SRH-001

D4ISRE B.

SRH 001

ARMY SECURITY AGENCY

Washington, D. C.

HISTORICAL BACKGROUND OF THE SIGNAL SECURITY AGENCY

VOLUME TWO

WORLD WAR I

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 simply listed and added as an appendix to volume Three.

HISTORIAN, ASA
20 April 1948

HISTORICAL BACKGROUND OF THE SIGNAL SECURITY AGENCY

VOLUME TWO: WORLD WAR I

Contents

Chapter Page

HISTORICAL BACKGROUND OF THE SIGNAL SECURITY AGENCY

VOLUME TWO: WORLD WAR I

CHAPTER I. THE FOUNDING OF THE CIPHER BUREAU

A. The Situation at Mobilization[1]

The entry of the United States into World War I on 6 April 1917 found the Army ill-prepared both cryptographically and cryptanalytically to meet the great demands which immediately faced it. The only code in current use (the War Department Telegraph Code 1915) was

[1] As the narrative develops, reference will be frequent to the testimony of Herbert O. Yardley, the chief of the Cipher Bureau from 1917 to 1929. Specific documents will be cited as occasion demands, but mention should be made at this time of a group of his papers dating from the period 1919-1920 recently collected (1945) in a paper of the Historical Unit of the Signal Security Agency: The Achievements of the Cipher Bureau (MI-8) in the First World War (IR 5094), hereafter cited as Yardley, Achievements. In 1931 Yardley published a series of sensational articles and an even more sensational book, The American Black Chamber (Indianapolis, Bobbs Merrill, 1931), hereafter cited as Yardley, Black Chamber. The articles, all of which appeared in The Saturday Evening Post, were: "Secret Inks," 4 April 1931 (3-4, 140-145): "Codes," 18 April 1931 (16-17, 141-142); and "Ciphers," 9 May 1931 (35, 144-149). Both the articles and the book must be read with extreme caution. They were ghost-written for $1000, it is alleged, by one Clem Koukol, an engineer in the employ of the American Telegraph and Telephone Company (see note on the flyleaf of the copy of the book owned by Mr. William F. Friedman). See also Volume III, Chapter IV.

recognized as insecure,[2] if not compromised,[3] and there was no central bureau assigned to the functions of cryptographic compilation or cryptanalysis of enemy communications.

The responsibility for forming an organization to fill the needs of the War Department in matters pertaining to the solution of intercepted cryptographic material fell to Major Ralph H. Van Deman, General Staff Corps, then in the War College Division.[4] What plans were made prior to mobilization are unknown: the measures adopted in the emergency suggest that no plans at all were made, a point on which there is fortunately a complete contrast between the two World Wars. The War Department was forced to rely for cryptanalytic assistance at least for a time, on the volunteer efforts of a group of patriotic civilians. The fact that a major war had already been raging in Europe for nearly three years apparently had not much accelerated military preparations:

[2] The Assistant Secretary of State on 13 July 1917 transmitted to the Chief, Military Intelligence Section, General Staff, a paraphrase of a cablegram stating that the "British Government considered the War Department's methods of coding cablegrams were unsafe and a menace to secrecy" (see Memorandum for the Chief of Staff from the Chief, Military Intelligence Branch, dated 2 April 1918, a copy of which is now filed in IR 4328).

[3] The same memorandum states that a copy of the War Department Telegraph Code 1915 had been stolen in Mexico and that from various sources it had been reported that a copy was in the hands of the German Government, as also stated by Yardley, Black Chamber, 40.

[4] Later Director of Military Intelligence. Major General Van Deman is still living in 1945.

Indeed, the policies of the Administration prior to 1917 had been based on strict neutrality, a view which in those days evidently pervaded the War Department as well as public opinion.

B. The Riverbank Laboratories

An offer was received from an unexpected source. At Geneva, Illinois, a suburb of Chicago, there was in 1917 an institution known as Riverbank Laboratories, of which the name is somewhat misleading. The Laboratories had been founded not long before as a philanthropic enterprise by a man of means known as Colonel George Fabyan.[5] His plan was to establish at Geneva, an organization apparently somewhat similar in scope and purpose, though not in size, to the Institute for Advanced Study, more recently founded by the Bamberger family at Princeton. The staff consisted of scholars and scientists, whose sole duty was to engage in research in their respective fields. Among the subjects studied at Riverbank Laboratories were genetics and cryptography. The former need concern us only because in the Department of Genetics was a young scientist, Mr. William F. Friedman. Before 1917 he had taken only a mild interest in cryptography but he was soon to transfer his activity to that field and to make it his life work. In the Department of Ciphers at this time was Miss Elisebeth Smith, later Mrs. Friedman, who also has continued in cryptanalytic work ever since that ti

[5] His military title had been conferred on Mr. Fabyan some years previously by the Governor of Kentucky.

In addition to these two persons, mention should be made of Dr. J. A. Powell, formerly director of the University of Chicago Press, and of Dr. John Matthews Manly, at that time and until his death in 1940 Professor of English and Head of the Department at the University of Chicago. Professor Manly, though not a member of the staff of Riverbank Laboratories, was in close contact with the work there and was regarded for many years as a leading authority on literary ciphers.

The Department of Ciphers had been organized as an attempt to apply scientific procedures to the Shakespeare-Bacon problem. It was believed by Colonel Fabyan that in certain works of the late sixteenth and early seventecth centuries there might be found a biliteral cipher which would afford proof that Francis Bacon, Lord Verulam, was the author of the plays commonly attributed to William Shakespeare. No scientific results were obtained in this direction, but it was the good fortune of the Government that the staff at Riverbank was then engaged in cryptographic processes and also trained in the rigid techniques used in scientific research.

The claim is made by Yardley[6] that the "search for this cipher had given Mr. Fabyan's staff no real experience even in the elements of cryptography," a judgement certainly unjust to the Riverbank experts. It is true that they could have had no experience at all in current military traffic, since at that time, even within the Army itself,

[6] Yardley, *Achievements*, 7. He makes no mention of Riverbank in *The American Black Chamber*.

only a few officers had had the opportunity of examining actual intercepts. Yet the contributions which they soon made to the field of theoretical cryptanalysis suggest that they were well acquainted with the history and literature of cryptography—they could hardly have been novices in the early months of 1917.

To gain acquaintance with military cryptography from a firsthand source, Dr. Powell was sent to the Army Service Schools at Fort Leavenworth, where he attended the course then being given by Lieutenant Joseph O. Mauborgne[7] and brought back the current treatise · the subject, Captain[8] Parker Hitt's Manual for the Solution of Military Ciphers.[9]

The achievements of the Riverbank staff were threefold:

a. Intercepted materials were submitted for solution to the experts there by various departments of the Government until the Cipher Bureau was well established in the fall of 1917.

[7] Afterwards the Chief Signal Officer (1937-1941).

[8] Now Colonel, Signal Corps, Retired.

[9] Fort Leavenworth, Press of the Army Service Schools, 1916. Yardley is wrong in stating (Achievements, 7, note 13) that Mr. Friedman also attended this course.

b. A vigorous training program was inaugurated at Riverbank under the auspices of the War Department. A group of four officers was trained in cryptography[10] for six weeks in October-November 1917; a second group of some sixty officers was trained in January-February 1918; while the third, and last, group, consisting of seven or eight, was trained in March-April 1913. Mr. Friedman prepared the instructional material, gave the lectures, and directed the school, the first of its kind in American history.

c. Research was conducted in the theory of cryptanalysis and an extensive series of technical papers was published by the Laboratories. Most of these were by Mr. Friedman; except where otherwise stated, he is the author.

Riverbank Publications

No. 15 A method of reconstructing the primary alphabet from a single one of the series of secondary alphabets, 1917.[11]

No. 16 Methods for the solution of running-key ciphers, 1918.

No. 17 An introduction to methods for the solution of ciphers, 1918.

No. 18 Synoptic tables for the solution of ciphers and a bibliography of cipher literature, 1918.

[10] Until 1921, when Mr. Friedman coined the term cryptanalysis, it was customary to use the word "cryptography" indiscriminately for what are now termed "cryptography" and "cryptanalysis." A memorandum for the Chief of Staff from the Chief, Military Intelligence Division, dated 13 May 1918 (copy now filed in IR 4152) states that the officers sent to Riverbank Laboratories were to be trained in cryptography [i. e. as distinct from cryptanalysis] and that through error they were trained in solution. The War Department, however, set up no guides or limitations for this program, other than that six weeks would be devoted to instruction in cryptography. As it turned out, a good many of the students were later assigned to cryptanalytic duties.

[11] In spite of the number, this was the first in the series.

No. 19 Formulae for the solution of geometrical transposition ciphers, 1918.[12]

No. 20 Several machine ciphers and methods for their solution, 1918.

No. 21 Methods for the reconstruction of primary alphabets, 1918.[13]

No. 22 The index of coincidence and its applications in cryptography, 1922.[14]

No. 50 The production and detection of messages in concealed writing and images, 1918.[15]

No. 75 Memorization methods, specifically illustrated in respect to their applicability to codes and topographical material, 1919.[16]

Synotic tables for the Star cipher, 1918.[17]

[12] By Captain Lenox R. Lohr, CE, USA, and William F. Friedman.

[13] By Elizebeth S. Friedman and William F. Friedman.

[14] A French translation of this paper had appeared in the preceding year as L'Indice de Coincidence et ses Applications en Cryptographie. (Paris, Imprimerie-Librairie Militaire Universelle L. Fournier, 1921). This (together with its appendix: see below) was the first paper in the history of cryptanalysis to use statistical methods.

[15] After No. 22, the numbers were no longer consecutive. From No. 50 on, they were to deal with secret inks: from 75 on, miscellaneous subjects.

[16] By H. O. Nolan, Ph. D.

[17] This and the following were not numbered.

An application of the science statistics to cryptography: appendix tho [sic] Publication No. 22.[18]

The collaboration of Colonel Fabyan's staff with the War Department continued not only in the early months of the War but also after the Cipher Bureau had been established in Washington and was running smoothly. The impression is given by Yardley[19] that, once his unit was available, the decline in cooperation was rapid, but as may be seen from the dates of the training courses for officers, Riverbank was still doing work for the War Department as late as April 1918. In the next month Mr. Friedman was commissioned first lieutenant and sent to France, where he remained on duty in the Radio Intelligence Section, General Staff, General Headquarters, until April 1919.[20] Yardley further maintains that "in spite of repeated admonitions by Colonel Van Deman, Mr. Fabyan was unable or unwilling to suppress his penchant for a publicity which was recognized as detrimental to the best interests of the service." This charge Mr. Friedman feels was rather unwarranted and it is possible that this was only Yardley's way of eliminating Colonel Fabyan from the picture. There were, however,

[18] This English edition, and a French translation (Application des Méthodes de la Statistique à cryptographie: appendice à la publication No. 22) were both printed in Paris by the Librairie-Imprimerie Militaire Universelle L. Fournier in 1922.

[19] Yardley, Achievements, 8.

[20] He then returned to Riverbank, where he remained until 21 December 1920; his long connection with the Signal Corps began on 1 January 1921.

disadvantages in the arrangement quite apart from any personal friction that might have existed between Yardley and Colonel Fabyan: the distance from Washington to Geneva; the fact that the War Department was not paying anything for the Riverbank work and could not therefore control it closely enough; the growth of the Cipher Bureau in Washington, making available to the Government facilities paralleling those at Riverbank; and, finally, the commissioning of both Mr. Friedman and Dr. Powell, all tended to cause the emergency operation to cease functioning.

C. The Coming of Yardley

To return to the early months of the War, Major Van Deman in his search for experts to form the Cipher Bureau had found that the only Army officers known to be competent in the field of cryptography were Captain Parker Hitt and Lieutenants Joseph O. Mauborgne and Frank Moorman. All three, as has been stated in Volume One, Chapter VI, Section H, had been on the staff of the Army Service Schools at Fort Leavenworth; Captain Hitt had written the Manual for the Solution of Military Ciphers in 1916, and the others had filled important positions either as instructors or administrators in the Army Signal School, but, though their services were requested, none of the three served

Lieutenant Herbert O. Yardley

1917

during the War in a purely cryptological capacity in Washington.[21]

While it was unfortunate that neither Colonel Hitt nor Lieutenant Colonel Mauborgne could be assigned to duty in a cryptographic unit, the great demand for highly trained officers in all branches of the Army and the experience of both these officers in other Signal Corps activities fully justified their assignment elsewhere. The experience of World War I, however, clearly showed the wisdom of training in advance of mobilization a larger number of officers whose services would not be in demand for other assignments when war came.

The situation outlined above made it necessary, therefore, for Major Van Deman to seek his experts in the ranks of civilians. Aside from the staff at Riverbank, the first recruit was Mr. Herbert O. Yardley, who was commissioned a first lieutenant, Signal Corps Reserve, on 29 June 1917 and assigned to active duty on 5 July 1917.[22] His qualifications for this work were derived from the fact that since

[21] Of the other officers described as having proficiency in cryptography in the memorandum cited in Volume One, Chapter VI, Section H, none was so far as is known, associated during the War with cryptography. Moorman served as Chief of the Radio Intelligence Section, General Staff, in France; Hitt as Assistant Chief Signal Officer in France; Mauborgne as Chief of the Research and Development Division of the Office of the Chief Signal Officer. As such Hitt and Mauborgne had some contacts with code and cipher production but they were also concerned with other activities.

[22] The date of the establishment of MI-8 is given as 10 June 1917 in a memorandum for the Chief of Staff from the Director of Military Intelligence, Subject: Plans for MI-8, 16 May 1919 (copy in IR 4366) but the date of Yardley's commission was 29 June as stated. Since he was born on 13 April 1889, he was commissioned at the age of twenty-eight.

16 November 1912[23] he had been a code clerk and telegrapher in the State Department Code Room, where, according to his own statement he "developed knowledge and skill in the solution of codes." Such knowledge and skill in the solution of codes, of course, formed no part of his official duties at the State Department: his task there was cryptographic, rather than cryptanalytic, in character, since the State Department has never maintained an independent cryptanalytic unit but has regularly depended on the War Department for such services.[24] The relatively modest statement quoted above, which was written in 1919,[25] was expanded in 1931 into the first chapter of The American Black Chamber. When the extraneous material of a sensational character is removed, the story given in that chapter is a brief one.

While a code clerk and telegrapher for the State Department (1913-1917), Yardley conceived the possibility of solving cryptographic systems and began to study works on cryptography in the Library of Congress.[26] These proved to be of little help—he even speaks con-

[23] The initial salary was $900 per annum; the highest was $1440.

[24] From 1919 to 1929, as will be later described, it bore a share of the War Department expenses met in maintaining a cryptanalytic service.

[25] Yardley, Achievements, 5

[26] Since Yardley knew no other language but English, a point which he conceals, books in other languages were, of course, closed to him, and in the period of this activity, works in English were few and elementary. Moreover, the Library of Congress had not yet received the extensive Fabyan collection.

temptuously of Captain Hitt's Manual, though he neglects to name the author—but assignment to the night shift afforded Yardley time for independent study. Without authorization, he began an attempt to solve current State Department messages, copies of which were available to him as a code clerk. Two years after he had begun, he presented to his superior, an unnamed official[27] who had compiled the State Department code, an analysis which, it is claimed, shocked the superior out of his complacency. It should be pointed out, since Yardley fails to do so himself, that, if he had access to State Department cables, he also had access to the code book and presumably also to decodings. He creates the impression, of course, that the analysis was done without any previous knowledge of the system, but since he was a code clerk, he must have had the incalculable advantage of knowing much about the general features of the code, and probably like most code clerks, had memorized the most frequent groups. His achievement may therefore have been much less than he claims. He also alludes[28] to "friendly connections previously established," through which he "had no difficulty in obtaining copies of code and cipher communications dispatched by various embassies in Washington."

[27] According to a note in the margin of Mr. Friedman's copy of Yardley's Black Chamber, 29, this was David Salmon, Chief of the Codes and Records Division, State Department.

[28] Black Chamber, 21.

Upon the outbreak of war Yardley at once attempted, but in vain, to get a release from the State Department so that he might seek a commission. Only after a call upon Colonel George S. Gibbs,[29] Signal Corps, gained him an introduction to Major Van Deman at the War College, was the release obtained, and he was commissioned a first lieutenant in the National Army. How much of this story is fact and how much fancy can hardly be determined, but Yardley was able to convince Major Van Deman of his competence, and he conducted the work of the Cipher Bureau so satisfactorily that ultimately, though not until 1923, he was given the Distinguished Service Medal.

Lieutenant Yardley was assigned at once to take charge of all code and cipher work for the Military Intelligence Branch with the aid of two civilian clerks whom he does not name. They were, however, James E. McKenna and John C. Meath and will both appear again later in the story. Failure to give much credit to his associates is characteristic of the man in every period—the only war-time subordinate whom he names in his book is Dr. Manly, who had volunteered his assistance in March 1917,[30] though his services were not accepted until later in

[29] Afterwards Chief Signal Officer (1928-1931). General Gibbs was later unable to recall having ever met Yardley (testimony of William F. Friedman, October 1945).

[30] Yardley, Achievements, 6. This is probably an error for April.

September and then for a time only as a civilian. At the beginning Yardley's exact responsibility was not sharply defined, but he was expected to encode and decode all Military Intelligence messages, supply enciphering tables, and attack enemy codes and ciphers.[31]

The Adjutant General's Office should have been responsible for the work of encoding and decoding, but, on pleas of greater security, the Military Intelligence Branch set up its own facilities and staff for this purpose. Even though one of the two clerks, James E. McKenna, newly commissioned a First Lieutenant (afterwards Captain), was soon given charge of this phase of the work, the volume of traffic grew to such an extent that the time and efforts of the entire staff were consumed, and there was no opportunity for Lieutenant Yardley to engage in research, that is, to attempt to solve enemy codes and ciphers. As a partial remedy, Major Van Deman now invited Dr. Manly to come to Washington as a civilian; he was commissioned as a captain on 5 November 1917 and assigned to active duty three days later. It was at first intended by Major Van Deman that Lieutenant Yardley would specialize in codes and Captain Manly in ciphers, but these two officers, deeming it undesirable that such a differentiation of function be made, suggested that a section be organized to deal with secret communications of all

[31]. Memorandum for the Chief of Staff from the Director of Military Intelligence, Subject: Plans for MI-8, 16 May 1919 (one copy is filed in IR 4366, another in the files of the Director of Communications Research).

sorts and that this section serve all departments on an equal basis and be located in Washington. The emphasis upon the location may have been the result of a desire to eliminate the Riverbank Laboratories. Conferences were held with representatives of the Navy and State Departments and of the Department of Justice, and later with the Postal Censorship and other official and semi-official organizations. These organizations agreed to send to the new section such cryptographic problems as came to their attention.[32] Lieutenant Yardley was in charge of the section, in spite of the fact that Captain Manly outranked him, at least after the date of the latter's commission.[33]

The unit was first set up at the War College, but in the spring of 1918 it was moved to new quarters at 1156 15th Street (near M Street) Northwest; in July 1918 to 1330 F Street, Northwest, the site of the present National Press Club; and in 1919, it occupied quarters in still another building at 7th and B Streets, Northwest.

D. Personnel

Though expansion was necessary, additional personnel were not added until the need for them was pressing. The second chapter of The American Black Chamber describes Yardley's first attempts to organize a Cipher

[32] Yardley, Achievements, 6.

[33] Manly's commission as a captain dated from 5 November 1917, while Yardley was not promoted to that rank until 27 February 1918. This information is on file in the Demobilized Personnel Records Branch, Adjutant General's Office, memorandum dated 28 August 1945, 1st indorsement.

Bureau at the War College.

> In the name of Van Deman I at once sent cables to London, Paris and Rome, urging that pressure be brought upon our Allies to send cryptographers to Washington competent to teach students in the solution of German military codes and ciphers. Also to send by pouch a few hundred examples of such messages and all available exposition on their solutions.
>
> The reply was that examples of German military code and cipher intercepts together with explanations were in the pouch, but that cryptographic instructors could not be spared.[34]

It was only in 1918 that Captain J. A. Powell was sent to France in order to obtain information concerning British and French methods. He conferred as early as 28 February 1918 with the Chief of the Second Section, General Staff (then Colonel Dennis E. Nolan), who wrote on that date to Colonel Van Deman in Washington as follows:[35]

> After conference with Captain Powell, I am satisfied that much good would result from a close liaison between the cipher section now being developed in your office and that at these headquarters. Captain Powell has looked over the situation, seen the general system of work of both the British and French, and has a clear understanding of the needs of our cipher section. One of those needs to which I wish to call special attention is that of mutual co-operation between all offices engaged in cipher work. We have arranged for keeping in touch with the British and French, but feel that much can be done in your office to better advantage than anywhere else.
>
> A large cipher section in Washington could be made very valuable. You can employ code and cipher experts who, for one reason or another, are unable to come to France. Modern radio-

[34] Yardley, Black Chamber, 37.

[35] The letter is now filed in IR 4151. The signature is countersigned with the initials of Lieutenant Colonel Frank Moorman, Chief of the Radio Intelligence Section, General Staff (see below, Chapter VIII).

> telegraphy will enable you to intercept many of the Continental code and cipher messages and thus have them while fresh. Our stations here will also copy many of these messages and send them to you by mail. We will also send you notes as to any solutions found or suspected as probable here, and, in addition, suggestions from the French and British cipher offices. If you, for your part, would send suggestions as to kind of code or cipher and any solutions discovered by your office, we will distribute them to the French and British, and make use of them in our own office.
>
> The British have a big cipher office in London, and another at their headquarters in France. The French have perhaps the biggest cipher office of all, in Paris. We are slowly developing such an office of our own. If to these four could be added a really big and efficient office in Washington, it seems to me we should soon be handling practically all the diplomatic and special codes and ciphers. These are all regarded as of great importance to us, and I cannot too strongly urge your most cordial support with all the facilities and men you are able to procure.

Additional evidence is available to show that the search for personnel was still going on in March 1918. On 21 March 1918 Colonel C. French, of the British Embassy in Washington, wrote Colonel Van Deman a letter enclosing a memorandum on the solution of codes, in which he included the following paragraphs:[36]

> I should like, if you will let me, to emphasize in this connection the importance of selecting the right kind of brain to do this work. For research of this kind requires an active, well trained and scholarly mind; not mathematical but classical. As an illustration of the right kind of man, one of my experts has suggested to me the name of a well known American scholar, Louis Herbert Gray of 25, Brimmer Street, Boston, Mass.[37] It is of course

[36] A copy of this correspondence is now filed in IR 4153.

[37] Professor Gray has been for many years Professor of Linguistics at Columbia University.

> undeniable that there may be a few men who, without having had university training[38] or without having acquired a great reputation for palaeographical work, nevertheless are well suited for this work. But there is no method of discovering such people.[39] Therefore the only test applicable is that of scholarship.
>
> When once you have got together two or three men of the right class they will soon map out the work of themselves. It is for this reason among others that detailed instructions of how to deal with the solution of codes would really be of little use, for whole volumes on this subject would be useless to the wrong kind of man, and the right man must and will prefer to work out his own line: and in so working would become an expert.

Colonel Van Deman courteously replied on 18 April 1918—the delay is significant--including the following paragraph on MI-8 personnel:

> You will, I am sure, be interested to know that while we do not think that men of University education possess any monopoly of logical thinking and power of analysis, we have not discriminated against them in organizing our Cipher Section. Among its members are four persons who are or have been university instructors, five who hold the degree of Ph. D., and three others who have had a thorough collegiate training.[40]

Yardley with characteristic dogmatism dismisses the problem of personnel in the following way:[41]

[38] Is this a direct reference to Yardley? There may be much more behind this letter than meets the eye.

[39] Precisely the most difficult problem before the Signal Security Agency in World War II.

[40] The instructors were probably Captains Manly, Beeson, and Mendelsohn and Miss Rickert. These four and Captain Knott were probably the holders of the Ph. D. degree. All will presently be identified.

[41] Black Chamber, 38.

> Judging from the letters I found in the files of the War College, nearly every one in the United States had dabbled in ciphers. The authors of these letters were either offering their services, or had a new and indecipherable cipher that the government should immediately purchase.
>
> From among the former I quickly selected a few scholars who appeared to have a superficial knowledge of ciphers, and ordered them commissioned.[42]
>
> The spectacle of an eager thin-faced lieutenant, surrounded by a group of scholarly captains, was indeed a noteworthy sight, and I was obliged to submit to a great deal of good-natured raillery. However, they seemed to enjoy my energetic illiteracy, which they kindly termed "native intelligence," and I was amused at their eagerness to master the principles of cryptography. . . . most of them were dismal failures.

He goes on, however, to mention Dr. Manly in a favorable light, but the latter is the only subordinate of Yardley's to be mentioned by name in The American Black Chamber.

A course of instruction in codes and ciphers was prepared, on the basis of Hitt's Manual for the Solution of Military Ciphers, as is clear from the lesson sheets in the files of the Signal Security Agency.[43] Having spoken contemptuously of Hitt's Manual at an earlier point, Yardley could hardly now acknowledge his indebtedness to Hitt.

Ultimately, subsections were organized for specialization—five of them in all:[44]

[42] At this time he was a first lieutenant.

[43] IR 4293.

[44] These subsections are called "bureaus" in a Brief Outline of Work Covered by M. I. 8 for the year ending June 30, 1919, a copy of which is now in the files of the Director of Communications Research

a. Code and Cipher Compilation (in Washington)
b. Communications (in Washington)
c. Shorthand (in New York)
d. Secret Ink (in New York and Washington)
e. Code and Cipher Solution (in Washington)

Just how many different persons were employed by MI-8, as the Cipher Bureau was called, cannot now be determined with certainty, but there are several sources from which names of employees can be derived:

a. A card file[45] contains the names of 270 persons. It does not, however, include fourteen persons whose names are known from other sources, and it is clear that it lists not only members of MI-8 but also frequent visitors on official business.

b. Two routing slips[46] give the names of the supervisors.

c. A payroll containing names of the persons employed on 1 May 1919.[47]

d. Records of the Shorthand Subsection[48] contain the names of six full-time employees, not listed elsewhere.

[45] Now in the files of the Director of Communications Research. See letter of Yardley to Major C. M. Millikin (10 December 1924) in IR 4160. The list of employees to which Yardley refers in a letter to an unknown person (ibid.), dated 20 October 1925, has apparently not survived. It contained the names of all who worked in MI-8 between August 1917 and 31 January 1919 and occupied eight legal-size pages.

[46] One is in IR 4474 attached to a letter dated 12 July 1918. The other, in IR 4494, is undated, but it is apparently later, since Yardley's name is omitted. It therefore must have belonged to the period when he was in Europe (November 1918—April 1919).

[47] Now in the files of the Director of Communications Research.

[48] For the evidence, see below, Chapter VI.

By combining all this evidence, and subtracting names which appear more than once, a total of 287 different persons is reached, but this does not mean that MI-8 ever had a strength that large. The late Lieutenant Colonel A. J. McGrail recalled in 1945 that there were fewer than 200 persons in MI-8 and this is confirmed by a memorandum for the Chief of Staff from the Director of Military Intelligence, dated 16 May 1919,[49] which states that the peak was reached in November 1918, when there were 18 officers, 24 civilian cryptographers, and 109 typists and stenographers, a total of 151 persons. This figure would, of course, not include any one who by that time had ceased to be employed in the Bureau, and there must have been many officers, at least, who had been sent to France—Captain Yardley was one.[50]

In addition to Captains Yardley, Manly, and McKenna, already mentioned, the following officers are known to have been on the staff of the Cipher Bureau at one time or another:

Captain David H. Stevens, who signed correspondence in the absence of Captains Yardley and Manly, and is now connected with the Rockefeller Foundati n.

Captain Thomas A. Knott, one of Manly's former pupils, now Professor of English at the University of Michigan.

[49] Copy now in IR.4366.

[50] F.B. Thomas, for example, was trained for work in France (see letter of Captain Manly to F. W. Allen, 5 November 1918, in IR 4204). See also a letter of Major James L. Collins to Yardley, dated 21 January 1921 (IR 4161), which refers to a Mr. F. B. Hyde of Washington, who may have worked in MI-8.

STAFF OF CIPHER BUREAU (MI-8), 1919

Left to Right

Seated: Captain David H. Stevens; Captain John B. Manly; Captain Thomas A. Knott; Captain Charles H. Beeson; Captain Charles Mendelsohn.

Standing: Captain Robert H. Marvin;/ Lieutenant Paul B. Woodfin; Captain Frederick B. Luquiens; Lieutenant William M. Barlow; Lieutenant George W. Bicknell; Captain Emmet K. Carver; Captain Hatheway; Lieutenant Robert O. Klotz; Captain Herbert S. Spencer.

At the time this photograph was taken Captain Yardley was absent on a trip overseas.

Captain Charles J. Mendelsohn, head of the German Code Solving Unit, afterwards a Reserve Officer engaged in part-time work for MI-3 in New York while Professor of History at City College. He was about to be called to work in the Signal Intelligence Service in 1937 but died before reporting for duty.

Captain Charles H. Beeson, now Professor Emeritus of Latin at the University of Chicago.

Captain Herbert S. Spencer, who was recommended for the commission by Mr. F. W. Allen, head of the Shorthand Subsection.

Captain Robert H. Mervin, a teacher of Spanish in the New York schools. He was also recommended by Mr. Allen.

Captain Frederick B. Luquiens, responsible for the solution of codes.

Captain A. E. Prince, who was in charge of Code Compilation.

Captain T. M. Childs, in the Communications Subsection. He must not be confused with First Lieutenant J. Rives Childs, who never became a captain.

Captain J. A. Powell, formerly of Riverbank Laboratories, who made a trip to France in an effort to obtain assistance from the British and French. He died about 1925.

Captain Emmett K. Carver, who was in charge of the Secret Ink Laboratory in New York, and was afterwords Professor of Chemistry at Harvard.

First Lieutenant A. J. McGrail, in charge of the Secret Ink Laboratory in Washington. Afterwards Professor of Chemistry in Providence College, Rhode Island, he was called to active duty in 1941 and remained continuously on duty until his sudden death on 30 April 1945. He was awarded the Legion of Merit posthumously in Section III, War Department General Orders No. 65, 9 August 1945, "for exceptionally meritorious conduct in the performance of outstanding services from May 1941 to April 1945." At the time of his death he was a Lieutenant Colonel and Chief of the Laboratory Branch, Signal Security Agency.

First Lieutenant G. C. Chandlee, who was a chemist.

First Lieutenant D. F. J. Lynch, who was also a chemist.

First Lieutenant Hugo S. Campagnoli.

First Lieutenant Henry D. Learned, who is known to have been on duty as a Naval Officer in the Office of Naval Communications in World War II.

Second Lieutenant P. S. Danner, a chemist.

Second Lieutenant Edward F. Snyder, also a chemist.

Second Lieutenant Lee West Seller.

Lieutenant Paul B. Woodfin, who remained with the Military Intelligence Division after the removal of MI-8 to New York in August 1919.

Lieutenant Ben Stinchfield.

Lieutenant A. R. Dodd.

Lieutenant [illegible] Klotz, first name unknown.

The following is a list of the persons known to have been employed as "cryptographers," i. e. as cryptanalysts, as they would now be called:

Mrs. Charlotte F. Baldwin (Spanish).
Mr. W. M. Barlow.
Mr. Paul Bernard
Mr. Claus Bogel (Mexican).[51]
Mrs. Clara S. Brokaw (German).
Mr. Henri S. Brown (afterwards commissioned).

[51] Mr. Bogel remained with MI-8 in New York until he joined the Office of Naval Intelligence in 1923.

Mr. Kent J. Brown (afterwards commissioned).
Miss Anna F. Carter.
Mr. Paul Dutko.
Miss Mary L. E. Francis
Mr. John Hornicek.
Miss Dorothea B. Jachens (Spanish).
Mr. Robert H. Keener (afterwards commissioned).
Mr. Samuel Kroesch.
Mr. Frederick Livesey.[52]
Mr. Elias Avery Loew.[53]
Miss Laura E. McClary.
Mrs. James J. Martin.
Mr. B. Q. Morgan.[54]
Mr. John S. Norris (afterwards commissioned).
Mr. John Rice, Jr.
Miss Edith Rickert.[55]
Mr. Martin B. Rund.
Mr. Austin E. Spear.
Mr. Edgar H. Sturtevant.[56]
Miss Anita Thomas.
Mr. John C. Weigel.
Mr. Victor Weiskopf (Mexican).[57]
Miss Ruth Willson (Spanish)[58]
Mr. Austin W. Works (afterwards commissioned).

[52] Mr. Livesey remained with MI-8 until 1923. It is he who figures in Chapter XV of The American Black Chamber as "Charles Mundy."

[53] Later Professor of Palaeography at the University of Oxford.

[54] Now Professor of German at the University of Chicago.

[55] For many years Miss Rickert was Professor of English at the University of Chicago.

[56] Now Professor of Linguistics at Yale University.

[57] Mr. Weiskopf was not officially an employee of MI-8 but of the Department of Justice. He had begun his interest in cryptography while an agent of the Department in Texas during 1916. He remained with MI-8 when moved to New York in 1919, and after the closing of the office in 1929 conducted a rate stamp and coin business until his death in 1940.

