally certain messages were shown to the Chief Signal Officer, beginning in January 1935. Soon there came a change in policy and in April 1936 the "Bulletin" was established as a proper means of bringing to the attention of G-2 and the War Department the texts of solved messages deemed to be of importance.

Japanese diplomatic traffic supplied the first translations for the Bulletin. The personnel engaged in this early solution work,

---

70. As is now (1946) well understood, this is a characteristic of the cryptographic systems of most governments.

under the general supervision of Mr. Friedman, were Messrs Rowlett, Kullback, and Sinkov, and later Messr Ferner, Snyder, Clark, and Bearce. By 1938 Mr. Rowlett had the direct supervision of Japanese solution; he and Mr. Ferner were concentrating in particular on the Japanese machine cipher, known to the Signal Intelligence Service as the "Red System".[71]

Though the Signal Intelligence Service had already studied a number of cipher machines during tests, the first study of a machine cipher in actual use by a foreign government was the Japanese Red machine. As the machine was first known, it contained two wheels, one to encipher the six vowels and the other to encipher the twenty consonants separately. Thus the resulting cipher text was composed of vowels enciphered only by vowels and and consonants enciphered only by consonants--an attempt to reduce telegraphic expense by producing artificial words in the cipher text. Later the "six" wheel was used for any six letters. A third wheel controlled the motion of the cipher wheels. In addition to the daily cipher sequences, 240 indicators for the wheel settings had to be solved. The system, put into use before 1932, was undertaken for study in 1935 and solved by 1936.

---

71. At this period colors were used as short titles; though they have been officially abandoned except for subordinate phases of systems, this short title is still used colloquially.

On 1 December 1938 the machine was modified by the addition of three special commutators of interrupted motion to encipher highly secret messages. The last message received in this system was dated 21 August 1941. It was superseded by the more secure "Purple Machine", a description of which will be included in the History of the Signal Security Agency.[72]

The friendly rivalry which had existed between the Signal Intelligence Service and the Code and Signal Section of the Navy in the solution of test messages was also evident in the task of interception and subsequent solution of diplomatic traffic. Each of the services attempted to intercept as much material as possible, to solve it immediately, and to gain credit for itself as the agency by which the information obtained was made available to the Government. Such a condition was, of course, highly undesirable, and steps were taken to eliminate the feeling of rivalry as much as possible. The first steps were, however, anything but successful. It was agreed after lengthy negotiations that the Army and the Navy would exchange all diplomatic traffic from their intercept facilities, and that both services would work on this traffic. But in order to avoid as much duplication of effort as possible it was agreed that the Army would receive all traffic

---

72. Attempts at the solution of systems used by other governments did not begin as early as these attacks upon the Japanese systems. For this reason, the earliest activities of that kind will be included in the History of the Signal Security Agency.

of days with an even date and the Navy all traffic of days with an odd date. This arrangement was deemed by the Chief Signal Officer and the Director of Naval Communications to be the most practical one, since all available traffic was necessary for solution and it was desirable to give both services equal opportunities for training, "credit," and so on.

H. Cryptanalysis in the Departments

One of the plans made for the Signal Intelligence Service in 1930 had included the sending of civilian cryptanalysts to work in Panama, Hawaii, and the Philippines, but no steps were taken to carry out this recommendation until it was learned in 1936[73] that G-2 in Panama was employing an amateur cryptanalyst and "thereby infringing upon the prerogatives of the Chief Signal Officer."[74] The civilian chief of the Signal Intelligence Service therefore recommended that if a cryptanalytic unit was thought to be essential at that time in the Panama Department, one of his assistants should be sent there to establish such a unit under the Signal Officer. Although the staff in Washington was small, this arrangement would not result in "losing the services of a man. . . but merely having him do in the field much of the work he now does,

---

73. Memorandum for Major Rumbough, signed W. F. Friedman, 16 January 1936 (SPSIS 201: A. Sinkov). The sources of all statements in this section are the 201 files of A. Sinkov (Panama Department) and S. Kullback (Hawaii Department).

