SRH-030

A HISTORY OF THE CODE AND CIPHER SECTION DURING THE FIRST WORLD WAR, PREPARED IN 1919 BY MAJOR HERBERT O. YARDLEY

M. I. 8 [1]

Code and Cipher Section [2]

Origins.

When war was declared, neither the War Department nor any other department of the Government possessed even a rudimentary organization for attack on codes and ciphers. Colonel Van Deman [3] (then Major Van Deman) recognized, however, that such an organization was absolutely indispensable and immediately began a search for experts to form it and train the necessary personnel.

The only officers of the Army known as expert in the subject were Colonels Parker Hitt (then a Captain) and Joseph O. Mauborgne and Frank

---

1. The document of which this is a verbatim transcription is now filed in the office of the Director of Communications Research, Signal Security Agency (file no. 277). Though unsigned, proof exists that it was prepared by Major Herbert O. Yardley and completed probably in July 1919. The evidence for this attribution is now filed in IR 4150 and has been transcribed in The Shorthand Subsection of MI-8 in the First World War (1917-1919), a publication of the Historical Unit (IR 5042). On 3 June 1919 Major Yardley wrote Mr. Franklin W. Allen, who had been head of the Shorthand Subsection of MI-8 in New York, that, at the request of the Director of Military Intelligence, he was then preparing an account of the work of MI-8. He enclosed for Mr. Allen's comments and revision a rough draft of the fourth paragraph, dealing with the work of the Shorthand Subsection. This draft is reproduced in appendix A of the publication cited. Appendix B presents Mr. Allen's revisions. As appendix B has been incorporated almost verbatim in the unsigned document, it is clear that Major Yardley was the author.

2. The official title was "The Cipher Bureau".

3. Colonel Ralph H. Van Deman, General Staff Corps.

Moorman (then Lieutenants)[4]. Colonel Van Deman endeavored to procure the services of these officers but Colonels Hitt[5] and Moorman[6] were sent to France with the American Expeditionary Forces and Colonel Mauborgne[7] was assigned to important administrative duties in the radio service of the Signal Corps. Accordingly it became necessary to find experts in civil life and enlist their services.

On June 10, 1917, a beginning was made by the commissioning as First Lieutenant (later as Major) of Herbert O. Yardley, who had several years' experience in code work in the State Department and had incidentally developed knowledge and skill in the solution of codes. He was put in charge of the code work of Military Intelligence with two

---

4. Brigadier General M. H. Macomb, War College Division, wrote on 2 August 1916 (file no. 4131-14, copy now in IR 4241) to the Chiefs of Staff of the Eastern, Central, Southern, Western, Hawaiian and Philippine Departments, that, in response to an earlier request for information, he had been sent by the Army Signal School, Fort Leavenworth, a list of officers known to be cipher experts. This list included Captain Parker Hitt, 19th Infantry, "undoubtedly the best cipher man in our service"; Lieutenant Joseph O. Mauborgne, 8th Infantry, who "has done some excellent work in this line and should be of value to the War College"; Lieutenant Charles A. Lewis, 9th Infantry; Lieutenant Edmund R. Andrews, 13th Infantry; Lieutenant Charles E. Stuart, 22nd Infantry; Lieutenant Clyde L. Eastman, 20th Infantry; Lieutenant Karl Truesdell, 25th Infantry; and Lieutenant Frank Moorman, 18th Infantry, who "is interested and would be glad to undertake work of this kind". The comment on Lieutenant Moorman was written by himself, as he was Acting Director of the Signal School at this time.

5. Colonel Hitt became Assistant Chief Signal Officer for the American Expeditionary Forces in France and was not actively engaged in cryptographic or cryptanalytic duties. (W.F.F.)

6. Lieutenant Colonel Moorman (then Major) was officer in charge of the unit (G-2, A-6) which performed cryptanalysis of German communications at General Headquarters, American Expeditionary Forces, France, 1917-1918.

