REF ID:A72903

SECRET

Col Bidwell
Office Military
History
Room 1D-638
P-151052,
(17)

From Chief Mil. History

Codes & Ciphers
Excellent

110479

G2-ASA 461
TO: OCMH FROM: G2-ASA DATE: AUG 12 1954 COMMENT NO. 2
Major W. E. Andruss/147/Ext620/ssl

1. The attached draft copy of a part of a "History of the Military Intelligence Division, Department of the Army General Staff," has been reviewed by Dr. Evert Conder, this headquarters, and his comments are transmitted herewith as Inclosure 2.

2. Mr. Friedman is no longer with the Army Security Agency, and can be contacted by addressing correspondence to the Director, National Security Agency, Washington 25, D. C. ATTN: Mr. William F. Friedman.

FOR THE ASSISTANT CHIEF OF STAFF, G2:

HARRY REICHELDERFER
Major General USA
Chief, Army Security Agency

2 Incls
1. n/c
2. Review of History

Rec'd Incl # 2 only
Don P.

DISPATCHED

1-54-8-23

SECRET

~~SECRET~~ Friedman D K C. Codes & Ciphers 0445186

Codes and Ciphers

The situation existing during the latter part of 1921 with reference to War Department activities connected with codes and ciphers was highly complicated. Although the ACofS G-2 continued to exercise full general staff supervision over the conduct of such activities, an official agreement had recently been concluded wherein the Chief Signal Officer would assume the sole responsibility for the future conduct of all code and cipher compilation (cryptography). On the other hand, the joint War-State Cipher Bureau, under Mr. Yardley in New York City, was still performing the entire code and cipher solution function (cryptanalysis) for the Army, while The Adjutant General remained charged with printing, storing, issuing, and accounting for all crypto-materials. As an additional involvement, the Navy Department recently had decided to build up a strong code and cipher organization of its own and these elements often appeared to be in active competition with the corresponding Army units. *

A considerable amount of cryptanalytic work was done by me in Sig C in connection with study of security of our own systems.

---

* Friedman, "History SIS," Secret, pp. 13-14.

Regardless of the many handicaps inherent in this faulty system of divided control, a large measure of important progress concerning code and cipher work could still be reported. Thus, shortly after the conclusion of World War I, Mr. Yardley managed

~~SECRET~~

Encl #1

The key figure in the rapidly developing Signal Corps cryptographic effort was Mr William F. Friedman A real veteran of this type of endeavor, Mr Friedman was one of the members of the select group of cryptographers originally employed by Mr George Fabyan at the Riverbank Laboratories in Geneva, Illinois, ~~in an attempt to prove the existence of a Francis Bacon cipher within the works of William Shakespeare.~~ * ~~(State, War Navy Justice)~~ none of ~~which~~ at that time had any personnel or facilities for such work.

in his patriotic assistance to the Government by way of establishing a unit for the solution of Code and cipher messages obtained in various ways by several Departments Additionally, as a first

* Fabyan, op. cit., passim.

What work did he ever write? I know of none maybe your reference here is to an article in American magazine of Jan 19 ?? ??

lieutenant in the Signal Corps during World War I, he continued to perform responsible cryptographic assignments both in MID and with the G-2 Section of the AEF in France Following the Armistice, however, with the Signal Corps desiring to grant him a permanent Army commission, the examining physicians unfortunately detected a "functional heart disturbance," and favorable action could not be taken in his case Nevertheless, he was immediately hired on an individual contractual basis by the Chief Signal Officer for the purpose of compiling a badly needed set of new War Department codes. On 16 November 1921, when he finally could be given permanent tenure as a War Department civilian employee, he was appointed to become Chief Cryptanalyst for the Signal Corps and placed in charge of a newly formed Code and Cipher Compilation Section of the Research and Development Division, Office of the Chief Signal Officer *

*"A Lecture on the Origin and Development of the Army Security Agency, 1914-1947," Confidential, March 1948, p 7, Army Security, Washington, D C Hereafter cited as "Lecture ASA," Confidential Mr Friedman's initial salary under this new appointment was $4,500 per annum.