74. Major W. O. Reeder, Duties of Civilian Cryptanalysts in Hawaii and Panama, 15 October 1937.

with the results immediately available to those who want them in Panama." He believed that the inevitable slowing of the work would have less serious consequences than the decentralization of signal intelligence activities which would result from the taking over of cryptanalytic functions by G-2, and hoped that the plan would result in obtaining backing from the Department Commanders for the work of the Signal Intelligence Service.[75]

To implement these recommendations in July 1936[76] Dr. Abraham Sinkov was sent to Panama where he reported to the Department Commander for duty. No written instructions had been given him in Washington and contact with him during his stay in Panama was maintained partly through channels and partly through personal correspondence.[77]

An intercept station was set up in Panama during Dr. Sinkov's stay[78] and apparently its program was influenced to some extent by the needs of the Signal Intelligence Service in Washington. Intercepts of Japanese messages were forwarded to Washington; those of

---

75. W. F. Friedman, Memo for Major Rumbough, 16 January 1936.

76. Letter of A. Sinkov to his friends in the SIS, dated 2 October 1936, in which he says that he left Washington three months earlier.

77. Memorandum cited in note 76.

78. Sinkov to Friedman, 16 April 1937: "The radio equipment for the intercept station will arrive on the next boat and I am hopeful that we will be able to begin our intercept program by the first of the next month."

other governments were classified and kept on file in Panama.[79] Mr. Friedman wrote in the summer of 1937:

> I would . . . very much appreciate your sending on all J intercept material. Our station at Ft. Monmouth has gone to pot since they took all the men away for the Texas exercise. As a result, we are getting very little European material and if you could get any of that for us, it would be appreciated.[80]

While in Panama Dr. Sinkov continued to work on Japanese Governmental systems. He was given material for the solution of diplomatic codes and ciphers and was taught the solution of the Red Cipher Machine[82] which had been solved in Washington about this time, in order that he might work on the current diplomatic system, "submitting occasional translations to G-2."[83] He was, however, handicapped by lack of material.[84] In the summer of 1937 the decision was made to discontinue work in the field on Japanese systems.

---

79. Sinkov to Friedman, 30 June and 15 July 1937; Friedman to Sinkov, 26 July 1937.

80. Friedman to Sinkov, 2 August 1937.

81. Sinkov to Friedman, 15 October and 7 December 1937.

82. Memorandum cited in note 73.

83. Sinkov to Friedman, 16 April 1937.

84. Sinkov to Friedman, 15 July 1937.

The director wrote:

> I think you can deduce the reasons when I tell you that they are based entirely on the desirability of avoiding the demise of the proverbial goose.[85]

Obviously, it was thought that activity in the Department might prove a danger to the security of cryptanalytic operations.

The decision placed Dr. Sinkov in a difficult position. The Signal Officer in the Department was in the habit of submitting some of the diplomatic messages to the Commanding General in order to win support for the intercept activity. If no more Japanese messages were to be read and translated, it would prove difficult to maintain this support. A compromise was therefore evolved. While work on the diplomatic traffic ceased, Dr. Sinkov continued to produce for the Signal Officer translations of messages in the simple commercial system—the Department even provided an officer who had been a language student in Japan to aid in production.[86]

During the remainder of his stay in Panama Dr. Sinkov gave some time to the study of Italian Government messages. They were chosen because, of European "Axis" stations, interception was easier in the case of Italy.[87]

---

85. Friedman to Sinkov, 2 August 1937; 1 September 1937.

86. Sinkov to Friedman, 12 September and 15 November 1937.

87. Sinkov to Friedman, 19 August 1937.

Meanwhile, in March 1937[90] Dr. Solomon Kullback was sent to Hawaii, apparently in response to a request for a code clerk.[91] He received no written instructions in Washington but reported for duty to be assigned by the Commanding General of the Hawaii Department.[92]

The cryptographic duties did not occupy much time. Soon after his arrival Dr. Kullback reported that "except when messages may pile up unduly, I will not be called on to do all the encoding, etc., of War department traffic."[93] No other mention of this task appears in the

---

88. Sinkov to Friedman, 11 January 1938. One of the governments studied was Traffic in one of its systems was studied intensively by an enlisted man in the Department, Private Stanley A. Kretlow, afterwards Captain in the Signal Security Agency. Kretlow reconstructed the permutation table of the code then being used.