7. Major General Joseph O. Mauborgne was Chief Signal Officer from 1 October 1937 to 30 September 1941, when he was retired.

clerks as assistants.[8]

The work of encoding and decoding our own cables and telegrams[9] increased so rapidly, however, that although First Lieutenant James E. McKenna was soon appointed to take charge of this branch of the work, the time of the whole staff was practically consumed by it and Lieutenant Yardley had no opportunity to devote himself to code and cipher attack. Late in September therefore, Col. Van Deman invited to Washington and later commissioned as Captain, Mr. John M. Manly,[10] who had offered his services in March, 1917. At first it was Col. Van Deman's idea to divide the code and cipher work and put Lieut. Yardley in charge of the former and Capt. Manly in charge of the latter, but these officers soon saw that such a division would be counter to the best interests of the work and at their suggestion a section was organized to deal with secret communications of all sorts. Furthermore it soon became clear that such a section - to obtain the best possible results - should be located in Washington and should receive information and materials from all departments of the Government and serve all equally.

In pursuance of this plan Col. Van Deman had conferences with representatives of the departments of State and Justice and the Navy, and arrangements for cooperation were completed whereby these departments agreed to send to Military Intelligence all documents suspected of containing secret communications, and Military Intelligence agreed to examine and report upon such documents. Later, similar arrangements were perfected with the Postal Censorship; and even official and semi-official organizations with which no definite plan of cooperation had been arranged gradually adopted the practice of depending upon Military Intelligence for cryptographical work.

---

8. This unit worked at the War College, but was later located successively in a building at 15th and M Streets, N.W., 1330 F Street, N.W., and finally at 7th and B Streets, N.W.

9. This purely cryptographic work should have been done by the Adjutant General's Office but on pleas of greater security G-2 set up its own facilities and staff for this purpose. (W.F.F.)

10. Both before and after the war Captain Manly was head of the English Department and Professor of English at the University of Chicago.

The Riverbank Laboratories.

Previous to these plans for cooperation and the organization of this central office, very little cryptographical material of any sort had been recognized as such by any department. A few official ciphers[11] were picked up from time to time and still fewer personal ciphers - innocent or criminal in character - drifted in from various sources. Most of these had been sent to Geneva, Illinois, where, under the name of The Riverbank Laboratories, Mr. George Fabyan[12] maintained a staff of persons to work upon various fads in which he was interested. Among these fads was the belief in the existence of a biliteral cipher in various works of the sixteenth and seventeenth centuries which showed that Francis Bacon was the author of works commonly ascribed to William Shakespeare and other writers. The search for this cipher had given Mr. Fabyan's staff no real experience even in the elements of cryptography but had aroused in him an intense interest in the subject. Consequently when war was declared it was natural that Mr. Fabyan as a patriotic citizen should offer the services of his staff to the Government. This was in April, 1917. As no official cryptographic section then existed, Mr. Fabyan's generous offer was accepted and various departments of the Government sent to him such ciphers as came to hand. As has been said above, his staff was without real cryptographic experience, and to remedy this Mr. Fabyan sent two of them - Mr. J. A. Powell[13] and Mr. W. F. Friedman[14] - to the Army Service Schools at Fort Leavenworth to take a course of instruction from Lieut. Mauborgne;[15]

---

11. On such systems see IR 5049.

12. An honorary title, conferred by the Governor of Kentucky, some years before 1915, gave him the right to be known as "Colonel Fabyan". (W.F.F.)

13. Dr. Powell had been head of the University of Chicago Press up to the time of his employment in 1917 by Colonel Fabyan. (W.F.F.)

14. At that time Mr. Friedman was in charge of the Department of Genetics at Riverbank Laboratories and took only a mild interest in the Bacon-Shakespeare work being done there. (W.F.F.)

15. An error: Mr. Friedman was not sent but studied Captain Parker Hitt's Manual for the Solution of Military Ciphers, a copy of which Mr. Powell brought back with him. (W.F.F.)

consequently they were thereafter much better equipped to solve such problems as were submitted to them.

