A BRIEF HISTORY OF THE SIGNAL INTELLIGENCE SERVICE

by

William F. Friedman

June 29, 1942

A BRIEF HISTORY OF THE SIGNAL INTELLIGENCE SERVICE

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

2. In June 1917 the cryptanalytic activities of the War Department were initiated by Colonel Van Deman, G-2, with the commissioning of H. O. Yardley as 1st Lieut., MID. Yardley, who had been a telegrapher at the State Department and had taken some interest in cryptography, was given two civilian employees to assist him. The work grew rapidly and by the autumn of 1917 the increased staff was organized as a section designated as MI-8, which was subdivided into 6 subsections with duties as indicated very briefly below:

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

01

and Postal, which were then separate organizations.

(2) Code and cipher compilation subsection. - Despite the fact that under Army regulations the compilation and revision of codes was a function of the Chief Signal Officer, compilation activities under the Signal Corps were apparently in a moribund state. Information having been received that the Germans possessed copies of the War Department Telegraph Code, MI-8 deemed it advisable to establish a code compilation subsection, and that subsection produced several codes such as Military Intelligence Codes No. 5 and No. 9, small pocket codes for secret agents, and the like.

(3) Training subsection. - In addition to training its own personnel MI-8 trained the majority of the personnel sent overseas for cryptanalytic duties with field forces, both AEF and Siberia.

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

(5) Shorthand subsection. - This subsection was organized to handle texts in various shorthand systems, especially German, which had to be deciphered.

(6) Communications subsection. - This was established in MI-8 for handling messages to and from military attaches and intelligence officers serving abroad. In a period of 9 months it sent and received about 25,000 such messages, practically all in code.

3. At the height of its development, which was reached in November 1918, MI-8 was, for those days, a rather large unit, consisting of 18

02

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

Rent, light, and heat		$3,900
Reference books		100
Personnel: Chief		6,000
	10 code and cipher experts @ $3,000	30,000
	15 code and cipher experts @ $2,000	30,000
	25 clerks @ $1,200	30,000
	Total	$100,000

The item for "rent, light, and heat" is explainable when it is noted that the bureau was to be moved from Washington with a view to hiding its existence. Of the $100,000 recommended, the State Department was to provide $40,000 and $60,000 was to be provided for expenditure by the A. C. of

S, G-2 on "confidential memoranda" against funds pertaining to "Contingency Military Intelligence Division"—that is, by vouchers not subject to review by the Comptroller General. The paper containing the recommendations made by the A. C. of S, G-2 to the Chief of Staff was "OK-ed" and initialled by Acting Secretary of State Polk on May 17, 1919, and on May 19 it was approved by the Secretary of War over the Signature of General March, Chief of Staff. The plan was put into effect, the bureau was installed in a private house at 22 East 36th Street, New York City, and all personnel together with existing records were moved thereto.

4. It is important to note that at that time no provision whatsoever was made for radio intercept as a source of raw material for cryptanalysis. A few words on this subject may not be amiss. Radio intercept of fixed station material in the U. S. by the Army during our active participation in the last war was rather fragmentary. The work was, of course, a responsibility of the Signal Corps, but radio communications could hardly compete with cable and wire communications as a source of raw material because not only did the large governments use cable in preference to radio, but also radio as a means of communication between widely separated fixed stations was then in its infancy. The Signal Corps did, however, have what were called "mobile tractor" units stationed on the southern border, and in late 1918 one large intercept station was established at Houlton, Maine, for the purpose of copying trans-Atlantic radio. The large intercept stations maintained by the Signal Corps in the AEF did furnish a large quantity of diplomatic traffic which was forwarded as raw material to G-2 in Washington, but as soon as the war was over all these sources of intercept material were

abandoned.

This was, of course, true to a certain extent but was not by any means the whole truth. At any rate by 1929 the flow of messages furnished G-2 had dwindled to a mere trickle. In about the year 1926 the intercept stations of the Coast Guard submitted to me informally a few radio intercepts of what appeared to be Japanese code messages, but these were only sporadic occasional intercepts of transmissions in the Far East. They were usually fragmentary and afforded very poor material. Such as they were, however, these occasional messages were turned over to G-2. There were, therefore, clear indications that if a serious attempt were made to obtain this material better copy could be obtained. However, no pressure was brought on the Signal Corps to set up a regular intercept service, and aside from a few relatively weak efforts to establish an intercept station in the Philippine Department there was no real intercept service until after 1929, when responsibility for cryptanalysis was transferred from G-2 to the Signal Corps. How this

came to pass [illegible] soon be detailed.