89. Sinkov to Friedman, 27 October 1937; Friedman to Sinkov, 10 November 1937.

90. Major W. S. Rumbough to Commanding General, Hawaiian Department, 15 February 1937.

91. Major W. O. Reeder, Duties of Civilian Cryptanalysts in Hawaii and Panama, 15 October 1937: ". . . if he(Kullback) was not sent in response to this request, the coincidence was chronological at least." It should be pointed out that while Dr. Kullback was competent to serve as a code clerk, he was much more expert than was necessary for such a position.

92. Ibid.

93. Kullback to Friedman, 25 March 1937.

correspondence except one reference to the effect that arrangements were being made to have the work done by others.[94]

Dr. Kullback's most valuable work during his brief stay in Hawaii was in obtaining interesting intercept material for the Signal Intelligence Service in Washington.[95] He helped to reconstruct the Japanese diplomatic net and what was believed to be a kana military net in which several Navy stations were found,[96] and was obviously able to give expert advice on the traffic which should have priority.[97] By September, however, he evidently thought that he had accomplished all that could be done along these lines because he wrote:

> From my experience to date I would say that it were better for somebody from the office (in Washington) to visit these stations, say yearly, or once every two years, to maintain closer and personal contact, than to assign a cryptanalyst.[98]

At the time of Dr. Kullback's departure for Hawaii it had been intended that he continue work on the solution of Japanese diplomatic codes and ciphers with material from Washington[99] but before the necessary charts and tables were sent, the loyalty of one of the enlisted

---

94. Kullback to Friedman, 6 April 1937.

95. Friedman to Kullback, 24 June 1937; 2 August 1937.

96. Kullback to Friedman, 6 April 1937, 27 May 1937, 17 September 1937.

97. Kullback to Friedman, 16 July 1937.

98. Kullback to Friedman, 17 September 1937.

99. Major W. O. Reeder, Duties of Civilian Cryptanalysts in Hawaii and Panama, 15 October 1937.

men in the intelligence detachment at Honolulu came under suspicion,[100] and the material was never sent. Dr. Kullback was advised not to attempt to reconstruct the tables.[101] He did some work, however, on Japanese diplomatic and Rikugun systems and other material was sent him from Washington,[102] He reported that he had never used enlisted men on this project and had "kept all idea of the J systems from them."[103]

While in Hawaii Dr. Kullback began a study of German systems, concentrating on a four-letter code with the help of an enlisted man who knew German.[104] He also revised for publication his paper on Statistical Methods[105] and worked on solution of the Kryha Cipher Machine.[106]

---

100. Ibid.; Friedman to Kullback, 14 April 1937.

101. Captain Harrod G. Miller to Kullback, 17 May 1937.

102. Kullback to Friedman, 23 April 1937; Friedman to Kullback, 7 May 1937; Kullback to Friedman, June 1937; Friedman to Kullback, 24 June 1937.

103. Kullback to Friedman, 17 September 1937, but see letter in which he speaks of working with one of the enlisted men and says,". . . if you feel that you can lend us . . . some of the Rikugun messages we could make copies of them here and send the originals back to you." Kullback to Friedman June 1937. Friedman replied, "I have gotten together . . . the Rikugun stuff and will send them on." Friedman to Kullback, 24 June 1937.

104. Kullback to Friedman, June 1937; 16 July 1937.

105. Friedman to Kullback, 27 November 1937; Kullback to Friedman, 3 February 1938; Friedman to Kullback, 14 February 1938.