Mr Friedman remained in this consequential position directly under the Chief Signal Officer until 1930. During this extended period, with the help of only one assistant, he succeeded in carrying the full weight of the entire code compilation load for the War Department. He was also personally responsible for the preparation of the first manual covering the subject of cryptanalysis for use by the United States Army *

1117

*TD Document No. 117, "Elements of Cryptanalysis," initially as a mimeographed report upon a series of lectures given at Camp Alfred Vail, issued in 1921, and then revised in 1923. printed, with numerous revisions, as a text book

The principal obstacle standing in the way of satisfactory progress for the War Department code solution program during these early peacetime years was the serious difficulty constantly encountered in securing sufficient intercepted material upon which to base a suitable analysis During World War I, this matter had been accomplished in a relatively simple manner by means of confidential arrangements concluded with commercial telegraph companies

period was the M-94 Cipher Device This contrivance, consisting of a metal shaft upon which were mounted 25 ~~cylinder filled by a series of~~ separately revolvable lettered disks, had been "invented" in 1917 by Maj (later Maj Gen) J O Mauborgne, Chief of the Engineering and Research Division, Office of the Chief Signal Officer * In 1921, therefore,

---

*See: WD, CSO, Articles on Cryptography and Cryptanalysis, Restricted, 1942, pp 100-03 This M-94 device was ~~practically~~ identical, both in form and principle, to the "Wheel Cypher" ~~wooden cylinder~~ invented ~~designed~~ in colonial times by Mr Thomas Jefferson Moreover, in 1914, Col Parker Hitt of the Army Signal Corps conceived the same idea, ~~but failed to construct any working model thereof,~~

---

following a series of security tests which twenty years later turned out to be badly inconclusive, the device was officially adopted as standard Army equipment. It was later also adopted by the Navy, including the Marine Corps, and the Coast Guard

Along with all other companion military intelligence activities, the post-war shortage of available funds also soon commenced to throttle the code and cipher effort of the War Department For example, the Black Chamber was able to receive its full $100,000 appropriation for FY 1920 only, while the following year this aggregate amount was cut exactly in half * Moreover, by 1929,

reached such an unsatisfactory state that Maj. O. S. Albright, Sig.C., the MID officer directly in charge of general staff supervision over such functions, decided to prepare a detailed study covering the subject in order to bring the matter forcefully to the attention of his superiors. When completed, this study strongly urged that all War Department activities of this special nature, including those connected with secret inks, should be concentrated without further delay under the direct supervision of the Chief Signal Officer. The recommendation was promptly accepted in full by Col. Stanley H. Ford, ACofS, G-2, and duly forwarded to the Chief of Staff, along with concurrences from the G-1, G-3, G-4, WPD, and CSO. Finally, on 5 April 1929, this basic change in functional responsibilities for the War Department received the formal approval of Chief of Staff General C. P. Summerall. *

---

* Friedman, "History SIS," Secret, Tab "C". See also: Report FY 1928-29, MID 248-20-394, Records of WDGS, MID, National Archives.

Before much could be accomplished under this new situation in the way of actually completing the transfer of the War Department cryptanalytic activities from New York City to Washington, D. C., there occurred one of the most amazing events in the entire history of military intelligence. Thus, in March 1929, with a new national administration entering into office, Mr. Henry L. Stimson was

appointed Secretary of State. For the first few months of his tenure, no Black Chamber bulletins were presented to him, in the hope that he might first have an opportunity to become sufficiently oriented in his duties to appreciate fully the tremendous import of their extremely valuable content. Early in May 1929, when the time was considered ripe for such action, several translations of Japanese coded messages were then placed on his desk. His reported reaction thereto proved to be both violent and critical. He not only let it be known in no uncertain terms that he regarded the interception of foreign governmental communications as a "highly unethical" procedure but also directed the State Department to cease immediately all further activities of this particular nature. *

---

* Ibid., p. 9. See also: Yardley. op. cit., Chapter XX. There are scattered indications available which might be considered as pointing toward a thesis that this unfavorable decision stemmed actually from President Hoover himself, rather than from Mr. Stimson. Such view finds some degree of support from an observation along the lines that, in 1940, when Mr. Stimson became Secretary of War for the second time, he proceeded to receive "Magic" intercept material regularly without any outward display of protest. In this same connection it should also be recalled that Col Van Deman previously had reported a decided unwillingness on the part of Mr. Hoover, while the latter was in charge of the European war relief program in 1919, to cooperate with the American intelligence authorities functioning at the Peace Conference in Paris.