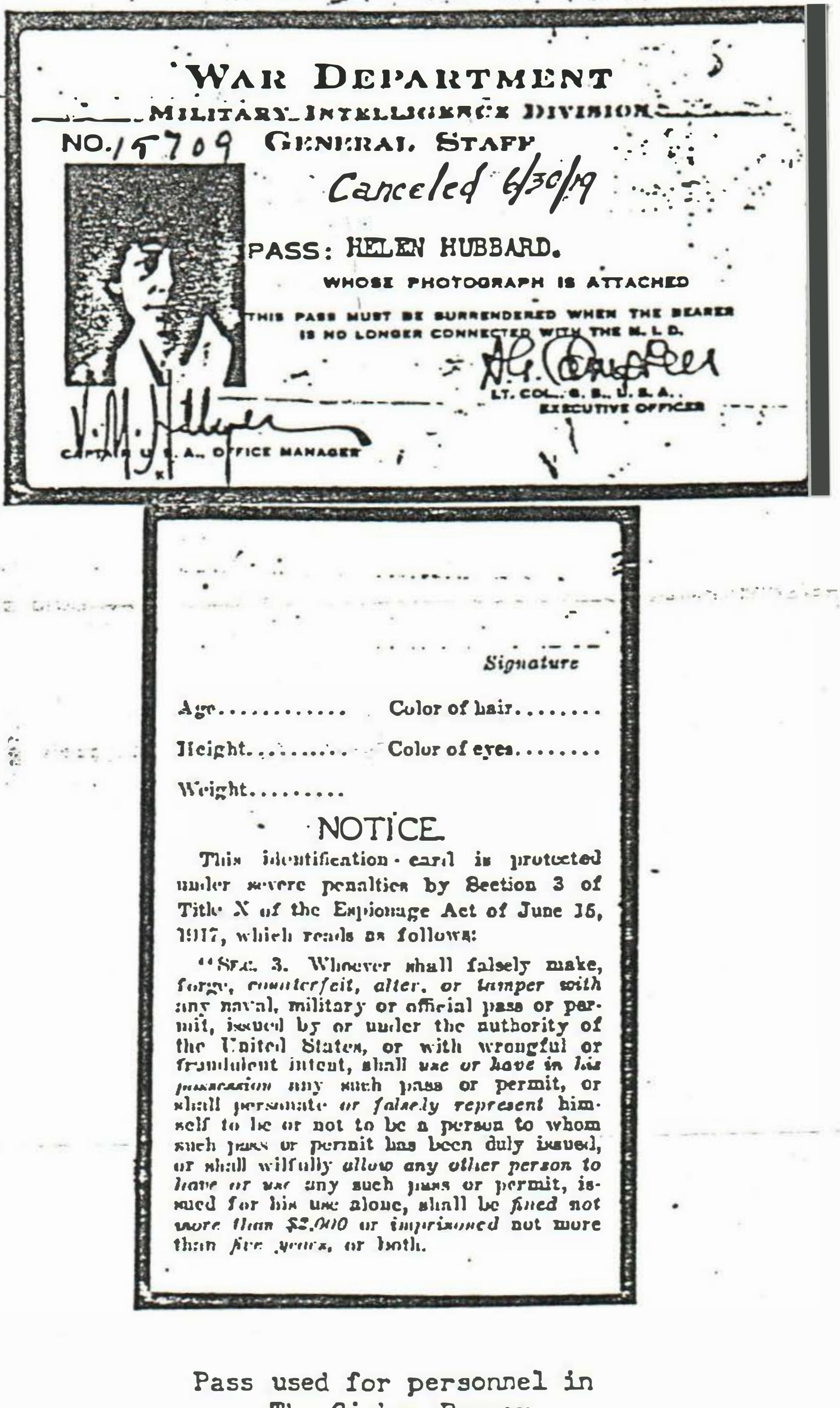
[58] Miss Willson likewise remained with MI-8 until 1929.

In addition to these persons, there were a number of others who occupied supervisory positions, of whom nothing else is known. These were:

Mr. Harry E. Burt.
Mrs. Bessie B. McQueen.
Miss Marion E. Woodward.
Mr. Frank J. Kennedy.
Miss Ruth Lansing.
Mr. Hulbert.
Mr. Theobald.[59]

The payroll mentioned above shows that, of the civilians on the list, one received $1,600, ten received $1,400, and one only $480 (apparently custodial personnel), the remainder received $1,200 a year. A bonus of $120 was given to 46 of these persons, but not to sixteen whose appointments were evidently too recent to have earned such a bonus. The 62 civilians on the payroll received as salary a total of $74,880 and as bonus a total of $6,200, the grand total being $82,080. This payroll is, however, that of 1919, after considerable reduction in force had taken place, and does not account for the Shorthand Subsection, for the Secret Ink Laboratories, or for military personnel. It seems clear that the total payroll of the Cipher Bureau for the entire period of its existence was probably considerably less than $500,000.

[59] It is interesting to note that among the other employees was Mr. Stephen Vincent Benet, afterwards a celebrated American poet, who was on the staff for only seven days in November 1918.



WAR DEPARTMENT

MILITARY INTELLIGENCE DIVISION

NO. 15709 GENERAL STAFF

Canceled 6/30/19

PASS: HELEN HUBBARD.

WHOSE PHOTOGRAPH IS ATTACHED

THIS PASS MUST BE SURRENDERED WHEN THE BEARER IS NO LONGER CONNECTED WITH THE M. I. D.

LT. COL., G. S., U. S. A.,
EXECUTIVE OFFICER

CAPTAIN U. S. A., OFFICE MANAGER

Signature

Age............ Color of hair........

Height.......... Color of eyes........

Weight.........

NOTICE

This identification-card is protected under severe penalties by Section 3 of Title X of the Espionage Act of June 15, 1917, which reads as follows:

"SEC. 3. Whoever shall falsely make, forge, *counterfeit, alter, or tamper with* any naval, military or official pass or permit, issued by or under the authority of the United States, or with wrongful or fraudulent intent, shall *use or have in his possession* any such pass or permit, or shall personate *or falsely represent* himself to be or not to be a person to whom such pass or permit has been duly issued, or shall wilfully *allow any other person to have or use* any such pass or permit, issued for his use alone, shall be *fined* not *more than $2,000* or *imprisoned* not more than *five years*, or both.

Pass used for personnel in
The Cipher Bureau

CHAPTER II. CODE AND CIPHER COMPILATION IN WASHINGTON

A. Organization of the Unit

In the period between the Civil War and the First World War all code and cipher compilation had been the work of the Chief Signal Officer, with the notable exception of the so-called "Cipher of the War Department," published by authority of The Adjutant General in 1904.[1] The Chief Signal Officer[2] had prepared the only code available in 1917 for current use, the War Department Telegraph Code 1915, which had been based on insecure principles[3] and was believed to have been compromised even before the outbreak of hostilities.[4] Even so, this code was continued in use throughout the War, chiefly because

[1] See Volume One, Chapter VI.

[2] See the Report of the Chief Signal Officer to the Secretary of War 1919 (Washington, Government Printing Office, 1919), p. 12, which lists as one of the functions of the Administrative Section "the supervision of the preparation of codes" but this was a pre-war arrangement dating from 4 November 1915 and was a function not much exercized in Washington during the War. The Signal Corps did, however, control code compilation in France (see the Report, pp. 536-538, and below Chapter VII).

[3] It was a one-part code but it must be admitted that in 1915 two-part codes were a novelty.

[4] For the evidence, see note 2 of Chapter I.

there was, at least until July 1918, no alternative to it.[5] No code had been compiled for use in an emergency, and none was being prepared. Moreover, there was in existence no unit charged with such a responsibility. The so-called "Tactical Code," at best only an abridgment of the War Department Telegraph Code 1915, had never been completed, and the "Interdepartmental Code" had been merely recommended as a desirable project: funds were never appropriated.

The Signal Corps did not relinguish its responsibility for code compilation, but the Military Intelligence Division decided to prepare a code for its own communications with military attachés. This was done, and later this product of MI-8 was used also for other War Department purposes. Thus it came about that what compilation was done in Washington during the War was performed by the Military Intelligence Division, not by the Signal Corps, though the latter did control code compilation in France.

The Code Compilation Subsection of MI-8 was organized in 1917 while the Cipher Bureau was still at the War College.[6] This came about as the result of a communication from the Assistant Secretary of State who on

[5] The encipherment tables used with this code will be described later.

[6] Yardley, Black Chamber, pp. 39-47. A more trustworthy account of this subsection, also by Herbert O. Yardley, appears in the history of MI-8 which is the first document in Yardley, Achievements, 12-14.

12 July 1917 transmitted to the Chief, Military Intelligence Section,[7] General Staff (then Colonel Van Deman), a paraphrase of a cablegram stating that "the British Government considered the War Department's method of coding cablegrams was unsafe and a menace to secrecy.[8]

The source of this information was not, of course, at once disclosed to the United States Government. It seems probable that the British Government was itself subjecting War Department traffic to cryptanalytic attack,[9] though it is not impossible that the American

[7] This same unit was afterwards known also as the Military Intelligence Branch and Military Intelligence Division. As the narrative develops, care will be taken to refer to the organization by the proper title in each instance, but it is not always possible to do so, particularly in the case of events which cannot be dated exactly. "There was one reason why we were so late in getting our system across the ocean. Up until August [1918] we were a branch of a division. At first thought, you would not realize that that was an obstacle, as there was only one superior between us and the Chief of Staff. If we only had one superior interested in what we were doing, it would have been different, but he was running a division made up of unrelated branches, which was unfortunate. The Chief of the Division would not know and would not know anything about what we were doing." Quoted from remarks by Brigadier General Marlborough Churchill at a lecture by Lieutenant Colonel Frank Moorman, 13 February 1920 (SIS 311.7, 1919-1940, Case No. 897).

[8] See Memorandum for the Chief of Staff from the Chief, Military Intelligence Branch, 2 April 1918, a copy of which is now filed in IR 4328.

[9] See William F. Friedman and Charles J. Mendelsohn, The Zimmermann Telegram of January 16, 1917, and its Cryptographic Background (Washington, United States Government Printing Office, 1932), p. 26, for a statement that in 1917 the British Government was probably reading American diplomatic traffic.

authorities in France had divulged to the British the nature of the American system. In any case, the expression of a lack of confidence in the cryptographic system used by an ally is a delicate matter, and it is probable that the British Government acted only when the danger to the security of British systems counterbalanced the desirability of reading American traffic.

The news must have been startling to the Military Intelligence Section when it was received: Yardley is probably not indulging his penchant for sensational exaggeration when he writes,[10] "No wonder the memorandum from the Assistant Secretary of State frightened the War Department! The Chief of Staff made a personal request for a prompt report." His official history,[11] however, merely states that shortly after the organization of MI-8 "it was learned that the Germans were reading confidential messages passing between Generals Pershing and Bliss and the Washington office."

In any case, the Code Compilation Subsection was then organized and placed under the direction of Captain A. E. Prince.[12] His name is not mentioned in The American Black Chamber, but the following

[10] Black Chamber, 40.

[11] Achievements, 12.

[12] Yardley, Achievements, 12; see also a letter of Yardley dated 25 December 1918 (IR 4149).

paragraph[13] can refer only to him:

> I promptly chose a man in the State Department Code Room whom I considered best qualified to follow my directions, and tempted him with a commission. I wished him to take immediate charge of a subsection which would compile codes and ciphers. I had no intention of being overwhelmed with the details of this work for I had much else before me. In a very short time the subsection was efficiently functioning with ten clerks assisting the man who had been put in charge. The arrangement was wholly satisfactory for the work was being done well, and I need to devote no more than an hour each day to reviewing some of the more important details.

The work of the Subsection ultimately included the preparation of encipherment tables for use with the War Department Telegraph Code 1915, and the compilation of six codes, as follows:

Military Intelligence Code No. 5[14]
Military Intelligence Code No. 9
The French Geographical Code
Geographical Code No. 2
The Casualty Code
The Ideal Correspondence Code

B. Encipherment Tables

When the War Department Telegraph Code 1915 was first issued, it was intended that code groups would be, when desired, enciphered by the use of a substitution table known as "The Table for Forming Five-Letter Code Words." Such a table was actually issued sometime in 1916 and was still in force in the office of The Adjutant General as late

[13] Ibid. pp. 40-41

[14] No Military Intelligence Codes were numbered 1-4 or 6-8.

as 2 April 1918[15] for the encipherment of communications other than those classified as secret. All confidential and semi-confidential communications from this source were thus being transmitted in an insecure code, which was almost certainly compromised, and enciphered by insecure tables not changed, so far as evidence now available indicates, since 1916.

The action of The Adjutant General in permitting this breach of good security regulations was not the result of necessity, for the Code Compilation Subsection had prepared, nearly a year before, a newer and better table for supplanting that issued in 1916. This is described as a "modification of the British, the State, and the Navy Department systems for enciphering codes.[16] It was intended for use by the Military Intelligence Section, General Staff, for enciphering all confidential[17], code messages between The Adjutant General of the Army and General Pershing, and between the Chief, Military Intelligence

[15] See Memorandum for the Chief of Staff from the Chief Military Intelligence Branch, Subject: Coding and Ciphering Cablegrams, dated 2 April 1918, par. 4 (copy in IR 4328). This memorandum bears the intials of H. O. Yardley and is therefore to be regarded as his dictation.

[16] Ibid. par. 3.

[17] The word "confidential" may here have been used in a general sense, rather than precisely as a classification lower than "secret". The word "secret" was apparently first adopted as a standard classification on 14 December 1917 in Change No. 6 to Compilation of Orders, par. 176 and was written into Army Regulations, 330-5[sic] on 22 January 1921. This information has been supplied by the Historical Division, War Department Special Staff, 9 April 1946.

Section, General Staff, and all intelligence officers and military attaches, and was to be changed at frequent intervals. As a matter of fact The Adjutant General did use this new and better table for secret cablegrams but not for messages of lower classification. Accordingly, a new directive was prepared for The Adjutant General, dated 4 April 1918, which read as follows:

> The Secretary of War directs that "Table for Forming Five-Letter Code Words" be discontinued as a means of enciphering all coded cablegrams between The Adjutant General of the Army, the Commanding General of the Expeditionary Forces in France, the Commanding General of the American Forces in England, and General Bliss; that secret tables, to be changed frequently, furnished by the Cipher Section, Military Intelligence Branch, Executive Division, be used for enciphering secret cablegrams between the foregoing, and that other messages be enciphered by another set of confidential tables also to be changed frequently. These two sets of tables will be delivered in person by an officer of the Cipher Section, Military Intelligence Branch, Executive Division to The Adjutant General of the Army at intervals of two weeks to be transmitted to the foregoing offices.[18]

Curiously enough, while these negotiations were taking place, the Chief, Military Intelligence Section, received from the Secretary of the General Staff a message transmitting a request from General Tasker H. Bliss, as follows:

> 1. Your attention is invited to the following extract from cablegram Number 74 from General Bliss:
>
> Paragraph 3. Please arrange to furnish a special perfectly safe code for confidential communications between General John J. Pershing and myself.

[18] Copy now filed in IR 4328, also bearing Herbert O. Yardley's initials. Par. 6 of the memorandum cited in note 12 states that The Adjutant General had been consulted and concurred.

2. The following reply has been sent to General Bliss this date:

Reference Paragraph 3 your 74 special code will be sent by a commissioned officer in near future.

3. The Chief of Staff directs that you prepare the necessary code and that you deliver it to the Secretary of the General Staff for transmission to General Bliss by a commissioned officer.[19]

Instead of compiling a new code or a separate cipher sheet for use between General Bliss and General Pershing, Captain Yardley consulted the Secretary of the General Staff (Colonel P. P. Bishop) and also Major Wilson of the General Staff. It was decided that the plan set forth in the directive of 4 April cited above would satisfy General Bliss' requirements, and no action was taken.[20] It should be pointed out that the task of compiling a code for an emergency such as this would have been beyond of the powers of the Code Compilation Subsection, which had then been at work on the preparation of Military Intelligence Code No. 5 for nine months and needed three months more to complete it.

Though the old "Table for Forming Five-Letter Code Words" was recognized as insecure and was prohibited for use in enciphering code messages sent to France, it was, surprisingly enough, continued in force for communications with the Commanding Generals of the Panama,

[19] Memorandum for the Chief of the Military Intelligence Section from the Secretary, General Staff, 3 April 1918, copy now filed in IR 4328.

[20] See Memorandum signed H. O. Yardley, 9 April 1919, copy now filed in IR 4328.

Philippine, and Hawaiian Departments. Not until August 1918 did the Code Compilation Subsection prepare a new encipherment table for this correspondence.[21]

C. Military Intelligence Code No. 5

This code, the first on which the Subsection began to work, was completed on 1 July 1918[22] and was printed at the Government Printing Office in the same year. Except for the great weakness that the bulk of the vocabulary was one-part in arrangement, this compilation marked a distinct advance over the previous codes used by the War Department.

Each group consisted of a pentagraph conforming to one of the following patterns:

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

The two-letter differential was used, every group having two vowels and two consonants and another letter which, of course, might be either. Pasted inside the front cover were the three mutilation

[21] See Memorandum for the Chief of Staff from Chief, Military Intelligence Branch, Subject: *Cipher sheets for Commanding Generals, Panama, Philippines and Hawaiian Departments*, 9 August 1918, copy now filed in IR 4328; and Memorandum for the Adjutant General of the Army from the Executive Assistant to the Chief of Staff, same subject, 10 August 1918, copy now filed also in IR 4328.

[22] Yardley, *Achievements*. 12.

tables, one for each pattern. The instructions (i-ix) were generally in accord with more recent practice, except that permission was given to include whole paragraphs of plain text in a coded message, provided that the encoded paragraphs did not discuss the same topics as those in plain text.

The code was sectional in that there was a general vocabulary (1-495) and three sections containing, respectively, the 365 days of the year, a numerical table for cardinal numerals (all numerals to 500 and many higher), and a numerical table for ordinals (all from 1st to 500th). No other sections appeared. The arrangement was one-part in the general vocabulary and two-part in the other sections. This made it necessary for the groups in the sections to appear also in the general vocabulary out of their alphabetical position, in order to provide a decode for them. Moreover, there were on every page, at the bottom, ten groups for the following frequent plain equivalents:

comma
the suffix "ing"
the suffix "ing" [sic]
paragraphs (s)
period
quote
semicolon
spell
spelling ends
unquote

These were also two-part in character and the groups therefore also had to appear on the pages of the vocabulary in their normal alphabetical sequence. In addition, on many pages variants were provided for very frequent groups; e. g., the main entry for the letter A was ABACE, but there were also the variants ABHIK, ACEHO, HAHFO, QACEN, and ZABUY.

These were not printed in the columns but in the blank space between the columns.

The serial numbers run from 01000 to 99999, which makes it appear at first glance that there are 99,000 groups in the code book, but this is illusory, since many of the possible serial numbers are omitted, in irregular pattern. Sample sequences are as follows:

01000	01100
01002	01101
01004	01102
01006	01103
01008	01104

On each page there are two columns with 48 groups each. The total number of groups is therefore 495 pages x 96 groups = 47,520 groups the maximum number permitted by the three permutation tables. The variants in the margin and at the bottom of the pages, as well as the groups in the sections, may be disregarded in computing the total, since each of them must appear in the main vocabulary which serves as a decode for the special groups.

The following statement appears in Yardley's Achievements:[23]

> This book . . . would have served its purpose well for a long time but for the fact that other organizations of the Army which had been permitted to use the book misused it in such a way as to destroy its security.

Against this statement it may be pointed out that other witnesses apparently did not believe the code compromised: it remained in

[23] P. 12

current use for military intelligence purposes until 1934 when the classification was lowered from SECRET to CONFIDENTIAL, and the book was reissued on 1 September 1934 with a new title-page made by pasting over the old a sheet bearing the following title: *War Department Confidential Code No. 1 (formerly Military Intelligence Code No. 5) SIGCOT*. This reuse of old material was justifiable, of course, only because of the lack of adequate funds to prepare new compilations.

D. *Military ntelligence Code No. 9*

Work on another code of the same general type, *Military Intelligence Code No. 9*, was initiated with certain improvements in plan and under pressure of necessity work was hastened to such a degree that the volume was ready for use on 2 December 1918.[24]

The improvements mentioned consisted of the adoption of the two-part principle throughout. While this was the only basic change, it was an important one, since it resulted in giving the code much greater security than had been inherent in the one-part features of *Military Intelligence Code No. 5*. The decode had 495 pages, each with two columns of 48 groups each, making a total of 47,520 groups, exactly

[24] Yardley, *Achievements*, 12-13. The implication there made is that a copy was taken by Yardley to France and was used there by him. It is known that it was used by the late Lieutenant Colonel McGrail, then a First Lieutenant, for encoding a few messages which in 1919 he sent for Secretary Baker from France (see Yardley, *Black Chamber*, copy of Mr. William F. Friedman, p. 40, marginal note of A. J. McGrail).

the same number as appeared in the earlier code. The code groups conformed to the same general pattern as those of Military Intelligence Code No. 5. The encode had several preliminary sections:

a. Days of the year
b. Cardinal numbers (1 to 500 and many higher)
c. Ordinal numerals (1st to 500th)

There were no variants printed in the margins or at the bottom of the pages, but frequent ideas had several groups assigned to them in the normal sequence: e. g., A had ten variant code groups.

All copies of Military Intelligence Code No. 9 were recalled about 1923, but it developed that the copy which had been issued to the office of the military attaché in Tokyo was supposed, according to careful investigation, to have been burned to ashes during the Tokyo earthquake and fire. While this investigation seemed to be conclusive, there remained a reasonable doubt in the minds of the authorities in the Office of the Chief Signal Officer. The other copies were stored in the vault in the Munitions Building and after a decade Military Intelligence Code No. 9 was reissued, still with the classification of SECRET, on 1 April 1933, with the new title-page made by pasting over the old a sheet bearing the following title: War Department Staff Code No. 2 (Formerly Military Intelligence No. 9), with the short titles SIGSYG (encode), and SIGPIK (decode). This reissue of old material was also the result of financial stringency.

E. The French Geographical Code

The Code Compilation Subsection produced two codes for use in France only. The first of these was known as the French Geographical Code, but the name was somewhat misleading: the code was French only in that the plain equivalents were all geographical names taken from maps of France. A cablegram from General Tasker H. Bliss, dated 10 June 1918, had suggested to The Adjutant General the preparation of a list of code words for all geographical[25] names in sections of France where military operations were then taking place, based on a French map of the scale 1-100,000. This was desirable because the codes then being used in France (see Chapter VII) did not provide for place names. As a result of this request a French geographical code was approved in a memorandum for The Adjutant General of the Army, from the Chief, Military Intelligence Branch, dated 1 August 1918. Three hundred copies were to be printed, each to be registered and given the following distribution:

50 copies to the Commander in Chief, American Expeditionary Forces
58 copies to The Adjutant General of the Army
20 copies to the Chief, Military Intelligence Branch
other copies to military attaches and special representatives.

A memorandum of 8 August 1916 directed the Chief, Military Intelligence Branch, to proceed with the printing of this code at the Government Printing Office.[26]

[25] The original copy of the telegram (filed in IR 4330) reads here "geological" but the meaning is clear.

[26] See IR 4330 for all these memorandums.

This code, which was finished 1 October 1918, is one-part and is provided with both five-letter and five-digit groups, so that it could be used in conjunction with other codes using either letters or digits. There are 10,800 code groups, of which 9,723 have plain equivalents, the remainder being blanks for addenda, arranged throughout the book at irregular intervals.

The plain equivalents are entirely made up of French geographical names "taken from a strip of the map of France (on a scale of 1;200,000) extending twenty-five miles on either side of the battle front as it existed on July 10, 1918, as well as from the Amiens, Paris, Lille, and Chalons areas." The names of the principal towns and cities throughout the remainder of France were also included in the list. The distinguishing feature of the letter code groups is the use of a double vowel in each group. There are three forms: (1) vowel-consonant-vowel-vowel-consonant; (2) consonant-vowel-vowel-consonant-vowel; and (3) consonant-vowel-consonant-vowel-vowel. The letter groups begin with ABAA and end with VUIKY. Though this code was to be used only in France, where the requirement of the cable companies that letter code groups should be pronounceable would not be effective, the code groups nevertheless met the requirement. (It was then customary to join two groups together, and send them as one group, which would then be charged for as one word. This practice was then allowed by the cable companies in transmitting messages to all points except those in the

United States, Alaska, Canada, and Mexico.)[27] . . .

Three mutilation tables are provided in the front of the code book, one for each of the three types of code groups.

Accompanying the five-letter code groups are five-digit code groups to be used alternately, but never without first enciphering them by a method to be supplied. These groups range from 00000 to 35997, with eclectic omissions. The digit groups are identical with those employed in other War Department code books, except those in Military Intelligence Code No. 5. That code contains none of the numbers which have been used in the French Geographical Code and consequently no confusion could result.

Encipherment could be applied to the code groups following any prescribed method employed with any code for which the French Geographical Code was used as a supplement.

F. Geographical Code No. 2

Geographical Code No. 2,[28] a new code made necessary by the

[27] On this question of permissible groups in international cable and radiotelegraphic language, see William F. Friedman, Report on the History of the Use of Codes and Code Language, the International Telegraph Regulations pertaining thereto, and the bearing of this history on the Cortina Report, to the International Radiotelegraph Conference of Washington: 1927 (Washington: United States Government Printing Office: 1928).

[28] Geographical Code No. 2 (Washington, October 1918). Work was on 17 October 1918, but the book was not ready for distribution until 15 November 1918.

changes in the front, was mimeographed in October 1918 as a supplementary code to be used in connection with any current code book, and was also one-part, with five-letter or five-digit groups, of which 26,742 had plain equivalents and 138 were blanks for addenda and 5 indicators, totalling 26,885 code groups. The plain equivalents were again entirely made up of French geographical names taken from "French maps scale 1:200,000 and covering the area beginning with the Battle Line as it existed September 15, 1918, north and east taking in all of Belgium, a small portion of Holland bordering on the Belgian Frontier; and Germany from the Belgian-French Frontier to about 25 miles beyond the Rhine." A map on page ii shows the exact territory from which the names were drawn.

The principle of the two-letter differential was employed in the construction of all the code groups which were either (1) consonant-vowel-consonant-consonant-vowel or (2) consonant-vowel-consonant-vowel-consonant in form. Each group therefore had two vowels and three consonants. If all consonants and all vowels are used, it is possible to have 28,880 combinations of five letters, while still maintaining the two-letter differential. Only about 27,000 geographical names were used, however, so all of the possible code combinations were not used. The first code group was BABAL and the last XOZYP. The pronounceability of the code groups, whether sent singly or in pairs, again satisfied, unnecessarily, the regulations of the cable companies.

This code contains a single Mutilation Table, a distinct advance over the three-part table necessary in the preceding code.

The five-digit code groups, ranging from 07500 to 83448 with eclectic omissions, were to be used as alternatives to the five-letter groups, but never unless the entire message was in digits. The main code book used for the body of the message would determine the manner in which code groups from this code book are enciphered.

It will be recalled that the French Geographical Code contained code groups employed by no other code--all groups having double vowels—and that this distinguishing characteristic made the code groups from that code immediately recognizable in traffic. Geographical Code No. 2 did not possess that feature. Therefore, indicators, five in number, were provided to designate what group or groups were taken from this code.

The indicators were all high—93758, 93812, 93973, 93985, 93987—but the normal code groups were lower, the last one being 83448. If the indicators were placed in the ninety-three thousands to facilitate decoding by making possible easy recognition of groups taken from Geographical Code No. 2, then this would correspondingly also aid the enemy cryptanalysts by showing them that a shift to other groups was occurring in the message. This weak point could have been eliminated by using lower numbers.

In the Introduction is a list of "modifying terms, articles, adjectives and prepositions" in an abbreviated form, covering almost seven pages, which are for the purpose of aiding the encoder and decoder when such abbreviations appear on a map or elsewhere.

G. The Casualty Code

The Casualty Code, as planned in the Code Compilation Subsection, must not be confused with another code of the same name compiled by the Code Compilation Section, General Headquarters, American Expeditionary Forces, in France.[29]

This code on which work was begun on 16 September 1918,[30] was intended to provide a substitute for the War Department Telegraph Code 1915 for the special purpose of casualty reports. The older code required from five to seven or eight groups to report a single casualty.

> The Casualty Code was planned to comprise a long list of names, necessary numbers and dates, the name of every individual organization in the Army, including all branches, together with a number of provisional organizations contemplated at that time, and a vocabulary sufficient for the purpose for which the code was intended. The names, dates, numbers, and vocabulary were not especially difficult to compile, but when an effort was made to secure a complete list or organizations, it developed that no department in Washington had such a list. Considerable difficulty was therefore experienced in obtaining the information necessary, but it was obtained. Probably this section had in its possession on November 15 data with regard to the various branches of our Army, which, had it been properly tabulated, would have formed the most complete and comprehensive catalogue of our military resources in existence.

[29] See Chapter VII.

[30] All evidence concerning this code is taken from Yardley, Achievements, 13-14.

The work on this book was nearly completed, when the signing of the armistice, and the necessity for the immediate compilation and production of Code No. 9, rendered further work undesirable. The materi l gathered at that time, however, is still in the possession of M.I 8[31] and would be available if the publication of such a code ever became necessary.[32]

H. The Ideal Correspondence Code

On 2 December 1918 instructions were given the Code Compilation Subsection to prepare a "pocket code" for use by military attachés when on duty away from their regular posts and for other special military agents in the field, particularly those who would go into enemy territory with the Army of Occupation. The necessity for concealing the true nature of this code resulted in the adoption of a subterfuge: the code was entitled the Ideal Correspondence Code, the publisher was stated to be the "Ideal Code Company, New York City," and a statement was made on the title-page that the purpose of the compilation was to disguise "commercial, journalistic and general correspondence." Actually, the code was a product of the Code Compilation Subsection and was printed at the Government Printing Office, though in type and format it was completely different from ordinary publications of that office.

The two-letter differential was used throughout, all groups being of the consonant-vowel-consonant-vowel-consonant formation. A mutilation

[31] It was probably later destroyed as obsolete material.

[32] Yardley, Achievements, 13-14.

table appears on the inside of the front cover. The arrangement is two-part, and both encode (called "code") and decode are printed in the same volume in a peculiar fashion. When the book is held so that the title-page is right side up, the right-hand pages alone contain the encode. The decode is printed on the left-hand pages but upside down, so that in decoding one must turn the book upside down, in which case the decode pages will also be on the right hand. The reason for such an arrangement was this: the code clerk could turn the pages with his left hand, using his right hand for writing. The left arm could cover the page on the left, concealing the printing on that page.

There is a numerical table on pages x-xvi providing for all ordinals and cardinals up to 500 and some higher than that. Each page contains 42 groups in each of two columns, and there are 148 full pages (12,432 groups), one page with 25 groups, and 532 groups for numbers, a total of 12,989 groups in all. Some of the plain equivalents are provided with variants: in one instance (cipher indicator) there are as many as 51, though more normally three is the usual number for very frequent words. Some of the plain equivalents reveal the military origin of the code, e. g. WARUH = "Commander, s, in Chief, Amex Forces." Unusually good provision is made for suffixes to be added to roots. Though the code embodied a number of ingenious features, it was never used very much and never was closely imitated.

A "distortion table" (merely an encipherment table based on monoalphabetic substitution) is given in the Introduction (p. vii)—one of the very few, if not, indeed, the only example in American cryptography of the publication of an encipherment table in the same volume as a code.

I. The AT&T Printing Telegraph Cipher

There remains to be discussed one important development in the field of code and cipher compilation in which M. I. 8 figured during the War, though not on its own initiative. This was the printing telegraph cipher designed by the engineers of the American Telephone and Telegraph Company which was the subject of a lengthy controversy between the Riverbank Laboratories, the Military Intelligence Division, the Signal Corps, and officials of the Company.[33]

The engineers of the Company had begun in the spring of 1916 to work on the problem of devising a printing telegraph cipher,[34] and they were later, during the War, requested by Colonel John J. Carty, Signal Corps, to continue their researches into the possibility of obtaining secrecy by some modification of the printing telegraph.

[33] See Report of the Chief Signal Officer to the Secretary of War 1919, p. 139. The story is told in detail in "Extracts from correspondence relating to solution of A. T. and T. Printing Telegraph Cipher," a document prepared in 1943 by Mr. William F. Friedman and now in the files of the Director of Communications Research.

[34] Letter of R. D. Parker, Telegraph Development Director, AT&T, to William F. Friedman, 16 March 1944, filed with "Extracts" cited in preceding note. See also a paper by G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," in American Institute of Electrical Engineers Journal, New York, February 1926, Vol. 45, pp. 109-115.

In an effort to speed the transmission of traffic between Washington and France, considerable attention had been given by the Signal Corps to the possibility of enemy interception of cables, since it was desired to send messages in plain text by this means. The conclusion drawn from careful study was that, though difficult, enemy interception of the cables was not beyond the range of possibilities and that "the printing telegraph system, without further invention, could not be depended upon to safe-guard a message sent in plain English against the efforts of an enterprising enemy with proper scientific knowledge and equipment.[35]

The AT&T engineers, cooperating with Lieutenant Colonel J. O. Mauborgne, Signal Corps, conducted a series of experiments, and finally devised apparatus whereby a message written in plain English could be quickly enciphered, printed in plain letters similar to the printing of a typewriter, and transmitted over a telegraph line and received at the distant end. This printed cipher telegram, copied upon the deciphering machine, would finally appear in plain English.