106. Friedman to Kullback, 24 June 1937.

His relations with G-2 in the Department presented no difficulties. They were apparently satisfied with translations of plain-text Rikugun messages the content of which might later be found in The New York Times.[107]

The decision to recall both cryptanalysts to Washington was made because of the very greatly increased burden of the work being done by the SIS in Washington and because it was believed that their services could be put to better use in Washington than in isolation in a Department.[108] The cryptanalysts themselves were in agreement with this decision. Dr. Kullback wrote on 17 September 1937:

> I think that I can be of much more service in Washington than here . . . We have neither the facilities nor the assistance to carry out real solution activities here and in any case the results of the same are of interest to Washington, not here . . .

I. Secret Inks

The specialized nature of the responsibilities of the Signal Intelligence Service in connection with secret inks also demanded highly qualified, technically trained personnel. At the close of the Fiscal Year 1931, steps were taken to establish a laboratory for research in the field of invisible inks and to obtain the necessary equipment and

---

107. Kullback to Friedman, 17 September 1937.

108. Friedman to Kullback, 1 September 1937; Friedman to Sinkov, same date. Major W. O. Reeder, Duties of the Civilian Cryptanalysts in Hawaii and Panama, 15 October 1937.

supplies within the limits of the small funds available. Originally it had been contemplated that this work would be conducted at Fort Monmouth but the establishment of a laboratory more conveniently located for War Department work was desirable.[109]

It was proposed that secret ink investigations be undertaken as soon as qualified personnel could be obtained. In 1931 this work was performed by a Military Intelligence Reserve Officer, Captain A. J. McGrail, who was considered the leading American expert in the field of secret inks. The Chief Signal Officer, then Major General Irving J. Carr, recommended that the enforced dependence on an officer outside the Signal Corps for such investigations be remedied as soon as possible. He requested that funds be made available by the Fiscal Year 1934 for the employment of a secret ink chemist, who possessed special training along these lines.[110]

In 1932 Captain McGrail was transferred to the Signal Corps Reserve. He was ordered to active duty with the Signal Intelligence Service for the customary two-week periods. During these terms of active service he worked in the small laboratory and "was able to impart some valuable information relative to methods and processes of detecting secret-ink writing" to two selected members of the Signal Intelligence Service.[111]

---

109. Supplemental Report to the Annual Report, 1931, p. 2d.

110. Ibid.

111. Annual Report, 1932, p. 8.

This method of instruction was continued until regularly employed personnel could make the tests of a routine character, but Captain McGrail was still consulted in the more difficult cases. It was therefore considered expedient to employ a chemist with specialized training, if he could be found, as soon as funds permitted.[112] The personnel authorized for the entire service, however, remained static and the slight increase authorized toward the end of the decade was diverted to more urgent tasks.

---

112. Ibid.

CHAPTER VIII. IN RETROSPECT

The reader will have already noted that, except for occasional digressions in which the events of World War II have been anticipated in order to show more clearly the significance of earlier developments, the narrative of the two preceding chapters, which cover the same period, has in general been ended with the year 1939. The reason is, of course, obvious: prior to that year the activity of the Signal Intelligence Service had consisted of a general preparation for a hypothetical war, though, to be sure, there was a strong emphasis upon a war with Japan motivated by Japan's operations on the Asiatic mainland and the precarious state of Japanese-American relations ever since World War I. After the beginning of 1939, however, events in Europe made it increasingly clear that in that quarter lay an equal, if not, indeed, a greater, danger to the peace of the United States.

Though for the twenty-seven months between the attack on Poland (1 September 1939) and that on Pearl Harbor (7 December 1941) the Signal Intelligence Service was still in a sense engaged in preparation for war rather than in actual conflict, henceforth that activity had indeed entered a new and greatly accelerated phase. For this reason, the narrative of events after 1939 has been made a part of the History of the Signal Security Agency in World War II for which the Historical Background of the Signal Security Agency is but a prolegomenon.[1]

---

1. In the History of the Signal Security Agency in World War II events prior to 1939 have been summarized wherever a knowledge of the background is essential to full comprehension of later developments.