In the maintenance of his cipher laboratory and later in instructing a large number of officers in the principles of cipher attack,[16] Mr. Fabyan spent a large sum of money. For the assistance he rendered in these ways he deserved and received the thanks of the departments concerned. After the cryptographic section of Military Intelligence had been organized and designated as a central office serving all departments, however, relations with Mr. Fabyan's laboratory gradually ceased - on the part of the departments, chiefly because of the advantages of dealing with an office centrally located in Washington; on the part of the Military Intelligence because, 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.[17]

---

16. A memorandum for the Chief of Staff from the Chief, Military Intelligence Division, General Staff, 13 May 1918 (a copy is now filed in IR 4152) stated that the officers sent to Riverbank Laboratories were sent there for training in cryptography but had been trained by error in cryptanalysis. On the other hand, when the student officers were detailed for the course, the War Department set up no guides or limitations, other than that six weeks would be devoted to instruction in cryptography. The word "cryptanalysis", coined by Mr. Friedman in 1921, was unknown at this time. Mr. Friedman recalls (1945) that there was some controversy with Major Yardley at a later time about this point, Yardley claiming that the officers had been sent for instruction purely in cryptography and not in solution. As it turned out, a great many of the students did get assigned to cryptanalytic duties. There were three groups of students, the first consisting of but four officers in October-November 1917; the second consisting of some sixty officers in January-February 1918; the third consisting of seven or eight in March-April 1918. Mr. Friedman prepared the instructional material, gave the lectures, and directed the school, the first of its kind in American history. Beginning in September 1917, Mr. Friedman gave up his work in genetics and became Director of the Department of Ciphers at the Laboratories, until in April or May 1918 he was commissioned first lieutenant and sent immediately to G-2, A-6, General Headquarters, in France. (W.F.F.)

17. No. This was just Yardley's way of getting Fabyan out of the picture. (W.F.F.)

Code and Cipher Attack.

In the cryptographic section itself - which will hereafter 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 attacks 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.

Shorthand Subsection.[18]

The earliest subsection to be organized in M. I. 8 was the Shorthand Subsection. Early in October, 1917, M. I. 8 began to receive letters and other documents supposed by the censors to be in cipher. Some of these upon examination proved to be Yiddish and Arabic and were put into the hands of our language experts, but others proved to be in shorthand systems and languages of enemy countries and neutral European countries and in English shorthand systems unknown to most English shorthand writers.

In these circumstances recourse was had to Mr. F. W. Allen, of the firm of Pulse & Allen, who responded promptly with the desired aid and very soon was doing a large amount of work for M. I. 8 and employing a number of experts and paying for their services connected with this work, until May, 1918, when he was requested to organize the work as a subsection of M. I. 8, which he consented to do, without remuneration.

---

18. This section is almost a verbatim copy of an earlier draft of these paragraphs, as revised by Mr. F. W. Allen. See the remarks in the Editor's Foreword.

He was then appointed Chief of the Subsection, with the status of civilian volunteer and with headquarters at his office in New York. Under Mr. Allen's direction three important results were accomplished:-

(1) Decipherment of Shorthand Systems. - A bibliography of works in public and private libraries in the United States on rare and foreign shorthand systems was compiled and a library was built up, for use in which all volumes that were needed were secured. Altogether fifty-four systems were studied and analyzed and the leading characteristics of each system were charted, so that in a short time experts could determine the system used in practically every document submitted and transcribe the stenographic notes into the language used.

(2) German Shorthand Experts for the A.E.F. - On June 17, 1918, M. I. 8 was instructed to locate, appoint and send to France fifteen expert stenographers who could take down verbatim examination of German prisoners of war. The Committee on Classification of Personnel in the Army having failed to locate a single person so qualified, Mr. Allen was requested to organize the search; and after writing several thousand letters to individuals, shorthand schools and stenographic societies, he was able to recommend the required personnel and assure a steady, though not a large, supply of men qualified as desired.

(3) Census of Foreign Stenographers. - In connection with the work described in the previous paragraphs, a census was made of shorthand writers throughout the United States writing foreign language systems, each of whom was carefully investigated and a record made of his history, citizenship, employment, connections and qualifications. This proved of great value in all phases of the work done by the Shorthand Subsection.