> "Many forms of this system are possible, each adapted to different circumstances. For some cases the best plan is as follows: Write the message to be sent first in plain English in the office where it originates; copy this message upon a typewriter keyboard which perforates a long paper tape. These perforations appear on the tape in telegraphic code and enciphered. The tape thus perforated and enciphered is sent to the

[35] *Report of the Chief Signal Officer to the Secretary of War 1919*, p. 139.

telegraph office, where it is passed through a transmitter and thus sent over the wire to the distant end, at which point it again appears, still in cipher, in the form of a perforated tape. This tape is delivered to its destination, where, being put through the deciphering machine, the message appears in plain English.

The sending of the enciphered message over the wire is accomplished as quickly as the sending of an ordinary message. The enciphering of the message or the deciphering of it is accomplished as quickly as an ordinary message can be copied upon a typewriter.

Manifestly a device such as this overcomes all of the delay caused by enciphering and deciphering, and if proved to be reliable in operation and if the enciphered message is in secure form, a method has been developed whereby the time of enciphering and deciphering is saved and the transmission of the message over the telegraph wire is accomplished as rapidly as the transmission of a message in plain English. In addition to this, the safety of the message is otherwise enhanced because of the reduction in the number of those who must possess the cipher and because the message in passing through the telegraph office is in the form of a strip of paper arbitrarily perforated."[36]

In his Report for the year 1919 the Chief Signal Officer stated that the speed and reliability of this apparatus had been thoroughly tested over lines carrying messages of the most confidential character from Hoboken to Washington and from Washington to Newport News. The cipher produced by this apparatus when used in accordance with the method devised by the Signal Corps was said to have successfully resisted all the efforts of cipher experts to solve it. These statements, while doubtless true at the time they were prepared for inclusion

[36] Quoted from the Report cited.

in the Report, antedated the conclusion of the matter, since the solution of test messages was not achieved until 8 December 1919.

It will be well to summarize the story in some detail. On 11 June 1918 Mr. Gherardi, an official of the Company, sent to Colonel George Fabyan, of Riverbank Laboratories, seven challenge messages with the following comment:

> I am not a cipher expert and would not presume to say what can or cannot be done, but should you and Professor Friedman decipher messages Nos. 1, 5, 6 and 7, I shall feel that I owe you both a good dinner. I have no doubt that you can decipher Nos. 2, 3 and perhaps 4. These, however, as you understand, are not the arrangement which we propose.

The next important document is dated 8 August 1918 and is a letter from the Director of Military Intelligence to the Chief Signal Officer:[37]

> 1. The mechanical means of enciphering messages with an arbitrary, meaningless running key of 999,000 letters, provided no two messages are enciphered at the same point on the tape as explained to Major Mauborgne, Signal Corps, and Captain Yardley, Military Intelligence Branch, by officials of the American Telegraph and Telephone Company, is considered by this office to be absolutely indecipherable.

Message No. 2 of the Gherardi challenge messages was solved on 22 March 1919, message No. 3 four days later; when message No. 4 was solved does not appear in the record but it was certainly solved.

When solutions of the three were announced, the proponents of the indecipherability of the printing telegraph cipher refused to accept this as proof of the insecurity of the system and claimed

[37] Since this document bears the initials of H. C. Yardley, it seems clear that he dictated for the signature of his superior.

that the three solved message had not been enciphered in accordance with the method actually used by the Signal Corps. Not being in a position to contest that claim, since the challenge messages were prepared by the Company and not the Signal Corps the Riverbank Laboratories continued to press for more test messages which would actually conform to the Signal Corps method. Finally, after much negotiation, they received on or about 6 October 1919 a set of 150 cipher tapes constituting "the total number of messages actually sent in one day by the four stations of the Printing Telegraph System . . . operated by the Signal Corps between Washington, Norfolk, New York City and Hoboken."

That at this date Colonel Mauborgne was still strongly of the opinion that attempts at solution would be unsuccessful is indicated by the following quotation from his letter to Colonel Fabyan dated 28 November 1919:

> . . . You know I never have admitted that you had any method for solving this cipher, and, as in the case of all these academic debates, you will give to produce the proof! ! ! . . . As you recognize, the by-products of this investigation are highly worth while even though there never was, as there never will be, a real solution.

Colonel Mauborgne was, however, mistaken, for on 8 December 1919, Colonel Fabyan was able to wire a report of success. Colonel Mauborgne now was willing to admit his error; for he wrote two days later:

> Your telegram of 5.00 p. m. of the 8th was received here about noon, the 9th. Your force is undoubtedly to be congratulated upon the decipherment of the messages which you announce in your telegram. I take off my hat to Riverbank!

and again on 29 December 1919:

> . . . You have done a great work and your contention of last March is sustained - that the method of using the printing telegraph cipher as used last year by the Signal Corps was decipherable. This is, perhaps, the toughest individual cipher you have ever had to tackle. To the victor belong the spoils!

The letter just quoted in part makes clear the precise limits of the achievement of the Riverbank solution:

> I . . . did not receive, until my return on Saturday, the little tape message which you had prepared, which demonstrated beyond a shadow of a doubt, that you had not only broken the one hundred fifty messages prepared on the printing telegraph according to the method used last year by the Signal Corps, but that you had also reconstructed the running key which enabled you to prepare messages to be sent to the Chief Signal Officer, to General Churchill and to myself, all of which were this morning put through without mishap, on the cipher machine here, using our key tapes according to existing methods.

The significance of the solution deserves some further comment. There is no doubt that it represented by far the most important cryptanalytic achievement of any American group; it is probable that it was far in advance of anything that had been done hitherto by any group elsewhere. That it took only two months to accomplish the feat was something that was made possible only by the preceding eight months of special studies by the small group under W. F. Friedman's leadership consisting of two or three cryptanalysts and a similar number of clerks. As a matter of fact, had it not been for a single error made by a clerk in the very first stages of the preparation of the material for solution, an error which remained undetected for over a month and a half, the solution would probably have been reached in a few days instead of about sixty. The principles underlying the solution, developed at that time, remained practically unchanged.[38]

After the solution had been accomplished, the principles and method were explained to Colonel Mauborgne and to Major Yardley. The latter undertook to "improve" the system by superimposing a method of encoding the indicators, which hitherto had been sent in clear. The method was submitted to Riverbank and a relatively simple solution was found, much to the chagrin of M. I. 8. Thereafter no further work on the whole problem was done by either the Signal Corps or M. I. 8. The need for the machines having passed, they were discontinued from service and sent to storage.

In conclusion it should be pointed out that the weakness of this system lay in part in its use of a double rather than a single tape of the type now known as "one-time," and that originally the engineers of the AT&T Company had wanted to use the single tape but were prevented from doing so by pleas, on the part of the Army officers who were shown the system, that the production and distribution of such keys would involve insuperable difficulties. Consider the following statements taken from the letter of R. D. Parker already

[38] They were embodied in technical papers on file in the files of the Director of Communications Research.

cited:

> I was "in" on this from the start and the printing telegraph cipher system, as originally proposed, contemplated the use of a random non-repeating key tape. We were disappointed at the first demonstration of this single key system to an officer of the Signal Corps in that he considered the problem of preparing and distributing key tapes insurmountable. I argued with him a bit at that time on the value of the secrecy obtained by the single key system. It is remembered that this argumentative attitude was out-of-line with the feelings of my bosses.

However, nobody seems then to have pointed out what still remains true, that one of the major objections to any one-time system is the impracticability of intercommunication, by this means, among a large number of stations. Were it not so, the one-time tape system would have reached full development long before 1943 and the SSA would not have had to adopt the two-tape system as an interim measure. In elaborating the latter, full advantage was taken of security principles based upon the 1919 solution at Riverbank Laboratories. It is doubtful if the interim system would have been adopted had it not been for these early studies, which therefore served a highly useful purpose in World War II.

J. Miscellaneous Material[39]

Cryptographic bureaus receive from the general public from time to time plans and proposals for new cipher systems which to their

[39] In this section will be discussed certain activities in the field of code and cipher compilation which were not carried on by the Code Compilation Subsection of M. I. 8 but rather by the Signal Corps.

inventors appear to be "absolutely indecipherable." Most of these prove upon close examination to be either too simple for security, or too complicated for practical use under the conditions of military communication. The United States Army has, as a matter of fact, never accepted a proposed system coming from an outside source, though doubtless it would do so in the event that a meritorious suggestion were made. The main reason why outside suggestions have proved so useless has been the fact that security has prevented the general public from gaining any knowledge of the conditions on which all cryptological development must be based. Consequently, inventors are doomed to failure.

During the War considerable correspondence passed between Riverbank Laboratories[40] and MI-8 concerning the running-key type of cipher. In this case the key consisted of intelligible text, usually taken from an ordinary book or novel.[41] The cryptanalysts at Riverbank had devised means of solving such a cipher, but as the Chief, Military Intelligence Branch, stated in a memorandum for the Chief of Staff dated 13 May 1918,[42] no enemy or neutral country was known to be using a running-key cipher, and a simpler and more rapid method of attack had been devised in MI-8 some months previously.[43] This type

[40] See Chapter I, Section B.

[41] See Riverbank Publication No. 16, cited above on p. 6.

[42] Copy now filed in IR 4152.

[43] Despite this statement, the method was not simple.

of cipher was regarded, however, by Colonel Parker Hitt and Lieutenant Colonel Joseph O. Mauborgne as indecipherable, and they challenged Captain Yardley to solve some sample messages. The challenge was accepted, and in the first week of December 1917 Yardley was able to solve the messages.[44] Accordingly, Colonel Mauborgne advised General Pershing not to use this type of cipher unless combined with transposition.

Another device investiaged by the Signal Corps, not by M. I. 8, at first appeared to have some merit. It was in the form of a typewriter of the type-wheel model. A key disk was so arranged that the copy obtained was a miscellaneous lot of letters which could be deciphered on any other machine of the same type, provided the operator was furnished with a key disk corresponding to the one used for enciphering the message. Arrangement of the plugs in these disks could be changed at the will of the correspondent's concerned. It was soon found, however, that there was a certain sequence to the letters and there was but little trouble in solving the cipher, if an expert was supplied with the number of messages written with the same key disk.[45]

[44] See letter of Yardley to General M. Churchill, 15 September 1919, in IR 4332; other correspondence in IR 4953; and a Memorandum for the Chief Signal Officer, from the Chief, Military Intelligence Branch, 15 March 1918, in which Colonel Van Deman reports that he had advised the Intelligence Officer, American Expeditionary Forces, that the system was not indecipherable. See Report of the Chief Signal Officer to the Secretary of War 1919, p. 240.

[45] This was solved by Lieutenant Friedman in France.

Another proposed system, known as the "H. J. Atchley Secret Code System,"[46] was in reality a cipher system using a device of cylindrical shape. A random-mixed cipher alphabet was written on an external cylinder, twenty-six other cipher alphabets on an internal cylinder, both cylinders being so arranged as to revolve on a common axis, with the inner alphabets made visible, one at a time, through an opening.

The H. G. Saal Company of Chicago desired in June 1917 to manufacture the device in quantity for Government use, at a cost of $10 each, if 5,000 devices were purchased, or at $5 each if 10,000 were purchased, but the company refused to give the Government the right of exclusive use.

Even so, it appeared that the Government might accept the proposal. Captain J. O. Mauborgne, then still at Fort Leavenworth, wrote that so far as he could see, the device was indecipherable. The same opinion was expressed by Captain W. N. Hughes, Jr., who visited the company and gave a favorable report on every detail except the price, which he thought should not exceed one dollar each. His recommendations were approved by the Chief, Military Intelligence Section, War College Division, in a memorandum dated 15 August 1917, addressed to the Chief Signal Officer, but the device appears never to have been adopted. It may be pointed out that it involved little more security than a cipher cylinder devised by the Confederates during the Civil War.

[46] The evidence on this system is filed in IR 4334.

The system known as the "Interlocking Cipher," submitted by James W. Pryor on 25 May 1918,[47] was rejected as too complicated. George H. Parke, of Williamsport, Pennsylvania, on 16 January 1918[48] submitted to the Department of Justice a sample message in what he described as "an absolutely new cypher built along entirely new lines. Absolutely, no person on earth knows anything whatever about it except myself." Whether any attempt was made to solve the sample message is not known.

[47] See IR 4335.

[48] See IR 4931.

CHAPTER III. THE COMMUNICATIONS SUBSECTION OF THE CIPHER BUREAU

The Communications Subsection of the Cipher Bureau, though not officially organized as such until somewhat later, grew out of the first operations performed by any personnel of the Cipher Bureau. When Herbert O. Yardley was commissioned first lieutenant on 10 June 1917, he was given two civilian assistants and was expected to carry on the work of encoding and decoding all Military Intelligence traffic, as well as of preparing tables for encipherment and the solution of enemy codes and ciphers.[1] The function of encoding and decoding, under the regulations then existing actually belonged to The Adjutant General's Office, but for reasons of greater security, it was assumed by the Military Intelligence Branch. The result was that the volume of traffic to be processed was soon so great that the time of Lieutenant Yardley and his two assistants was entirely consumed in this relatively mechanical task. First Lieutenant James E. McKenna was

[1] The chief source of information concerning this subsection is Yardley's paper: *M. I. 8, Code and Cipher Section,* the first of the documents collected in Yardley, *Achievements* (5-6, 14-15). This paper includes all the data contained in his *Brief Outline of Work Covered by M. I. 8 for the Year Ending June 30, 1919* (copy now in the files of the Director of Communications Research) and in a Memorandum for the Chief of Staff from the Director of Military Intelligence, Subject: *Plans for M. I. 8*, 16 May 1919 (*Ibid.*, another copy in IR 4366). A single paragraph on the work of the subsection appears in *The American Black Chamber* (48).

soon after appointed to take charge of this work,[2] but how many assistants he ultimately had is unknown.

For two years the Communications Subsection maintained cable and telegraphic communication with about forty military attachés and intelligence officers in foreign countries and with hundreds of intelligence officers stationed in all camps and important cities within the United States. The office was open for business twenty-four hours a day. Special wire connections made possible exceptionally fast service, particularly with Paris, the most important center, from which cable messages are said to have been often received "within less than a half hour after the time of sending." This interval must obviously have been that between the time of filing and the time of receiving the dispatch, and doubtless did not include the time needed for encoding and decoding the message.

Approximately half of the volume of messages transmitted was sent in cryptographed form, the rest, surprisingly enough, in plain text. No messages were sent, it would appear, in unenciphered code: only enciphered code and plain text were used.

From September 1918 to May 1919, the subsection sent and received 25,000 messages, containing 1,300,000 words. Yardley was impressed with the fact that the use of code had effected great economies in

[2] If he is the unnamed man mentioned by Yardley (Black Chamber, p. 48) he had had experience as a code clerk for the State Department.

telegraphic expenses: the last paragraph of his account of the Communications Subsection states that it was estimated that the saving to the Government was at least fifty percent of what the cost would have been, had only plain-text messages been sent.

EXCURSUS ON WOODROW WILSON'S COMMUNICATIONS WITH HOUSE

Though not a part of the activity of the Communications Subsection of the Cipher Bureau, the communications systems which President Woodrow Wilson used for correspondence with his friend and confidential agent, Colonel E. M. House, are of interest because they illustrate the type of cryptography used by eminent statesmen of the period. The chief source of our information is Ray Stannard Baker's voluminous biography, Woodrow Wilson, Life and Letters (Garden City: Doubleday Doran), especially volumes V (1935) and VI (1937).

The earliest reference to cryptography in Baker's book concerns the compromise of a State Department code (V, 204), and appears in a letter to Ambassador Walter H. Page, 14 September 1914:

> I cannot tell you how chagrined both the Secretary of State and I are that the leaks should have occurred of which your discussed cable of the other day spoke. We have for some time been trying to trace them, for they have occurred frequently, and we are now convinced that our code is in the possession of persons at intermediary points. We are going to take thorough going measures.

In spite of the many burdens which the President bore, he was serving as his own code clerk, at least for some of the messages. Mrs. E. T. Brown, a visitor to the White House, wrote on 21 February 1915 to her friend Mrs. H. S. Mitchell (V, 260):

> The poor President has had an epidemic of cipher dispatches—one to make last night, which took him until nearly midnight, and two to read today which took him every spare moment between Church, & driving and dinner--and when he came to dinner the second was not quite worked out yet.

On 30 January 1915 (V, 307) Colonel House, as he was leaving for Europe, set up a special code in which proper names were used as code equivalents for prominent statesman and countries, e. g.

plain text	code word
Allies	Wilmot
Austria	Zeus
England	Zenobia
France	Warren
Germany	Zadok
Greece	Wendell
Italy	West
Roumania	Whitney
Russia	Winter
Asquith	York
Bakhméteff	Wizen
Bernstorff	Walter
Crown Prince	Yammer
Gerard	Youth
Grey	White
Hindenburg	Yonder
House	Beverly
Jusserand	Young
Kaiser	Dante
Marye	Zenith
Page (T. N.)	Yew
Page (W. H.)	Yucca
Penfield	Zebra
Sharp	Keen
Spring Rice	Winkle
Stovall	Pelham
Van Dyke	Zion
Von Bethmann-Hollweg	Alto
Von Jagow	Othello
Whitlock	Zenda
Willard	Zeal
Zimmermann	Wolf

Note the suggestive nature of the code words for Grey and Sharp: Baker comments on the list that "an expert could probably have solved [the system] in an hour."

During the trip for which Colonel House prepared the foregoing list, he received from the President a cablegram dated 8 March 1915, the clear text of which is given by Baker (V, 318) as follows:

> There is nothing special to report on this side, and you do not need instructions. Your admirable letters and telegrams keep me posted in just the right way. Your cable of today gives me the feeling that there is at least some real hope. This is just a message of personal greeting and to express the hope that the journey you are about to undertake may be accomplished without untoward adventure and in perfect health. You may manage all the rest. I have no anxiety about it.

The cipher text of this message (as well as President Wilson's shorthand draft) appear on page 317 as follows:

> For Beverly. Misspend rosebud Plunkets repulses upsets mightier innerly upstream apogee lamely bedsite slacked joined bates orthoepic impleader jetson presidency truncation contaries spines graduation francs smallness smells burdocs rightfully pavo Hoosiers solemnized jitter lowlanders moons nugify growth bedside foddered hopping smiter jaunties blendons pomposity sunk lobar alkalize unpunished Tacoma argol bedsore mislead nonpluses Nester truss lobular lignum baby pouched hundreds Benthamite adhesion.

After the President's marriage to Mrs. Galt, some of the labor of encoding and decoding was borne by her (VI, 52-53):

> The President's papers reveal the fact that almost at once Mrs. [Edith Bolling] Wilson began to coöperate with her husband in his lonely labour. In February we find notes and memoranda showing that she was helping him with the difficult tasks of coding and decoding the most confidential dispatches to and from Europe. They worked together, she with the secret code keys, spelling out the messages word by word, and he at the typewriter, setting them down. Or they reversed the process, he writing out his dispatches and she translating them into the

code symbols ready for transmission. They spent many hours of many nights in this painstaking employment.[3]

Note Baker's precise use of code vocabulary: during the Peace Conference he had served as confidential secretary to the President and so doubtless was familiar with code work.

The same volume contains a reproduction (143) of the plain text in Wilson's handwriting of a message to House at the Embassy in London, followed (144)[4] by the code text, also in Wilson's handwriting, of the same message, and (145) by the same code text in typing (on Wilson's own machine by the President himself). The date is 11 January 1916. As can be seen from the illustrations, the groups are of five digits, interspersed with code words taken from House's code (Zenobia = England; Zodek = Germany. It is difficult to determine whether the code is one-part or two-part, since we do not know which units of the code group formed the page symbol and which the line symbol, and the length of the code groups is not marked off in the plain text. There seems to be no correspondence between the alphabetical range of the plain-text units and the numerical range of the code groups. There is no information available as to whether any form of encipherment was used.

A similar exhibit of a Wilson message to House[5] was on view in

[3] There is another reference to Mrs. Wilson's work on the code messages on page 176.

[4] Figures 1-3 reproduce these pages.

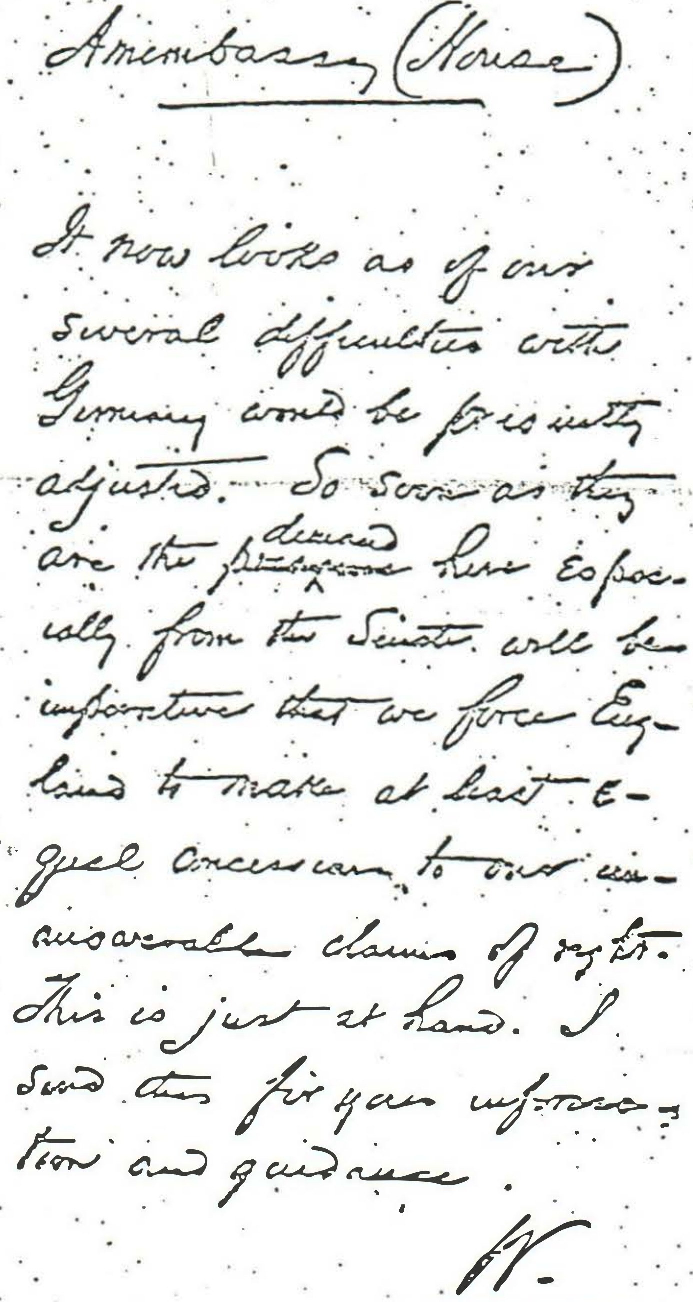
[5] Wilson to House No. 5, 30 October 1918, discussing the coming Peace Conference: the plain text is given by Baker (VIII, 533).

a display case in the Library of Congress[6] in the spring of 1946. The plain text in Wilson's penciled script is marked off in code-group lengths. There is only one repetition, the word "include" represented by the code group 42904.[7] The cipher text, also in Wilson's handwriting, shows that the code was one-part. After encoding the message, the five-digit groups were converted to five-letter groups by a process in which, apparently, each digit in each position in the code group could be converted to one of two variants. Thus, the code group 42904 appears once as FOCEQ and the second time as KOCEQ. Every intial 4 is represented by either F or K. The same phenomenon was also visible in the case of the final digit of other groups—it would probably have been noted in every instance, had full examination of the message been possible.

[6] The exhibit was in a case on the north side of the corridor leading to the Rotunda, second floor, main building, and had been on view for several months. Examination of the message, which took place on 11 May 1946, was hampered by the fact that the corridor was crowded with visitors and it was necessary to prevent undue attention from being drawn to the examination by taking a quick look and then returning, several times, after an interval.

[7] Of course, other words are repeated in the plain text but no other code group is repeated.

[illegible]



Amembassy (House)

It now looks as if our several difficulties with Germany would be presently adjusted. So soon as they are the demand here especially from the Senate will be imperative that we force England to make at least equal concessions to our unanswerable claims of right. This is just at hand. I send this for your information and guidance.

W.

39608 — 33391 — 37200 -

67906 - 32040 - 22114 - 52927.

12726 - ZodAK - 65092 - 29004 - 72610

20885 - 68613 - 54058 - 43336 - 49674

46352 - 22643 - 65062 - 42217 - 17802

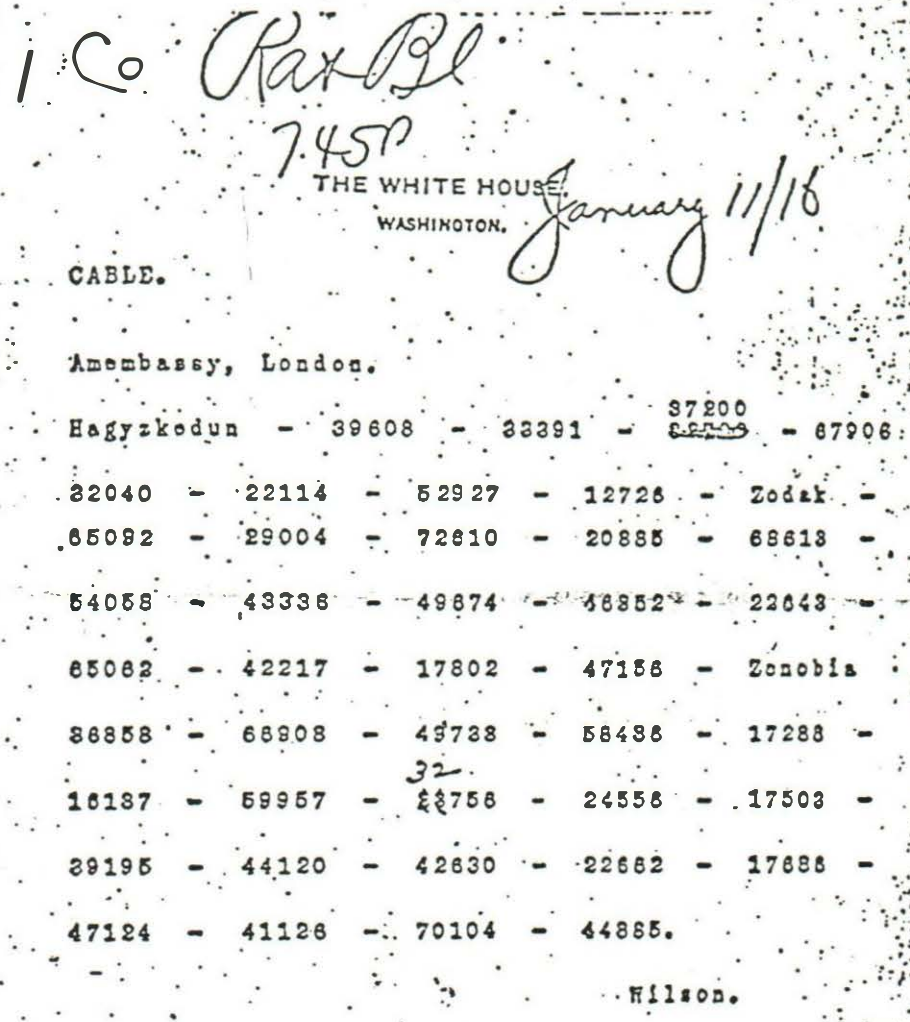
47156 - Zenobio - 36858 - 66908 - 49733

58436 - 17288 - 16137 - 59957 - 32756

24556 - 17503 - 39195 - 44120 - 42630

22662 - 17680 - 47124 - 41126 - 70104

44885 -



1 Co Rat Bl

7.45P

THE WHITE HOUSE. January 11/16
WASHINGTON.

CABLE.

Amembassy, London.

Hagyzkodun - 39608 - 33391 - 37200 ~~[illegible]~~ - 67906:

32040 - 22114 - 52927 - 12726 - Zodak -
65082 - 29004 - 72810 - 20885 - 68613 -
54058 - 43336 - 49874 - 46852 - 22643 -
65082 - 42217 - 17802 - 47158 - Zenobia
36858 - 66808 - 49738 - 58436 - 17288 -
16137 - 59957 - 32756 - 24558 - 17503 -
39195 - 44120 - 42630 - 22682 - 17688 -
47124 - 41126 - 70104 - 44885.

Wilson.

47-

Three documents showing President Wilson's method of communicating with Colonel House, in London. The message was written out in the President's own hand, and signed "W." It was then transferred into the complicated code figures and letters by Mrs. Wilson (the code word "Zadok" signifies Germany, and "Zenobia," England). The President then copied out the figures on his own typewriter, for transmission by the Department of State.

CHAPTER IV. CODE AND CIPHER SOLUTION IN THE CIPHER BUREAU

A. The Evidence from Yardley's Reports

An attempt to write a history of the work done in MI-8 on the solution of enemy codes and ciphers encounters the difficulty that a reasonably large portion of the records of that subsection are no longer available.[1] One of the greatest losses, from the point of view of the historian, is the file of progress reports, which would have been invaluable in dating events and showing what achievements were considered significant at the time. Though much important

[1] Some of the files in the possession of MI-8 (probably everything pertaining to cryptanalytic work) were taken to New York in 1919 when Major Yardley moved his small staff there. There they remained until 1929, when, together with the files of the period 1919-1929 and those of the Shorthand Subsection which had never been in Washington, they were brought to Washington and became the property of the newly formed Signal Intelligence Section, Office of the Chief Signal Officer. They ultimately passed to the Signal Security Agency and were reexamined with care in the spring of 1945 in connection with the preparation of this History. A number of special historical papers have been prepared on various phases of the work and will be cited as occasion demands. That these files are incomplete is quite clear from the fact that there exists a card file containing an index by subject matter of the cryptanalytic files of MI-8. References are there made to many folders which have disappeared. The cause of their disappearance is a matter for speculation. A particularly important lacuna is the complete absence of a record of the work done on secret inks, though the Shorthand Subsection is well represented. Some of the missing material may be in the files of the Administrative Records Branch, where there is also other MI-8 material, chiefly copies of letters forwarding reports of individual solutions of no great interest.

material is missing, the part which has survived is considerable, and it is still possible to determine the main outlines of the story on every occasion,[2] though not always the complete details.

There exist, for example, three historical documents which were all prepared by Major Herbert O. Yardley soon after the war. These were in 1945 collected in a paper of the Historical Unit, Signal Security Agency, entitled *The Achievements of the Cipher Bureau (MI-8) during the First World War: Documents by Major Herbert O. Yardley*. The contents of the paper are as follows:

a. A short history of the Cipher Bureau, prepared in 1919.—It is largely concerned with achievements other than those in the field of solution, but its paragraphs on this topic will be noticed shortly.

b. A memorandum for the Director of Military Intelligence, Subject: *Number of alien codes and ciphers broken*, 5 June 1920.—This is a more complete form of another report on the same subject contained in a memorandum dated 16 May 1919 which will be mentioned later.

c. Exhibits prepared in 1919 and 1920 to justify the continuance of a unit like MI-8.—The emphasis here is entirely on solution.

[2] It had been planned to exploit the recollections of Lieutenant Colonel A. J. McGrail, Chief of the Secret Ink Laboratory in Washington and later Chief of the Laboratory Branch, Signal Security Agency, but his untimely death on 30 April 1945 prevented this project. He was, however, at the time of his death preparing the history of his branch and fortunately had completed that part of the narrative which concerned World War I. His recollections on other phases of the work in MI-8 died with him. Incidentally, he was the only member of MI-8 in Washington who also served with this Agency at a later date. It has not been deemed possible, for reasons of security, to make contacts with other MI-8 personnel known to be living.

The first document contains two short paragraphs[3] ostensibly devoted to the work of the Code and Cipher Solution Subsection:

> In the cryptographic[4] section itself—which will hereafter[5] for the sake of clearness, be referred to as M. I. 8—as in the whole organization of Military Intelligence, the increase in personnel was closely dependent upon the pressure of the work itself. During the first year of the war, additions to the staff were not made until they were absolutely necessary. The growth was therefore slow and the time of the staff fully occupied by current routine work. Plans for attack upon large problems or for research into new methods had constantly to be postponed because of the unescapable [sic] demands of the daily work. In fact, it was not until the beginning of August, 1918, that the staff was enlarged sufficiently to permit of serious attack upon the large numbers of code messages in various codes which had been accumulating in the files.
>
> The results obtained should be judged in the light of these facts. And for the future it should be borne in mind that an adequate personnel of clerks and typists as well as of cryptographers is necessary for satisfactory results in code attack, and that the personnel is not adequate unless it is large enough to release the time of one or more experts for research.

This short statement is surprising: it contains no reference to any specific achievement of the subsection but merely discusses personnel problems. The brevity here contrasts strongly with the fullness of

[3] Yardley, Achievements, p. 9.

[4] Until 1921 American use of this term implied what has since been called cryptanalysis, as well as the purely cryptographic operations.