Before concluding this study of the historical background, however, it will be well to summarize the achievements of the Signal Intelligence Service in the nearly ten years after its founding in 1930. This can best be done by a comparison of the situation existing in 1939 with that prior to the mobilization of 1917. It will be recalled[2] that in 1917 the United States Army faced its new responsibility for both protection of its own communications and cryptanalytic attack upon the communications of the enemy and other foreign governments.[3] The Chief Signal Officer had, indeed, been officially entrusted with the task of code compilation but the only code ready for use was a one-part affair, provided with a not very secure form of encipherment for the more secret messages, and it had been printed under insecure conditions and was believed, with, as it proved, complete justification, to be already compromised. No unit within the Army was charged with solution. Indeed, there were only three officers who were regarded as expert in the field. Thus it was that reliance had to be placed at least for a time on the efforts of the cryptanalysts at Riverbank Laboratories. Both in Washington and in France, the Army was

---

2. See above, Volume One: Chapter VI, and Volume Two: Chapter I.

3. While the unpreparedness in this field was probably no greater than in other phases of military science, it should be said in defense of the Army of thirty years ago that in that period radio communications were only beginning to undergo large-scale development. World War I was the first in which radio communications played a significant part.

forced to build new organizations from the very foundation and this while the War was already in progress. What is surprising is that anything was achieved in the eighteen months during which the War lasted: the personnel engaged in the work were hardly seasoned before the Armistice rendered their efforts largely no longer necessary.

In comparison with this state of unpreparedness in 1917, the Army approached the outbreak of what proved to be World War II reasonably well prepared. In spite of the extremely limited funds available for the entire signal-intelligence program, much was accomplished. A group of Regular Army officers had been trained in all phases of signal intelligence and were ready for administrative duties on high levels. A nucleus of expert cryptanalysts, while far from adequate in number to face the tasks which ultimately they were assigned, had been throughly trained in all methods of solution then known. The art of cryptanalysis had been developed along scientific lines far beyond the highest point of efficiency reached in World War I and the groundwork was well laid for still greater advances when, in actual operations, new problems would present the necessity for finding new solutions. Automatic machinery had been placed in the service of statistical analysis to make possible computations not hitherto dreamed of. Cryptanalytic continuity, which had been broken off completely in 1930 at the time of the dissolution of MI-8, had, at least in the case of the Japanese systems, been resumed.

Intercept stations had been established for the systematic gathering of the raw material without which there is no hope of cryptanalytic solution. The chief deficiency in the field of solution was the fact that lack of funds prevented the training of enough cryptanalysts.

For the protection of Army communications, an ambitious program of code compilation had been completed, made possible by the then revolutionary use of tabulating machinery. Moreover, the manual ciphers had been greatly perfected and were far more secure than the best that had been used by the Army in World War I, yet even more significent advances in this field were made in the development of automatic cryptographic machinery. The M-134-A cipher machines had been put into production and were in some cases in use. A more practical machine, the SIGABA, with equally high security, had been invented--though the later phases of its development had been carried on by the Navy, the basic ideas underlying the machine were contributed by the personnel of the Signal Intelligence Service--and was , though the Army did not know it in 1939, almost ready for production. These machines subsequently served as the basis for all research and development in World War II in the field of automatic cryptographic machinery. Though limited funds prevented any real development of methods for the protection of speech communications and picture communications, these had been at least conceived. A small beginning, also, had made for the provision of secret ink facilities, though

here again lack of money prevented the development which was known to be desirable.

Thus it will be seen that the Signal Intelligence Service, while in no way failing to exploit the experience of World War I in the field of cryptology, had never blindly assumed that if and when another conflict broke out, it would be merely a repetition of the same conditions as had been encountered in 1917-1918. Careful attention had been paid to all of the scientific research and development which had made possible the use of new, speedier, and more secure techniques of signal communications.

The Signal Intelligence Service was therefore well prepared for the task which faced it. Looking backward over the whole period of the peace, it is possible now to see that the two chief problems which in those years hampered progress were (1) the lack of unified control over all phases of cryptology during the first decade, and (2) the extremely limited funds with which the Signal Intelligence Service had to do all that was necessary in the second.