5. As indicated in Par. 3 above, the $100,000 appropriation set up in 1919 took care of the bureau for the FY 1920, that is from July 1, 1919 to June 30, 1920, but when in June 1920 it came time to set up the budget for FY 1921, the purse strings were already beginning to be pulled tighter. Many of the "old-timers" in G-2 had gone to other assignments; those remaining and the newcomers in G-2 apparently had neither the background nor the influence to press the matter. The appropriation was at once cut in half, that is, to $50,000, of which the State Department share still continued to be $40,000. The theory was, evidently, that since the work done by the bureau was primarily, if not solely, for and of interest to the State Department, all or nearly all of the funds should be provided by that department. The War Department overlooked some very important points in the situation—points which will be brought up and emphasized later in this summary. In order not to break the continuity of the history at this point, it will be stated merely that year by year the funds provided for the maintenance and operation of the bureau became more and more constricted until by the autumn of 1929 the following tabulation, based upon a letter dated July 17, 1929 from Major O. S. Albright, G-2 to the Chief Signal Officer (General Gibbs), shows how the bureau had been permitted to deteriorate:

Rent		$3,000
Books, postage, travel, transportation, misc.		2,370
Personnel:	1 Chief (Yardley)	7,500
	1 Code & ciper expert	3,660
	1 translator (Jap)	3,750

1 secretary		1,800
1 clerk-typist		1,600
1 clerk-typist		1,320
	Total	$25,000

In the foregoing total appropriation of $25,000 the State Department furnished $15,000, the War Department $10,000. The activities of the bureau had by this time become so reduced that it was sending in only occasional translations of a few Japanese diplomatic messages. No research whatsoever was conducted in cryptanalysis; there were no training activities, no intercept, no code compilation, no secret ink work. The personnel consisted of six persons all told and 37½% of the total payroll went to one man, who had little interest other than to continue as long as possible to maintain himself in the sinecure into which he had been permitted to establish himself.

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

07

only a secondary interest in the "bulletin" for the information it gave, the primary interest of the War Department in cryptanalytic studies in peace time was that it was intended to provide a means for training of personnel for immediate war-time effectiveness. Major Albright found that not only was there very little if any training being conducted but also that all the persons in the bureau, except for one clerk receiving the least pay, were "getting along in years"—their potential usefulness for possible war time service practically nil. Moreover, the bureau was now hidden away in a public office building in New York (under cover of the "Code Compilation Company" for alleged purposes of security) and far away from direct supervision of anybody connected with the War Department or of G-2, so that nobody knew what was going on, how the office was administered, etc. Yardley devoted most of his time to two or three private enterprises (commercial code compilation, real estate brokerage, consultant in code matters to commercial firms) and he was having a "field day" at Government expense. There were, in addition, several other weighty factors which motivated Major Albright in preparing a G-2 study recommending that the bureau be taken out of G-2 and its functions transferred to the Signal Corps, chief among which was the desirability, if not necessity, of placing all cryptographic and cryptanalytic work of the War Department under one agency, rather than distributing it among three (The Adjutant General, for printing, storage, issue, and accounting of codes; The Chief Signal Officer, for compiling codes and ciphers; Military Intelligence for solution of codes and ciphers). A memorandum on the same subject was

08

prepared by Lieut. Col. W. E. Wilson ... the War Plans and Training Section of G-2, and is also attached hereto. The reasons given in Major Albright's study and in Col. Wilson's memorandum were apparently deemed valid by the Chief of Staff, for Major Albright's recommendations were approved in April 1929 and steps were soon initiated by G-2 and the Chief Signal Officer to put them into effect. The recommendations carried with them merely the wording of a changes to be made in AR 105-5, specifying the duties of the Chief Signal Officer, these duties being enlarged to include the printing, storage, distribution, and accounting of codes and "in time of war the interception of enemy radio and wire traffic, the goniometric location of enemy radio stations, the solution of intercepted enemy code and cipher messages, and laboratory arrangements for the employment and detection of secret inks."