[5] That is, in Yardley's report: the official title was the Cipher Bureau, a designation verified by the fact that the dating stamp used in MI-8 so marked all incoming documents.

the description of the work of other subsections. They are from two to five times as long as this description, are specific, and give a definite idea of what was achieved. Why, then, the silence on such matters in the present instance? The reason is probably to be found in a healthy regard for security.

The second document presented in Yardley, Achievements, is a memorandum which he prepared on 5 June 1920, giving the status of solution on that date. The difficulty involved in using this memorandum to evaluate the work done in Washington is that it includes indiscriminately the work of MI-8 both in Washington before August 1919 and in New York after that date. To determine which of the solutions there mentioned had been accomplished before the move to New York, there is available another and earlier document, which does not, however, include any solutions reached between 16 May 1919 and the time of the removal to New York, approximately 1 August 1919. The document in question is a memorandum for the Chief of Staff from the Director of Military Intelligence (Subject, Plans for M. I. 8)[6] and must have been based on a rough draft by Captain Yardley now lost. Paragraph 3 lists the foreign cryptographic systems then readable as follows:

[6] One copy is filed in IR 1366; another in the files of the Director of Communications Research. See also Volume Three, Chapter II.

Total	578

It was predicted that by the end of June, with adequate personnel, would be solved, in addition to those listed. Moreover, it was stated also that in the eighteen months of its existence the subsection had made readable 10,735 messages sent by foreign governments.

This impressive total of 573 solved systems was reached by counting each solution of a simple or different specific key used on a basic system as the equivalent of the long and painstaking solution of a code; there can, however, be no comparison between the analytic skill or time required in the solution of the two types of systems.

During the summer of 1919, as will be described in detail in Volume Three, Yardley moved his unit to New York and continued work there, chiefly in the field of cryptanalysis, though some work was done for a short time in cipher-key compilation. On 5 June 1920 he made the report in which he listed the principal codes and ciphers which were readable on that date.[7] The list in this case is naturally longer since over a

[7] A copy is now filed in IR 4158.

year had passed. It is not, however, possible to state exactly how much work was actually accomplished in Washington, since, as has been said, there is no report covering specifically the period between 16 May 1919 and 1 August 1919. The 1920 list contains several items the dates of which are known from other sources and can therefore be definitely set down as achievements of the New York period. With these omitted, the list is as follows:

Total[8]	697

Details concerning the solution of these systems will be given later in the sections describing the specific problems, but certain facts should be pointed out which qualify the claims made in both the reports of 16 May 1919 and June 1920. In the first place, while the text of the later memorandum[9] merely states that the list is composed of the "principle [sic] codes and ciphers than [sic] can be read at present,"

[8] Yardley's total of 713 systems was obtained by including three (really only two codes!), and four more codes which had been solved after the move to New York.

[9] The text of the earlier memorandum is more careful: it merely points out that the systems are readable.

the subject heading is "Number of alien codes and ciphers broken." The word "broken," an older term for what is now called solution, surely implied solution by cryptanalytic means, yet the list contains a number of systems which became readable, at least in part, through the possession of compromised versions of the code books, e. g. ;

and a number of the cipher systems. No mention, moreover, is made of any assistance from the

Yet the real achievements of the Code and Cipher Solution Subsection were many and, given the status of cryptographic studies at the beginning of the War, they were highly praiseworthy, needing no exaggeration to make them impressive. The following paragraphs are taken from the memorandum of the Director of Military Intelligence to the Chief of Staff, 26 May 1919, already cited, and are indicative of what General Churchill, and doubtless also Major Yardley, then considered the value of the work done by MI-8:

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

10. A letter dated 21 March 1918 (copy in IR A153) from in Washington, was accompanied by a memorandum on code messages and their solution. The writer of the memorandum had participated in code reconstruction, but it is quite evident that he had never been faced with a really difficult problem. See above Chapter II. material was also received by the German Code Solving Unit (see the longer discussion in Section B.)

1. Insight into German Secret Service.[11]

a.) The Waberski Cipher is an official letter of introduction given by Minister von Eckardt to Pablo Waberski, a secret agent of the German government, addressed to all German consular agents in Mexico, ordering them to furnish him aid and support, provide funds, and forward his messages in code as official. This was captured on a German spy and was a principal factor in his conviction. For this cipher and its decipherment see Exhibit A.[12]

b.) The von Magnus Cipher—known officially as "Document PGR"—is a very long and elaborate quadruple transposition cipher, addressed by the German Charge d'Affaires in Mexico City to all German consular officials in Mexico, giving directions concerning the careful and complete destruction of correspondence, accounts, receipts, lists, registers, and all other papers having to do with "the Secret Service and the representatives of the General Staff and the Admiralty Staff" and the preservation of "the strictest silence concerning the existence and activities of these representatives now and for all future time, even after the conclusion of peace." For this cipher and its decipherment see Exhibit B.[13]

c.) Of the numerous German code messages deciphered by M. I. 8, two belong specifically under this head. The first was sent out by wireless from Nauen and intercepted by our stations sixty-four times between January 13 and February 2, 1918. It includes an order from the German

[11] On German systems see section B of this chapter.

[12] This exhibit is now filed in IR 4366; it is a duplicate of Exhibit II in Yardley, Achievements, Part III.

[13] This exhibit is now filed in IR 4366; it is a duplicate of Exhibit III in Yardley, Achivements, Part III.

Foreign Office to the recipient to avoid negotiations with the Japanese, because "communication through you is too difficult" and the Japanese have "representatives in Europe"; and presents a plan for providing Mexico with arms, and machinery and technical staff for the manufacture of arms and air-craft. The second message — also a wireless from Nauen, intercepted in February 1918 — informs the German Minister in Mexico of the deposit of ten million pesetas in the German Oversea Bank, Madrid, which he is authorized to offer to the Mexican Government as a "preliminary amount" "on supposition that Mexico will remain neutral during war." See Exhibit BB.[14]

2. Special War Measures. The most important message of this character deciphered by M. I. 8 is the code cablegram sent by Embassador [sic] von Bernstorff on January 21, 1917 to the German Consul at Manila ordering him to take up at once the question of making useless the machinery of interned German vessels or, in case that proved impossible, of sinking them. (for message and decipherment see Exhibit C.)[15] It will be noted that this message was sent ten days before the declaration of unrestricted submarine warfare. If the U.S. Government had possessed at that time an organization capable of deciphering this and the other messages relating to this subject — as was later done by M. I. 8 — precautions against the crippling of these vessels could have been taken, with a saving to this government conservatively estimated at twenty-five millions of dollars.

[14] This exhibit is now filed in IR 4366; it is a duplicate of Exhibit V. in Yardley, Achievements, Part III.

[15] This exhibit is now filed in IR 4366; it is a duplicate of Exhibit I in Yardley, Achievements, Part III.

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

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

b.)[16] In 1916, when the Germans made their great withdrawal in Flanders, the code experts of the British gave G. H. Q. advance information not merely of the fact of the intended withdrawal but also of the time and manner of it. But at the time the officers in charge of operations were skeptical of code attack and put no faith in the information until they woke one morning and found the Germans gone. Similar skepticism, says Colonel Moorman, awaited the first message deciphered by G-2, A-6, giving definite information of an intended attack, but in this instance also the attack itself authenticated the work of the code-men.

[16] This and the following paragraph confirm the statements made concerning British cooperation.

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

The exhibits mentioned as forming the third document in Yardley, Achievements all refer to specific problems and will be mentioned as occasion demands in following sections of this chapter.

B. Solution of German Diplomatic Systems

In World War I the chief antagonist of the United States was Germany, and it is natural that the chief effort was made and the chief success obtained in regard to this opponent.[17]

The outstanding success, judged from present perspective, was that of the unit, directed by Captain Charles J. Mendelsohn, which solved the German diplomatic codes, yet nothing concerning this work

[17] The story of the work of American cryptanalysts at General Headquarters in France on German military codes and ciphers will be told in Chapter VIII. The present chapter is limited to work done in MI-8 in Washington.

appears in The American Black Chamber.[18] For the story, the reader is referred to the monographs by Captain Mendelsohn himself, which have appeared as follows:

a. Studies in German diplomatic codes employed during the World War: I. Code 18470 and its derivations; II. The "Fuenfbuchstabenheft"; III. German methods of code encipherment. (Washington: United States Government Printing Office, 1937).

b. An encipherment of the German diplomatic code 7500[19] (Washington: United States Government Printing Office, 1938).

These have recently (1945) been summarized in a paper of the Historical Unit, Signal Security Agency: German Cryptographic Systems during the First World War (IR 5096), which contains an evaluation of all German systems used during the period in question.[20]

[18] This cannot be the result of any enmity between Major Yardley and Captain Mendelsohn. The two were on friendly terms, and Mendelsohn maintained a quasi-official relationship to the cryptanalytic unit in New York, working there as his duties as Professor of History in New York University permitted. He was a reserve officer in the Military Intelligence Division at that time, and he was also associated with Yardley outside of office hours in a business venture.

[19] Reference should also be made to a monograph prepared by Captain Mendelsohn in collaboration with Mr. William F. Friedman, The Zimmerman Telegram of January 16, 1917, and its cryptographic background. (Washington: United States Government Printing Office, 1938).

[20] The pertinent parts are in section III, pp. 27-53.

The first German diplomatic code known to MI-8 was designated as Code 13040,[21] a short title derived from the discriminant used in the messages.

The task of MI-8 therefore was to use this partial reconstruction to decode intercepted traffic and to complete the reconstruction as far as possible.

Code 13040 was of a hybrid type, now called repaginated: that is, new page numbers were assigned to the one-part code in blocks of four. Thus, the code was one-part within sequences of four pages but two-part as regards sequences of blocks. Pages which contained frequent groups were given two cipher page numbers to decrease the frequency. A further rearrangement was made on each page in that blocks of ten groups were rearranged on the page. The code had, in addition

[21] Prior to the War Ambassador von Bernstorff had deposited with the State Department a copy of the one-part German code in the English language known as *Englischer Chiffre 9972*. The reason for this unusual situation was a desire on the part of the Germans to obtain a channel for diplomatic traffic between Washington and Berlin. See the full story in Friedman and Mendelsohn, *The Zimmermann Telegram of January 16, 1917*, already cited, and *German Cryptographic Systems during the First World War* (IR [illegible]), par. 13.

to the main vocabulary, four special sections. Those containing groups for message numbers, dates, and frequent references and for miscellaneous common phrases, were both placed before the vocabulary; those for proper names and for grammatical inflections, both after the vocabulary.

The same basic code was also used with two encipherments known, respectively as codes 5950 and 26040. In the case of 5950, the page numbers were different, i. e. pages 10-14 of 13040 became in 5950 pages 114-118, etc., and the blocks of ten groups on the pages were renumbered so that the order of blocks was different. Code 26040 was an encipherment of code 13040 by application of an additive or subtractor; that is, when the message had been encoded, a number between 100 and 999 was either added to or subtracted from each group. The number used as additive or subtractor was indicated to the recipient in the message by a group artfully concealed.

Having begun their first project with the advantage of knowing something of British experience, the cryptanalysts of MI-8 were ready to attack new problems on which the British had sent no information. For their study there was a considerable body of material which had been intercepted in France. A knowledge of the position of the discriminant used with code 13040 and its two derivatives led to the discovery of similar discriminants in the raw traffic. Solution was ultimately reached in the case of the six codes having as discriminan s 18470, 12444, 1777, 2310, 2815, and 80574. As was later discovered, the last three were simply variants for the same code, so there were only four different codes represented in the list; furthermore, as solution progressed, it was found that all four were merely conversions of the same basic one-part code to which the hypothetical designation of XX was given. Whether XX had ever been used in traffic or was merely a step in the compilation of the codes which were so used, was never determined. In any case, XX never appeared in any intercepted traffic: if it was used at all, it was at a date anterior to the experience of the cryptanalysts in MI-8.

It will serve no useful purpose to recount here in full detail the steps by which solution was reached—the reader who is interested will find a complete record in Mendelsohn's monographs already cited. Certain facts became apparent: code XX was one-part in arrangement and not dissimilar to code 13040, but it definitely was a different compilation. The chief difference was the absence of the section containing frequent phrases, though XX did contain sections for grammatical inflections, for variant discriminants, and for geographical and personal names, in addition to the general vocabulary. The vocabulary was arranged in one-part fashion except for the insertion of a few numerals, punctuation, and frequent words on each page, according to a complicated and subtly concealed pattern. The size of the code was in excess of 27,700 groups.

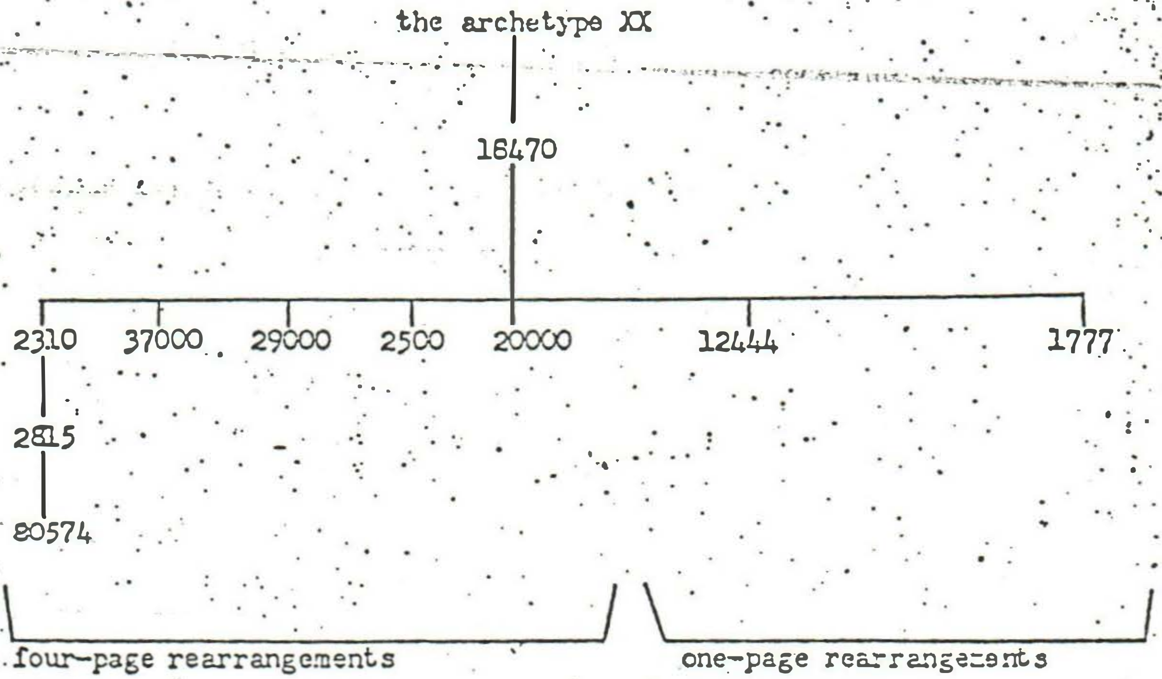
To convert XX to one of the forms in which it was used, e. g., code 18470, changes were made both in the page numbers, by a pattern somewhat similar to that used in the case of code 13040, and in the line symbols, were also changed, but in this instance not according to any pattern that was ever discovered. Some doubt was entertained as to whether the Germans had printed two copies of the code, one for encoding and the other for decoding, or whether they had used a single printing, but this point did not affect the result.

Code 12444 was a conversion of code 18470 by a simple monoalphabetic substitution of the last digit of the code group, and a renumbering of the pages—this time not in blocks of four pages but singly. The same means was used to form code 1777, but in forming code 2310-2815-30574, a single encipherment, the page numbering was again accomplished in blocks of four.

Since all these hybrid codes bore a mathematical relationship to each other, once solution was begun, conversion tables could be constructed so that any fact discovered in one instance could at once be exploited in as many other instances as possible.

In April 1919, while MI-8 was still functioning in Washington, American officials then in Holland were approached by a person whose identity was never learned by the cryptanalysts with the offer that this unknown, designated thereafter in MI-8 as "the Dutchman," 22 would sell the United States much information concerning the German systems. The purchase of the material never took place even though it was brought to Washington in December 1919 with this end in view. While the matter was under review, however, the material was photographed and then returned as "not wanted." Although this information was not obtained by MI-8 during the War, it will be well to say that the material contained, inter alia, a reconstruction of a code known as 2500, with tables for converting this code into three other forms, known as 37000, 29000, and 18400. Upon examination code 18400 proved to be identical with code 18470, though that code had never been used with the discriminant 18400 in any traffic intercepted by the Americans. "The Dutchman" believed that Code 2500 was the basic book from which the others were, as he said, "derivated." With this view, Captain Mendelschn was in disagreement for what seem excellent reasons, but it was clear that 2500, 37000, 29000, and 20000 were really related to the archetype XX. A stemma was therefore prepared of all these related codes, as follows:

[22] It was, of course, recognized that he was probably not a Dutchman, but from the evidence it is clear that he had participated in the reconstruction of German diplomatic codes in some cryptanalytic bureau with considerable resources at its disposal. The Dutch Government is not likely to have supported the bureau in which this man worked, and the point cannot be settled, but it is worth suggesting that he may have been a former member of such a bureau previously maintained by the then defunct Imperial Russian Government.


the archetype XX
16470
2310
37000
29000
2500
20000
12444
1777
2815
80574
four-page rearrangements
one-page rearrangements

The German Code Solving Subsection received from a variety of urces compromised copies of other German codes which were available or study and for decoding any traffic which might be intercepted. These were:

a. The Englischer Chiffre 9972, which had been deposited by von Bernstorff while he was yet in Washington.

b. Boy-Ed's code, a system devised chiefly for reporting ship movements. The code groups were words: e. g., HUBBARD, HUBER, HUBERTY, HEINZ, or HAY, could stand for Greece.

c. The Von Igel Code was available in a reconstruction received from an unknown source. It was a one-part code having slightly more than 10,000 groups. Only one message in this code was available, one which had been sent by von Papen to Berlin on 4 August 1915. How this reached MI-8 is unknown.

d. The Handels-Schiffs-Verkehrsbuch fur den chiffrierten Verkehr mit deutschen Handels-Schiffen (H. V. B.), 2te Auflage, Berlin, 1913, was obviously received from the British. The arrangement was one-part and sectional. The code, which as the title indicates, was published for the use of shipping companies, was used by the German Navy and by counsuls in Spain as well. A few messages were intercepted in it.

A fairly large volume of messages in German commercial codes was intercepted and read, chiefly traffic between Germany and German firms in South America. Since the records now extant consist only of work-sheets with the decodings written in, it is probable that the codes involved were regularly published commercial compilations available in the open market, and that this traffic did not require cryptanalytic techniques.

C. Solution of German Cipher Systems

In the memorandum dated 5 June 1920 Yardley reported as readable five German intelligence ciphers. Which cipher systems were meant is not entirely clear, but it is certain that two of them were the berski cipher and the von Magnus cipher.

The Waberski cipher was found, among other papers, on the person of a German agent arrested as Pablo Waberski at Nogeles, Arizona, on 1 February 1918. The true name of the man was Lothar Witcke or Witzke; he was proved by the document to be a German spy and at his trial was condemned to death. He was, however, not executed, the sentence having been commuted to life imprisonment by President Wilson on 4 June 1920. Later, on 23 November 1923, Waberski was deported to Germany and is believed to have died there.

The document in question was forwarded at once to MI-8 and was received there, according to the Official Record of Waberski's trial, on 7 February 1918. Its importance was not, however, realized at once, though several persons in MI-8, including Yardley, tried their hands at solution and failed. Then, Captain John M. Manly took up the task, spent a week on preliminary work, two weeks more on the solution which was achieved on 18 May 1918, and, with Miss Edith Rickert, worked out the details of the system after the message had been read.[23]

The document had been dated 15 January 1918 and solution showed it to be a letter of introduction to German consular officials in Mexico signed by the German Minister, von Eckhardt. It consisted of 432 letters and proved to be a route transposition, the route being diagonal and controlled by two mixed numerical keys, the horizontal 2-9-8-1-4-3-6-5-7, and the vertical 5-3-8-9-4-6-7-1-10-11-2-12. Letters were taken in groups of four, except at the end where three were taken, and inscription was by diagonals, transcription by the numerical sequence of the horizontal key, one letter at a time. The text, translated, is as follows:

> To the Imperial Consular-Officials in the Republic of Mexico
>
> Strictly Secret!
>
> The bearer of this is a citizen of the Reich who under the name of Pablo Waberski is travelling as a Russian. He is a German secret agent.

[23] The statements in this paragraph are based on mariginal notes by William F. Friedman in his copy of Yardley, Black Chamber, 153-171, reporting comments of John M. Manly made on 15 June 1934. The account of the solution by Yardley himself is faulty. The impression is there given that the importance of the message was realized immediately and solution speedily, if not easily, arrived at.

> I beg you to afford him protection and assistance, also advance him on demand, up to one thousand pesos of Mexican gold, and send his code telegrams to this embassy as official consular dispatches.
>
> Von Eckhardt.

The von Magnus cipher was a message ordering the destruction of all archives in all German consulates in Mexico. Transmitted on 16 January 1919, it was solved and read by MI-8 on 22 April 1919. The text was sent in groups of ten letters, the system being a columnar transposition in eighteen columns.[24]

The three additional intelligence ciphers reported as readable must have been included among the following:

a. An open code system said to have been used by German agents in France. A cover letter was written in such a way that the number of syllables in each three words would refer to a three-digit code group corresponding to a single letter of the plain text.

b. Another open code system in which German agents in France and Switzerland inserted want-ads in the newspapers. The first letter of each sentence would indicate, by reference to a cipher table, which word in that sentence was significant in the secret text. This information was obtained from the Italian military attaché in Washington.

c. A third open code was known from information received from an American intelligence officer. The plan involved the insertion of a feeble sort of joke in a newspaper, containing thinly veiled references to the words of the secret text.

[24] See Exhibit III, Yardley, Achievements, pages 27-30; Black Chamber, pages 149-153, and IR 4606.

d. Still another system of similar type, said to have been used in the Balkans, consisted of phrases in Spanish and German which represented secret texts previously agreed upon.

e. Copies of newspapers sent through the mails by German agents were marked by pin pricks or with lemon juice in such a way as to spell out the secret text. The Department of Justice had intercepted such messages which were apparently read in MI-8.

f. At least six different versions of monoalphabetic substitutions were known to have been used by German agents in the United States. All of these were learned of from outside agencies.

g. At least two polyalphabetical substitution tables were known, and there were, also digraphic substitutions used by German officers in Mexico.

h. In addition to the transpositions already noted, Germans were believed to have used grilles, but whether MI-8 solved them or not, is not clear.[25]

D. Solution of

The cryptographic systems of only one other European government were extensively[26] studied by the experts in MI-8, those of

[25] From time to time MI-8 learned of small codes designed for limited use in espionage in the United States, but none of these codes have been solved in the Bureau.

[26] Some attention was given to the systems used by other European governments

but in most cases this consisted merely of filing traffic which was received, more or less by accident, from the sources of interception. The scant information available in these cases, and also in the similar instances of a few non-European governments, is summarized in Data on Miscellaneous Cryptographic Systems [illegible], a paper of the Historical Unit, Signal Security Agency ([illegible]).

by espionage activity, was made.[28] The code as originally printed was a single

had to be prefixed to the message.

[28] The photographs now filed in II. 84. The story of the capture of this code which appears in Yardley's book, The American Black Chamber (chapter viii, pp. 172-195) probably contains a good deal of fancy. The truth about this activity is that an agent was sent from Washington to obtain a copy of the code but he acted so indiscreetly that his purpose in coming to became known to representatives of the intelligence officer on duty in the Department. The agent was approached with the offer that, if he would patiently wait for a short time, the code could be obtained for him by the representatives of the intelligence officer. The story is told in considerable detail in testimony given to Mr. William F. Friedman by one of the persons who actually assisted in the photographing of the document.

was made drunk, and while drunk, the key to the office safe was stolen from him. An impression of the key was made and the key returned to the without arousing his suspicion. Utilizing the knowledge of the movements, a time was selected when it was known that he would be away from his office and the code was then photographed. These operations had to be repeated, since on the first try one of the pages was not photographed clearly.

[29] See a memorandum written by Mr. William F. Friedman in 1931, quoted in IR 5093, pages 11-14; also a paper by Miss Ruth Wilson, who participated in the solution, now filed in IR 6297. The latter paper fails to make clear the fact that the codes had been partially compromised: the implication is that all the codes were reconstructed entirely by analysis.

[30] See the list of folders containing the translations, presented on pages 17-18 of IR 5093.

1929, the latter until 1935. Weiskopf had been an employee of the Department of Justice as early as 1916, when he was sent to Texas as a confidential agent. For a long time he remained on the payroll of the Department of Justice on loan to MI-8.

When work on [redacted] first began in MI-8, Weiskopf's services were obtained, and with him there became available an extensive amount of information concerning miscellaneous systems used by [redacted] with code. Frequency counts of the groups were made, and good use was made of the probable word method. In the case of this code it is possible to get some idea of when solution began: the earliest message studied was sent on

Thus, the intelligence obtained from the reading of this traffic was not made available until the period after the Armistice.

G. Solution of the

The solution of the was the first problem undertaken by the Code and Cipher Solution Subsection. Captain F. B. Luquiens undertook this assignment, assisted by a large staff of clerical personnel and by experts in the Spanish language, among whom Mr. Victor Weiskopf was one. The chief source of information concerning the project is a document entitled which is almost certainly the work of Captain Luquiens himself. The document contains a full account, step by step, of the solution.

and the system was never completely

35. The rough draft of this paper has been reproduced in Captain F. B. Luquiens' Description of the Solution of the now filed in I. [illegible], a paper of the Historical Unit, Signal Security Agency (I. [illegible]). See also Spanish-American Material in the Files of MI-8, listing a paper of the Historical Unit (I. [illegible]), particularly par. 4.

I. Miscellaneous Problems

In addition to the diplomatic problems already discussed, the experts in MI-8 attacked many problems of a cryptanalytic nature arising from material received from a variety of sources.

One such problem was to be found in a series of messages submitted by the telegraph companies. All of the messages were filed in September 1917.[40] They had been enciphered by a transposition of the words of the plain text. Though the transposition was solved, the resultant decipherments are not entirely clear, and the suspicion remains that in addition to the transposition, some form of open code was also involved. Among the persons who had filed these messages with the telegraph companies were

[40] IR 452 now contains the texts of those messages.

Considerable interest was shown in the possibility that enemy agents might use for transmission of messages chess problems printed in newspapers. Colonel Van Deman sent a letter on 13 April 1918 to the various officials of the Censorship[41] calling attention to this source of danger:

> It has often been suggested that messages in cipher may be and are being transmitted by the standard symbols for chess moves. Careful investigation convinced us that it is not possible to convey a message and at the same time play a correct game. It appears, however, that it is possible to devise a system whereby the positions of the pieces in a chess problem can be made to convey a message and at the same time satisfy the conditions of good play.

Whether any actual chess problems were found to be suspicious in character is not known: the Military Attache in London reported to Colonel Van Deman on 16 April 1918 that the British had been holding up chess problems, examining them, and allowing those to pass which appeared innocent. One suspicious problem had been found in eighteen months. The French were impressed sufficiently by Colonel Van Deman's letter to recommend to the Bureau de la Presse a ban against chess problems in French papers. An elaborate analysis of means of conveying a message in a chess problem was received from Captain D. M. Liddell, of the Equipment Division, Signal Corps, in New York, dated 6 May 1918.[42]

[41] To R. L. Maddox, Chairman, Censorship Board, Washington, and to Captain Benjamin M. Day, Executive Postal Censorship Committee, New York (see IR 5015).

[42] Copy now filed in IR 5015.

There exist in the files several folders containing other ciphers which were received from various sources but were never solved. One such problem consisted of a message in letters which was submitted on 18 April 1918 by Lieutenant Herbert W. Rogers, Industrial Service Section, Office of the Chief of Ordnance.[43] Two of the experts each spent two hours on the problem without success. This may have been a sample message in a new system devised by Lieutenant Rogers or a message which had come to him in line of duty.[44]

[43] IR 4952.

[44] Miscellaneous cipher problems of no great importance are now filed in IR 4486, IR 4568, IR 4928, IR 4939, and IR 4931. Various records of MI-8 (log books, notebooks, memorandum pads, etc.), of little historical value, are filed in IR 4347, IR 4348, IR 4376, and IR 4377.

In his work at Harvard Professor Richards had the aid of Professors Baxter, Kohler, and Lamb of that university, but in the summer of 1917 Professors Kohler and Lamb joined the chemical staff to withdraw from the project on account of pressure of administrative duties at Harvard. To fill the vacancy, a young chemist, Dr. Emmett K. Carver, was assigned to assist Professor Richards. Richards had been, in fact, offered a commission as captain in the United States National Army (the equivalent of the present-day Army of the United States), but the condition of his health made it impossible for him to accept.

In November 1917 the Military Intelligence Branch set up a laboratory in the Postal Censorship at 641 Washington Street, New York City, which was placed under the direction of Dr. Carver, who in April 1918 was commissioned a captain in the National Army. In the late spring of 1918 a second laboratory was set up in Washington in the office of the Military Intelligence Division at 1330 F Street, Northwest, a building which occupied part of the site of the present National Press Club. This laboratory was placed in charge of Dr. A. J. McGrail, a graduate of Harvard University (B. A.) and The Catholic University (Ph.D.), who was commissioned a first lieutenant in the National Army.

In December 1917 Captain J. A. Powell was sent abroad to establish liaison with the British and French in all matters pertaining to the

CHAPTER V. THE SECRET INK LABORATORIES[1]

Early in 1917 Colonel Van Deman became interested in the question of secret inks and applied to the National Research Council for help. Dr. Marston P. Bogert, Chairman of the Chemistry Committee of the Research Council, requested Professor Theodore W. Richards, of Harvard University, to undertake this study, and the first scientific work on secret inks ever done in this country was carried out by Professor Richards in the Wolcott Gibbs Laboratory at Harvard. It may be pointed out that Professor Richards at that time was outstanding among American chemists--he had been Exchange Professor at the University of Berlin and had in 1914 received the Nobel Prize in Chemistry, the first American chemist ever to receive this award. For many years he was the leading authority in the world on the question of the atomic weight of the elements.

[1] This section is based very largely on an account being written in the spring of 1945 by the late Lieutenant Colonel A. J. McGrail, Signal Corps, then Chief of the Laboratory Branch, Signal Security Agency. Colonel McGrail had been a first lieutenant in the Washington laboratory during World War I, and an officer in the Military Intelligence Reserve from 1919 to 1941, and since that time had been on duty with the Signal Intelligence Service and its successor, the Signal Security Agency, until his untimely death on 30 April 1945. The account was not complete at the time of Colonel McGrail's death, but it fortunately told the story of secret ink activity from 1917 to the point at which the account can be carried on through the recollections of other members of the Laboratory Branch.

work of MI-8. He sent back what is described as a voluminous report,[2] but this was composed almost wholly of material on cryptanalytic work—there may have been some information on secret ink, as Yardley implies. It is certain, however, that much help was derived from a visit of Mr. Stanley W. Collins, Chief Chemist of the British Censhorship, who came to the United States in the summer of 1918, bringing with him complete files of information on enemy inks, methods of detection, and actual exhibits of enemy secret letters.[3] He devoted two months to the instruction of the American chemists.

[2] See Yardley, Achievements, 11-12.

[3] The substance of his main report appears in The American Black Chamber (62-69), disguised as a lecture given by Mr. Collins, with interruptions by Captain Yardley, who refers to the visitor as "Dr. Collins.". A lecture was indeed, given by Mr. Collins, but the statements made in the book are taken, rather, from his written report which he brought with him. One copy of this report was retained by Lieutenant McGrail with official permission; the other had disappeared from the files of the Military Intelligence Division as early as 1929, when Captain McGrail, then on temporary duty as a reserve officer, searched for it in vain. In June 1931 he saw in the window of Putnam's Bookstore, 45th Street, New York, an exhibit of Yardley's book, The American Black Chamber, in which were a number of photostats of documents bearing numbers exactly corresponding to those in Mr. Collins' report. The inference is that the bookseller was given these secret British documents by Yardley. See a letter of Captain McGrail to William F. Friedman, 29 June 1931 (SPSIS 201: A. J. McGrail).

In his work at Harvard Professor Richards had the aid of Professors Baxter, Kohler, and Lamb of that university, but in the summer of 1917 Professors Kohler and Lamb joined the chemical staff to withdraw from the project on account of pressure of administrative duties at Harvard. To fill the vacancy, a young chemist, Dr. Emmett K. Carver, was assigned to assist Professor Richards. Richards had been, in fact, offered a commission as captain in the United States National Army (the equivalent of the present-day Army of the United States), but the condition of his health made it impossible for him to accept.

In November 1917 the Military Intelligence Branch set up a laboratory in the Postal Censorship at 641 Washington Street, New York City, which was placed under the direction of Dr. Carver, who in April 1918 was commissioned a captain in the National Army. In the late spring of 1918 a second laboratory was set up in Washington in the office of the Military Intelligence Division at 1330 F Street, Northwest, a building which occupied part of the site of the present National Press Club. This laboratory was placed in charge of Dr. A. J. McGrail, a graduate of Harvard University (B. A.) and The Catholic University (Ph.D.), who was commissioned a first lieutenant in the National Army.