Friedman strongly urged that four young civilians ~~without any previous experience in cryptological work~~ should be carefully selected and assigned to the new SIS in order to undergo intensive training under his own personal direction This praiseworthy project was first officially authorized and then maintained in the face of many subsequent obstacles, largely through determined support furnished by Maj. David M Crawford, Chief of the War Plans and Training Division, Office of the Chief Signal Officer. * The

---

* Ibid., p. 12.

---

ultimate value to the nation of such a forward looking personnel policy becomes plainly evident upon the realization that, of the men originally selected to participate in this unique type of training, all occupied key positions in communications intelligence during World War II and three of them later served as divisional chiefs within the departmental security agency itself *

---

* The first four men to be chosen under this special training program were Mr (Colonel) Frank B. Rowlett, Mr. (Colonel) Abraham Sinkov, Mr Solomon Kullback, and Mr John B Hurt They all developed into outstanding figures in the field of military cryptology during World War II ~~with Mr. Sinkov still serving the Army Security Agency in a very responsible capacity as late as 1954.~~

---

2. During FY 1932, the sum of $200 was allocated to the SIS from available Signal Corps funds for the purpose of procuring equipment and supplies in support of a small secret ink laboratory. Two years later, Mr. A. J. McGrail, a nationally prominent chemist who was also a Military Intelligence Reserve Officer, was persuaded to devote a considerable amount of his personal time to instruct additional personnel concerning secret ink techniques. From this modest start, the SIS gradually succeeded in organizing an up-to-date Laboratory Branch, which continued to function in an outstanding manner for the rest of the peacetime period. *

---

* Ibid., p. 19. Captain (later Lieut. Col.) McGrail was later transferred to the Signal Corps Reserve.

---

3. The acquisition of suitable and sufficient foreign coded material for satisfying SIS cryptanalytic requirements continued to constitute a major problem for the Signal Corps authorities to solve. Moreover, the Communications Act of 19 June 1934, establishing the Federal Communications Commission, * failed in any manner

---

* 48 Stat 1064-1105.

---

to relax the strict prohibitions earlier proclaimed in the Radio Act of 1927 against interception activities in the United States.

For this reason, several proposals had been already advanced prior to 1932, by the responsible military intelligence officials, to install an American intercept station on Chinese territory but this particular project was finally abandoned during that year because of ~~inveterate~~ State Department opposition. The Signal Corps, however, stubbornly continued to operate six widely scattered intercept stations located at Fort Monmouth, N. J.; Fort San Houston, Tex.; Presidio of San Francisco, Calif.; Fort Shafter, Hawaii; Fort McKinley, Philippines, and Quarry Heights, Canal Zone. Unfortunately, the material obtained from these stations ~~still remained~~ unsatisfactory for War Department cryptanalytical purposes, since the communication units concerned had to be considered as being primarily occupied in training activities under the direction of their own respective area commanders. * On 30

---

* "Lecture ASA," Confidential, p. 23.

March 1938, therefore, following a vigorous appeal in the matter to the Chief of Staff, General Malin Craig, by the ACofS G-2, Colonel McCabe, the Chief Signal Officer, General Mauborgne, was granted specific authority "to maintain and operate in time of peace under strictest provisions to insure secrecy, such radio intercept and cryptanalytical services as are necessary for training and national defense purposes." * This momentous decision

Army Field Code
War Department Confidential Code
Division Field Code
Air-Ground Liaison Code
Alphabets for M-138 Cipher Device *

---

* See: "General Mobilization, Unit Plan and Accompanying Papers," 1 Jul 36, Confidential, MID f/w 24-481-490a, Records of WDGS, MID, National Archives.