BIBLIOGRAPHY

Baker, Ray Stannard: Woodrow Wilson, Life and Letters (Garden City: Doubleday, Doran, Vol. V, 1935; Vol. VI, 1937).

Barnes, Howard R.: Report of the Code Compilation Section, General Headquarters, American Expeditionary Forces, December 1917--November 1918 (Washington: United States Government Printing Office, 1935).

Bates, David Homer: "A rebel cipher despatch, one which did not reach Judah P. Benjamin," Harper's Weekly, June 1898, pp. 105-109.

———. "Lincoln in the Telegraph Office," Century Magazine, Vol. LXXIV, New Series Vol. LII, May to October, 1907.

———. Lincoln in the Telegraph Office (New York: Century, 1907; reprinted, New York: D. Appleton-Century, 1939). [An expanded version of the preceding item.]

Brown, J. Willard: The Signal Corps, U. S. A., in the War of the Rebellion, with numerous illustrations and maps (Boston: U. S. Veteran Signal Corps Association, 1896).

Burnett, Edmund C. "Ciphers of the Revolutionary Period," American Historical Review, Vol. XXII (1916-1917).

Chief Signal Officer: Reports to the Secretary of War for the Fiscal Years 1898, 1900, 1901, 1902, 1913, 1914, 1915, and 1919 (Washington: Government Printing Office, 1898-1919, as indicated).

Childs, J. Rives: The history and principles of German military ciphers. [Unpublished monograph now in the Army Security Agency Library.]

———. German military ciphers from February to November 1918 (Washington: United States Government Printing Office, 1935). [Based on the preceding item.]

Clinton, Sir Henry: Papers (William L. Clements Library, Ann Arbor, Michigan.)

Fitzpatrick, John C. : The diaries of George Washington 1748-1799 (Boston, 1925).

———. The writings of George Washington (Washington: United States Government Printing Office, 1931-1944), Vol. XXX.

Friedman, William F. : A brief history of the Signal Intelligence Service. [Filed in the Office of the Director of Communications Research.]

———. Advanced military cryptography (Washington: Government Printing Office, 1935, revised 1943). [= AG TM 11-485]

———. American Army Field Codes in the American Expeditionary Forces in the First World War (Washington: United States Government Printing Office, 1942).

———. Analysis of a mechanico-electrical cryptograph (Washington: United States Government Printing Office, Part I, 1934; Part II, 1935).

———. A method of reconstructing the primary alphabet from a single one of the series of secondary alphabets (Geneva, Illinois: Riverbank Publication No. 15, 1917).

———. An application of the science statistics to cryptography: appendix tho [sic] Publication No. 22 (Geneva, Illinois: Riverbank Publication, unnumbered).

———. An application of the science statistics to cryptography: appendix tho [sic] Publication No. 22 (Paris: Librairie-Imprimerie Militaire Universelle L. Fournier, Riverbank Publication, unnumbered, 1922).

———. An introduction to methods for the solution of ciphers (Geneva, Illinois: Riverbank Publication No. 17, 1918).

———. Application des methodes de la statistique à cryptographie: appendice a la publication No. 22 (Paris: Librairie-Imprimerie Militaire Universelle L. Fournier, Riverbank Publication, unnumbered, 1922).

———. Elementary military cryptography (Washington: Government Printing Office, 1935 and 1943). [AG TM 11-484]

———. Elements of cryptanalysis (Washington: Government Printing Office, 1923, Training Pamphlet No. 3, Office of the Chief Signal Officer).

———. Field codes used by the German Army during the World War (Washington: United States Government Printing Office, 1935).

———, with Lenox R. Lohr: Formulae for the solution of geometrical transposition ciphers (Geneva, Illinois: Riverbank Publication No. 19, 1918).

———. General solution of ADFGVX Cipher (Washington: United States Government Printing Office, 1934). [Based on Elements of Cryptanalysis and Childs' History and Principles of German Military Ciphers]

———. L'indice de coincidence et ses applications en cryptographie (Paris: Imprimerie-Librairie Militaire Universelle L. Fournier, 1921). [Translation of the same paper published in English in 1922].