In December 1917 Captain J. A. Powell was sent abroad to establish liaison with the British and French in all matters pertaining to the

In the New York Laboratory suspect letters from the New York Censorship were examined, contents of parcel post packages were checked, and much work was done for American and Allied intelligence agencies which operated in the New York area. The Washington Laboratory received each day packages of mail from the Censorship Stations at Key West, New Orleans, San Antonio, San Francisco, and Seattle. In addition, it examined suspect letters and materials which were submitted by the Military Intelligence Division and other agencies.

The Office of Naval Intelligence early in 1918 set up a laboratory in a building which is still standing at 1710 New York Avenue, Northwest. This laboratory was well supplied with chemicals and was far better equipped with apparatus than was either of the Army laboratories, but it was directed by an ensign who in civil life had been a fingerprint expert. It accomplished little, and on 25 September 1918 the equipment and supplies were taken over by the Army Laboratory on F Street.

During the War the Army Laboratories found and developed fifty letters in secret ink and aided in the prosecution of the German agent Maria de Victorica; but with the signing of the Armistice, the censorship of mail was discontinued and in February 1919 the two Army Laboratories were consolidated into one at New York. From that date until June 1919 a great deal of research was done. In the summer of 1919 the New York Laboratory was closed, its equipment and supplies turned over to the salvage authorities, and its records were sent to the Military Intelligence Service and promptly lost.

At what date Captain Carver made his trip to Great Britain and France for study in the laboratories there is unknown,[4] nor is much known of the trip made to France in 1919 by Lieutenant McGrail beyond the fact that he assisted Secretary Baker at the Peace Conference by handling the coding of some of his telegrams.

A paragraph written by Major Yardley in 1919 as part of a general report on the work of MI-8 contains the following significant passage:[5]

> Correspondence and other preliminaries delayed for a painfully long time the establishment of a laboratory in M. I. 8. This did not actually take place until the removal to 1330 F Street in July 1918. The laboratory was, however, at this date able to function immediately in highest efficiency. Its record under Captain Carver—and in his absence, under Lt. A. J. McGrail—is one of thorough equipment for any problem in its field and of great usefulness. On an average over 2000 letters per week were examined from July 1, 1918 to February 1, 1919.

The favorable comments concerning the two chemists are interesting in the light of statements made in Chapter iii ("Secret Inks") of The American Black Chamber. Yardley fails to mention the two officers by name but gives the impression that they were not really competent to do their work. The three chapters in that volume which treat of secret ink solution[6] are untrustworthy accounts of events[7]

[4] Yardley Achievements, 11-12.

[5] Ibid.

[6] Chapter III: "Secret Inks" (55-76); Chapter IV: "Patricia" (77-89); Chapter V: "Madame Victorica" (90-119).

[7] P. 89.

which Captain Yardley was often in no position to descrite from first-hand experience. He was, for example, in France at the time when Lieutenant McGrail, and not a convicted counterfeiter, as Yardley maintains, was able to replace a seal on a Mexican letter[8] addressed to a high Mexican official (not to Carranza, as Yardley states). The long story[9] on the detection of a secret-ink letter written in Greek contains many inaccuracies.[10] The writing had already been brought to light by the application of heat from a small electric stove, even before the letter was sent to Washington. This was done by Lieutenant Colonel R. M. Campbell, Military Attaché in Mexico City. The method of protecting a message against the effectiveness of the iodine vapor test had been discovered as early as 1915 by the British and French (not, as Yardley maintains, by the Americans in 1918). The Patricia letter, moreover, was not found by a censor on the Mexican border, but by the San Francisco Censorship which sent the letter to Washington

[8] The authority for this statement and the other criticisms following, is to be found in marginal notes by Colonel McGrail in Mr. William F. Friedman's copy of The American Black Chamber. This copy of the book contains many criticisms from other firsthand sources.

[9] Pp. 55-60.

[10] The original documents accompanying the letter are now on file in the Office of the Director of Communications Research; the letter itself is in the Laboratory Branch.

because it was suspected of containing code. When some one in MI-8 thought she saw traces of secret writing between the lines of the letter, it was brought to Lieutenant McGrail who placed it under an ultra-violet lamp and read it—it was never treated chemically.

Apropos of Yardley's comments on Madame Victorica, it should be pointed out that she arrived in the United States on 22 January 1917, was arrested on 27 April 1918, and the letters were obtained and developed—some of them--in July 1918, when they were more than a year old. Her arrest led to the discovery of the letters, rather than the reverse. Enough evidence has been presented to show the essentially false and misleading character of the information on secret inks given in The American Black Chamber.

The Washington laboratory also supplied trained chemists requested by Paris in August 1918 to provide secret ink facilities for the testing of soldiers' mail. A small laboratory had been set up at the Base Censor's Office in Paris on 11 July 1918 under the direction of Captain Lucien J. Desha, Sanitary Corps. The first two months were spent in getting equipment and in experimental work. The first work was done by Captain Desha and four enlisted men, but trained chemists were needed. First Lieutenants G. C. Chandlee and D. F. J. Lynch, both trained in the Washington laboratory, spent a week in the British Laboratory in London, and reported for duty at the Base Censor's Office in Paris on 4 November 1918. On 13 November 1918 Second Lieutenants

P. S. Danner and Edward F. Snyder reported to the Base Censor directly from the Washington laboratory.

The close relations established by the Military Intelligence Division and the branches of the British Postal Censorship doing similar work made possible collaboration between the Base Censor's laboratory and these British offices. Most of the mail examined at the Paris laboratory was from soldiers in France to correspondents in neutral countries. During the period of the occupation of Luxembourg and Germany, several hundred letters from various divisions of the Army were tested each day. When this laboratory was closed on 8 February 1919, a total of 53,658 letters had been examined for secret writing. Of these, 428 reacted in such a manner as to require further examination but only two letters were found to contain secret writing.[11]

[11] Statements concerning the Paris laboratory are taken from an "Extract from Final Report of G-2-D, G. H. Q., A. E. F., May 1, 1919" (SPSIS 311.7, 1919-1940, Case No. 697, 1 May 1919.

CHAPTER VI. THE SHORTHAND SUBSECTION IN NEW YORK[1]

A. Organization and Personnel

The need for shorthand experts arose when, in October 1917, the Cipher Bureau began to receive from the Postal Censorship Committee certain documents suspected of containing ciphers. Some of these proved upon examination to be Yiddish and Arabic, while others were found to be shorthand notes. The latter were doubtless submitted to the stenographers available in the War Department, but some could not be read. The unreadable shorthand notes were apparently in foreign languages, or foreign systems of shorthand, or both.

To process this material, the services of Mr. Franklin W. Allen were secured. How Mr. Allen was selected for the task is unknown; the two accounts of the Subsection made by Major Yardley and Mr. Allen merely state that "recourse was had to Mr. F. W. Allen." He was, however, a partner in Hulse and Allen, a well-known firm of law reporters, with main offices at 165 Broadway, New York, and branch offices in a

[1] The evidence for all statements made in this chapter is to be found in a somewhat fuller account prepared in April 1945 by the Historical Unit, Signal Security Agency: The Shorthand Subsection of MI-8 in the First World War (1917-1919), and documented as IR 5042. Appendix A of IR 5042 is a rough draft of paragraphs on the Shorthand Subsection written in 1919 by Major Herbert O. Yardley, while Appendix B is the same draft as revised by F. W. Allen, chief of the Subsection. In addition to these two documents, the entire files of the Subsection were utilized.

number of other cities, including Washington. Hulse & Allen were official reporters for the Interstate Commerce Commission and the Federal Trade Commission. The choice of Mr. Allen for this work was peculiarly fortunate, for not only was he successful in handling the difficult problems presented to him as a shorthand expert and in recruiting linguists and stenographers for other units, but he also served throughout the war without compensation and, until May 1918, paid out of his own pocket all the expenses of his organization. He was, however, later reimbursed for these expenditures. The extent of Mr. Allen's contributions of time and money had by May 1918 become so great that he was requested "to organize the work as a sub-section of MI-8, which he consented to do, without remuneration," being granted the status of Chief of the Subsection as a civilian volunteer, and the staff was sworn in as Government employees. This unit is described as the earliest of the subsections formed in MI-8: since the Secret Ink Laboratory in New York was set up in November 1917, this statement must refer to the beginning of work by Mr. Allen, not to the formal organization of May 1918.

The earliest dated document now in the files is a letter of 29 December 1917 (IR 4238) from Captain Yardley to Mr. Allen, but the preliminary negotiations had apparently been completed at this time. On 11 July 1919 the Shorthand Subsection came to an official end: after 8 February 1919 there was no full-time shorthand expert working for MI-8, but special problems were processed on an hourly basis.

The Shorthand Subsection functioned in Mr. Allen's own office, which at first was at 165 Broadway, but was moved to the second floor of 244 Madison Avenue in May 1918. No charge was made by Mr. Allen for the space used by the Government, though most of the time there were at least three persons at work besides Mr. Allen himself. The latter did not apparently make the necessary transcriptions himself: he was probably not able to read the foreign systems of shorthand, but he deserved credit for organizing and directing the unit.

Six persons were employed on a full-time basis, not always simultaneously. The chief of these was Armand B. Coigne of Philadelphia, who was then so young that the prospect of his induction into the Army created considerable concern in the unit. Mr. Coigne performed the duties of examiner and classifier and also appears to have acted in Mr. Allen's absence as administrative assistant. To some extent he served as an investigator for Major Nicholas Biddle, who was Chief of a Military Intelligence unit at 302 Broadway: at least he was authorized to carry identification card No. 499. Mr. Coigne was on the Government payroll from about 24 May 1918 until 8 February 1919.

Miss Maria Norman, a highly trusted employee in spite of her German citizenship, was the Stolze-Schrey German stenographer. She worked from about 24 May 1918 until about 11 January 1919. In addition to transcribing the Stolze-Schrey problems, she also gave a good many shorthand and language tests to applicants for positions.

Besides Miss Norman, the German staff included at separate times two Gabelsberger stenographers, Franz D. May and Egon Eisenhauer.

did not, however, remain long with the unit and was ultimately replaced by Eisenhauer.

For Spanish shorthand there were two stenographers, both Spanish subjects, Vincente M. Noriega and José R. Alvarez. Noriega was able to command the largest salary paid to any one in the unit, ($175 per month.) In addition to these persons, a number of others worked from time to time on an hourly basis.

The expenses of the Shorthand Subsection were paid in the following manner: certain of the employees were paid by check received from the office of Major Biddle, while other expenses were paid in cash by Mr. Allen, who was later reimbursed by Major Biddle upon presentation of an account with supporting vouchers.

The total cost to the Government may be set down as follows:

Salaries	$3,563.39
Other expenses	785.53
Telephone charges	1,085.92
Miscellaneous (11 July 1919)	65.39
Initial expenses of Mr. Allen	641.41[2]
Total	$6,141.64

2. IR 5942, p. 7 and appendixes C, D, and F.

Mr. Allen himself was not the only person who gave voluntarily of his time and energy to the success of the work. Letters of appreciation were prepared for ten persons, mostly prominent shorthand experts, and signed by the Director of Military Intelligence. Several other persons, who, for unknown reasons, did not receive letters of appreciation, made similar contributions to the work. Mr. Allen was himself thanked in a personal letter signed by Secretary Baker, dated 3 October 1919.

The security of the Shorthand Subsection, existing as it did, in New York City, remote from the War Department, was relatively neglected. No document was ever marked SECRET and few were marked PERSONAL AND CONFIDENTIAL. No special military channels for communication between New York and Washington seem to have existed as the regular mails were used. Whether the more important documents were registered is unknown, since the envelopes were not preserved. To judge from the size of the telephone bills, communication of this type must have been frequent. Mr. Allen regularly signed himself as "Official Reporter, Shorthand Subsection, Military Intelligence, General Staff," and his letters to Washington always bore the information that his correspondents were also associated with Military Intelligence activity. He sent out much correspondence which might presumably be read by enemy aliens—some of it was—but even these circulars frankly divulged his official position.

B. The Shorthand Problem

The primary task of the unit, and the only one which engaged the attention of most of the persons on the MI-8 payroll, was the processing of shorthand documents. The expert knowledge of the staff probably solved many of the problems encountered without more training than they possessed at the outset, but it was well understood that in the traffic studied there would be represented many different systems of shorthand, and among these not only the well-recognized systems such as Gabelsberger and Stolze-Schrey in German, but also obscure systems used by only a few people. The first problem was therefore the preparation of an adequate bibliography on the subject of shorthand, with the ultimate creation of as large a shorthand library as possible. Accordingly, lists of special shorthand libraries were obtained, among others books on foreign systems of shorthand in the Chicago Public Library, the New York Public Library (Beale Collection), the Gabelsberger Shorthand Society of New York, the Phonographic Institute, Cincinnati, the John Crerar Library in Chicago, and the libraries of certain experts. From these sources, and probably others also, two card files were prepared:

a. Bibliography of foreign shorthand textbooks and manuals in public and private libraries in the United States; and

b. Bibliography of English shorthand publications in libraries in the United States.

Neither of these two card files is now available, but the library which was collected for use by the experts in the Subsection became the property of the Signal Intelligence Service at its foundation in 1930. It forms the nuclous of the somewhat larger collection used since February 1943 by the Special Examination Unit of the Signal Security Agency. In February 1945 there were 115 titles which could be definitely traced to the Shorthand Subsection Library, of which at least thirty-two titles came from the library of the Gabelsberger Shorthand Society. These had been obtained, apparently without payment, through the kindness of the president of the society, Dr. Rudolf Tombo, and the secretary, Mr. Jacob Compter.

The collection as finally built up by the Shorthand Subsection can be classified in the following way:

a. English and American systems of shorthand;
b. Gabelsberger shorthand;
c. Stolze-Schrey shorthand;
d. Various other foreign shorthand systems;
e. Masterpieces of German literature transcribed in shorthand.

Among the foreign systems represented are some in French, Spanish, Italian, Hungarian, Turkish, modern Greek, and the southern Slavic languages.

Using this material as fast as it was obtained, the shorthand experts prepared charts of the chief characteristics of each known system. A total of 54 different systems was ultimately included.

When a shorthand document was received for study, an attempt was made on the basis of these charts to identify the system with those already known to the experts. In some cases, however, no success could be obtained by this method, and then Mr. Allen would send photostats of the document to any experts not on the staff whose knowledge might be presumed to cover the systems used in the documents in question. When this source also failed, the shorthand notes would be studied by the experts precisely as if they were dealing with cipher. Frequency studies would be made of the characters in the document and compared with similar frequency tests of known systems. In this way it was possible to transcribe the text of shorthand notes in systems completely unknown to the staff.

Weekly progress reports were submitted from 14 June 1918 to 20 January 1919 and are still extant in TR 4387. A total of 76 questioned documents came to the Subsection from the following sources:

a. MI-8 in Washington: 46 problems;
b. The Executive Postal Censorship Committee in New York: 22 problems;
c. The Bureau of Investigation, Department of Justice: 2 problems;
d. The Office of Major Biddle in New York: 4 problems;
e. Other sources: 2 problems.

Upon receipt a document was at once studied by a member of the staff and a report was forwarded by Mr. Allen at the earliest possible date, giving the following facts:

a. The language used;
b. The shorthand system used;
c. A transcription in the original language;
d. An English translation of the text.

The following documents were received from MI-8 in Washington:

(1) The Francisca Martin note (IR 4238)
(2) The Teresita letter (IR 4238)
(3) The Castellanos letter (IR 4268)
(4) Unknown problem (IR 4179)
(5) The Brother Antonio correspondence (IR 4194)
(6) Unknown German problem (IR 4191)
(7) The Genoveva-Chita letter (IR 4263)
(8) The John F. James Letter (IR 4252)
(9) The Arthur de Villers notebooks (IR 4255)
(10) The Maria Roblos Leon notes (IR 4171)
(11) The N. Grayson papers (IR 4198)
(12) The Felix Conde letter (IR 4199 and IR 4252)
(13) The Fabela papers (IR 4183)
(14) The May Anderson letter (IR 4187)
(15) The José Ibarra Sanchez (IR 4271)
(16) The Bouilla letter (IR 4182)
(17) The People's Council Correspondence (IR 4263)
(18) The Hermann Lange notes (IR 4274)
(19) The Miss Z. Jacobs letter (IR 4251)
(20) The Reyes O letter (IR 4257)
(21) The Gallaga letter (IR 4231)
(22) The notes of Lieutenant Commander Coulman of the "Planet" (IR 4196)
(23) Papers from the German Legation at Stockholm (IR 4230)
(24) The Paul E. Hernandez letter (IR 4259)
(25) The Matthew Kiernan notes (IR 4270)
(26) The Hernandez letter (IR 4173)
(27) The Grand Rapids notes (IR 4178)
(28) The Ernest Eichenberg notes (IR 4190)
(29) The Alejandro Finco letter (IR 4267)
(30) The Luiz Valenzuela letter (IR 4236)
(31) The Rodriquez-Villalobos notes (IR 4240)
(32) The Cota letter (IR 4195)
(33) The Bravo letter (IR 4181)
(34) The Josefina Valarde case (IR 4239)
(35) The Jesus Cortes letter (MI-8 No. 10110-656)
(36) The Mrs. Mollie Frico Cook letter (IR 4200)
(37) The Zurita letter (IR 4150)

(38) The Rodriguez-Villareal letter (IR 4150)
(39) The Gretchen Sander letter (IR 4170)
(40) The Margrit letter (IR 4176)
(41) The Juan Janez letter (IR 4150)
(42) The G. Hallemon notes (IR 4150)
(43) The Mollie letter (IR 4150)
(44) Four words of shorthand (IR 4150)

Most of these problems produced only negative results: persons suspected of illicit communications were often exonerated when the shorthand notes which they had written could be read. In a few cases, however, the evidence showed that the writers had been engaged in questionable practices or that the writers were known to be enemy agents, and the transcription of the notes proved valuable to the authorities who were investigating the cases.

One of the latter cases was that of the People's Council correspondence (No. 17). This problem originated with the Intelligence Officer of the Western Department on 8 June 1918 and was submitted to Mr. Allen on 14 June 1918. It consisted of three shorthand notebooks photographed by Ignatius McCarthy, special agent of the Department of Labor, who on the night of 6 June 1918 gained access to the offices of the People's Council in the Foxcroft Building, San Francisco, and seized the three notebooks and other papers. They were the property of Bluma Zalaznek, alias Bluma Krause, then under secret indictment, but little is known of these notes. Mr. Allen wrote to Captain Yardley in Paris on 30 August 1918 (IR 4149) that the problem would produce about 400 pages when completed. The documents themselves are missing.

A second case submitted 3 September 1918 which was of considerable interest because a German Naval Officer was involved, was that presented in the notebook taken from Lieutenant Commander Coulman of the "Planet." But the notes consisted merely of records of Coulman's reading, the plan of an original short story, some material on religious matters and Coulman's opinions on society and the war.

The office of the Postal Censorship Committee, also called the Executive Postal Censorship Committee, was located at 641 Washington Street, New York City. On duty in this office was Captain Benjamin N. Day, who forwarded twenty-two shorthand documents to Mr. Allen, as follows:

(1) The Mount Hermon School case (IR 4249)
(2) The Gertrude Fox note (IR 4256)
(3) The Luisa Sanchez notes (IR 4243)
(4) The "J. G." note to José Herrera (IR 4256)
(5) The Tully-Lozano card (IR 4262 and IR 4243)
(6) The C. F. de la Reguera notes (IR 4243)
(7) The Frank P. Lucey notes (IR 4243)
(8) The A. Caballero notes (IR 4256)
(9) The P. K. Wilson notes (IR 4243)
(10) The Lamentin Letter (IR 4266)
(11) The Emil letter (IR 4184)
(12) The Garcia-Gonzalez letter (IR 4234)
(13) The Langmaack letters (IR 4172)
(14) The Weinhart letter (IR 4175)
(15) The Friscilla letter (IR 4253)
(16) The Romero letter (IR 4186)
(17) The Juan Fernandez letter (IR 4174)
(18) The Berliavsky letters (IR 4193)
(19) The Bernardo Pago Canido letter (IR 4197)
(20) The Vincentico P. Aguayo letter (IR 4185)
(21) The W. R. Grace commerical letter (IR 4235)
(22) The Grutter letter (IR 4233)

Of these the Mount Hermon case was important (though the results were negative), because in the period before the War the School had employed two Germans who disappeared at the outset of hostilities. The note to José Herrera may have been sent by a man engaged in espionage, but the transcription led to nothing. The Langmaack letters, sent by a German in Lima to his brother in Mexico, showed clearly hostile intent, though probably no subversive activity. The case of the Juan Fernandez letter is different. This problem was submitted on 26 August 1918; the report is dated three days later. The letter was signed "P" and addressed to a post office in Camaguez, Cuba. "P" wrote in Spanish, using the Marti system. He appears to have been a pacifist, laments the drafting of his friend, and speaks hopefully of German victory.

Two documents, neither of much interest, were submitted by the Bureau of Investigation, Department of Justice:

(1) The John Rinder case (IR 4265)
(2) The letter from the German mother (IR 4247)

Somewhat more significant were the problems submitted by Major Biddle's office:

(1) The Victor Weiss note (IR 4390)
(2) The letter to Count Bernstorff (IR 4155)
(3) The Edmund Vater alias Edmund Walter papers (IR 4237)
(4) The Pan-American Supply Company letters (IR 4155)

Weiss had a criminal record and was being held on charges of blackmail by the New York police. His notebook proved conclusively that he had been engaged in espionage activity. The letter to Count von

Bernstorff was of importance only because the addressee was well known: it proved merely to be a greeting. Edmund Vater was an itinerant peddler who may have been engaged in espionage. The Pan-American Supply Company letters were unimportant.

C. Recruiting for MI-8

During May 1918 Mr. Allen had been successful in recruiting shorthand experts for his Subsection and it was doubtless this success that led Captain Yardley to ask him on 4 June 1918 to extend his recruiting to other fields. Ultimately, recruiting involved the supply of:

a. Linguists for MI-8;
b. Army Field Clerks for France;
c. Army Field Clerks for the Siberian expedition.

The first request was for three experts who could think in German, were willing to work for $1,400 a year, and were above draft age. A week later a similar call was made for three persons

Ultimately, Mr. Allen stated[3] that he had supplied six cryptographers to MI-8. The names of only

[3] IR 5042: appendix B.

four are known, Misses Anita Thomas, Dorothea B. Jachens, Ruth Willson, and Anne F. Carter. He also mentions having supplied twelve candidates for commissions, of whom the names of ten only are known:

Captains	F. B. Luquiens
	Robert H. Marvin
	Herbert S. Spencer
Lieutenants	H. G. Campagnoli
	Eugene Jackson
	Robert H. Keener
	Charles G. Montross
	John S. Norris
	H. C. Skinner
	Austin W. Works

On 17 June 1918 General Pershing requested in cablegram No. 1323 "fifteen stenographers competent to take down examinations of German prisoners." In the course of events, this request was referred for action to Mr. Allen by the Chief, Military Intelligence Branch. Mr. Allen had no success in getting any candidates from the Committee on Classifications of Personnel in the Army. He accordingly wrote a large number of letters to representative persons in the law reporting profession, consulted employment agencies known to furnish German stenographers for commercial and legal purposes, and even advertised in German-American newspapers. As the replies were received, each suggestion was followed to its conclusion, and each person to whom Mr. Allen wrote was asked to make recommendations in turn. The result was that a very large number of persons was enlisted in the search,

and a census of German stenographers was compiled. This census contained the names of approximately 400 stenographers writing German systems of shorthand. A difficulty which plagued the search was the fact that, at first, only native-born Americans were eligible, but this requirement was later relaxed and naturalized citizens could be appointed.

How many stenographers were ultimately obtained is not known but the following were sent to France:

Jacob Bleibtreu
John W. Greb
Arthur Hurtig
Seymour F. LeBell
Frank H. Lomer
Otto A. Milbauer

About 15 August 1918 a special call was received to supply two persons qualified for appointment as Army Field Clerks to serve as stenographers with the American Expeditionary Forces in Siberia. Two men were located on three days notice, but the name of only one of these is known, Henry H. Werblow.

CHAPTER VII. CODE COMPILATION IN FRANCE

A. Introduction

In the summer of 1917, when the first units of the American Expeditionary Forces arrived in France, only three authorized cryptographic systems were available. The first was the large code designed for administrative telegraphic correspondence, the *War Department Telegraph Code 1915*,[1] but in addition to the insecure features of this code, it was not adapted for rapid and efficient tactical operations. The second was the well-known Vigenère cipher system (with repetitive keys and reversed standard alphabets); the means employed was a simple celluloid device called the Army Cipher Disk. The third was a field cipher system called the Playfair Cipher, copied from the British cipher of the same name. Measured by the standards of 1941, the American Expeditionary Forces were cryptographically unprepared. The British and French allies were, moreover, very reluctant, for obvious reasons, to divulge their hard-earned information on communications security.[2] By 11 November 1918, however, the American

[1] See Volume One, pp. 110-114, for a description of this code which in addition to being one-part, had, as was later learned, been compromised.

[2] This was in France. The insecurity of the *War Department Telegraph Code 1915* was so great that they did reveal its unsatisfactory nature to the authorities in Washington. See above, pp. 28 ff.

Expeditionary Forces had caught up and even, in some cases, surpassed the other Allies, so that the latter were even adopting American cryptographic methods.[3]

Four important factors led to the increased use of codes and ciphers for wartime communications. The first was the augmented use of wire communication following the great inventions of the nineteenth century. The second factor was the greater mobility of tactics made possible by many inventions in the field of transportation and the consequent increase of speed of communications made necessary thereby. The invention of the radio and its speedy adoption as a military aid was the third factor. This created one problem, the danger of radio interception, and solved another, the great demand for wire formerly used so much in telegraphic communications. The fourth factor was the invention and development of aircraft and the speedy adaptation of aircraft to military operations.[4]

Cryptographic systems in the American Expeditionary Forces embraced three forms: manual ciphers, cipher devices, and codes, both unenciphered and enciphered. The United States Army Cipher Disk was the only cipher device known to the American Expeditionary Forces. This device, though taught at the Army Signal School in the

[3] William F. Friedman, *American Army Field Codes in the American Expeditionary Forces during the First World War* (United States Government Printing Office: Washington, 1942), p. 1.

[4] *Ibid.*, pp. 2-3.

A ri an eqltion ry Forces, was never Us-d in France. The ?lay fair tipher,: elso taught at th signal School, was not ver secure. Prior to 1914 th'e highest headquarters nd the headqu rers staffs in t!e u rted St tcs Army had alono en;lo-d cee systems in communications. In the field certni disadvantares in the use of a codo system \icre encountered. First there was the difficuty of COIpi-ig and reproduci g codes by fi'ld forces under field conditions. Se' ond1 th e was the blem of the proper distribution of copies, whi" -had to be sen to many -idely". cattered orgaizatio . Thi., 'there nas the r tte'r of the proper safeg u dig and accouting for the e copies.[5]

A aptain:(l!o:ard R. Bares), three second lieutenans, ad one corp ral cc:pri;ed the Code Compilation Sc tion o'rg'nized in Decec . ⓟ 1917. Th uit wa a Sign n Corps organization and a short account of its work appea; 'as Chapter XXXIII in the Report of the Chief Si nl Officer to the SecretarY of :a 1919. They Ylere assigned 'to duty at General lieaduat rs, ericon E editionay Forces, nnd at once set to T:ork CCop i i & for field use small codes theh a .ed "trench codes".[6]

[5] Ibid., pp. 4-5.

[6] Ibid., p. 9; Howa n R. B nc , Renrt of C:de Com: lation Section, Gcnc r Headrmnrtc:s, A ric.n Exreditionary Forces, DEconbe! 1917-November 1918, (United States GovcrrJcnt Print i Office, Washington, 1935), p. 2.

B. The American Trench Code

The American Trench Code[7] was a sectional, one-part code, using groups of three letters or four digits. It was issued in 1918 by command of General John J. Pershing, signed by Brigadier General James G. Harbord, Chief of Staff, and Benjamin Alvord, Adjutant General, and was printed in the Adjutant General's Printing Office, France.

This code, designed to be distributed as far down as and including companies actually in the line, was printed in a breast-pocket, paper-bound, edition, about 4-1/2 by 7 inches in size. The code was printed in an edition of 1,000 copies, but never actually reached the front line, because the danger of capture was considered too great. Its lowest point of actual use was therefore regimental headquarters.

The code book consisted of 32 pages of code groups, numbered 4 through 35, with one page of instructions for the use of these groups. Two opposing pages were taken together to form a cryptographic page, each containing space for 100 groups. The size of the code was therefore 1,600 groups. Five blanks at the end were prepared for addenda. The line symbols were the dinomic sequence 01 to 00. Paralleling the two-digit code groups down the page were two-letter line symbols of vowel-consonant form (J, Q and X were omitted and the digraphs AH and OH were omitted also), making exactly 100 digraphs to correspond to the

[7] Friedman, op. cit., pp. 9, 132-139; Barnes, op. cit., pp. 2-6; *The American Trench Code* (The Adjutant General's Printing Office, 1918).

100 dinomes. At the top of each double page appeared the page symbols, which were either two digits or single letters. The digit page symbols ranged from 12 to 27, the letter page symbols being all consonants (H, J, Q and X were omitted). The code clerk was expected to form code groups, either digits or letters, by prefixing the page symbols to the line symbols. In this way digit code groups would range from 1200 to 2700 inclusive, while letter groups would range alphabetically from BAB to ZYZ, no J, Q, or X, ever appearing.

The first 131 plain equivalents provided for the hundred plain dinomes, a few decimals, and the days of the week and months, as well as a few frequent abbreviations. Then, beginning with code group 32 on page 13-C (the plain equivalent of which was A,) the plain equivalents progressed in alphabetical sequence throughout the remainder of the code book, i. e. the code was one-part and sectional.

Starting with the second page (6-7) there appeared in the right-hand margin of each page, near the bottom, four lines containing the following:

—ed—-1721---HEG
—ing-—1999---LYW
—-ly—2083—MUZ
-ment—-2121—-NEG

These are the most commonly used prefixes and suffixes which, although they appeared in their proper places alphabetically were also repeated on the margin of each page to save time in hunting for them.

In case a phrase was used several times in the same message, different code words were to be chosen each time, and, if possible, the phrase was broken up into separate words. When numbers were sent in the clear, they were always to be preceded by the figures 2370 or the letters RUF, a code group meaning "Read next (following) group in clear". The loss of a code book was to be reported by number at once through military channels to General Headquarters, American Expeditionary Forces. The code group 1592 = FYM stood for "Code lost (memorize group)".

With the code were employed monoalphabetic encipherment tables—30 different tables were issued. Such a table was prepared on a separate card, then called a "distortion table", which accompanied each copy of The American Trench Code, but was not printed in the code book. Additional security was effected in this manner, because the distorted alphabet would be frequently changed. Figure 5 shows the appearance of the card.[8]

The effect of the use of such a table was small, since all that was involved was monoalphabetic substitution. The enemy cryptanalyst was expected not to recognize the code group FAG when he saw it in the distorted form OGZ, but since all plain code groups had the form of consonant-vowel-consonant, such a group would at once cause him to

[8] Friedman, op. cit., p. 142; Barnes, op. cit., p. 5.

13-a

THIS TABLE MUST NOT FALL INTO THE HANDS

OF THE ENEMY

1. If destroyed to prevent capture, report will be made to the office to which its return is ordered.

2. This table will be used from 3 a.m. .... to 3 a.m. ...., after which it will be returned in sealed envelope to.......................................

ENCIPHER

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	U	V	W	Y	Z
g	k	h	w	a	o	z	n	t	f	i	l	y	b	e	s	r	d	p	c	v	u	m

DECIPHER

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	r	s	t	u	v	w	y	z
E	O	V	T	P	K	A	C	L	B	M	Z	H	F	U	S	R	I	Y	W	D	N	G

Key word..........................
Service message...................
Private message...................

Figure 5

suspect that a different code was involved. By separating the intercepted traffic into the consonant-vowel-consonant type and the other messages, code reconstruction could progress on the basis of unenciphered code. If in some way, the remaining traffic could be sorted into homogeneous piles, they also were material for unenciphered code reconstruction. The use of a "Distortion Table" amounted only to the issuance of a new code with the same plain equivalents: it did not cut down frequencies within messages or within the volume of unenciphered traffic.

Physical security of the code book was provided for in the ninth and eleventh instructions for using the code (page 3), where the burning of all papers used for encoding and decoding the message was ordered, and direction is given that subordinates were to be informed where the code was being carried so as to save it in an emergency. The tenth instruction states: "Your secret instructions for this code must always be used in connection with it." Neither a copy of these secret instructions nor the distortion tables which acccompanied the code are available. The copy available is marked with the notation by Mr. William F. Friedman (1921) that the American Trench Code was issued about March 1918 but was immediately recalled as too easy to solve. With this judgment, posterity can only concur.

C. The Front Line Code

The Front Line Code,[9] a sectional, one-part code, using a two-letter group, was issued by General Headquarters, American Expeditionary Forces, in 1918. An edition of 3,000 copies was printed and distributed for emergency use down to companies. This code and the American Trench Code probably did not remain in force longer than two months, and there is a possibility that they were never used except for training purposes. The size was about 3-1/4 by 7-1/2 inches, and it more easily fitted a pocket than the American Trench Code.