---

5. Lack of adequate funds to sustain vital research and development for communications intelligence equipment was of grave concern to the SIS authorities during the early stages of the operations of that agency. Accordingly, electric control for a machine designed to speed up encoding and decoding procedures could not make an initial appearance until 25 July 1933, when a patent covering an invention of this type was filed on behalf of Mr. Friedman himself. *

---

* Designated as the "M-134-A Converter," this new machine was completed by 1937 but, due to subsequent fund limitations, only a few models were actually available for use at the time of Pearl Harbor. See: "Lecture ASA," Confidential, pp. 18 and 25. On 2 Apr 36, all SIS inventors, including Mr. Friedman, made a complete assignment of their individual patent rights to the Secretary of War.

Early in 1935, enough money was also secured enabling the SIS to purchase several IBM machines for necessary assistance in the

performance of its many complicated mathematical tasks. * Important

---

* See: "Supplement to Annual Report of Chief Signal Officer for FY 1936," CC Sig 319.1, National Archives.

---

improvements were further introduced relating to manual cipher devices for use in the field, through the adoption of the Strip Cipher, a new contrivance made up of lettered paper strips which could be inserted along a flat metal container, devised by Mr Friedman; and a hand-operated code converter recently developed by the Swedish inventer Mr. Boris Hagelin. *

---

* "Lecture ASA," Confidential, p. 17.

Finally, toward the latter part of the period, significant progress was reached in the construction of an electrical automatic coding and decoding machine that gave distinct promise of being able to satisfy all of the official military characteristics previously formulated for guiding developments along such lines. * The basic

---

* See: Ibid., pp. 26-28.

---

principles involved in this particular machine were promptly revealed to the communications authorities of the Navy, so that this extremely valuable piece of military intelligence equipment could be effectively standardized between the two services without further delay. *

045186

~~SECRET~~

110479

A REVIEW OF THE HISTORY OF THE MILITARY INTELLIGENCE DIVISION, DEPARTMENT OF THE ARMY GENERAL STAFF

The section, "PEACETIME NEGLECT, 1919 - 1941" will not be commented upon because the reviewer does not feel competent to do so, since he is only familiar with this section in a general historical way.

The section, "CODES AND CIPHERS," is well written, and as far as can be checked against records of the Army Security Agency, is as complete as a short chapter could be. Only a few corrections were noted and these were not serious.

On page 137 there is a reference to Herbert O. Yardley's book, "The American Black Chamber." Although in this case, the statements cited here are substantially correct, other statements in his book should be checked against known sources before being relied upon.

The last sentence on page 140 needs clarification. Although the Cipher Device M 94 was in wide use throughout the Army, there were also available, in limited numbers, two high grade converters for use in important message centers. These were Converters M-134A and M-134C. The first converter was placed in service in Corps Areas and major Headquarters in late 1937. The second converter was issued in late 1941. Converter M-134A was declared obsolete in 1943 after Converter M-134C was in full use. The Cipher Device M 94 was also declared obsolete in 1943.

In the Cipher Device M 94, and similar devices, there were four separate inventors. The first was Jefferson, who was the first and original inventor in colonial times. The second was Etienne Bazeries, of France, who invented a similar device in 1891, and had no knowledge of Jefferson's invention. The third was Captain Parker Hitt, who also without knowledge of either Jefferson or Bazeries devices, conceived the same idea. The fourth, and last, was General Mauborgne. He had examined Hitt's invention in 1917, and about 1920 made the M 94.

The last paragraph on page 149 is not accurate. Mr. Sinkov is not with the Army Security Agency but is with the National Security Agency (NSA). Mr. Rowlett is presently with the CIA, Mr. Kullback is with NSA, and Mr. John Hurt has retired.

On page 156, there were 69 of this Converter in use. It was almost impossible to secure funds for development of machines, and still harder to get money to manufacture them.

On the same page in reference to the IBM machines. These were rented, not purchased.

~~SECRET~~

Encl 2

0-548-20

~~SECRET~~

On page 157 in reference to the paper strips. This was a modification of an invention by Parker Hitt, who in 1915 conceived the idea of "unrolling" the alphabets of the M 94 into long metal rods with a scrambled alphabet pasted upon one surface of the rod. The present strip system, M 138, was developed around the year 1934.

Evert Conder

DR. EVERT CONDER
Historian, National Defense