7. However, before anything could be done actually to transfer the activity a new and very disturbing factor entered into the picture. In March 1929 a new administration took office, in which Mr. Stimson became Secretary of State. For a few weeks no "bulletins" from the cryptanalytic bureau in New York were given him, the intention being to "go slow" until he had become sufficiently well oriented in the duties of his office to warrant bringing to his attention the highly secret activities engaged in by War and State Departments by means of funds provided in large part by the latter Department. Early in May 1929, however, the time was deemed ripe for this measure, but it was with some trepidation that a few translations of Japanese code messages were placed on Mr. Stimson's desk. His reaction was violent and his action drastic. Upon learning how the material was obtained, he characterized the activity as being highly unethical and

09

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

8. In October 1929 I was sent to New York to take over the boxed up records and files and to oversee their transportation to Washington. The cryptanalytic activities, research, and training now being under the Chief Signal Officer, steps were taken to reorganize the bureau and its work. The funds available were, of course, very slim--only what remained of the War Department's contribution of $10,000 for the FY 1930 was available, because the remainder of the State Department's share of $15,000, as indicated above, had already been withdrawn by the State Department. An offer of employment was made to Mrs. Wilson, the Japanese expert with Yardley, but she was unable to accept, since it involved moving to Washington and she had a husband and child in New York. Another employee, Mr. Victor Weiskopf, had a business in New York and refused to move to Washington. The female clerical employees were deemed unsuitable for our purposes and, moreover, having no Civil Service status they could not be taken on by transfer. An offer of temporary employment was made to Yardley but he refused the tender. Instead, he proceeded secretly to prepare a book which first appeared in the form of articles in the Saturday Evening Post and which in much expanded form later appeared under the title "The American Black Chamber." The book and articles were highly sensational and made damaging disclosures concerning the most secret activities ever conducted by the Government. Before the appearance of the articles and book, however, he had taken certain steps to protect himself from possible prosecution for his disclosures, among which was to resign his commission as Major in the Military Intelligence Reserve. Of course, had the authorities understood the real purpose of his resignation they might have prevented it so as to retain some hold on him. But being in ignorance of the real motives and deeming it just an act of pique, the resignation was accepted. The unfortunate

consequences attendant upon the publication of the book need elaboration herein. Suffice it to say that

our precarious relations with Japan were brought to a boiling point when about 30,000 copies of the Japanese translation of The American Black Chamber were sold in Tokyo in a period of less than a month (perhaps the book was subsidized by the Japanese Government itself.). The bad odor into which all cryptanalysts and cryptanalytic activities fell, as a result of the difficulties which the publicity given the matter by Yardley's disclosures occasioned high government officials, had a bad effect upon the attempted reorganization of the cryptanalytic bureau by the Chief Signal Officer. Funds were hard to get, and State Department support was lacking, if not in the other direction altogether. The most serious consequences of Yardley's disclosures, however, came 10 years later and their effects can hardly be estimated. I refer here to the jolt which his book gave the Japanese cryptographers, leading them out of their blissful ignorance and causing them to develop really complex methods which are now giving us many difficulties. The same is true probably as regards the German and Italian cryptographers--their education has been entirely at Uncle Sam's expense and the final consequences of Yardley's work can not yet be foreseen. They may well turn out to be disastrous.

9. However, the Chief Signal Officer proceeded, energetically as possible under the circumstances, to carry out the mission assigned him. The code and cipher solving section was placed under the War Plans and Training Division since the compilation section was already there. A rather detailed directive which was prepared by G-2 and approved by the Secretary

12

of War Exhibit 47, became the guiding plan of the reorganized service, which was now named the Signal Intelligence Service. Its personnel consisting of myself and one or two clerks soon was augmented by a half dozen more employees. Training literature and courses were prepared and put into good usage at once. A great deal was done in expanding our cryptographic work also, by preparing reserve editions of existing codes, compiling new codes and ciphers, developing cipher apparatus, and so on. Cryptanalytic work was put on a firm basis of research and training, with emphasis on the latter, for there existed no intercept service and the raw material could not be obtained

Hence an intercept service now was organized and grew very slowly. All phases of signal intelligence were unified under one service and taken under study and action. Moreover, cooperation with the Navy in the work was also initiated. How the activity has expanded since then requires no comment at this time. However, a few words about relations with the Navy are pertinent.