The code book consisted of twelve pages, of which pages 3-12 had plain text and their equivalent code groups on them. This code was strictly a letter code, without the use of digit groups. There were 500 two-letter code groups of which 25 were blank at the end of the code book. These code groups were arranged alphabetically, running from AB to ZZ. Each letter of the alphabet was used except J, Q, and X. Doublets were omitted but not double vowels, except AE, IE, OE, UE and YE. The digraphs might therefore have a vowel or consonant in either position or both.

The code was sectional only to the extent that the first ten were the digits 0-9. There was no syllabary proper, except that a code group stands for each plain-text letter. As a result, words which

[9] Friedman, op. cit., pp. 9-10, 223-229; Barnes, op. cit., p. 6; The Front Line Code (Adjutant General's Printing Office, 1918).

were not in the code had to be spelled out by digraphs for single letters. Eight nulls were provided throughout the code with the following plain equivalent wording: "(This group means nothing)." No code group read: "Code lost."

For encoding, a code group was substituted for each plain equivalent. No words were to be sent in the clear in the message.

The same type of distortion table which was used for the American Trench Code was also used for this code, the cipher equivalents being frequently changed.

As in the case of the American Trench Code, provisions were made in the instructions for the physical security of this code book and all worksheets connected therewith. The preparatory remarks also alluded to secret instructions to be used with the book, but they are no longer available.

A code of only 500 groups is, of course, insecure when not enciphered, and impractical in any case because of the lack of many groups. When words were missing, they had to be spelled out. Moreover, the same criticism applies to the monoalphabetic substitution encipherment tables as was made of those used with the American Trench Code.

D. The "River Series" Codes

When the principle of the two-part code was adopted in compiling

American Expeditionary Forces field codes, the name Potomac Code[10] was given to the first of a series designated by names of American rivers. It was issued on 24 June 1918 in an edition of 2,000 copies, and, like all subsequent trench codes in the "River Series" and "Lake Series," was sectional and two-part. The code group was formed of three letters, and variant groups were introduced. The code was issued to all combatant troops down to battalions. Although intended for communication within the division, it could also be used for messages to higher headquarters. G-2 had planned the distribution of the code in three editions—one to regiments, one to Army Headquarters, and one to be held in reserve at General Headquarters. With the Potomac Code began the policy of relieving the front line of all possible extra work in connection with compiling systems or enciphering and deciphering the code messages, thus transferring this security burden to headquarters. Secrecy was provided by the frequent revision and reissuance of code books. Messages in this code could be transmitted by any means, but radio or ground telegraph was not to be employed unless more secure means were unavailable. The code was captured in July 1918, one month after its issue.

The Potomac Code was printed in typewriter type, about 7-1/4 by

[10] Ibid., pp. 17, 153-159: Barnes, op. cit., pp. 6-7, 13-15; The "Potomac" Code, General Headquarters, American Expeditionary Forces, (Adjutant General's Printing Department, G. H. Q., A. E. F., 1918.)

9-3/4 inches in size. Besides 10 blank lines for addenda, it contained 1,787 plain equivalents and 681 variants, making 2,478 code groups. The code book consisted of two pages of instructions, 18 pages of encode, and 35 pages of decode. On each page of the encode were two columns of 50 lines each, making 100 lines to the page, but in the margin of each column (except the first column) was a null, 35 nulls in all. Under each null was printed a list of spelling groups, usually with some code variants. These spelling groups and the number of times each appeared in the encode are as follows: Ed (8), En (7), Er (7), Es (8), Ing (11), Ion (10), Ll (9), Ly (9) Nd (11), Re (8), S (9), St (11), Th (11). Nulls were never repeated, but some of these spelling groups were.

The first page (5) of the encode consisted of the numerals 0 to 99. Following these were code groups for 100, Decimal point, 4.2, 5.9, 9.2, 9.45, 9.5, 155, 240, and months of the year. Thereafter, the general vocabulary followed, including letters, spelling groups, words and phrases. The days of the week were listed in their respective alphabetical order. Variant code groups were frequent. One code group read "Codo lost (memorize group)...DAY."-

In the Decoding Section, the nulls and spelling groups were, of course, incorporated in the body of the plain equivalents. The trigraphic groups were formed with either consonant or vowel in any position, but E, I, H, T, and U, were not used in first position; D, H, Q, T, and Z, were never used in second; and I, Q, and Z, were never used in third. No group contained a repeated letter.

In transmitting a message in this code, the number of the message and the hour of filing were sent in clear text preceding the first code group, and the order directing transmission was sent in clear and placed under the message, but the signature itself was only sent when absolutely necessary, and then in code. As a rule, the point of origin of a message could be indicated by a code group in the code book. When the context of the message clearly indicated the addressee, addresses were not to be used, but when used they were always to be encoded. For every ten code groups a null was prescribed, placed at irregular intervals. A null was always to be used between double letters, in case the word was spelled out.

The messages were to be kept short, but if a long message needed to be sent, it was always to be divided into two or more parts sent as separate messages. When the message was long, unnecessary words were to be left out. This sequence was always to be adhered to: number of message, hour of filing, body of message, order directing transmission.

The instructions included the following provisions for security:

> Messages once transmitted in clear or in any other code or cipher must not be repeated in this code.
>
> Messages once transmitted in this code must not be repeated in any other code or cipher or in clear.

From June to November 1918 a series of 14 codes was prepared—

nearly three codes per month. On 15 July the Suwanee Code,[11] 2,500 copies followed the Potomac Code, but contained no radical change. This code was likewise a sectional, two-part, field code using a trigraphic group with variants, and it was issued to all combatant troops down to battalions. Its code groups numbered 2,500[12] (1,787 plain equivalents, 45 blanks, and 668 variants). The instructions for its use were exactly the same as for the Potomac Code, even to the two examples, though not their code groups. The 35 nulls and spelling groups were placed in the same manner in the margin of each column (except the second column of page 22) with, of course, co equivalents different from those used in the preceding code. One group read: "Code lost (memorize group)....LOB."

The preliminary section containing numerals and a few special groups was identical with that in the Potomac Code. The encode filled 18 pages, the decode 25 pages, both being identical with pagination of the Potomac Code. In contrast to the ten blank lines for addenda in the Potomac Code, the Suwanee Code had 45 blanks.

The code groups again might have a consonant or vowel in any position, but no E, H, I, T, or U in first position; no D, H, Q, T,

[11] Friedman, op. cit., pp. 18, 160-164; Barnes, op. cit., p. 7; The "Suwanee" Code, General Headquarters, American Expeditionary Forces, (Adjutant General's Printing Department, G. H. Q., A. E. F., 1918.)

[12] All later field codes were the same size, though the number of plain equivalents would fluctuate somewhat.

or Z, in second; and no H, I, Q, or Z, in third.

The Wabash Code,[13] also a sectional, two-part code, using trigraphic groups with variants, was issued in an edition of 2,700 copies on 31 July to all combatant troops down to battalions in the First Army. It followed the same general plan as the two preceding codes. It contained 1,768 plain equivalents, 51 blanks, and 681 variants, making 2,500 code groups, as in its predecessor. The instructions for its use were the same as in the case of the two "River Series" codes previously described, with the exception, of course, that the code groups for the plain equivalents in the sample message were different. The location of the nulls and spelling groups was again the same. One group read: "Code lost (memorize group)....LPU." The pagination was the same as for the other two codes in this series, and so was the preliminary section of numerals and special groups.

This code left 51 blanks at the end of the encode for addenda and the code groups assigned to them were two-part in order. Hence, there was no blank section at the end of the decode, as in the case of the Potomac Code and the Suwanee Code.

Following the Wabash Code came the Mohawk Code,[14] issued on

[13] The "Wabash" Code, General Headquarters American Expeditionary Forces, (Adjutant General's Printing Department, G. H. Q., A. E. F., 1918.)

[14] The "Mohawk" Code, General Headquarters American Expeditionary Forces, (Adjutant General's Printing Department, G. H. Q., A. E. F., 1918.)

3 August, in an edition of 3,200 copies. It was captured in October 1918. This code was also sectional and two-part, using four-digit groups with variants, the first code using digit groups to be prepared for the American Expeditionary Forces. Again, there were 2,500 code groups—1,771 plain equivalents, 44 blanks, and 685 variants. The code groups ranged from 2500 through 4999.

The pagination for this code followed the same pattern used in the first three "River Series" codes. There was one null in the margin of each column (except the last) of the encode but there were no spelling groups. One group reads: "Code lost (memorize group).... 3782." The preliminary section of numerals and special groups were again the same as in the previous codes of the series. There were 44 blanks for addenda with code groups in two-part order.

The Allegheny Code[15] was issued on 12 August in an edition of 3,200 copies. It was also a sectional, two-part code using a four-digit group with variants. Its code groups were 2,477 in number, counting 1,773 plain equivalents, 47 blanks and 657 variants. The first group was 1500, the last 5996, a total of 2,019 groups being omitted according to an irregular pattern. This marked a definite advance toward greater security but the code was captured by the Germans in October 1918.

[15] Friedman, op. cit., pp. 18, 173-175; Barnes, op. cit., p. 7; The "Allegheny" Code, General Headquarters, American Expeditionary Forces, (Adjutant General's Printing Department, G. H. Q., A. E. F., 1918.)

The *Allegheny Code* closely resembeld the *Mohawk* in spelling groups printed in blocks, numerals, and the first 21 plain equivalents. There were however, 47 blanks (instead of 44) for addenda, again arranged in two-part order. The instructions for the use of the code were the same as before with the usual exception, i. e., the code groups used as illustrations were different.

On 2 September the *Hudson Code*[16] was issued in an edition of 3,200 copies. It was also a sectional, two-part code using a four-digit group with variants. Its code groups were 2,485 in number— 1,909 plain equivalents, 46 blanks, and 530 variants. The range was again from 1500 to 5996, with 2,011 groups omitted in an irregular pattern.

In pagination and lack of spelling groups printed in blocks, the form of the *Allegheny Code* was followed, but there were some changes in the placing of the sequence of numerals (00 to 100) and in the special words on the second page, where the months of the year and the days of the week no longer appeared but were given in normal alphabetical progression throughout the encode. At the end of the encode were 46 blanks for addenda, in two-part order.

Instead of one null in the margin of each column as was the case in all the preceding codes of this series, there were five to each

[16] Friedman, *op. cit.*, pp. 18, 175-178; Barnes, *op. cit.*, pp. 7, 16-17; The "*Hudson*" *Code*, General Headquarters, American Expeditionary Forces, (Adjutant General's Printing Department, G. H. Q., A. E. F., 1918.)

column (except the last), making a better reminder to the code clerk that nulls should be used. This made a total of 175 nulls, at least one to be used for every ten code groups in a message. In this code the group reading "Code Lost (Memorize this group)...2222" did not appear in the code proper. Instead, it was printed in red (as is the copy number) on the outside cover of the code book.

The last code in the "River Series" was the Colorado Code,[17] issued on 24 September in an edition of 3,200 copies, again using letter groups instead of digits. From the beginning of the "River Series" of codes, the code books had been gradually reduced in size until the final format of 5-1/2 by 7-1/2 inches had been reached as compared to the 7-1/4 by 9-3/4 inches of the Potomac Code. Another innovation was the printing of sixteen spelling groups at the bottom of each two pages, with two or more variants for each plain equivalent. On the outside cover were printed in black these words "Memorize This Group: 'DAM——Code Lost'".

This code was sectional and two-part and used a three-letter group with variants. No explanation of the abandonment of the four-digit type of code group and a return to the three-letter type is

[17] Friedman, op. cit., pp. 18, 179-183; Barnes, op. cit., p. 7; The "Colorado" Code, General Headquarters, American Expeditionary Forces, (Adjutant General's Printing Department, G. H. Q., A. E. F., 1918.)

available. The first three of the "River Series" of field codes—the Potomac, the Suwanee, and the Wabash—were three-letter codes. The next three of the same series—the Mohawk, the Allegheny, and the Hudson—were four-digit codes. The last of the series--the Colorado—and all four of the "Lake Series," which were issued prior to 11 November 1918, were three-letter codes. The four-digit code group was probably found to be less practicable in transmission.

Again, there were 2500 code groups—1,929 plain equivalents, 51 blanks, and 520 variants. The preliminary section of numerals, etc. follows exactly the pattern of the Hudson Code. At the end of the encode were 51 blanks which had two-part characteristics. There were five nulls in the margin of each column (except the last two), as in the Hudson Code. The total number of nulls was 190 groups. The group reading "Code Lost (Memorize this Group)...DAM" did not appear in the code proper. Instead, it was printed in black on the outside cover of the code book, so as more easily to be memorized, and read: "Memorize This Group: DAM—Code Lost." The instructions for the use of the code were the same as before with the usual exception, i. e., the code equivalents were different.

E. The "Lake Series" Codes.

Sometime in September 1918 it was decided to issue a new series of codes, known as the "Lake Series," to the Second Army, and to reserve for the First Army alone the use of the current edition of the "River Series". The first code issued in the "Lake Series" was the Champlain Code,[18] of which 2,500 copies were distributed on 7 October 1918. To differentiate between the two series, the cover printing on the "River Series" was in black ink, that of the "Lake Series" in red ink.

The Champlain Code was also sectional and two-part, using a three-letter group with variants. It contained 1,931 plain equivalents, 69 blanks, and 500 variants, making a total of 2,500 code groups. The Champlain Code closely resembled the Colorado in nearly every respect. One slight difference was in the treatment of the spelling group where "-nt" was replaced by "-un" in the proper alphabetical position.

At the end of the encode were 69 blanks for addenda, in two-part order, and the instructions for the use of the code were the same as before with the usual exception; i. e., the code groups were different.

Instructions had been issued directing that all messages sent in the "River Series" should be preceded by a three-letter group (not actually a code group but an unenciphered discriminant), which

[18] Friedman, op. cit., pp. 18, 189-191; Barnes, op. cit., p. 7; The "Champlain" Code, General Headquarters, American Expeditionary Forces, (Adjutant General's Printing Department, G. H. Q., A. E. F., 1918.)

would indicate the particular code used. Thus a Hudson message was preceded by HUD; a Colorado by COL; an Osage by OSA, etc. These instructions when used for the "River Series" were issued separately and no mention of these discriminants was made in any code book prior to the issuance of the Huron Code on 15 October 1918. The discriminants thereafter appeared on the outside cover of each code book as well as in the preliminary instructions in the code book itself.

The second of the "Lake Series" of field codes was the Huron Code,[19] 2,500 copies of which were issued on 15 October. In the back of the code book was prepared a detachable double receipt for the convenience of officers who received and returned the code books. This code was also sectional and two-part and used three letter code groups with variants. There were 2,500 code groups in this code—1,927 plain equivalents, 60 blanks, and 513 variants. In every respect except the assignment of code groups to values and the number of blanks for addenda (60 in this case), the Huron Code vocabulary followed the norm set by the Champlain.

The instructions for the use of the code underwent several changes worthy of special mention. First, all the "River Series" codes and the first code of the "Lake Series" codes state in their instructions that the code book is issued "to all combatant troops down to battalions".

[19] Friedman, op. cit., pp. 18, 192-194, 211; Barnes, op. cit., p. 8; The "Huron" Code, presumably published by General Headquarters, American Expeditionary Forces, but no statement in the code book appears to that effect.

and that, although "it is primarily intended for communication within the division," it "may be used for messages to higher headquarters." Beginning with the Huron Code and continuing on through the Osage Code, the instructions state that the code book is to be issued "to division, brigade, regimental, and battalion headquarters of your division. Whether or not it is issued to neighboring divisions must be determined by you before you send them telegrams encoded by its use." This departure tended to bring about greater security, as the distribution of the code book was not so wide as before.

Second, a phonetic alphabet for use in telephoning messages was included in the instructions. When such messages in this code were sent by this means, they were always preceded by the word "Huron". The phonetic alphabet provided is as follows:[20]

A	Able	N	Nan
B	Boy (Baker)	O	Opal (Oboe)
C	Cast (Charlie)	P	Pub (Peter)
D	Dock (Dog)	Q	Quack (Queen)
E	Easy	R	Rush (Roger)
F	Fox	S	Sail (Sugar)
G	George	T	Tare
H	Have (How)	U	Unit (Uncle)
I	Item	V	Vice (Victor)
J	Jig	W	Watch (William)
K	King	X	X-ray
L	Love	Y	Yoke
M	Mike	Z	Zed (Zebra)

"Example: If the operator receives 'buy' as 'vie,' and difficulty is experienced in distinguishing 'B' from 'V' 'buy' may be spelled 'boy-u-y.'''

[20] In parenthesis are placed the 1945 equivalents when these are different.

Third, this was the first code to bear instructions for the use of a discriminant. Instruction 4 read: "Coded messages sent by telegraph or radio will be preceded by the group 'HUR.'" On the outside cover of the code book was this statement: "Precede every message in this code by 'HUR'".

Fourth, the last instruction which had not appeared previously in any of the American Expeditionary Forces field codes studied so far, stated that any new words or changes since the last edition (the *Champlain Code*, in this instance) had been marked with an asterisk (*). As some of these new words seem quite useful, it is odd that they were not included in former editions. A list of them is given here to show that type of word or phrase formerly omitted is now considered desirable: *call letter*, *Chief of Staff*, *consult*, *distance*, *done*, *enemy being relieved*, *enemy reinforcements*, *furnish*, *in the neighborhood of*, *intensifier*, *is this correct*, *known*, *liaison officer*, *list next* (not a new word--the *Champlain Code* lists it), *not received*, *observer*, *owing to*, *receiving station*, *same*, *Second Army*, *Second Army Hdqrs*, *sending station*, *shelled*, *shells*, *side*, *signal officer*, *stubborn*, *table*, *town*, *vicinity*, *wave length*, *withdrawn*. On the outside cover of the code book were these words: "NOTE: The * indicates new word or phrase."

One other new feature of this code, not mentioned in the instructions, was the placing of three code groups to be substituted for the word "o'clock," listed both in alphabetical position and on the first page (p.3) near the numerals. In the first column the variants appear in this order: VPN, OSY, BET; in the second column: OSY, BET, VPN.

The last innovation in this code was the incorporation in the front of the code book of the Emergency Code List with digraphic groups. The complete list is:

EMERGENCY CODE LIST

To be used only with the "Huron Code."
To be issued down to companies.
To be used only for communications within divisions.
To be completely destroyed, by burning, when in danger of capture or
after a new code has been issued.
Precede Every Message in This Code by "RO"

About to advance	SP	AB	Gas is being released
Ammunition exhausted	BX	AF	Trenches
Are advancing	XF	AG	At
At	AG	AP	Objective reached
Attack failed	FS	AV	Enemy fire has destroyed
Attack successful	XA	AW	Relief being sent
Barrage wanted	BD	AX	Captured
Be ready to attack	SM	AZ	Look out for signal
Being relieved	ZB	BD	Barrage wanted
Captured	AX	BF	Right
Casualties heavy	BJ	BJ	Casualties heavy
Casualties light	SF	BM	Using gas shells
Center	XY	BP	Left
Enemy	PF	BS	Enemy trenches
Enemy barrage commenced	SB	BX	Ammunition exhausted
Enemy fire has destroyed	AV	BY	Wire entanglements destroyed
Enemy machine gun fire serious	ZF	CA	Our
Enemy trenches	BS	CB	Situation serious
Everything O. K.	CZ	CM	Message not understood
Everything quiet	FC	CP	Need water
Falling back	SX	CX	Raiders have left
Gas is being released	AB	CZ	Everything O. K.
Have broken through	FG	FA	How is everything
How is everything	FA	FB	Recall working party
Increase range	XG	FC	Everything quiet
Left	BP	FM	Stopped

Look out for signal	AZ	FS	Attack failed
Machine gun ammunition needed	XB	FX	Using high explosive shells
Message not understood	CM	FY	Tank stuck
Message received	ZP	FZ	Not ready
Near	SA	PB	Trenches have been occupied
Need water	CP	PF	Enemy
Not ready	FZ	PG	Have broken through
Objective reached	AP	PM	Strong attack
Our	CA	PO	Rush
Our artillery is shelling us	PV	PV	Our artillery is shelling us
Raiders have left	CX	PX	Reinforcements needed
Recall working party	FB	SA	Near
Reinforcements needed	PX	SB	Enemy barrage commenced
Relief being sent	AW	SC	Troops
Relief completed	XP	SF	Casualties light
Rifle ammunition needed	SZ	SM	Be ready to attack
Right	BF	SP	About to advance
Rush	PO	SX	Falling back
Situation improving	ZX	SZ	Rifle ammunition needed
Situation serious	CB	XA	Attack successful
Stopped	FM	XB	Machine gun ammunition needed
Stretcher bearers needed	ZJ	XF	Are advancing
Strong attack	PM	XG	Increase range
Tank stuck	FY	XP	Relief completed
Trenches	AF	XY	Center
Trenches have been occupied	PB	ZB	Being relieved
Troops	SC	ZF	Enemy machine gun fire serious
Using gas shells	BM	ZG	Stretcher bearers needed
Using high explosive shells	FX	ZP	Message received
Wire entanglements destroyed	BT	ZX	Situation improving

On 28 October the Osage Code,[21] the third of the "Lake Series" made its appearance in an adition of 2,500 copies. It was also sectional and two-part using a three-letter code group with variants. It contained 2,500 code groups—1,927 plain equivalents, 65 blanks,

[21] Friedman, op. cit., pp. 18, 195-197; Barnes, op. cit., p. 8; The "Osage" Code, presumably published by General Headquarters, American Expeditionary Forces, but no statement in the code book appears to that effect.

and 508 variants. Again, the resemblance to the preceding code was close. Every message in this code was proceded by the group "OSA". At the end of the encode were 65 blanks, in two-part order.

The instructions for the use of the code were word for word the same as those in the Huron Code, except where different code groups took the place of the code equivalents in the examples shown. The new words or changes, indicated by an asterisk (*), employed since the last edition (the Huron Code) were CO, -ed, all concerned, chasse, continuous, court, dawn, -de, designate, echelon, endeavor, engine, farm, formation, low, message center, permission, reference, relay, replace, rolling barrage, shell-fire, try, unquote, where is your front line? . The code book, however, listed a total of 121 groups as new or changed words or phrases since the Huron Code, whereas there were actually only 25 such groups.

For this code, too, there was an Emergency Code List incorporated into the code book immediately preceding the instructions for the use of the code. The plain equivalents were exactly the same as given in the corresponding emergency list of the Huron Code, and so were the digraphic groups, but they were assigned in a different two-part order.

The last of the "Lake Series" to be issued prior to 11 November 1918 was the Seneca Code[22] which appeared on 6 November 1918. This

[22] Friedman, op. cit., pp. 18-19, 184-188, 212; Barnes, op. cit., pp. 8, 19-23, 29; The "Seneca" Code, presumably published by General Headquarters, American Expeditionary Forces, but no statement in the code book appears to that effect.

code was sectional and two-part, using three-letter code groups with variants. It consisted of 1,900 plain equivalents, 102 blanks, and 498 variants, *making* 2,500 code groups in all. Every message in this code was preceded by the group "SEN" as discriminant.

Certain innovations are worthy of note. The plain equivalents were no longer printed with initial capital letters. The first page contained groups for the ordinals first to tenth and for *battalion*, *brigade*, *corps*, *division*, *minutes* and *regiment*.

At the end of the Encoding Section the instructions for the use of the code were word for word the same as those in the code book for the *Osage Code*, except where different code groups take the place of the code equivalents in the examples shown. The new words or changes, indicated by an asterisk (*), employed since the last edition (the *Osage Code*) were: *aero*, *arrange*, *by radio*, *Commanding Officer*, *Corps Commander*, *each*, *enemy aeroplane*, *mission*, *practicable*, *pursuit*, *radio station*, *such weighted message*, *wrong*, *your brigade*, *your P. C.*, *your regiment*. Forty-four words or phrases were marked in the code book as new words or changes since the last edition, but only 21 were correctly so marked.

For this code, likewise, there was an Emergency Code List incorporated into the code book immediately preceding the instructions for the use of the code. The plain equivelents and the code groups were exactly the same as given in the emergency lists of the *Osage* and *Huron* codes, but the groups were assigned to the plain equivalents in a completely different order.

F. *Field Codes Nos. 1, 2, and 3*

Three other codes, designated as *Field Code No. 1*, *Field Code No. 2*, and *Field Code No. 3*,[23] were printed by the American Expeditionary Forces after the Armistice and were thus never used. They were later brought to the United States, "kept in reserve for about three years, and then destroyed as obsolete." File copies, however, were preserved.

Captain Barnes does not even mention them. From the format of the code books, however, it seems clear that they were later than the *Seneca Code*, for all three of these numbered field codes not only contained the Emergency Code List, which was employed by the *Huron*, *Osage*, and *Seneca* codes, but they also had small initial letters for the common nouns, a feature present for the first time in the *Seneca Code*. As has been said elsewhere, the *Huron*, *Osage*, and *Seneca Codes* were the last field codes to be issued before the Armistice. At that time, three other field codes—the *Niagara* in the press and the *Michigan* and the *Rio Grande*, in manuscript—were

[23] Friedman, *op. cit.*, pp. 19 note, 198-208-210; *Field Code No. 1*, *Field Code No. 2*, *Field Code No. 3* (all printed by Adjutant General's Department, General Headquarters, American Expeditionary Forces).

in preparation. Mr. Friedman, however, states[24] that 14 codes were prepared from June to November 1918, an average of nearly three a month, but all these are accounted for without including the three field codes now being described.

Field Codes Nos. 1, 2 and *3* show strong affinities with the *Huron*, *Osage*, and *Seneca* trench codes, especially the latter. The discriminants were, respectively, "FC1," "FC2," and "FC3".

These three field codes are also two-part and sectional, using three-letter code groups with variants. *Field Code No. 1* contained 2,500 code groups—1,890 plain equivalents, 95 blanks, and 515 variants. *Field Code No. 2* contained 2,500 code groups—1,890 plain equivalents, 104 blanks, and 506 variants. *Field Code No. 3* contained 2,500 code groups—1,890 plain equivalents, 105 blanks, and 505 variants. The instructions for the use of the codes are identical, word for word, with those in the *Seneca Code*, except where different code groups take the place of the code equivalents in the examples shown, and except that new words and phrases are not marked with an asterisk (*).

[24] Friedman, *op. cit.*, p. 19; Barnes, *op. cit.*, p. 8. Though fourteen codes were compiled, apparently not all were used: Lieutenant Colonel Frank Moorman in his *Final Report of the Radio Intelligence Section, General Staff, General Headquarters, American Expeditionary Forces* (Washington, 1935), p. 34, lists the following codas as "placed in service": *Suwanee Code* (1 August 1918); *Wabash Code* (24 August 1918); *Mohawk Code* (21 September 1918); *Allegheny Code* (12 October 1918); *Colorado Code* (7 November 1918).

For each of the three field codes, likewise, there was an Emergency Code List, incorporated into the code book immediately preceding the instructions. The lists are identical with those in the "Lake Series," except for the assignment of the plain equivalents to code groups.

G. The Staff Code

During the period of preparation of the field codes, the Code Compilation Section of the American Expeditionary Forces was also preparing a Staff Code.[25] The need for this was great, since only the War Department Telegraph Code 1915 then existed for high echelon communications, and this was not intended for active operations in a foreign country but mainly for cables. The new Staff Code, made primarily for communications within France, was completed in June 1918, and 1,000 copies were printed. In contrast to the field codes, which were all small, this was believed to be the largest and most comprehensive code ever printed in the field.

The Staff Code was one-part and sectional, having four-letter and five-digit code groups. There were 30,800 code groups, of which 572 (pp. 196-207) and 408 (pp. 309-313) were left blank for addenda. On each page there were 100 groups, 50 to a column. In each column

[25] Friedman, op. cit., pp. 19, 213-220; Barnes, op. cit., pp. 24, 27, and Enciphering and Deciphering Tables opposite page 27; The Staff Code, General Headquarters American Expeditionary Forces, A. G. O. Printing Department, G. H. Q., A. E. F., 1918.

the plain equivalents formed a separate sequence, known, respectively, as the Left-hand Column and the Right-hand Column, until code group 40,200 (LWBC) was reached on page 208, where the Left-hand Column began to follow the sequence employed by the Right-hand column from the beginning. The digit groups, however, ran consecutively throughout the code book, from 20,000 through 50,799, each column or series having a separate and distinct sequence four-letter group. In the Left-hand Column were given in alphabetical order the proper names, spelling groups and numerals, less commonly used articles of equipment and supply, together with a list of the Army organization in France. Commonly used words and phrases, i. e. the vocabulary, were placed in the Right-hand Column.

There were no caption headings in this code, and it was only necessary to take the words as they occurred in the message and look them up in the code book, for the arrangement was alphabetical throughout. For example, in encoding "Following supplies urgently needed", one simply looked up "Following" and the entire group would be found. In a caption code, it would be necessary to look up under the word "supplies", or under the word "needed".

Variants appeared throughout the code book in the margin of the page, arranged alphabetically. Words such as: with, to, commanding officer, paragraph, period, etc., employed variants. Their mission, as always, was to prevent the too frequent repetition of code groups used for common words in long messages.

The code groups in the Right-hand Column were built up entirely of consonants; those in the Left-hand Column contained two vowels and two consonants, the vowels being always separated by at least one consonant.

In messages where clarity was of the utmost importance, certain phrases were provided, such as: begin quote, begin spelling, end of message, end of word, comma, period, interrogation point, question mark, quotation begins, quotation ends, etc. Throughout the code book marginal references were made here and there to certain parts of the Left-hand Column so as to facilitate the encoding of messages; e. g. "See left-hand column for hours and minutes" (reference on page with "A. M.").

The Left-hand Column contained the following types of plain equivalents:

a. Digits
b. Words combined with digits
c. Hours and minutes
d. Ordinals, singly and in combination
e. Fractions
f. Cardinals
g. Years
h. Higher numbers
i. Proper names interspersed with spelling groups
j. Blanks for addenda.
k. Continuation of the general vocabulary

Beginning with page 208 (code group 40,200) the Left-hand Column lost its complete identity and subjoined the Right-hand Column in the consonantal alphabetical progression towards the end of the plain sequence beginning with the letter J. The Left-hand Column code groups then changed their appearance to conform to the code groups in the Right-hand Column, i. e., they lost their two-consonant, two-vowel form and assumed an all-consonant form.

The Right-hand Column began on page 6 and continued on through page 207 as a separate entity. On page 208, it combined with the Left-hand Column and the two go on together to the end of the code book, page 313, the last 408 groups being blanks for special use.

In order to bring about still further security over and beyond the use of digit groups, a distortion or encipherment table was provided for the Staff Code. This table consisted of an Enciphering Table and a Deciphering Table, and was a type of digraphic substitution based on a random sequence.

As part of the instructions of the Staff Code, there was also a Date and Hour Table, used to designate "concisely and accurately the exact date and hour of a message."

A permutation table was printed in this code book, and instructions were given for correcting errors in transmission.

H. American Radio Service Code No. 1

The only radio service code used by the American Army before October 1918 was the French Radio Code, but there was constant trouble owing to the difference in language. In that month, an American radio code, with about 1,000 words and phrases, was compiled.

It became known as American Radio Service Code No. 1,[26] 2,000 copies of which were printed. This code was issued to "all continuous wave radio stations down to and including brigades, and to all artillery units equipped with continuous wave radio." Radio operators, chiefs of posts, and officers of the Army and subordinate units could use this service code for official as well as for practice telegrams. In cases where no special abbreviations were furnished for radio service messages, this code was used. The usual security instructions formed a part of the code book.

The code was two-part and sectional. The encode consisted of six sections, each arranged alphabetically as follows:

a. phrases used in transmission
b. adjustments
c. net operations
d. miscellaneous
e. radio apparatus
f. vocabulary

The groups were composed of three digits without variants, the words, phrases, and syllables totalling 952 plain equivalents with provision made for 48 blanks divided unequally at the end of each of the six sections of the encode. This makes 1,000 code groups. At the end of the code book was a full page of conventional abbreviations, e. g. "RU.....We are having trouble, "RF.....Signals weak, etc.

The instructions for the use of the code followed the pattern set forth in previous code books.

[26] Friedman, op. cit., pp. 20, 237-243; Barnes, op. cit., p. 28; American Radio Service Code No. 1, Adjutant General's Office, General Headquarters, American Expeditionary Forces.

I. Miscellaneous Codes

The Code Compilation Section of the American Expeditionary Forces also prepared several other codes, no copies of which are now available for study. One of these was merely an addenda sheet, printed in 1,000 copies, (March 1918) to the War Department Telegraph Code 1915.[27] It not only provided groups for plain equivalents which had been omitted from the original code, but also added code groups disguising names of transports and more French cities and towns.

The Telephone Code[28] (sometimes called the "Female Code") a means of disguising names of organizations and commanding officers by using first and last names of women, was issued in March 1918 with an encoding section only. G-3 received 500 copies of this code for distribution. Originally its use was intended to be restricted to the telephone only, but actually it was used with other types of messages. Although no copy of the code book is extant, sample pages appear in the reports of Friedman and Barnes.

Another code, no copy of which is now extant, was a short three-letter code[29] prepared in June 1918 for use in six of the principal telegraph offices to conceal the movements of troops. To replace

[27] Friedman, op. cit., p. 19; Barnes, op. cit., p. 8

[28] Friedman, op. cit., pp. 20, 244-246; Barnes op. cit., pp. 8-11.