(4) Expert Linguists for M. I. 8 and the A.E.F. - About July 1, 1918, as a result of the increasing pressure of work in M. I. 8 and frequent calls from the American Expeditionary Forces, France, for officers with a thinking knowledge of German for codes and cipher work, Mr. Allen was requested to find, investigate and recommend six cryptographers and twelve candidates for commissions.

The persons whom he selected and recommended have been among the best qualified for our work, several having occupied executive positions in our own office and all of these officers who were sent to France having proved thoroughly efficient. Moreover, several of the officers whom he chose, in turn recommended strong, well-equipped men and women for various positions in France and the United States.

About August 15, a sudden call was made on M. I. 8 for Army Field Clerks, with an intimate knowledge of the Russian people and language, to accompany the Intelligence Section of the American Expeditionary Forces to Siberia, and Mr. Allen, on three days' notice, furnished two qualified candidates.

Secret Inks.

That the enemy was using secret inks for some of his communications was known in a general way from a very early date. The first actual case that came to attention, however, seems to have been that of a letter written with invisible ink in Modern Greek and brought across the Mexican border in the shoe of an illiterate woman. This was developed by simple processes in M. I. 8 but many suspicious documents did not yield to treatment. Information of a general nature was obtained from the British and the French concerning German technique in this field, and after much correspondence M. I. 8 was put in possession of all the knowledge of our allies in these three ways:

(a) By a voluminous report transmitted through Captain J. A. Powell, who was sent abroad in December 1917 to establish liaison with our allies in all matters of this general nature.

(b) By the visit to America at the expense of M. I. 8. of Mr. E. F. Collins, one of the best of the British experts in the detection of secret inks.

(c) By the visit of Captain Emmett K. Carver of M. I. 8 to Great Britain and France for study in the laboratories there.

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[19] - is one of thorough equipment for

---

19. Lieutenant Colonel A. J. McGrail was the only member of MI-8 in Washington who later also was a member of the Signal Security Agency in the Second World War. From 1941 until his death on 30 April 1945 Colonel McGrail was in charge of all work involving secret ink and photography.

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.

Instruction in Code and Cipher Work.

Besides instructing Military Attaches and their assistants in the proper use of our own codes, M. I. 8 was obliged to conduct courses of instruction for several groups of persons;

(a) Officers and field clerks for M. I. 8, for G-2, A-6, A.E.F., and for the corresponding section of the expedition to Vladivostok.

(b) Intelligence Officers for duty at home and abroad.

One of the most interesting by-products of this instructional work was a treatise on the organization of the German Army, more accurate and comprehensive, it is believed, than any similar treatise in the possession of the Allies. This was prepared by a member of M. I. 8 for use in instructing code-attack officers for the work at the front.

Code Compilation.

Shortly after the organization of M. I. 8 it was learned that the Germans were reading confidential messages passing between Generals Pershing and Bliss and the Washington office. This was known to be due to the possession by the Germans of copies of the Army Code Book[20] of 1915, the only book available for our use, and to the inadequacy of this book to resist attack under such conditions. Preparations were made for the compilation of a new and better book and a special subsection was organized under the leadership of Captain A. E. Prince for this purpose. This book[21] was completed on July 1, 1918, and 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. Work upon another book[22] -

---

20. War Department Telegraph Code 1915, a one-part code. It was used for unenciphered nonsecret communication, and with cipher tables for secret communication. The code itself had been printed by a commercial firm in Cleveland!! (W.F.F.)

21. Its designation was "Military Intelligence Code No. 5" but, so far as is known, there never were any similar codes numbered 1-4. (W.F.F.)

22. This two-part code was designated "Military Intelligence Code No. 9" and was little used. It was later revived with a new title-page as "War Department Staff Code No. 2", and held in reserve. It was probably never used.

with certain improvements in plan - was begun immediately and under pressure of necessity was hastened to such a degree that the volume was ready for use when the Director of M. I. D. went to France, December 2, 1918.