10. Cryptanalytic activities in our Navy Department were practically non-existent until after the close of the last war, during which, as was noted above, whatever problems they had in cryptanalysis were referred to MI-8. But in 1921 the Navy, recognizing the important role which cryptanalysis was bound to play in future, began building up a large unit in the Navy Department, with echelons afloat. Whereas the Army placed emphasis upon civilian training, the Navy placed emphasis upon officer training; and for each dollar the Army was able to obtain for cryptanalytic and cryptographic work the Navy was able to obtain three to five dollars, until by

1939, as far as concerned numbers of officers and civilian personnel engaged in these activities, amount of equipment on hand, and funds available for research, the Navy had considerably outstripped the Army. However, it may be said, with some justifiable pride perhaps, that while they were ahead of us in quantity we were ahead in quality, for all the important developments in both the cryptographic and the cryptanalytic fields must be credited to Army personnel. At first, cooperation between the two services was intermittent and at times very indifferent--the usual mutual suspicions and jealousies pervaded our relationships. But, happily, for the past three to five years cooperation has been much more wholehearted, with the result that it may now be said without reserve that, as regards their cryptographic and cryptanalytic activities, cooperation between the Army and Navy is so close as to be the same as though they were under one head. This, of course, is as it should be and must be in order to gain the desired result from such activities.

11. It would be of utmost value to the winning of this war if the Government were now in a position to read the codes and ciphers of all the foreign powers whose actions and probable intentions are of interest and importance in our prosecution of the war. It could have been in this fortunate position had it given to cryptanalytic studies the attention which it deserves during peace time and had provided funds for their continuity on a scale sufficient for the purpose for which they are intended. The matter can be summarized very succinctly in this statement: Actual or physical warfare is intermittent, but mental, that is, cryptanalytic, warfare is continuous. It is vital that this be understood by those who exercise the control over such studies, and a few words on this point are given in the next paragraph.

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

(1) It must be realized that cryptanalytic activities have no counterpart in civil life. Therefore, on the outbreak of war there is no important source from which trained, experienced personnel can be drawn for immediate usefulness. Since skill in cryptanalysis can hardly be developed in a short time and cryptanalytic units capable of producing quick results can not be improvised in a hurry, unless there is a good-sized nucleus of such trained and experienced personnel no good cryptanalytic operations can be conducted in the early phases of a war, that is, just at the time when results can usually be obtained most easily and when such results are extremely important. Moreover, it is in the upper strata of cryptanalytic brains that continuity in studies is most important. It is possible, under pressure, to obtain large numbers of recruits of high intelligence from colleges and universities, but until they have had at least five years actual experience and training they are wholly unprepared to attack the most difficult problems encountered in modern, up-to-date secret communications. Consider the present "purple" system, for example. It required almost two years of concentrated effort to break down this system and it was indeed fortunate that this had been accomplished by September 1939. If we had not been able to start this study until December 1941 it would not have been possible to read those messages short of two years' study, if at all, because the problem is so difficult to begin with and moreover the volume of traffic available for analysis would be so small compared to what it was before December 7, 1941. Moreover, if we did not have the two years' experience

successfully employed would be extremely more difficult, if it could be done at all before too late to be useful. Again, our present difficulties with Japanese military systems are in large part occasioned by our failure to devote sufficient study to these systems over the past few years; but it must be realized that limitations on funds and personnel made such studies impossible because with the small staff of SIS personnel from 1930 to 1940 it was all that this personnel could do to keep abreast of the Japanese diplomatic systems, for which G-2 was clamoring.

(2) Continuity in cryptanalytic studies also requires continuity in intercept work, for without the basic raw material no studies at all can be conducted on actual traffic and purely theoretical studies may be far off the real target altogether, no matter how successful. Continuity in intercept work means, of course, that the equipment and personnel of the intercept service have to be maintained and thus these are available on the outbreak of war, for immediate, useful work. Unless cryptanalytic studies are pursued the need for the maintenance of adequate intercept stations soon disappears, for it presently begins to look as though the work done by the intercept personnel is useless and funds for this activity are withdrawn.

(3) Continuity in cryptanalytic studies is necessary because cryptanalysis is not a static science or art--it must progress as the cryptographic science progresses. In the past few years great strides have been made in the latter, especially as regards the development of complex electrical and mechanical cryptographic devices and machinery. Moreover, the cryptanalytic work done during the last war has been publicized. As alluded to above, "The American Black Chamber" in particular has exercised a wide influence in putting certain nations which had been quite backward in their cryptography on their guard, causing them to engage in studies and

developments for the improvement of their codes and ciphers. The result is that the cryptographic systems of these nations have become more and more difficult to analyze. But it is important to note that improvement in cryptography usually comes in successive small steps, and if the opposing cryptanalyst can keep in step with these progressive increases in complexity he can, as a rule, be in a position to read the new systems almost as fast as they are put into usage, but if there is much of a lag in the cryptanalysis the cryptography gets too far ahead for the cryptanalyst to catch up quickly.

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

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

William F. Friedman

William F. Friedman,
Head Cryptanalyst.

June 29, 1942.