[29] Friedman, op. cit., pp. 20, 147-149; Barnes, op. cit., pp. 8, 12.

this edition, there was issued in the next month one more complete, containing about 1,300 words and phrases. Only photostatic copies of the original codes were distributed. Barnes shows part of a printed page of this code, and Friedman presents a report on it written by Captain Hitchings of the British Army Code Solving Section, based on an attempt at solution: the code itself was not available to him. The code was two-part, and for that reason a complex one, says the British captain. He states that "it abounds in alternative equivalents," i. e., variants, in modern terminology, a statement not confirmed by the reproduction of part of one page of the code shown by Barnes. Some attempt was made to avoid combinations of letters likely to be mistaken in Morse code.

Another of these codes was a short two-letter code[30] prepared in September 1918 in an edition of 6,000 copies, with the primary purpose of meeting the needs of the front line where none of the "Trench Codes" or other means of secret communication was available. This code was known as the Emergency Code List and was distributed down to companies. Only about 50 commonly used phrases comprised the code book, and the arrangement was two-part, the group a digraph. When each issue of the "Trench Codes" appeared, a new edition of the Emergency Code made its appearance. Beginning with the Huron Code,—

[30] Friedman, op. cit., p. 20.

the second of the "Lake Series"—issued 15 October 1918, the Emergency Code was inserted, as has been indicated above, in the front of the book for ready reference.

A fifth code was the <u>Casualty Code</u>[31] which was a short code list, employing a three-letter code group, for reporting casualties, prepared and printed in May 1918. This code was later printed as a General Order. It is here reproduced in full:

Report following accidentally killed	AWL
Report following killed in action	BOX
Report following died of wounds	COW
Report following died of disease	DAY
Report following missing in action	END
Report following severely wounded	FEW
Report following slightly wounded	GAS
Drowned—Body recovered	INK
Drowned—Body not recovered	JAR
Death in line of duty	KIT
Death not in line of duty	LEG
Result of own misconduct	MOP
Not result of own misconduct	NAG
All in line of duty, not result of own misconduct	OAK
All entitled to wound chevron	PUN
Not entitled to wound chevron	RAM

An Army regulation made the printing of codes, as distinct from compilation, a function of The Adjutant General's Office, in cooperation with the Signal Corps and under the supervision of the Code Compilation Section. The field codes were therefore printed by the printing office of the Adjutant General's Office at General Headquarters. Except for General Orders and Bulletins, codes were given priority over other

[31] Friedman, <u>op. cit.</u>, pp. 20, 230-231; Barnes, <u>op. cit.</u>, p. 28.

printed matter. The Adjutant General's Office likewise exercised the function of distribution of codes, but did not give satisfaction in this respect. Therefore, the heavy packages containing code books had to be distributed to Army Headquarters by officers of the Radio Intelligence Section at General Headquarters, acting as special couriers. The personnel of the Radio Intelligence Section of the Army then distributed the packages to division, corps, and troops. This problem has since World War I been eliminated by concentrating all code work, including compilation, printing, distribution and accounting in the Signal Corps.[32]

The Code Compilation Section cooperated closely with G-2 at General Headquarters throughout the war. The number of copies to be printed for each "Trench Code" was determined by G-2, and the copies were distributed through it. Several violations of communications security were committed by our radio operators. Entire messages were still sent at times, in plain text. In order to avoid this as much as possible, the intercept stations of the Signal Corps were given the additional duty of monitoring American transmissions and making a report of violations. This report was studied by the

[32] Friedman, op. cit., p. 21; Barnes, op. cit., p. 30. The arrangement, of course, has been different since the creation, in September 1945, of the Army Security Agency, but the statement in the text was true until then.

control or so-called "Security Section," set up for this purpose under the Code Solving Section of the Radio Intelligence Section, G-2, General Headquarters, and consisting of trained officers who had participated in cryptanalysis of German codes and ciphers.[33]

The sending of messages which had been cryptographed by the codes described in this paper involved a great deal of supervision in order to preserve constant communications security. The four most prevalent types of violations of this security committed by our radio operators in the American Expeditionary Forces were: (1) use of plain language in the same message with code or cipher; (2) repetition of a message in any code or cipher other than that in which first sent; (3) repetition of a code or cipher message in plain language; (4) repetition of a plain language message in code or cipher.[34]

J. The Secret "Instructions"

A photostat of Colonel Hitt's personal copy of the "Instructions for use of Code and Cipher in Armies and Lower Units," issued by General Headquarters, American Expeditionary Forces in France, is available[35] for study. The cover bears the simple injunction "Not

[33] Friedman, op. cit., p. 22; Barnes, op. cit., p. 31.

[34] Friedman, op. cit., p. 23; Barnes, op. cit., p. 34.

[35] Files of the Director of Communications Research.

to be taken into Front Line Trenches" but the titlepage indicates the precise nature of the booklet which was also printed in 1918 by the A. G. Printing Department, G. H. Q., A. E. F. The date of these instructions is 22 March 1918. A prefatory note emphasizes that it is expressly forbidden:

a. To use plain language in the same message with code or cipher.
b. To repeat a message in any code or cipher other than that in which first sent.
c. To repeat a code or cipher message in plain language.
d. To repeat a plain language message in code or cipher.

The instructions proper begin with general notes on the observance of rules, on the guarding of the instructions and on special precautions to be taken. Then follows a section on preparation of messages for transmission, including general instructions on how messages should not be prepared, how messages may be prepared, and how messages should be prepared, in enciphered code, plain code, Playfair cipher, and plain language. Instructions are also included for practice messages in the same four types of cryptographic system, and for service messages. The final sections deal, respectively, with the various types of communication:

a. radiotelegraphy
b. earth telegraphy
c. telephone
d. buzzerphone
e. telegraph
f. visual
g. messengers
h. pigeons
i. dogs
j. other means

and with distribution of code books and cipher cards.

One of the most interesting points which come to light from a reading of these instructions is the fact that whenever a code book could not be burned, it could be destroyed by dipping the pages into water and then rubbing the sheets briskly until the printing disappeared. The ink used by the printers was apparently soluble in water. A similar technique was used in World War II by the Germans: code books were printed in ink soluble in water but after the printing had been dissolved, experts of the Signal Security Agency were able to restore the printing sufficiently to permit the reading of the text.

K. Conclusion

The field codes which were compiled by the American Expeditionary Forces well supplied the need which arose when our military forces were thrown into actual combat, and except for the use of complicated encipherments such as additives or subtractors, code compilation has made little progress since.[36]

No encipherment was intended to be used with any of the codes which were produced by the Code Compilation Section.

The letter code seems to have been more in favor than the digit group code in the field code series, as may be judged from the fact that of the fourteen field codes (Field Codes Nos. 1, 2, and 3 must

[36] The more significant developments in cryptography have been in ciphers and code encipherments rather than in code compilation.

be included in this count) prepared by the American Expeditionary Forces from June to November 1918, only three—the Mohawk Code, the Allegheny Code, and the Hudson Code--were digit codes. The letter codes all use three-letter groups; the digit codes are all four-digit groups. It seems, therefore, that the preference for letter codes probably was caused by facility of transmission, rather than security.

The speed with which the codes herein described were compiled was amazing and served immediate purposes without long, unnecessary delays. Satisfactory, too, was the thoroughness with which the code compilers worked, so that when the codes were put to use they brought about the security necessary for the transmission of secret messages. Though the American Expeditionary Forces had begun to operate without the proper means of disguising messages and could not always obtain help from the British and French forces they soon had such a list of usable codes that the British and French came to recognize the value of the American compilations.

L. "The American Black Chamber" on Code Compilation in France

It will be well at this point to notice certain statements made by Herbert O. Yardley in The American Black Chamber concerning the codes being used in France by the American Expeditionary Forces. The pertinent paragraphs appear on pages 42-46, as follows:

One[37] of the young officers whom we had trained confirmed this when he arrived at General Headquarters in France. He had received his instruction and practical experience in my bureau. Having observed the necessity for revising the War Department's communications in this country, he was eager to learn whether the codes and ciphers of General Pershing in use at the Front were safe.

The first thing[38] which this young officor did after arriving in France was to induce his superiors to intercept by wireless our own radio code and cipher messages along the American sector. These codes and ciphers were used to transmit the most secret and important messages and by those who employed them they were considered safe.

Without[39] any knowledge of the American method of encipherment, the young officer solved these messages within a few hours. The system was wholly inadequate and as a means of insuring secrecy was little more than a farce.

Through decipherments of German intercepted cipher messages, our Cipher Bureau in France knew that the enemy maintained a large staff of skilled cryptographers. All radio messages of the Allies and of the Americans were intercepted and sent to the German Cipher Bureau for attack. If this young American officer, who was still merely a student cryptographer, could solve these messages, the

[37] Second Lieutenant (afterwards First Lieutenant) J. Rives Childs, in charge of the Cipher Solution Subsection at General Headquarters. See Chapter VIII; Volume Three: Chapter III.

[38] Lieutenant Childs reached General Headquarters in February 1918 and that the test made by him took place in May 1918. This statement is based on marginal notes by Colonel Moorman and Mr. William F. Friedman in the latter's copy of The American Black Chamber (ad loc.).

[39] Lieutenant Childs was in possession of the code and knew the method of encipherment—he had merely to recover the cipher alphabet which had been used. This fact should not be allowed to create the impression that he was less competent than Yardley makes him out to be. The messages were purely test messages prepared for that purpose at General Headquarters.

German cryptographers, with their long experience of code and cipher solution, without question had also solved and read these telegrams even more quickly than he. And once the system was broken, the enemy could solve every message as easily as the person to whom it was addressed.

As it happened, the contents of this particular decipherment were so important and their secrecy so imperative that the young officer's memorandum on the matter threw the General Staff into a panic of confusion.[40] From these wireless intercepts he learned the disposition of troops along the St. Mihiel salient, the number and names of our divisions, and, finally, the actual hour at which the great American offensive would be launched. This, then, the enemy knew![41]

The herculean effort of flattening out the salient, which for four years had formed a hugh "pocket" inside the French line, cutting off communication and stopping railways between Verdun and Toul, was the task of the Americans. And by reading the intercepts, the Germans had already learned in detail, just as easily as this young officer had learned, plans and preparations for the great American offensive. Incredible! No wonder the General Staff was in a panic. In these messages were contained some of the most important stratagems of the World War.

The Germans considered their position in the salient impregnable. General Pershing knew that the enemy had several lines of defense, the second known as the Schroeter Zone, another as the Hindenburg Line or Kriemhilde Position. What was to happen to the great American offensive of 1918 if the enemy was prepared for it? Of, if the defenses were not considered strong enough now to meet the offensive, was the enemy, warned by our messages withdrawing?

[40] The excitement is categorically denied by Colonel Moorman, who was present, whereas Captain Yardley was himself in Washington and did not reach General Headquarters until December 1918 when the Radio Intelligence Section was about to cease operations.

[41] Anachronism: the test took place in May; the codes were perfected in July, and the St. Mihiel offensive did not take place until the following September.

The latter was the case. Our young officer had shown the General Staff the leak in the offensive, but it was too late to swoop down upon the Germans in a surprise attack. The messages were already in their possession and a retreat had begun. The American offensive of September 12, 1918, was considered a triumph; but it represents only a small part of what might have been a tremendous story in the annals of warfare, had the Germans not been forewarned. The stubborn trust placed in inadequate code and cipher systems had taken its toll at the Front. The enemy had actually been taken into American confidence, through the non-secrecy of communications. It was not a surprise attack which was achieved. Pershing pursued an already retreating horde and entered St. Mihiel on September thirteenth. The salient was broken, but the surprise attack never came to pass. Too many staff officers in France had, like our authorities in Washington, placed a childish unfounded trust in an encipherment which could not be read at sight.

Seldom are the curtains drawn back so that the intricate secret plots, dangers and discoveries may be known. In a history of the World War, one reads the story of this amazed young officer, in some short uninformative generalization. He knew that the code and cipher systems were inadequate; but all he could do was reveal his findings and give warning to the General Staff. The story of his revelation is one which, like many others enacted behind a curtain of warfare, is seldom told. It was too late to undo the damage after the young officer had revealed the inadequacy of the codes and ciphers. Of this whole episode we read but one sentence in a history of the World War:

> Despite all Pershing's precautions for secrecy in the St. Mihiel sector, the Germans expected attack and began to withdraw.

By reading contemporary history of the World War we are led to believe that inefficiency was found on this side of the Atlantic only. Such is not the case. In fact, the foregoing incident is but one of the tragedies of the American Expeditionary Forces, led by General Pershing. The Signal Corps in France was using inexpert and ineffective codes and ciphers to carry over the wireless the secret orders of the General Staff in France.[42]

[42] "Had it not been for the Signal Corps, there would have been much greater casualties on the St. Mihiel front. I was not in the Signal Corps at that time, but in M. I. D." (William F. Friedman in his copy of The American Black Chamber).

CHAPTER VIII. THE RADIO INTELLIGENCE SECTIONS IN FRANCE

A. Organization of the Sections

There were in the American Expeditionary Forces in France two units both known by the same name, the Radio Intelligence Section. The first of these was the Radio Intelligence Section, Signal Corps,[1] afterwards known as the Radio Section of the Radio Division, Signal Corps, concerned primarily with interception and goniometric activity; the other, the Radio Intelligence Section, General Staff, known familiarly as "G-2, A-6," was concerned primarily with cryptanalytic attack upon the German military codes and ciphers.[2] The bulk of the present chapter will be concerned with the latter organization; unless otherwise specifically stated, it is the unit meant.

On 28 July 1917 Captain (afterwards Lieutenant Colonel) Frank Moorman, then of the Coast Artillery but later of the General Staff Corps,[3] was detailed to form the Radio Intelligence Section, General

[1] Information concerning this organization is taken from the Report of the Chief Signal Officer 1919 (Washington: Government Printing Office, 1919).

[2] Information concerning this organization is largely based on Part III of Lieutenant Colonel Frank Moorman's Final Report of the Radio Intelligence Section, General Staff, General Headquarters, American Expeditionary Forces (Washington: Government Printing Office, 1935), short title SIGSEE.

[3] Captain Moorman had in 1916 been the Acting Director of the Army Signal School at Fort Leavenworth. See Volume One: Chapter VI.

176

Staff, a unit which performed functions approximating those of a signal intelligence detachment in World War II, though it had other duties, the nature of which will shortly appear.

Until 25 September 1917 Captain Moorman worked without assistance but on that date First Lieutenant (afterwards Captain) H. A. Berthold, Coast Artillery Corps, was assigned to duty with Captain Moorman, and, on 11 October, Army Field Clerk Harry Block joined the two officers. The Radio Intelligence Section was part of the Information Division, of which the chief was Major (later Colonel) A. L. Conger, General Staff Corps. The Information Division in turn belonged to the Intelligence Section of the General Staff under Major (later Brigadier General) D. E. Nolan, General Staff Corps, the Assistant Chief of Staff, G-2.

Captain Moorman began his work without the benefit of previous planning by others: there were no records and no material on which to work. It was vaguely known that the Radio Intelligence Section was intended to read German code and cipher messages, but how this was to be done and the details of obtaining messages were not specified. Most of the time from 28 July to 29 October 1917 was spent in a study of British and French methods and in consultation with the Signal Corps as to the part to be played by personnel of that corps in liaison with Captain Moorman's staff. Visits to both British and French offices were made and much valuable information obtained.

Two difficulties were encountered at first, as Colonel Moorman afterwards testified:[4]

> One is the difficulty in getting men who are trained in the work. General Nolan expressed the situation very well toward the latter part of the war when he said that he started in with a misconception of what was required. He said that the next time he would put into this work the best brains of the country. He also admitted that he had not appreciated the importance of the code and the cipher work.
>
> Next, we lacked liaison with Washington. I do not think that Washington understood our problems in the beginning. We did not understand Washington, and did not make any particular effort to appeal to them for help.

As American troops then occupied no definite part of the front, an agreement was made with the French to permit American stations to be established in the vicinity of the Meuse for the purpose of intercepting messages on which the Section could practice the methods of solution learned from the French and British.

In addition, arrangements were made with the Signal Corps to furnish men and instruments for intercepting messages and transmitting them to the Section. The first messages, intercepted by the American station at Gondrecourt, were received on 29 October 1917, but these were few in number, since the station was too far from the battle line for successful interception in volume. Moreover, a number of the intercepts proved to be meaningless practice messages transmitted by stations attached to the American Signal School at

[4] Lecture by Lieutenant Colonel Frank Moorman before the officers of the Military Intelligence Division, General Staff, 13 February 1920 (SPSIS 350.001).

Langres. Considerable time was spent on them under the mistaken belief that they were German messages. What German cryptanalysts may have made of them, if they were intercepted by the Germans, is a matter for speculation.

On 12 November 1917[5] the intercept station had been opened by the Radio Intelligence Section of the Signal Corps at Souilly with one sergeant and eight men of the Second Field Signal Battalion. Continuous twenty-four hour service was maintained, and from the date of opening to the end of the month the station recorded a total of 393 messages and 1,173 calls, which, with data as to the time of calls, wave lengths, and the like, were upon receipt immediately turned over to the Radio Intelligence Section of the General Staff, for training purposes. The work turned in by this station showed an increase in the efficiency of the personnel and clearly demonstrated the advisability of placing the intercept operators, after they had received preliminary training at the Langres and Gondrecourt schools, as near the front line as practicable for their advance training.

The intercept station at General Headquarters recorded and turned over to the Radio Intelligence Section of the General Staff

[5] The Radio Division was then under Major Louis R. Krumm. See Report of the Chief Signal Officer to The Secretary of War 1919, pp. 304-305.

an average of 15 messages and 7 press reports a day during November 1917. Owing to the limited personnel available (only two operators), the station was open during the day only.

The British First Army was visited in order to obtain as much information as possible regarding the British Radio Intelligence Service and the equipment in use and the training given by the British Army. After careful consideration of the British and French systems, plans were formulated for a radio intelligence section in an army, sufficiently flexible to fit any army which might be established and which could be duplicated as additional armies were created. Provisions were made for the radio equipment necessary for one army, with a reasonable amount of reserve equipment. This equipment was apparently obtained from the French, as French equipment seemed best adapted to the purpose and was available.

Captain Stith G. McCutchen, Signal Corps, and 54 men from the United States arrived on 10 December 1917 for assignment to the Signal Corps' Radio Intelligence Section. Captain McCutchen and 39 of the men were sent to the Army Signal Schools at Langres for training. A five-week course was outlined for these men, who were expert operators and needed only special instruction with the French equipment and operating methods used, actual working conditions being simulated at the schools as far as possible. Nine of the men were sent to the intercept station at Souilly and six were assigned to the press station at General Headquarters.

With increasing knowledge of the methods of the Allies and the increasing size of the American forces in Europe, the field of activity of the Radio Division began to broaden. By the middle of December a definite partition of duties in the Division had been effected, with Major Krumm confining his attention to the executive work concerned with the radio programs and policies and Captain Loghry having complete charge of the Signal Corps Radio Intelligence Section.

This Radio Intelligence Section, later termed the Radio Section of the Radio Division, Signal Corps, American Expeditionary Forces, was charged with the operation of the necessary grounded circuit listening stations, radio intercept and press stations and goniometric stations, and the operation of such auxiliary equipment (telephone and telegraph connections) as might be required to collect and report all pertinent information regarding the activity, character, and location of enemy radio and ground telegraph stations in the armies operating opposite American forces. This Section operated in connection with the Radio Intelligence Section of the General Staff, to which all information was transmitted and which accomplished the necessary deciphering and interpretation of the information collected. Because of the necessity of absolute accuracy for the proper transcription of the information collected, the Radio

Intelligence Section, Signal Corps, required the most expert radio operators for intercept and goniometric stations and persons capable of speaking German for the listening stations.

From the date the first intercept was received at General Headquarters, messages came in so fast that the personnel of the Radio Intelligence Section, General Staff, were unable to handle them all, and it became necessary to enlarge the section. Officers and clerks were obtained from all available sources: some were detailed from divisions, some from replacement depots, some from Washington, and some from men reclassified at Blois. In the case of officers, a search was made for men of high mental caliber who also knew German, but considerable difficulty was encountered.[6] The qualifications for enlisted men were somewhat lower: ability to work effectively was the essential qualification and a knowledge of German only a desirable competence.

The growth of the Radio Intelligence Section of the General Staff stimulated the Signal Corps to assign more and more of its personnel to the task of interception. After considerable expansion, by the time the Americans actually took over a sector there were available both the means and the experience necessary for handling the work.

[6] "The difficulty experienced in finding men who could actually think without a guardian was surprising. It is to be hoped that one of the aims of the future will be to develop this ability in men chosen for code and cipher work." (<u>Final Report</u> cited in note 1, p. 15).

152

Exactly eighty persons were members of the General Staff Radio Intelligence Section at one time or another from 28 July 1917 to 2 January 1919, the date of Colonel Moorman's final report, when only five[7] of the eighty were still on duty in the Section. Colonel Moorman lists all the personnel under him together with their ranks, dates of duty, and the units to which they were ultimately transferred, arranged in order of the date of reporting for duty. In this list there are seventy-seven names which, rearranged according to rank, are as follows:

Lieutenant Colonel

*Frank Moorman

Captains

H. A. Berthold
C. H. Matz
E. M. Nourse
H. E. Osann
*P. B. Whitehead

First Lieutenants

C. W. Bird**
K. Bromley**
H. G. Campagnoli**
J. R. Childs
N. M. Coursall**
E. E. Falk
*William F. Friedman**
Eugene Jackson***
Robert H. Keener***
Frederick Livesey
C. G. Montross***
J. S. Norris***
E. F. Roosevelt**
V. L. Sailor**
H. C. Skinner***
Townsend
(other names unknown)**
Austin M. Works***

[7] Names marked with one asterisk (*) before the name are those of the five still on duty on 2 January 1919. Names marked with two asterisks (**) are those of persons who had originally been trained at Riverbank Laboratories; names marked with three asterisks (***) are those of persons known to have been trained in MI-8; where the others were trained is unknown, except in the case of Colonel Moorman himself who had been trained at the Army Signal School.

Second Lieutenants

A. E. Billing
R. Chamberlain
M. F. Eiseman
R. W. Gilmore
J. A. Graham**
J. F. Gunster**
W. J. Ladwig
D. D. Millikin**
L. M. Sellers**
E. D. Woellner**

Army Field Clerks[8]

H. K. Bellgardt
Leonard Bickwit[9]
Harry Block
G. E. Daney
G. B. DePierri
*W. O. Dodge
P. B. Gallagher
H. Gussack
H. J. Heiman
C. E. Hufnagel
H. C. Jacques
F. J. Kennedy
W. E. Kilborn
J. L. Koeppler
S. L. Kresser
W. C. Lyon
*A. S. Mangene
S. R. March
J. A. McKenna
J. O. Meeth[10]
A. L. Perrie
Dew T. Sapp
L. E. Sherer
S. S. Shook
S. A. Snyder
Samuel Tartalsky
W. A. Visconti
E. J. Vogel[11]

Noncommissioned Officers

Sergeant Major	E. R. Guldner
Color Sergeant	J. J. Wahl
Sergeant	E. S. Anderson
Sergeant	J. P. Nathan
Sergeant	C. L. Rosenthaler
Corporal	J. Thunder
Bugler	L. W. Robbins

[8] This rank corresponded to Warrant Officer.

[9] In World War II Lieutenant Colonel Bickwit served with the Signal Security Agency and was Chief, Signal Intelligence Service, China-Burma-India Theater in 1944 and 1945.

[10] Later Meeth was a member of the staff of the New York office of MI-8.

[11] In World War II Major Vogel served as Chief, Special Examination Unit, Signal Security Agency and also in the European Theater of Operations.

Privates First Class

E. L. Froy
J. T. Graham
C. C. Kyle
J. W. Mehan

Privates

E. L. Alberson
J. E. Endrum
L. E. Hendricks
R. V. Scott
H. N. Tooliatos

To this list should be added three other names derived from a list of former personnel in G-2, A-6, to whom letters were sent on 17 May 1919, cautioning them of the need for secrecy in regard to their war work.[12] The persons whose names appear on the later list but not on that of Colonel Moorman are as follows:

Captain Herbert O. Yardley
Corporal Jess Krueger
Corporal Lester H. Wolff

The later list also indicates that several of the persons named had received promotions after they left the Radio Intelligence Section;

Ultimately, the Radio Intelligence Section was divided into the following subdivions:

First Army Radio Intelligence Section
Second Army Radio Intelligence Section

[12] See letter from Assistant Chief of Staff, G-2, General Headquarters, American Expeditionary Forces, to Director of Military Intelligence, War Department, Subject: Preservation of Secrecy in Regard to Code and Cipher Work, 20 May 1919, copy now filed in IR 4154. See also Volume Three: Chapter III, Section D, on the importance of this letter.

185 2-C 19

Goniometric Subsection
Office of the Adjutant
Security Subsection
Code and Cipher Solution Subsection

The development of each of these subsections will be given in turn.

B. First Army Radio Intelligence Section[13]

In January 1918 First Lieutenant (later Captain) C. H. Matz, Infantry, was detailed to take charge of the work of radio intelligence with the proposed American First Army. Lieutenant Matz was given reports such as it was presumed he would receive at Army Headquarters and was required to make deductions from them and to submit his reports as though the Army were actually in operation. On 3 April he was assigned two clerks to assist in his work, and all were moved to a separate room where they worked out their own organization and conducted a small-scale Army Radio Intelligence Section. A special telegraph line was carried to the office, where messages were received directly from the Signal Corps stations and acted upon in all respects as they would have been at Army Headquarters.

The small group worked first at Toul, beginning on 12 June 1918, on material from the sector extending from the Meuse to the Moselle. On 20 July 1918 the personnel of the office was transferred to La Ferte sous Jouarre (Seine et Marne) to join the staff of the First Army,

[13] For the evidence see Final Report, p. 16 and enclosure C: Final Report of First Army, pp. 29-36.

then forming. A preliminary study was being made of the sector which the First Army had planned to take over when orders were received to cease work on this sector. On 13 August the Section moved with the remainder of G-2 to Neufchateau. Since upon the departure of the Section from Toul another staff had continued operations in the Meuse-Moselle sector, the personnel of the Radio Intelligence Section of the First Army, with the exception of the chief, was transferred back to Toul and augmented by the personnel already there. Upon the transfer of the First Army headquarters to Ligny-en-Barrois the entire office at Toul was moved on 30 August 1918 to Ligny, from which point it operated during the St. Mihiel attack of 12 September 1918.

The Radio Intelligence Section after the establishment of an advanced P. C. of the Army Headquarters, remained at Ligny until 10 October 1918, when it moved to the advanced P. C. at Souilly, where it remained until after the close of hostilities on 11 November 1918.

The total personnel which served at one time or another with the Radio Intelligence Section of the First Army was as follows:

Captain Charles H. Matz	Chief
Lieutenant Robert W. Gilmore (1-20 Sept.)	Assistant Chief
Lieutenant John A. Graham (23 Sept.)	Assistant Chief
Army Field Clerk Wm. C. Lyon	Goniometric Section
Army Field Clerk John A. McKenna	Goniometric Section
Color Sergeant John J. Wahl	Goniometric Section
Army Field Clerk John C. Meeth	Code Section
Army Field Clerk Henri C. Jacques	Code Section
Army Field Clerk Sterling R. March	Code Section
Sergeant Edgar S. Anderson	Code Section
Army Field Clerk Walter H. Kilbourn	Secretary

The technical side of the work of observing the enemy's communication services was performed by the Radio Section, Signal Corps, First Army. This work consistod of the operation and maintenance of the necessary apparatus, stations, etc., by means of which the actual observation was made. All results were transmitted by the Radio Section to the Radio Intelligence Section for study and interpretation. Although these two sections were entirely separate and distinct organizations, the former belonging to the Signal Corps and the latter to the Second Section of the General Staff, the closest possible liaison and cooperation between the two was essential.

The work of the Radio Intelligence Section will be briefly described under successive headings:

1. The location of enemy radio stations and the grouping of these stations into divisional, corps, and army nets.

Enemy radio stations were located by bearings from radiogoniometric stations located at intervals along the front. These stations were able to measure within approximately two degrees the direction from which the signals of an enemy radio station came. By the intersection of lines drawn from two or more of these goniometric stations in the direction of the enemy station a quite accurate map-location of the enemy station could be obtained.

Though, when an important message was decoded, the location of the sending station was obtained by goniometry, the primary duty of the goniometric section was to locate daily all enemy stations heard and, by connecting these stations by lines indicating an exchange of messages, to determine groups of stations belonging to divisions, corps, and armies.

The radio traffic of a division would normally be contained almost entirely within its own limits, and similarly with corps and armies, so that theoretically the intercommunication of stations should have disclosed clearly the boundaries of units. But actually the enemy, with the intent of destroying this source of information, indulged in a carefully regulated camouflage activity whenever possible, having stations communicate regularly across division, corps, and army boundaries, so that the grouping of stations into actual nets was very difficult. Under very active conditions, however, the necessary traffic of stations was so great that camouflage was impossible, and the various nets showed up clearly.

From the location of stations also the depth of the enemy echelons could be determined, as well as the presence of his troops in doubtful areas, and, during war of movement, the positions along which he was organizing resistance.

2. The interception and decoding of enemy radio messages.

Intercept stations were maintained at proper points along the army front to listen in continually for enemy radio messages. These stations were connected by direct wire with the Radio Intelligence office and intercepted messages were telegraphed in directly.

The enemy had in general use, during the period in which the First Army was functioning, two different types of codes and one cipher system. The first of these codes, of trinumeral type, and called the "Three-Number Code",[14] was used principally by certain miscellaneous units, such as artillery groups, etc. for communication within divisions. It was the German "front-line code" and consisted of a base containing letters, syllables, phrases, and code names, and a separate distortion table for each division and miscellaneous unit, which changed at intervals averaging ten days or two weeks. With a fair amount of text, it was possible to decode messages in this code with considerable success. Except during times of great activity, the enemy apparently took great care to prevent information of importance being sent in this code. Identifications of units, however, and occasionally more vital information were often found from decoded messages.

During periods of activity, particularly during the St. Mihiel attack, the enemy used this code much more freely, and highly important information was obtained from decoded messages.

The second code employed groups of three letters commencing with K, R, A, U, or S. A separate edition was used by each army,

[14] On German systems, and their solution see below, Section G, pp. 202-211.

changing at intervals of from two weeks to a month. This code, because it was a true two-part code, was very difficult of solution and, on account of the great number of words and phrases and alternative groups which it contained, the principal study of it was done for each army by the Code Solution Section of General Headquarters. All text received was forwarded to the Code Section of General Headquarters, where an exhaustive study was made of the code, and all solutions were sent by wire to the armies. Messages of considerable importance were sent in this code, but during period of functioning of the First Army the code was never solved sufficiently to be of great value, though upon two occasions when a code was captured much valuable information was obtained from the messages.

The cipher employed was of a very difficult substitution—transposition type (ADFGVX Cipher) used only for high command communications. It was apparently used between Army, corps and division stations, and for messages of great importance. Messages sent in this cipher were practically safe from danger of solution.

In the spring of 1918 the enemy adopted a policy of the strictest caution and conservatism in regard to code messages, with the result that when the First Army began functioning the probability of obtaining information of value from these messages was decidedly less than it was during the earlier part of the war.

3. The interception and decoding of enemy ground telegraph (TPS) messages.

This was accomplished through listening stations located close to the front. TPS stations had a very limited range and were used by the enemy only in his forward units. For this reason the messages sent were rarely of importance. The code used was generally the "Three-Number Code", and any messages intercepted were copied on the daily report sheets sent to the office of the Radio Intelligence Section by the various listening stations. Indications of considerable importance were obtained by a close watch of the activity of enemy TPS stations, their approximate locations as determined by the intensity of their signals, and changes in their sending procedure. Reliefs were often indicated in the latter manner.

4. The interception of enemy telephone conversations.

This was accomplished by the same listening stations which intercepted enemy TPS messages, but owing to the care which the enemy had begun to exercise in controlling his conversations and in the location of his lines, no highly important conversations were overheard during the period of functioning of the First Army. This had been the case in the earlier days of the war, when much information was obtained from intercepted telephone conversations.

The value of listening stations for both TPS and telephone conversations was found during war of movement to be considerably diminished, owing to the difficulty of maintining close contact with the enemy long enough to install the necessary apparatus.

5. The interception of radio signals from aeroplanes ranging for hostile artillery and the location of the planes sending these signals.

This service primarily belonged to war of position, since a complete system of telephone lines between goniometric stations and a control station for which warnings of these flights could be sent to air pursuit groups was necessary. During movement of the front it was necessary to move goniometric stations forward frequently, so that it was practically impossible to maintain the proper telephone lines. Hence, with the exception of the brief time when the First Army was engaged in position warfare, this branch of the service received no opportunity to function at its full value.

During the earlier days of the war the Allies on stable fronts, particularly the British, attained great success in the determination of the location of hostile ranging planes and the interruption of these flights through warnings sent to their own air service.

6. The policing of American telephone lines near the front for dangerous conversation which might be overheard by the enemy.