Other notable achievements of this subsection were the following:

(a) Two Geographical Codes. - In July, 1918, a cable from General Tasker H. Bliss requested that a "list of code words be gotten out for the geographical names of all that section of France in which operations are now taking place, or are likely to take place in the future, based on the French map having a scale of 1: 100,000 feet". This cable was referred to the Director of Military Intelligence for action; work was immediately begun on the FRENCH GEOGRAPHICAL CODE, and the book of 360 pages, containing the names of approximately 9750 places in France within twenty-five miles of each side of the then battle front, was finished October 1.

By that time, since the theatre of military operations had materially shifted, it was considered desirable to issue a new code, incorporating the former, and also covering all of Belgium, the lower part of Holland, Germany to a distance of twenty-five miles beyond the Rhine, and that portion of Northern France not embraced in the former code. Work was begun October 17, and the book came from the printer about November 15, 1918. This code, FRENCH GEOGRAPHICAL CODE No. 2, contained approximately 26,500 names of cities, towns, forests, hills and streams.

(b) A casualty code. - THE CASUALTY CODE, begun September 16, 1918, was in no sense of the word to be a secret code, but was designed purely to promote facility and economy in the transmission of casualty reports. In this work the War Department Telegraph Code of 1915 had been in use, but as it never had been designed for such a task, from five to seven or eight code groups were required 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 of 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.

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 material gathered at that time, however, is still in the possession of M. I. 8, and would be available if the publication of such a code ever became necessary.

(c) Pocket code. - On the second of December, 1918, instructions were given to the Compilation Section to prepare a "pocket code", [23] for the use of Military Attaches when on duty away from their posts, and other special military agents in the field, particularly those agents who would go into enemy territory with the army of occupation or in other capacities in which the use of code communications was desirable. Within two weeks of the time when work was started the volumes were ready for distribution. The force had previously worked on the manuscript at odd times, and the devising of a new method of preparing the "copy" for the printer made possible this record speed. Fifty copies of the book were immediately sent to Europe for distribution, and those who have had occasion to use the book have been highly pleased. The book contains 13,000 code groups, words and phrases.

In addition to code compilation, this subsection furnished new encipherment tables every two weeks to all users of our own codes and to such of our officers as were obliged by circumstances to continue the use of the Army Code Book of 1915.

Communications.

For two years the Communications Subsection has maintained cable and telegraphic communication with about forty Military Attaches and Intelligence Officers in Foreign countries, and with hundreds of Intelligence Officers stationed in all camps and important cities within the United States. The section has been open twenty-four hours a day. By

---

23. The Ideal Correspondence Code, ostensibly a publication of the Ideal Code Company, New York, 1918, but actually printed at the Government Printing Office on paper and in a format unlike other government publications. (E.F.F.)

means of special wire connections exceptionally fast service was provided, particularly with the most important center, Paris, whence cable messages were often received within less than one-half hour from the time of sending.

Practically half of the enormous amount of cable correspondence handled by this office was in the form of code messages. Since the principles of security required that the code words of each message be enciphered to prevent the possibility of the messages being read by the enemy, it was necessary to subject each code message to two complete translations. The obvious impossibility of distributing the work evenly according to clock or calendar resulted in intermittently overloading the section, but because of the splendid spirit shown by the entire commissioned and civilian personnel in subordinating their personal convenience to the needs of the work, and their willingness to "carry on", often for double the regular number of working hours, the work was kept up to the minute at all times and was always performed with exceptional efficiency.

From September, 1918 to May, 1919, this subsection sent and received 25,000 messages, about half plain text and half code, containing 1,300,000 words.

It is perhaps not generally recognized that our use of codes has resulted in great economy. Wherever they have been used, - and they have been used by the Military Intelligence Division, The Adjutant General's Office, the A. E. F., France, and other War Department offices,- the cost to the Government of cable and telegraphic communication has been reduced at least fifty per cent. The use of the Geographical Codes resulted in even greater economy by eliminating the necessity for spelling out foreign place names.