———. The index of coincidence and its applications in cryptography (Geneva, Illinois: Riverbank Publication No. 22, 1922).

———. The index of coincidence and its applications in cryptography (Washington: United States Government Printing Office, 1935). [Revision of the preceding].

———. Methods for the reconstruction of primary alphabets (Geneva, Riverbank Publication No. 21, 1918).

———. Methods for the solution of running-key ciphers (Geneva, Illinois: Riverbank Publication No. 16, 1918).

———. Military cryptanalysis (Washington: United States Government Printing Office, Part I, 1938 and 1942; Part II, 1938, 1941, 1943; Part III, two editions, 1939; Part IV, 1941).

———, Editor: Principles of solution of cryptograms produced by the I. T. & T. cipher machine (Washington: United States Government Printing Office, 1931).

———. Report on the history of the use of codes and code language, the international regulations pertaining thereto, and the bearing of this history on the Cortina Report, International Radiotelegraph Conference of Washington: 1927 (Washington: United States Government Printing Office, 1928).

———. Several machine ciphers and methods for their solution (Geneva, Illinois: Riverbank Publication No. 20, 1918).

———. Synoptic tables for the Star Cipher (Geneva, Illinois: Riverbank Publication, unnumbered, 1918).

———. Synoptic tables for the solution of ciphers and a bibliography of cipher literature (Geneva, Illinois, Riverbank Publication No. 18, 1918).

———. The Principles of indirect symmetry of position in secondary alphabets and their application in the solution of polyalphabetical substitution ciphers (Washington: United States Government Printing Office, 1935)

-----. The production and detection of messages in concealed writing and images (Geneva, Illinois: Riverbank Publication No. 50, 1918).

-----, with Charles J. Mendelsohn: The Zimmermann Telegram of January 16, 1917, and its cryptographic background (Washington: United States Government Printing Office, 1932).

Funston, Frederick: Memories of two wars (New York: Scribner's, 1911).

Giddings, Howard A. : Exploits of the Signal Corps in the War with Spain (Kansas City: Hudson-Kimmerly, 1900).

Gilden, Yves: The contribution of the cryptographic bureaus in the World War (Washington: United States Government Printing Office, 1935). [Reprinted from the Signal Corps Bulletin, 1933-1934]

Grant, Ulysses Simpson: Personal memoirs (New York: Charles L. Webster & Co., 1886).

Hall, Courtney R. : Development of the Office of Chief Signal Officer, Part I: 1917-1943. [OCSigO SPSEO-100, Project D-1]

Haswell, John H. : "Secret writing: the ciphers of the ancients and some of those in modern use."

Haswell, John H. : "Secret writing: the ciphers of the ancients and some of those in modern use," Century Illustrated Monthly Magazine, Vol. LXXXIV, Vol. LXXXV (1912-1913).

Historical sketch of the Signal Corps (1860-1941). (Fort Monmouth, New Jersey: Eastern Signal Corps Schools Pamphlet No. 32, 1942).

Hitt, Parker: Manual for the solution of military ciphers (Fort Leavenworth, Press of the Army Service Schools, 1916).

[Hurt, John B., translator]: Course in cryptography translated from the French work of General Givierge (Washington: United States Government Printing Office, 1934).

Kullback, Solomon: General solution for the double transposition cipher (Washington: United States Government Printing Office, 1934).

----. Statistical methods in cryptanalysis (Washington: United States Government Printing Office, 1935, revised, 1938).

Jefferson, Thomas: Papers, Vol. CCXXXII, item 41575 (reproduced in Articles on Cryptography and Cryptanalysis, reprinted from The Signal Corps Bulletin, Washington: United States Government Printing Office, 1942).

———. German cryptographic systems during the First World War (Historical Unit, Signal Security Agency, 1945). [IR 5096]

———. Japanese codes and ciphers 1917-1929 (Historical Unit, Army Security Agency, 1946).