This was also accomplished by means of listening stations, and a great deal of dangerous conversation was overheard during the functioning of the First Army. Such conversation was reported to the proper authorities for disciplinary action with a view to impressing upon the offenders the dangers of loose conversation and the necessity of its elimination, because it was a possible source of information to the enemy.

7. The distribution of our American trench codes to division, corps, and army troops.

Altogether five issues of the American Trench Code were placed in service, on the following dates: Suwanee, 1 August 1918; Wabash, 24 August 1918; Mohawk, 21 September 1918; Allegheny, 12 October 1918; Colorado, 7 November 1918.

The preparatory work of the Radio Intelligence Section for the St. Mihiel operation (10 August—1 September 1918) consisted chiefly in a study of the enemy communication services in the St. Mihiel salient with a view to detecting any changes in organization or procedure prior to the operation which might reveal the enemy's intentions.

No change of any sort was observed until 8 September. At that time unmistakable signs of nervousness on the part of the enemy became noticeable along the southern side of the salient. The activity of radio stations in this region mounted steadily from 8 to 11 September. The radio station attached to the observation post on the Butte de Montsec was exceedingly active during this period, an indication that continual reports on movements within our own lines were required. On 9 September listening stations in the Bois d'Apremont [redacted] an abnormal amount of telephone communication within the [redacted] lines, and on the same date a listening station near Limey [redacted] that enemy ground telegraph stations had apparently moved to [redacted] rear. A similar phenomenon was noted by a listening station [redacted]y on 10 September. This withdrawal of enemy ground telegraph [redacted] was an indication of an echeloning in depth of the enemy's [redacted] and of a fear of surprise attack.

[redacted] the western side of the salient, however, conditions appeared [redacted]al. The conclusion arrived at then was that the enemy antici[redacted] attack between St. Mihiel and the Moselle but entertained less [redacted] about the sector between Les Esparges and St. Mihiel.

[redacted] some days previous to the date set for the attack, however, [redacted]ons from other sources of intelligence pointed to the inten[redacted] the enemy to withdraw from the salient, and every means [redacted]e was adopted by the Radio Intelligence Section to detect any [redacted] such a withdrawal. Evidence from other sources that the [redacted]al was imminent kept increasing, but no indication that it had [redacted]s found from the enemy's communication service. Finally on [redacted]ber the day before the attack, the situation became acute. [redacted]vidence pointed to the fact that the enemy had already [redacted]shed his withdrawal. On the evening of the 11th, however, [redacted] received during the day from goniometric stations disclosed [redacted] that all enemy radio stations were still in their normal [redacted]s and in operation—an impossible condition had the enemy actually withdrawn. Hencc, in spite of all other indications, the Radio Intelligence Section was able to show positively that the enemy still occupied the salient.

With the development of the attack it bccame evident that the enemy's communication servico was at first thrown into considerable confusion. However, on 14 September a reorganization along the new line became evident and quickly developed.

During the progress of the attack considerable infcrmation of importance was gained from decoded radio messages. This included identifications and the location of various P. C.'s, but particularly the warning of an enemy counterattack in the region of the Soulevre Farm in time to inform the troops concerned.

The work of the Radio Intelligence Section preparatory to the first main attack of the Argonne-Meuse operation consisted in a study of the enemy communication services west of the Meuse. Facilities for such a study in this sector were far less favorable than in the St. Mihiel salient, principally because the enemy made very little use of radio for his communications. For several days prior to the attack of 26 September signs of nervousness on the part of the enemy were observed, though to a less extent than before the St. Mihiel attack.

The attack of 26 September evidently disclosed to the enemy the need for a more complete radio organization west of the Meuse, fcr immediately upon the stabilization of the line following the first phase of the offensive, a considerable concentration of stations in this region became apparent. This concentration began 1 October and by 5 October it was complete. The distance of divisional stations from the front indicated that the enemy's forces were echeloned in great depth.

From the establishment of communications along the new line until about 17 October indications pointed to the intention of the enemy to hold the positions that he then occupied. Occasional identifications were obtained, including the location of corps headquarters at Stenay and Beaumont; but, generally, decoded messages contained information of small importance.

On 17 October however, a general withdrawal of radio stations west of the Meuse bogan. During the following week practically every station between the Meuse and the Aisne, a total of seventeen, many of which were close to the front, disappeared. This was strong evidence that the enemy was planning a withdrawl of his forces, and this evidence was confirmed by reports from other sources. On 24 October stations began to reappear west of the Meuse, but farther to the rear than before. It soon became evidence that a reorganization of radio nets was taking place approximately along a line corresponding to the Freya Stellung. This seemed strong evidence of the enemy's intention to withdraw to this position. But about 29 October this reorganization ceased and, taken in connection with other information, it was decided that the enemy's plans for a withdrawal had been changed, and his new intention was to hold the line he then occupied.

In preparation for the second phase of the Argonne-Meuse operation an attempt was made to deceive the enemy as to our own intentions by allowing him to acquire false information by means of his own Radio Intelligence Service. Prisoners taken east of the Meuse, between Beaumont and Fresnes about 20 October declared that the enemy was fearful of an attack in the direction of Briey and Metz. Accordingly, a plan was evolved to increase these fears and thereby divert his attention and his forces from the west of the Meuse. This plan consisted of establishing an army net of radio stations opposite the front Beaumont-Fresnes and sending messages between these stations in a cipher which the enemy could solve through apparent carelessness in its use. These messages were of a nature which would make the enemy think that an attack by this new "army" was imminent. Furthermore, telephone lines were established along the front in a manner which would enable the enemy listening stations to overhear conversation carried on over these lines. This conversation was also such as would indicate a coming offensive. This plan was put into operation on 23 October and was carried on until after the operation west of the Meuse started on 1 November. This camouflage apparently met with considerable success. Enemy radio stations were frequently given orders to be on the alert, and our own listening stations reported that on 26 October enemy ground telegraph stations were drawn back—both very good evidence of the fear of an attack. It later developed that two enemy divisions were held in reserve at Metz even after the attack west of the Meuse began, because of the fear of an attack east of the Meuse.

C. Second Army Radio Intelligence Section[15]

The Second Army Radio Intelligence Section was formed on 22 September 1918 by taking one officer and two clerks from the trained First Army Radio Intelligence Section and adding First Lieutenant (later Captain) Philip B. Whitehead, Field Artillery, as officer in charge, and four clerks from General Headquarters. The personnel from the First Army Section were also replaced from General Headquarters.

The personnel on duty in the Second Army Section were as follows:

Captain Philip B. Whitehead (Chief)
Lieutenant Robert W. Gilmore (Assistant Chief)
Lieutenant E. H. Falk
Army Field Clerk G. B. DePierri
Army Field Clerk J. A. McKenna
Army Field Clerk Sterling R. March
Corporal Lester H. Wolff
Corporal Jess Krueger
Private L. E. Hendricks
Private J. E. Endrum
Private L. W. Robbins
and four telegraph operators

[15] See Final Report p. 16 and enclosure D, pp. 37-40.

This organization made all preparations for active service and submitted routine reports up to 11 November 1918, but the signing of the armistice found it still untried in actual battle. The chief of the unit prepared an illuminating report on the duties performed by each member.

Duties of each member of the personnel:
Officer in Charge—Captain Whitehead:
Supervision of all work and reports of the Section.
Liaison with other sections of G-2, with other branches of the service, with neighboring armies, with G.H.Q and G.Q.G.

Assistant to Officer in Charge—Lieutenant Gilmore:
In charge of office during absence of Captain Whitehead.
Has given special attention to reports on listening stations, airplane intercepts, and collection of information from prisoners and documents.

Officer in charge of Code Distribution—Lieutenant Falk:
Distribution of code books.
Reports on infraction of regulations regarding the use of codes by our own troops.

Chief Clerk--AFC DePierri:
Receives and distributes all incoming messages, reports, and mail.
Typewriting and Stenography.
Responsible for form and appearance of reports and for their distribution when prepared and signed.
In charge of files and records of the office.

Goniometric—AFC McKenna, and Private Hendricks:
Tabulate all goniometric bearings and prepare daily station-location report from goniometric bearings.
Keep record of intercommunication of stations.
Keep list of permanent designation of stations and their daily call signs for each day.
Prepare daily and trimonthly map showing location and grouping of stations.

Activity—Corporal Wolff:

Records all intercepted messages as fast as received and tabulates the activity of each station.
Calls attention immediately to unusual activity of any station or group of stations.
Keeps a record and a graphic chart of daily activity on army front and of activity of each station.
Keeps a daily record and chart of different kinds of codes used.
Prepares trimonthly chart of activity.

Decoding—AFC March, Private Endrum, and Private Robbins:

Decode incoming messages.
Prepare daily report on messages decoded.
Prepare telegraphic reports on new solutions.
Keep records of all code solutions received and sent out.

Code men work in three shifts as follows:

8:00 a.m. to 5:00 p.m.
3:00 p.m. to 12:00 p.m.
12:00 p.m. to 8:00 a.m.

Airplane Adjustment and Listening Stations—Corporal Krueger:

Tabulates reports from airplane intercept station and prepares daily and trimonthly summary of airplane wireless activity.
Tabulates reports from listening stations and prepares daily and trimonthly summary of activity.

Records kept.—The records kept by this office are mainly in the form of reports, as follows:

Daily, by telegraph:

(1) Summary of activity for preceding day. Distribution: G. H. Q. File.
(2) List of stations heard during preceding day with their location by coordinates. Distribution: G.H.Q. G.Q.G. Armies on each flank. File.
(3) New solutions for enemy codes. Distribution: G.H.Q. Armies on each flank. File.

Occasional, by telegraph:

(4) Unusual activity or changes in number or location of Stations. Distribution: G.H.Q. Armies on each flank. G.Q.G. File.

2/301 0-5G

Daily, written:

(5) Indications from activity of enemy liaison service. Distribution: A.C. of S., G-2, 2nd Army. G.H.Q. 1st Army. Radio Officer, Signal Corps. File.

(6) Intercepted enemy communications. Distribution: A.C. of S., G-2, 2nd Army. G.H.Q. 1st Army, File.

(7) Map showing location and grouping of field radio stations. Distribution: A.C. of S., G-2, 2nd Army, G.H.Q. G.Q.G. File.

Trimonthly:

(8) Enemy liaison service with map showing location and grouping of enemy field radio and T.P.S. stations, and a graphic chart showing activity of radio stations, airplane adjustment, ground telegraph and telephone. This map should also show areas in which airplane adjustment was especially active.

Distribution:

A.C. of S., G-2, 2nd Army.
G.H.Q.
G.Q.G.
Each Corps of 2nd Army.
Armies on both flanks.
Chief Signal Officer
Radio Officer.
File.

(9) Report on 6th, 16th and 26th of each month giving call signs used by each station during preceding five days. Distribution: G.H.Q. (by courier). G.Q.G. (by telegraph). File.

Special Reports (when necessary):

(10) Infraction of regulations concerning use of code by our own troops, in the form of a letter to the Commander of the Corps concerned, through the Adjutant General.

(11) Special reports to A.C. of S., G-2, 2nd Army, on any information of immediate importance.

D. The Goniometric Subsection

The Goniometric Subsection, of which First Lieutenant E. H. Falk, Field Artillery, and Second Lieutenant E. D. Woellner, Infantry, were the officers, submitted a detailed report containing the following paragraphs which will describe their work:[16]

> Purpose of the goniometric service.—The fundamental principle of this service is to determine the location of enemy radio stations.
>
> From this information the following deductions may be made:
>
> 1. Gaining information regarding the enemy's order of battle, regardless of the actual contents of the messages.
> 2. Furnishing information which is of value towards the solution of trench codes.
> 3. Furnishing information to the Air Service regarding the location of hostile registering aeroplanes.
>
> Procedure of locating radio stations.—The actual functioning of goniometric stations is under the supervision of the Signal Corps. These stations are installed along the entire front at approximately 10-kilometer intervals, the general locations of which are determined by these headquarters.
>
> Telegraphic reports are received from each station at specified intervals containing the following information concerning enemy radio stations heard during these intervals:
>
> a. Call-signs of hostile sending stations.
> b. Bearings obtained on sending stations (expressed in azimuth).
> c. Degree of accuracy of measurement (very good, good, or poor).
>
> In case slightly varied measurements are obtained on the same station, an average is computed, taking into consideration the degree of accuracy.

[16] See Enclosure E, pp. 41—46 Final Report.

The principal apparatus necessary to carry on work in this office is the "map board." This consists of a table of suitable dimensions to accommodate a map (1/80,000 scale) of the area concerned. Locations of gonio stations are indicated by placing a protractor (complete circle) on the map, with its center over the exact geographical position occupied by the station in the field, and its zero degree mark pointing due north. A thread of suitable length is fastened at one end at the center of each protractor by means of a thumb tack, and at the other end to a small weight. To lay off a given bearing from a given station, move the weight attached to that station so that the outstretched thread will read the proper azimuth on the protractor.

The location of an enemy station is determined by the intersection of threads representing bearings obtained by two or more stations.

Information obtained on enemy order of battle.—Before any deductions can be made concerning movements of hostile units, as indicated by radio evidence, it will be necessary to have a comprehensive knowledge of the German forward radio organization.

Army headquarters and corps headquarters are supplied with sending stations, but these stations are generally only used during active operations, and are therefore usually difficult to locate.

Divisions in line are normally supplied with stations at headquarters of the division, brigade, regiments, and at the command post of the commander of the front-line troops. Stations the farthest forward, or which are located on high hills, are also used by observation posts. This organization, however, was not always strictly adhered to, probably due to an insufficient supply of material, in some cases only three stations having been used by a division.

A complete divisional radio organization, called a "group" (DIFUA), is assigned to the division and moves with it. These groups are defined by the radio traffic within the division and by general characteristics which can only be observed with experience and careful study. During the latter months of the war the enemy introduced an extensive system of camouflage which rendered the determination of groups very difficult. This camouflage consisted of a methodical exchange of messages between forward stations in neighboring divisions or "Lateral liaison."

One of the most significant changes to be observed is the withdrawal or disappearrace of divisional and corps stations.

Information furnished to the code section—Since different hostile armies employ different trench codes, the code section is desirous of obtaining information which will enable it to sort intercepted messages properly according to codes.

It is therefore necessary to furnish daily lists showing the locations of all active stations and their call signs heard during the preceding day.

By means of a system of naming hostile stations arbitrarily, a given station could be followed in spite of the daily changing of call signs. This enabled the code section to detect signatures in messages and trace the movements of military units.

Information furnished to the Air Service.—Considerable hostile artillery registration was done by aeroplanes, which sent radio signals to the batteries.

Owing to the shorter wave length employed by registering aeroplanes, special goniometric instruments are installed for the purpose of locating these planes. After a certain plane has been located, this information is communicated immediately to the Air Service, for the purpose of sending out pursuit planes. Since registration planes usually carry on their work from behind the enemy lines and are not easily discovered by visual means, the Air Service has expressed its urgent need of this information.

Registration activity in certain sectors may be regarded as a barometer of hostile intentions. Thus an increase might denote the arrival of new batteries, either in preparation for an attack or to resist our attack.

E. The Office of the Adjutant

The work of the Adjutant of the Radio Intelligence Section ultimately included what has since been called distribution of cryptographic systems, since dissatisfaction was experienced in the way in which the matter had been handled by The Adjutant General, American Expeditionary Forces. First Lieutenant H. B. Campagnoli was placed in charge. His report,[17] presented below in full, will adequately explain the work done:

[17] Enclosure F, Final Report, pp. 47—49.

The office of Adjutant of the Radio Intelligence Section has under its care the following duties:

1. Distribution of code books.
2. Distribution of coordinate strips and squares.
3. Distribution of liaison tables.
4. Publication of conventional signals used by the enemy.
5. Distribution of official mail and telegrams; coding and decoding of all telegrams.
6. Supplies of the section.

1. Distribution of code books.—An armed force in the field during combat or at rest is in need of code books as one of its requisites to assure success to its arms. The reason for using code at the front is to puzzle the enemy as to the present and future movement of troops; therefore, it is apparent that code books should be carefully taken care of and protected to the utmost so that they do not fall into the hands of the enemy.

It has been found necessary to create a central office at General Headquarters so as to simplify the work, so make distribution more speedy, and to assure a good checking system in regard to code books.

At present this office receives a new issue of code books from the Code Compilation Section. After experimenting for some time as to the number of books to an issue it was found practicable to print 2,500 each time. Along with the code books we received Emergency Tables which are issued down to companies, while the code books are distributed only as far down as battalions. After checking up the new issue we begin at once to pack them in packages of 24 each, inclosing also 33 emergency tables. After a package is wrapped, it is checked, sealed and the corresponding number of the books in a package indicated on the wrapper. The packages are then stored and kept here until asked for by one of the armies. When a call is received for a new issue the books are either sent by courier or by Motor Despatch Service. In the case of the courier, they are sent as originally wrapped, but if sent by M. D. S. the inner wrapper is stamped "secret" and addressed in full; and as all secret documents they are sent in double wrappers. A standard form of receipt has been adopted for every issue, differing only as to the name of the code. To simplify its working all the receipts are made out at General Headquarters and sent along with the books. Each individual code book contains in a detachable form a receipt which is to be filled out by the officer who is responsible for that book. The forms of other receipts are made out as attached.

In the beginning when there was no large American force in France and when the different divisions were brigaded with the French or British armies it was found advisable to have the code books issued direct to the separate divisions and when obsolete returned direct to General Headquarters. However, since the formation of the different American armies this process has been eliminated and we send a whole issue of code books direct to the Asst. Chief of Staff, G-2, of the army in question and his office is responsible for the code books. Therefore, the only receipt that is remitted to us is the receipt of the whole issue. It has been found advantageous to destroy the code books as soon as possible after it has been assured that the code has fallen into the hands of the enemy, and in such a case we are to be forwarded a certificate of destruction giving the numbers of the code books destroyed. A reserve supply of new books is to be kept at all times at the office of the A. C. of S., G-2. When the working code has been captured by the enemy, the issue held in reserve is to be placed into immediate service; we in turn are to refurnish the A. C. of S., G-2 office with a new set. In order to meet this continued emergency our office keeps in reserve one or more sets of code books.

To keep track of the code books issued to the armies and other independent organizations, we have devised a double-entry book system. We record on the books the number of code books received, with the date; when they are issued to the armies, the number issued, and also the number of the books as individuals. We have to be very careful in the recording of code books issued to independent organizations because they usually receive a smaller number than is issued to an army. Again we have to reserve certain issues for each army and not supply anyone else with the same code book.

At times, when we hear that a code book has been captured, we see to it that a number of the obsolete books are returned to us for the use of our Code Schools and Divisions in training.

For further information regarding regulations governing distribution, see G. O. No. 172 G.H.Q., A.E.F.

2. Coordinate strips and squares.--The coordinate strips and squares are issued for the use of the office of the Radio Officer of an army. The Adjutant's office is as in the case of the code books the central office of distribution, as far as the American armies are concerned. The French Headquarters supplied us with the coordinate strips as it was found practicable to have the same alphabet coordinates and more expedient to have them printed under the supervision of French Headquarters. As soon as we received said strips we had tables printed in an amount corresponding with the number of strips. Each American Army was supplied with 1,000 strips and 1,000 tables which were used by the aerial observers. When a coordinate strip or square fell into the hands of the enemy or was suspected, French Headquarters was to notify us of it and at the same time advise us when a new coordinate strip was to be put into service. We in turn telegraphed the Radio Officers of the different armies and the Chief Radio Officer of the Army Group, advising them of the date and hour that the new strips were to be placed in service. Instead of having coordinate strips named as in the case of code books they were numbered. The Armies were usually supplied with one or two strips as reserves, which were to be held in as secret a place as possible.

3. Liaison tables.—For the use of encoding signals of List No. 2, page 79, Liaison for all Arms, there has been issued to the American Armies certain tables which are changed from time to time. These tables and the coordinate strips and squares go hand in hand as they are both used by aero observers at the same time. The liaison tables contain phrases which are transmitted in code; they pertain to the general enemy situation at the front, while the coordinate strips with the aid of a map give the location of enemy positions wanted by our armies. This information is transmitted by wireless. Armies were instructed to notify this office immediately should there be reason to believe that a certain table had fallen into the hands of the enemy and we in turn were to notify by telegram the radio officers of the armies at the same time fixing the date that the new table was to take effect. The usual time given for changing tables was not less than 48 hours and not more than 72 hours after the sending of the telegram.

4. Conventional signals.—This office publishes whenever requested by the Officer in Charge of this Section a new edition of the conventional signals used by the enemy for communication between aeroplanes and troops. These signals are compiled from reports captured by our forces, or our allied forces, or through intercept by radio, and put into phamphlet [sic] form. A sufficient number of these pamphlets is printed for distribution to the different armies and intercept stations.

5. Mail distribution and telegrams, coding and decoding.—All official mail and documents whether incoming or outgoing pass through this office and are from here distributed to the proper parties. Outgoing mail is distributed according to a list which shows the offices or officers to whom mail under a certain distribution should be sent. A copy of the codes in use by the various armies and also a copy of the General Staff code book are kept in this office as all coding and decoding of messages are cared for in the Adjutant's office.

6. Supplies.—All kinds of supplies whether expendable or non-expendable are to be supplied through this office. The Adjutant is liable for everything that has been ordered from another department and at the same time he is to see that needed supplies are always at hand.

7. Recommendation.—It is my belief that it would be more practicable to make the Code Compilation Section part of the Radio Intelligence Section, so as to expedite and simplify the work on code books. Said section should include also a number of officers whose particular duty would be to study past and present code books and improve them and make the necessary changes.

F. The Security Subsection

Lieutenants Falk and Woellner also signed the report on the Security Subsection which had the duty of monitoring Army traffic to detect violations of good security regulations. A part of their report[18] is presented as follows:

[13] Enclosure G, Final Report, pp. 50—52.

310

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

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

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

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

2
311
0-0

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

A complete record is made of the original messages. The individual groups are recorded alphabetically or numerically as the case may be. This recording shows the frequency of recurring groups in the code and valuable information is thus obtained as to the deficiencies of the code in general and how these deficiencies may be corrected. From the statistics gathered in this way it will show whether or not the proper use of the alternate code values for a single word, letter, number, or phrase are being used and if null groups are being used in proper proportion. One of the chief violations of instructions has been the insufficient use of null groups and second to this is the neglect of using the code variants.

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

G. Code and Cipher Solution Subsection

A large part of the activity of the Radio Intelligence Section was spent, of course, in attempts to solve German codes and ciphers in order to further the production of intelligence. The story of these efforts has been published in a series of studies as follows:

German Military Ciphers from February to November 1918. Technical paper of the Signal Intelligence Section, War Plans and Training Division, War Department (Washington, United States Government Printing Office, 1935).

Field Codes used by the German Army during the World War. Short title: SIGFEG. Technical paper by William F. Friedman, War Plans and Training Division, War Department (Washington: United States Government Printing Office, 1935).

Principles of solution of military field codes used by the German Army in 1917. Short title: SIGWIX. Technical paper of the Signal Intelligence Section, War Plans and raining Division, War Department (Washington: United States Government Printing Office, 1935).

In addition to these, reference should be made to a report by First Lieutenant J. Rives Childs: "The History and Principles of German Military Ciphers,"[19] as yet unpublished in full but forming the basis of part of the first study cited.[20]

The simplest German cipher used during the experience of the American cryptanalysts was a monoalphabetic substitution employed for only a few days in August 1918 by the German commander, General Kress von Kressenstein, in the Black Sea area. Either the general himself or one of his staff prepared the cipher, but only three days after it was introduced on 5 August 1918, von Kressenstein was directed to abandon it, as it had been solved at once in the cryptanalytic bureau in Berlin.

[19] Now in the Army Security Library.

[20] See also German Cryptographic Systems during the First World War, a publication of the Historical Unit, Signal Security Agency (IR 5096), sections IV-V.

The American solution was reached by orthodox methods of cipher analysis, making use of the unique character of the German letter C which must be followed either by H or, more rarely, by K.

The so-called "Wilhelm" or "Fuer GOD" cipher was also a substitution which was in use between 1916 and the fall of 1918 without change of keys. It was employed for communications between Berlin (POZ) and a clandestine station in Africa using the call signal GOD—hence, the short title "Fuer GOD" taken from the preamble. The solution in this case was reached by British cryptanalysts, but the German keys were recovered by Lieutenant Childs himself.

Basically, the system employed a modified form of Vigenère square containing twenty-two thoroughly mixed cipher alphabets. The alphabets to be used were controlled by one of 30 repeating key words or phrases. When all 30 keys had been used, the cycle was repeated.

The Germans also used a double transposition cipher, a system much more secure than those already described. Single transpositions were also used to some extent, and when one was located it usually could be solved by anagramming. These transpositions used a mixed numerical key, perhaps based on a key word or phrase, usually quite long, that was never recovered. The plain text would be written in a rectangle having the width of the numerical key, and then the cipher text would be constructed by reading down the columns, beginning with number 1 of the key and following in numerical progression. Double transpositions applied the same method, but once the cipher text was reached, it was then treated exactly as the original plain text had been. The use of the double transposition was, of course, relatively very secure. Solution was based, in the main, on the fortunate discovery of messages in which the cipher clerks through error had neglected to transpose twice. When the daily key had been recovered in this way, it could be used to read other messages in which the same key had been used for a double transposition. Had the Germans used a different key for each transposition, the task of solution would have been complicated beyond measure.

The ADFGX cipher, later known as the ADFGVX cipher, was still more secure, being a combination of substitution and transposition. A square was employed, in the cells of which were written, in mixed sequence, twenty-five letters of the alphabet (J being omitted). The coordinates across the top and down the left of the square were the five letters, A, D, F, G, and X. Thus, if the letter P were found to be at the intersection of column G and row D, it would be enciphered as DG. In this way, the enciphered text of a message would be twice as long as the plain version. When the cipher digraphs had replaced their plain equivalents, the resultant text was then treated to a numerical-key columnar transposition. The later modification of this basic system consisted only in the use of a square containing six columns and six rows, instead of five, making 36 cells in all, sufficient for a complete alphabet and the ten digits. The sixth letter V was added to the coordinates used; otherwise, there was no change. Both the squares and the transposition keys changed daily on the Western Front, but the changes on the Eastern Front occurred only at intervals of two days until September 1918, when the interval was lengthened to three days.

The combined efforts of the cryptanalysts in each of three Allied armies succeeded in solving only ten keys used on the Western Front, but since those were keys for days on which heavy traffic was transmitted, approximately fifty percent of the messages sent in this cipher were read.

The Germans on the Western Front were using during the years of America's participation in the conflict a number of different types of codes. Several of these, e. g. the aviation codes, the telephone codes, and the like, did not form the subject of much study on the part of the American cryptanalysts. The two types of codes which were studied intensively were the three-letter codes, used behind the three-kilometer danger zone, and the three-digit code, used within the danger zone.

As the result of combat operations copies of three of the three-letter codes were captured:

Satzbuch 152,[21] captured 28-29 September 1918, used by the German Fifth Army from 23 September to 3 October 1918.

[21] Copy now filed in IR 4341. This is "Marcel Code No. 2".

2/816
0 C 22

Satzbuch 140,[22] date of capture and distribution unknown.

Verzifferungsbuch 05 [23] date of capture and distribution unknown.

All three are two-part codes using a three-letter group. Satzbuch 152, which is typical, is divided into the following sections:

Vorbemerkungen (introduction)
Wichtige Meldungen (important reports)
Allgemeine Meldungen (general reports)
Stations = und Betreibsmeldungen (station and service reports)
Wettermeldungen (weather reports)
Ortsnamen (place names)
Militarische Decknamen (military cover names)
Zählen (numbers)
Uhrzeiten (time signals)
Buchstaben und Silben (letters and syllables)
Hilfs = Signale (auxiliary signals)
Wörterbuch (vocabulary)
Buchstabierverfahren (distortion)

The other two codes are, in the main, similar in type, the differences being minor in character. The use of a trigraphic group limited, of course, the size of the code to 17,576 groups, but there was a further limitation in that only three, four, or five letters were used in first position. The maximum number of permutations ranged therefore from 2,028 to 3,450 groups. Later editions added umlauted vowels (Ä, Ö and Ü) to the letters possible in second and third position, so the maximum became 4,205 groups in those editions. The codes were, therefore, small in size but doubtless adequate for the limited purpose for which they were used.

[22] Copy now filed in IR 4901. American short title unknown.

[23] Copy now filed in IR 4327. American short title unknown.

Only in the case of Satzbuch 152 is the American short title known: it was "Marcel Code No. 2." Two short titles were regularly given to each code as it appeared in the traffic, one based on the code group limitation, the other an arbitrary name. The first series was known as "Fritz Codes", or "KRU codes" from the fact that only K, R, and U, appeared in first position. This series appeared as follows:

No. 3	29 August to 30 October 1917
No. 6	31 October to 26 November 1917
No. 11	27 November to 26 December 1917
No. 14	27 December 1917 to 28 January 1918
No. 19	29 January to 28 February 1918
No. 23	1 March to 4 April 1918
No. 28	5 April to 5 May 1918

Following the "Fritz codes" was a series consisting of only two codes, the "Jean codes," in which the compilers had added S to K, R, and U, in first position, hence the name, "KRUS codes":

No. 1	6 May to 23 May 1918
No. 2	24 May to 20 June 1918

Soon another innovation appeared in the "André codes": the code groups used as first letter not only K, R, U, and S, but also A, hence the title "KRUSA codes". These were:

No. 3	21 June to 14 July 1918
No. 7	15 July. to 21 July 1918
No. 8	1 August to 14 August 1918
No. 9	15 August to 21 August 1918

The final innovation consisted of adding to the possible letters in second and third position the German umlauted vowels Ä, Ö, and Ü. For this reason, these codes were called the "KRUSÄ codes" and were

2/8
31
0-0

also given the short title "Marcel codes". They were used as follows:

No. 1	22 August	to 22 September	1918	
No. 2	23 September	to 3 October	1918	(= Satzbuch 105)
No. 3	4 October	to 12 October	1918	
No. 4	13 October	to 3 November	1918	
No. 5	4 November	to 11 November	1918	

Thus far, all these codes were used in the G Sector only—in the H Sector, similar series were all called by the short title "Albert" after it became known that the French Code Office had been using this short title, but prior to that time the codes which later became known as "Albert Codes" Nos. 6, 7, and 8, were known to the American cryptanalysts as "Nancy Codes" Nos. 1, 2 and 3, respectively. The "Albert Codes" were as follows:

KRU Type

No. 6	(= Nancy No. 1)	28 December	to 25 January	1918
No. 7	(= Nancy No. 2)	26 January	to 21 February	1918
No. 8	(= Nancy No. 3)	22 February	to 21 March	1918
No. 9		22 March	to 4 April	1918
No. 10		5 April	to 29 April	1918

KRUS Type

No. 11	30 April	to 19 May	1918
No. 12	20 May	to 6 June	1918
No. 13	7 June	to 30 June	1918

KRUSA Type

No. 14	1 July	to 14 July	1918
No. 15	15 July	to 6 August	1918
No. 16	7 August	to 21 August	1918

KRUSÄ Type

No. 17	22 August	to 16 September	1918
No. 18	17 September	to 21 October	1918
No. 19	22 October	to 11 November	1918

2
319
0-0 ?

The Germans evidently trusted for security to two factors: (1) the frequent change of code and (2) the two-part arrangment, since no encipherment was ever used with the three-letter codes.

The three-digit code was employed by the Germans after 10 March 1918 within the three-kilometer danger zone. The maximum number of groups in such a code is, of course, only a thousand. The code was one-part in arrangement and in unenciphered form was of so low security that the Germans recognized that its value was only to be found in economy. The messages were therefore usually, but not always, enciphered by a form of substitution which affected only the first two digits of the code group, the third being left in unenciphered form. The code book itself was given a wide distribution but the encipherment tables, known as "Geheimklappe" (secret flaps) were prepared usually by division headquarters. The "Geheimklappe" were cipher squares 10 x 10 in size with dinomes in the cells. The first digit of the plain group controlled the row and the second the column at the intersection of which the cipher dinome was found. Such encipherment was weak: it produced no greater security than is present in a hybrid code which has been formed by repaginating a one-part code. The cipher dinomes were not page symbols but their effect was the same. All traffic enciphered by the same key would show the characteristic repetitions of unenciphered code: the only effect of the encipherment was the partial introduction of two-part characteristics. Moreover, since the third digit never changed, no matter what encipher-

2
320
0-0 ??

ing table was used, the third digits of code groups representing frequent words would exhibit characteristic patterns permitting their identification.

The methods used in the attempts to solve the three-letter and three-digit codes have been described in great detail by William F. Friedman, who, as a first lieutenant, participated in the solution.[24] It will serve no useful purpose at this point to enter into these technical details. The methods were those now recognized as standard procedure in the solution of unenciphered codes: study of the relative frequencies of the different code groups; positing of probable words; exploitation of violations of good security principles made by the enemy cryptographic clerks; exploitation of captured cryptographic material and of the long experience possessed by both the British and French, and, last but not least, the exercise of the cryptanalysts' ingenuity and acumen.

[24] William F. Friedman, Field Codes used by the German Army during the World War (Washington, United States Government Printing Office, 1935); see also German Cryptographic Systems during the First World War, a paper of the Historical Unit, Signal Security Agency (IR 5096).

2
321