———. The Achievements of the Cipher Bureau (MI-8) in the First World War (Historical Unit, Signal Security Agency, 1945). [IR 5094]

———. The Shorthand Subsection of MI-8 in the First World War (1917-1919) (Historical Unit, Signal Security Agency, 1945). [IR 5042]

Mendelsohn, Charles J.: An encipherment of the German diplomatic code 7500 (Washington: United States Government Printing Office, 1938).

———. Studies in German diplomatic codes employed during the World War: I. Code 18470 and its derivatives; II. The "Fuenfbuchstabenheft"; III. German methods of code encipherment (Washington: United States Government Printing Office, 1937).

[Moorman, Frank]: Final report of the Radio Intelligence Section, General Staff, General Headquarters, American Expeditionary Forces (Washington: United States Government Printing Office, 1935).

Myer, Albert James: A manual of signals: for the use of signal officers in the field (Washington, press unknown, 1864; second edition New York: D. Van Nostrand, 1866; other Van Nostrand editions 1868 (two), 1871, 1872, 1874; another Washington edition, press unknown, 1870; Government Printing Office editions in 1877 and 1879.

[Nolan, H. O.]: Memorization methods, specifically illustrated in respect to their applicability to codes and topographical material (Geneva, Illinois: Riverbank Publication No. 75, 1919).

Paltsits, Victor Hugo: "The use of invisible ink for secret writing during the American Revolution," New York Public Library Bulletin, Vol. XXXIX (1935).

Peckham, Howard H. "British secret writing in the Revolution" Michigan Quarterly Alumnus Review, 9 November 1938.

Permutation tables for the most important commercial codes (Washington: United States Government Printing Office, 1934).

Plum, W. R. : The Military Telegraph during the Civil War in the United States, with an exposition of ancient and modern means of communications, and of the Federal and Confederate cipher systems; also a running account of the War between the States (Chicago: Jansen, McClurg & Co., 1882).

Pratt, Fletcher: Secret and urgent (Garden City: Doubleday Doran, 1942).

Principles of solution of military field codes used by the German Army in 1917 (Washington: United States Government Printing Office, 1935). [The author was an officer (perhaps Captain Hitchings) in the British Code Solving Section, General Headquarters, British Expeditionary Forces, 1918.]

Rowlett, Frank B. : Further application of the principles of indirect symmetry of position in secondary alphabets (Washington: United States Government Printing Office, 1935).

Sherwin, Oscar: Benedict Arnold, Patriot and Traitor (New York: Century, 1931).

0 0 336

Sinkov, Abraham: The existence of alphabets having no interval repetitions (Washington: United States Government Printing Office, 1934).

———. Permutation tables involving a feature of non-transposability (Washington: United States Government Printing Office, 1934).

Van Doren, Carl: The secret history of the American Revolution (New York: Viking Press, 1941).

Vernam, G. S. : "Cipher printing telegraph systems for secret wire and radio telegraphic ccommunications," American Institute of Electrical Engineers Journal Vol. XLV (1926), 109-115.

Whitehead, Philip B. : Notes on the liaison service and the liaison intelligence service of the German Army during the World War (Washington: United States Government Printing Office, 1935). [Based on his report of 1919].

[Willson, Ruth]: Japanese U-Type codes [IR 4876].

[Yardley, Herbert O.]:

———. Brief outline of work covered by M. I. 8 for the year ending June 30, 1919.

———. Brief summary of work during last year [1926]. [IR 4159]

———. Brief summary of work during 1927 [IR 4159].

———. "Ciphers" The Saturday Evening Post, Vol. 203, 9 May 1931, 35, 144-148.

———. "Codes" ibid., 18 April 1931, 16-17, 141-142.

———. Crows are Black Everywhere (New York: Putnam's, 1945). With Carl Grabow.

——. "Secret inks" The Saturday Evening Post, Vol. 203, 4 April 1931, 3-4, 140-145.

——. Secrets of Japanese Diplomacy [never published]

——. The American Black Chamber (Indianapolis: Bobbs Merrill, 1931).